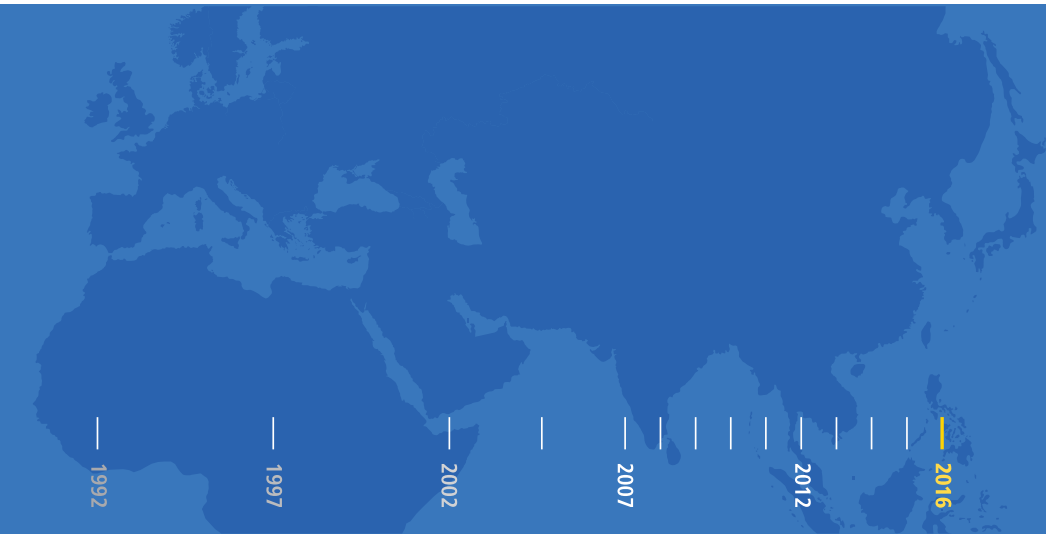
Publikationen
zur rechtlichen Zusammenarbeit

Прирачник за европското законодавство за заштита на податоците



ГЕРМАНСКА ФОНДАЦИЈА ЗА МЕЃУНАРОДНА ПРАВНА СОРАБОТКА
IRZ
Stabilitätspakt für Südosteuropa
Gefördert durch Deutschland
Stability Pact for South Eastern Europe
Sponsored by Germany
FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Прирачник за европското законодавство за заштита на податоците

Преводот на овој прирачник на македонски јазик, како и печатењето на оваа публикација се овозможени од страна на Германската фондација за меѓународна правна соработка, регистрирано здружение (ИРЗ) со средства од германскиот придонес кон Пактот за стабилност на Југоисточна Европа.

Макавеј
Скопје, 2016

германска фондација за Меѓународна Правна Соработка
IRZ

Stabilitätspakt für Südosteuropa
Gefördert durch Deutschland
Stability Pact for South Eastern Europe
Sponsored by Germany

Наслов на оригиналот:
Handbook on European data protection law

Издавач: МАКАВЕЈ Скопје, 2016

Лектура: Весна Ацевска

Превод на македонски јазик: Наташа Андреевска-Томовска, дипломиран толкувач по германски и англиски јазик при Филолошкиот факултет „Блаже Конески", Скопје.

Правна лектура на преводот: Д-р Александар Љ. Спасов, дипломиран правник (доцент на Правниот факултет „Јустинијан Први", Универзитет „Св. Кирил и Методиј", Скопје).

Редакциска координација на македонското издание: Д-р Штефан Пирнер, адвокат.

Редакциска соработка на македонското издание: Драгана Радисавлевиќ, дипломиран правник со положен правосуден испит и Дана Трајчев-Божиќ, В.А., студии по медиуми и комуникации.

Ракописот за овој прирачник беше завршен во април 2014 година.

Ажурираните верзии во иднина ќе бидат достапни на интернет-страницата на Европската агенција за основните права (ЕАОП) на: fra.europa.eu, на интернет-страницата на Советот на Европа на coe.int/dataprotection и на интернет-страницата на Европскиот суд за човековите права во менито Судска практика (Case-Law) на: echr.coe.int.

Повеќе информации за Европската Унија може да најдете на интернет (http://europa.eu).

Овој прирачник е подготвен на англиски јазик. Советот на Европа (СЕ), Европскиот суд за човековите права (ЕСЧП) и Европската агенција за основните права (ЕАОП) не преземаат одговорност за квалитетот на овој превод на македонски јазик. Ставовите изразени во овој прирачник не се обврзувачки за Советот на Европа и за Европскиот суд за човековите права. Во прирачникот се упатува на низа коментари и прирачници. Советот на Европа и Европскиот суд за човековите права не ја преземаат одговорноста за нивната содржина, ниту пак нивното вклучување во овој список претставува каква било форма на поддршка за тие публикации. Други публикации се наведени на интернет-страниците на библиотеката на Европскиот суд за човековите права на: echr.coe.int.

Предговор

Овој прирачник за европското законодавство за заштита на податоците е подготвен заеднички од страна на Европската агенција за основните права (ЕАОП) и Советот на Европа во соработка со Административната служба на Европскиот суд за човековите права. Тој е трет во низата на правни прирачници кои се заеднички подготвени од страна на ЕАОП и Советот на Европа. Во март 2011 година е објавен првиот прирачник за европското право за недискриминација, а во јуни 2013 година е објавен вториот прирачник за европското право во врска со азилот, границите и имиграцијата.

Одлучивме да ја продолжиме нашата соработка во врска со една многу актуелна тема со која секојдневно се сретнуваме, имено, заштитата на личните податоци. Европа има еден од најдобрите системи за заштита во оваа област, кој е заснован на Конвенцијата бр. 108 на Советот на Европа, на инструментите на Европската Унија (ЕУ), како и на судската практика на Европскиот суд за човековите права (ЕСЧП) и на Судот на правдата на Европската Унија (СПЕУ).

Целта на овој прирачник е да се подигне свеста и да се подобри информираноста за прописите за заштита на податоците во државите-членки на Европската унија и на Советот на Европа, служејќи им на читателите како главна референтна точка. Наменет е за неспецијализирани правници, судии, национални органи за заштита на податоците и други лица кои работат во областа на заштитата на податоците.

Со стапувањето на сила на Договорот од Лисабон во декември 2009 година, Повелбата за основните права на Европската Унија стана правно обврзувачка, а со тоа, правото на заштита на личните податоци доби статус на посебно основно право. Од клучно значење за заштитата на ова основно право е подоброто разбирање на Конвенцијата бр. 108 на Советот на Европа и на инструментите на Европската Унија кои го трасираа патот за заштита на податоците во Европа, како и судската практика на СПЕУ и на ЕСЧП.

Би сакале да му се заблагодариме на Институтот за човекови права „Лудвиг Болцман“ за неговиот придонес во подготвувањето на овој прирачник. Исто така, би сакале да ја изразиме нашата благодарност до канцеларијата на Европскиот супервизор за заштита на податоците за неговата помош во текот на под-

готвителната фаза. Особена благодарност упатуваме до единицата за заштита на податоците на Европската комисија за време на подготвувањето на овој прирачник.

Филип Боаја

Генерален директор за човекови права и владеење на правото при Советот на Европа

Мортен Кјерум

Директор на Европската агенција за основните права

Содржина

ПРЕДГОВОР 1

КРАТЕНКИ И АКРОНИМИ 7

КАКО ТРЕБА ДА СЕ КОРИСТИ ПРИРАЧНИКОТ 9

1. КОНТЕКСТОТ И ИСТОРИЈАТОТ НА ЕВРОПСКОТО ЗАКОНОДАВСТВО ЗА ЗАШТИТА НА ПОДАТОЦИТЕ 13
   - 1.1. Правото на заштита на податоците 14
   - Клучни точки 14
     - 1.1.1. Европската конвенција за човековите права 14
     - 1.1.2. Конвенцијата бр. 108 на Советот на Европа 16
     - 1.1.3. Законодавството на Европската Унија за заштита на податоците 18
   - 1.2. Постигнување урамнотеженост на правата 23
   - Клучни точки 23
     - 1.2.1. Слобода на изразување 24
     - 1.2.2. Пристап до документи 28
     - 1.2.3. Слобода на уметноста и науката 33
     - 1.2.4. Заштита на сопственоста 34

2. ТЕРМИНОЛОГИЈАТА ВО ВРСКА СО ЗАШТИТАТА НА ПОДАТОЦИТЕ 37
   - 2.1. Лични податоци 38
   - Клучни точки 38
     - 2.1.1. Главни аспекти на поимот за лични податоци 39
     - 2.1.2. Посебни категории на лични податоци 47
     - 2.1.3. Анонимизирани и псевдонимизирани податоци 48
   - 2.2. Обработка на податоци 50
   - Клучни точки 50
   - 2.3. Корисниците на лични податоци 53
   - Клучни точки 53
     - 2.3.1. Контролори и обработувачи 53
     - 2.3.2. Корисници и трети страни 59
   - 2.4. Согласност 60
   - Клучни точки 60
     - 2.4.1. Елементите на валидната согласност 61
     - 2.4.2. Правото на повлекување на согласноста во секое време 66

3. ГЛАВНИТЕ НАЧЕЛА НА ЕВРОПСКОТО ЗАКОНОДАВСТВО ЗА ЗАШТИТА НА ПОДАТОЦИТЕ 67
3.1. Начелото за законита обработка 69
Клучни точки 69
3.1.1. Барањата за оправдано мешање според Европската конвенција за човековите права 69
3.1.2. Условите за законито ограничување според Повелбата на Европската Унија 73
3.2. Начелото за определување и за ограничување на целта 75
Клучни точки 75
3.3. Начелата за квалитет на податоците 77
Клучни точки 77
3.3.1. Начелото за релевантност на податоците 78
3.3.2. Начелото за точност на податоците 79
3.3.3. Начелото за ограничено задржување на податоците 80
3.4. Начелото за правична обработка 81
Клучни точки 81
3.4.1. Транспарентност 82
3.4.2. Воспоставување доверба 82
3.5. Начелото за одговорност 84
Клучни точки 84

4. ПРАВИЛАТА НА ЕВРОПСКОТО ЗАКОНОДАВСТВО ЗА ЗАШТИТА НА ПОДАТОЦИТЕ 87
4.1. Правилата за законита обработка 89
Клучни точки 89
4.1.1. Законита обработка на нечувствителни податоци 90
4.1.2. Законита обработка на чувствителни податоци 96
4.2. Правилата за безбедност на обработката 100
Клучни точки 100
4.2.1. Елементи на безбедноста на податоците 100
4.2.2. Доверливост 103
4.3. Правилата за транспарентност на обработката 105
Клучни точки 105
4.3.1. Информација 106
4.3.2. Известување 109
4.4. Правилата за унапредување на усогласеноста 110
Клучни точки 110

4.4.1. Претходна проверка 110
4.4.2. Службеници за заштита на личните податоци 111
4.4.3. Правила на однесување 112

5. ПРАВАТА НА СУБЈЕКТОТ НА ПОДАТОЦИТЕ И НИВНОТО СПРОВЕДУВАЊЕ 115
5.1. Правата на субјектите на податоците 117
Клучни точки 117
5.1.1. Правото на пристап 118
5.1.2. Правото на приговор 125
5.2. Независен надзор 128
Клучни точки 128
5.3. Правни средства и санкции 133
Клучни точки 133
5.3.1. Барања до контролорот 134
5.3.2. Барања поднесени до надзорниот орган 135
5.3.3. Барање поднесено до суд 136
5.3.4. Санкции 142

6. ПРЕКУГРАНИЧЕН ПРЕНОС НА ПОДАТОЦИ 145
6.1. Природата на прекуграничниот пренос на податоци 146
Клучни точки 146
6.2. Слободен пренос на податоци меѓу државите-членки или договорните страни 148
Клучни точки 148
6.3. Слободен пренос на податоци во трети земји 149
Клучни точки 149
6.3.1. Слободен пренос на податоци поради соодветна заштита 150
6.3.2. Слободен пренос на податоци во посебни случаи 152
6.4. Ограничен пренос на податоци во трети земји 153
Клучни точки 153
6.4.1. Договорни клаузули 154
6.4.2. Обврзувачки корпоративни правила 156
6.4.3. Посебни меѓународни договори 156

7. ЗАШТИТАТА НА ПОДАТОЦИТЕ ВО КОНТЕКСТ НА ПОЛИЦИЈАТА И НА КРИВИЧНОТО ПРАВОСУДСТВО 163
7.1. Правото на Советот на Европа за заштита на податоците во полициски и во кривично-правни предмети 164
Клучни точки 164

7.1.1. Препорака за полицијата 165
7.1.2. Конвенцијата од Будимпешта за компјутерскиот криминал 169
7.2. Правото на Европската Унија за заштита на податоците во полициски и во кривично-правни предмети 170
Клучни точки 170
7.2.1. Рамковна одлука за заштита на податоците 170
7.2.2. Поспецифични правни инструменти за заштита на податоците во прекуграничната соработка на полицијата и на органите на кривичниот прогон 172
7.2.3. Заштитата на податоците во Европол и во Европравда 174
7.2.4. Заштитата на податоците во заедничките информациски системи на ниво на Европската Унија 178

8. ДРУГИ ПОСЕБНИ ЕВРОПСКИ ЗАКОНИ ЗА ЗАШТИТА НА ПОДАТОЦИТЕ 187
8.1. Електронски комуникации 188
Клучни точки 188
8.2. Податоци за вработување 193
Клучни точки 193
8.3. Медицински податоци 196
Клучни точки 196
8.4. Обработка на податоци за статистички цели 199
Клучни точки 199
8.5. Финансиски податоци 202
Клучни точки 202

ДОПОЛНИТЕЛНА ЛИТЕРАТУРА 205

СУДСКА ПРАКТИКА 211
Избор од судската практика на Европскиот суд за човековите права 211
Избор од судската практика на Судот на правдата на Европската Унија 215

ИНДЕКС НА ПРЕДМЕТИ 219

Кратенки и акроними

ОКП (BCR)	Обврзувачко корпоративно правило
ЗТК (CCTV)	Затворено телевизиско коло
ЗДСЕ (CETS)	Збирка на договорите на Советот на Европа
Повелба (Charter)	Повелба за основните права на Европската Унија
ЦИС (CIS)	Царински информациски систем
СПЕУ (CJEU)	Суд на правдата на Европската Унија (пред декември 2009 познат како Европски суд на правдата, ЕСП)
СЕ (CoE)	Совет на Европа
Конвенција бр. 108 (Convention 108)	Конвенција за заштита на поединците во однос на автоматската обработка на личните податоци (Совет на Европа)
УОК (CRM)	Управување на односи со корисници
Ц-ШИС (C-SIS)	Централен шенгенски информациски систем
ЕНА (EAW)	Европски налог за апсење
ЕЗ (EC)	Европска Заедница
ЕКЧП (ECHR)	Европска конвенција за човековите права
ЕСЧП (ECtHR)	Европски суд за човековите права
ЕСЗП (EDPS)	Европски супервизор за заштита на податоците
ЕЕО (EEA)	Европска економска област
ЕАСТ (EFTA)	Европска асоцијација за слободна трговија
ЕАМИБ (ENISA)	Европска агенција за мрежна и информациска безбедност
НОЕ (ENU)	Национално одделение за Европол
ЕТХВП (ESMA)	Европско тело за хартии од вредност и пазари

ТТМ (eTEN)	Трансевропски телекомуникациски мрежи
ЕУ (EU)	Европска Унија
ЕПП (EuroPriSe)	Европски печат за приватност
ЕАГИС (eu-LISA)	Европска агенција за големи информатички системи
ЕАОП (FRA)	Европска агенција за основните права
ГСП (GPS)	Глобален систем за позиционирање
ЗНТ (JSB)	Заедничко надзорно тело
НВО (NGO)	Невладина организација
Н-ШИС (N-SIS)	Национален шенгенски информациски систем
ОЕСР (OECD)	Организација за економска соработка и развој
PIN	Личен идентификациски број
ЕПИ (PNR)	Евиденција на патнички имиња
ЕЕПО (SEPA)	Единствена европска платежна област
ШИС (SIS)	Шенгенски информациски систем
SWIFT	Друштво за светски интербанкарски финансиски телекомуникации
ДЕУ (TEU)	Договор за Европската Унија
ДФЕУ (TFEU)	Договор за функционирањето на Европската Унија
УДЧП (UDHR)	Универзална декларација за човековите права
ОН (UN)	Обединети нации
ВИС (VIS)	Визен информациски систем

Како треба да се користи прирачникот

Овој прирачник дава увид во важечкото законодавство на Европската Унија (ЕУ) и на Советот на Европа (СЕ) во врска со заштитата на податоците.

Прирачникот е создаден за да им помогне на правниците кои не се специјализирани во областа на заштитата на податоците. Наменет е за адвокати, судии и за други правни практичари, како и за лицата што работат за други органи, вклучувајќи ги и невладините организации (НВО) кои можат да се сретнат со правни прашања поврзани со заштитата на податоците.

Тој е прва референтна точка за правото на Европската Унија и за Европската конвенција за човековите права (ЕКЧП) кога станува збор за заштитата на податоците и објаснува како е регулирана оваа област во согласност со правото на Европската Унија и според Европската конвенција за човековите права, како и во врска со Конвенцијата на Советот на Европа за заштита на поединците во однос на автоматската обработка на личните податоци (Конвенција бр. 108) и според други инструменти на Советот на Европа. Во уводниот дел на секое поглавје, е прикажана табела со применливите законски одредби, вклучувајќи и избор од значајната судска практика на двата одделни европски правни система. Потоа, релевантните закони на овие два европски правни поредока се претставени еден по друг според нивната применливост за секоја од темите. Тоа му овозможува на читателот да ги увиди сличностите и разликите на двата правни система.

Табелите на почетокот од секое поглавје ги содржат темите кои се обработени во тоа поглавје, како и применливите законски одредби и друг релевантен материјал, како што е судската практика. Редоследот на темите може во извесна мера да се разликува од структурата на текстот во поглавјето, ако тоа е во прилог на концизното претставување на содржината на поглавјето. Во табелите се содржани правото на Советот на Европа и правото на Европската Унија. Тоа би требало да им помогне на читателите да ги пронајдат клучните информации што се однесуваат на нивниот случај, особено ако подлежат само на правото на Советот на Европа.

Правниците во државите што не се членки на Европската Унија, а се членки на Советот на Европа и договорни страни на Европската конвенција за човековите права и на Конвенцијата бр. 108, можат да ги погледнат информациите што се релевантни за нивната држава така што ќе преминат директно на поглавјата што се однесуваат на Советот на Европа. За правниците во државите-членки на Европската Унија, релевантни се двете поглавја, затоа што за тие држави

обврзувачки се двата правни поредока. За тие што имаат потреба од повеќе информации на одредена тема, предвиден е делот во прирачникот под назив „Дополнителна литература".

Правото на Советот на Европа е претставено низ кратки упатувања до избрани предмети на Европскиот суд за човековите права (ЕСЧП). Тие се избрани од големиот број пресуди и одлуки на Судот кои се однесуваат на заштитата на податоците.

Правото на Европската Унија е содржано во усвоените законодавни мерки, во меродавните одредби на договорите и во Повелбата за основните права на Европската Унија, во согласност со неговото толкување во судската практика на Судот на правдата на Европската Унија (СПЕУ, кој пред 2009 година беше познат како Европски суд на правдата (ЕСП)).

Судската практика што е опишана или цитирана во овој прирачник дава увид во големиот корпус на судската практика на Европскиот суд за човековите права и на Судот на правдата на Европската Унија. Упатствата на крајот од прирачникот служат како помош за читателот во барањето на некоја судска практика на интернет.

Покрај тоа, во текстуални полиња на сина заднина, дадени се практични илустрации со хипотетични сценарија со цел дополнително да се објасни примената на европските прописи за заштита на податоците во практиката, особено во случаите кога не постои конкретна судска практика на Европскиот суд за човековите права и на Судот на правдата на Европската Унија. Другите текстуални полиња, прикажани на сива заднина, даваат примери кои се преземени од извори надвор од судската практика, како што е законодавството.

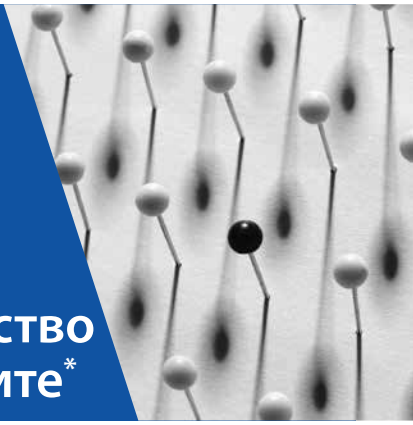
Во уводниот дел на прирачникот накусо е опишана улогата на двата правни система кои се воспоставени со Европската конвенција за човековите права и со правото на Унијата (поглавје 1). Од второто до осмото поглавје се опфатени следните теми:

- терминологијата во врска со заштитата на податоците;
- главните начела на европското законодавство за заштита на податоците;
- прописите на европското законодавство за заштита на податоците;
- правата на субјектот на податоците и нивното спроведување;

- прекуграничниот пренос на податоци;
- заштитата на податоците во контекст на полицијата и на кривичното правосудство;
- други посебни европски закони за заштита на податоците.

1

Контекстот и историјатот на европското законодавство за заштита на податоците*



Европска Унија	Обработени прашања	Совет на Европа
Правото на заштита на податоците		
Директива 95/46/ЕЗ за заштита на поединците во однос на обработката на личните податоци и на слободниот пренос на таквите податоци (*Директива за заштита на податоците*), Сл. весник на ЕУ 1995 L 281		ЕКЧП, член 8 (право на почитување на приватниот и семејниот живот, домот и преписката) Конвенција за заштита на поединците во однос на автоматската обработка на личните податоци (Конвенција бр. 108)
Постигнување урамнотеженост на правата		
СПЕУ, заеднички предмети C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert v. Land Hessen*, 2010 година	Општо	
СПЕУ, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy u Satamedia Oy*, 2008 година	Слобода на изразување	ЕСЧП, *Axel Springer AG v. Germany*, 2012 година ЕСЧП, *Mosley v. the United Kingdom*, 2011 година
	Слобода на уметноста и науката	ЕСЧП, *Vereinigung bildender Künstler v. Austria*, 2007 година

* Во законодавството на Република Македонија, попрецизно во Законот за заштита на личните податоци (Службен весник на Република Македонија, бр. 7/05, 103/08, 124/10 и понатаму) се користи терминот *личен податок* односно *лични податоци* со идентично значење на тука употребените термини *податок* и *податоци* односно *data*. Со цел да се задржи автентичноста на оригиналниот текст на англиски јазик, во овој превод се користат термините *податок* и *податоци*, како и *заштита на податоците (data protection) (заб. на ред.)*

СПЕУ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 2008 година	Заштита на сопственоста	
СПЕУ, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 2010 година	Пристап до документи	ЕСЧП, *Társaság a Szabadságjogokért v. Hungary*, 2009 година

1.1. Правото на заштита на податоците

Клучни точки

- Според членот 8 на Европската конвенција за човековите права, правото на заштита од прибирање и употреба на лични податоци претставува дел од правото на почитување на приватниот и семејниот живот, домот и преписката.
- Конвенцијата бр. 108 на Советот на Европа е првиот меѓународен правно обврзувачки инструмент кој се занимава исклучиво со заштитата на податоците.
- Според правото на Европската Унија, заштитата на податоците првпат е регулирана со Директивата за заштита на податоците.
- Според правото на Европската Унија, заштитата на податоците е признаена како основно право.

Правото на заштита на приватниот живот на поединецот од мешање од страна на други лица, а особено од страна на државата, првпат е пропишано во меѓународен правен инструмент во членот 12 од Универзалната декларација за човековите права (УДЧП) на Обединетите нации (ОН) од 1948 година за почитувањето на приватниот и семејниот живот.[1] Универзалната декларација за човековите права влијаела на развојот на другите инструменти за човекови права во Европа.

1.1.1. Европската конвенција за човековите права

Советот на Европа е основан по Втората светска војна за да ги приближи државите на Европа во заложбите за унапредување на владеењето на правото,

1 Обединети нации (ОН), Универзална декларација за човековите права (УДЧП), 10 декември 1948 год.

демократијата, човековите права и општествениот развој. За таа цел, во 1950 година, Советот ја усвои Европската конвенција за човековите права (ЕКЧП) , која стапи на сила во 1953 година.

Државите имаат меѓународна обврска да ја почитуваат Европската конвенција за човековите права. Сите држави-членки на Советот на Европа ја инкорпорирале или ја спровеле Конвенцијата во своето национално законодавство, со што се обврзани да постапуваат во согласност со одредбите на Конвенцијата.

Со цел да се осигури дека договорните страни ќе ги почитуваат своите обврски што произлегуваат од Европската конвенција за човековите права, во 1959 година во Стразбур, Франција, основан е Европскиот суд за човековите права (ЕСЧП). Тој суд осигурува дека државите ги почитуваат своите обврски во согласност со Конвенцијата со разгледување жалби на поединци, на групи на поединци, на невладини организации и на правни лица поради наводна повреда на Конвенцијата. Во 2013 година Советот на Европа брои 47 држави-членки, од кои 28 истовремено се и држави-членки на Европската Унија. Жалителот што се обраќа до Европскиот суд за човековите права не мора да биде државјанин на некоја од државите-членки. Европскиот суд за човековите права може да разгледува и меѓудржавни жалби што една или повеќе држави-членки на Советот на Европа ги поднеле против друга држава-членка.

Правото на заштита на личните податоци е дел од правата што се заштитени со членот 8 на Конвенцијата, кој го гарантира правото на почитување на приватниот и семејниот живот, домот и преписката и ги поставува условите под кои се допуштени ограничувањата на тоа право[2].

Европскиот суд за човековите права во својата судска практика разгледувал многу предмети во кои станувало збор за прашања поврзани со заштитата на податоците, а особено со такви прашања што се однесувале на следењето на комуникациите[3], различните облици на надзор[4] и заштитата од складирање на лични податоци од страна на државни органи[5]. Тој појаснил дека членот 8 на Европската конвенција за човековите права не само што ги обврзува државите

2 СЕ, Европска конвенција за човековите права, ЗДСЕ Бр. 005, 1950.

3 Види, на пример: ЕСЧП, *Malone v. the United Kingdom*, Бр. 8691/79, 2 август 1984 година; ЕСЧП, *Copland v. the United Kingdom*, Бр. 62617/00, 3 април 2007 година.

4 Види, на пример: ЕСЧП, *Klass and Others v. Germany*, Бр. 5029/71, 6 септември 1978 година; ЕСЧП, *Uzun v. Germany*, Бр. 35623/05, 2 септември 2010 година.

5 Види, на пример: ЕСЧП, *Leander v. Sweden*, Бр. 9248/81, 26 март 1987 година; ЕСЧП, *S. and Marper v. the United Kingdom*, Бр. 30562/04 и 30566/04, 4 декември 2008 година.

да се воздржат од секакви дејства со кои би можело да се повреди ова право на Конвенцијата туку и дека во определени околности позитивно ги обврзува активно да се залагаат за делотворна заштита на приватниот и семејниот живот[6]. Голем дел од овие предмети детално ќе бидат разгледани во соодветните поглавја.

1.1.2. Конвенцијата бр. 108 на Советот на Европа

Со појавувањето на информатичката технологија во 60-тите години на минатиот век се зголеми потребата за подетални правила за заштитита на поединците по пат на заштита на нивните (лични) податоци. До средината на 70-тите години, Комитетот на министри при Советот на Европа усвои повеќе резолуции за заштита на личните податоци, кои се однесувале на членот 8 на Европската конвенција за човековите права[7]. Во 1981 година била отворена за потпишување Конвенцијата за заштита на поединците во однос на автоматската обработка на личните податоци (Конвенција бр. 108)[8]. Конвенцијата бр. 108 беше и остана единствениот правен обврзувачки меѓународен инструмент на полето на заштитата на податоците.

Конвенцијата бр. 108 се применува за секоја обработка на податоци и во приватниот и во јавниот сектор, како што е обработката на податоците од страна на судската и извршната власт. Таа го заштитува поединецот од злоупотреби кои би можеле да настанат при прибирањето и обработката на лични податоци, и истовремено има за цел да го регулира прекуграничниот пренос на лични податоци. Во поглед на прибирањето и обработката на личните податоци, начелата кои се утврдени во Конвенцијата, првенствено се однесуваат на праведното и законито прибирање и автоматската обработка на податоци, кои се складирани за определени легитимни цели и кои не се користат за цели што не се споиви со нив, ниту се чуваат подолго отколку што е потребно. Тие начела се однесуваат и на квалитетот на податоците, а особено на тоа дека мора да бидат соодветни, релевантни, точни и да не бидат прекумерни (пропорционалност).

Покрај тоа што содржи гаранции во врска со прибирањето и обработката на лични податоци, Конвенцијата, во отсуство на соодветни законски гаранции,

6 Види, на пример: ЕСЧП, *I. v. Finland,* Бр. 20511/03, 17 јули 2008 година; ЕСЧП, *K.U. v. Finland,* Бр. 2872/02, 2 декември 2008 година.

7 СЕ, Комитет на министри (1973 година), Резолуција (73) 22 за заштита на приватноста на поединците *vis-à-vis* електронските банки на податоци во приватниот сектор, 26 септември 1973 година; Совет на Европа, Комитет на министри (1974 година), Резолуција (74) 29 за заштита на приватноста на поединците *vis-à-vis* електронските банки на податоци во јавниот сектор, 20 септември 1974 година.

8 СЕ, Конвенција за заштита на поединците во однос на автоматската обработка на личните податоци, Совет на Европа, ЗДСЕ Бр. 108, 1981 година.

ја забранува обработката на „чувствителните“ податоци, како што се расата, политичката определба, здравјето, верата, сексуалниот живот или криминалното досие на лицето.

Конвенцијата го предвидува и правото на информираност на поединецот за кого се прибираат податоци и, ако е потребно, на нивно коригирање. Ограничувањата на правата кои се утврдени во Конвенцијата се можни само ако се загрозени некои попретежни интереси, како што се државната безбедност или одбраната.

Иако Конвенцијата овозможува слободен пренос на лични податоци меѓу државите што се нејзини договорни страни, таа исто така наметнува извесни ограничувања на таквиот пренос до држави чија правна регулатива не предвидува еднаква заштита.

Заради натамошен развој на општите начела и правила кои се пропишани во Конвенцијата бр. 108, Комитетот на министри при Советот на Европа усвои неколку препораки кои не се правно обврзувачки (види ги поглавјата 7 и 8).

Сите држави-членки на Европската Унија ја ратификуваа Конвенцијата бр. 108. Во 1999 година таа беше изменета со цел да ѝ се овозможи на Европската Унија да стане нејзина договорна страна[9]. Во 2001 година беше усвоен Дополнителен протокол кон Конвенцијата бр. 108, со кој беа внесени одредби за прекуграничен пренос на податоците до држави што не се договорни страни, таканаречени трети држави, и за задолжително воспоставување на национални надзорни органи за заштита на личните податоци[10].

Изгледи

По одлуката за модернизација на Конвенцијата бр. 108, јавното советување одржано во 2011 година овозможи потврда на двете главни цели на тој потфат: поефикасна заштита на приватноста во дигиталната ера и зајакнување на механизмот за следење воспоставен со Конвенцијата.

9 СЕ, Измени на Конвенцијата за заштита на поединците во однос на автоматската обработка на личните податоци (ЗДСЕ Бр. 108) со кои им се овозможува пристап на Европските заедници и кои се усвоени од Комитетот на министри во Стразбур, на 15 јуни 1999 година; Член 23 став 2 на Конвенцијата бр. 108 во неговиот изменет облик.

10 СЕ, Дополнителен протокол кон Конвенцијата за заштита на поединците во однос на автоматската обработка на личните податоци, во врска со надзорните органи и прекугранични пренос на податоци, ЗДСЕ Бр. 181, 2001 година.

Кон Конвенцијата бр. 108 можат да пристапат држави што не се членки на Советот на Европа, како и неевропски земји. Потенцијалот на Конвенцијата како универзален стандард и нејзиниот отворен карактер може да послужат како основа за унапредување на заштитата на податоците на глобално ниво.

Досега 45 од 46 држави што се договорни страни на Конвенцијата бр. 108 се држави- членки на Советот на Европа. Уругвај, првата неевропска земја, пристапи во август 2013 година, а Мароко, држава што беше поканета да пристапи кон Конвенцијата бр. 108 од страна на Комитетот на министри е во постапка на формализирање на пристапот.

1.1.3. Законодавството на Европската Унија за заштита на податоците

Правото на Европската Унија се состои од договори и од секундарното право на Унијата. Договорите, имено Договорот за Европската Унија (ДЕУ) и Договорот за функционирањето на Европската Унија (ДФЕУ), се одобрени од страна на сите држави-членки на Европската Унија и уште се нарекуваат и „примарно право на Европската Унија". Регулативите, директивите и одлуките на Европската Унија се усвоени од нејзините институции кои се овластени за тоа со договорите; тие често се нарекуваат „секундарно право на Европската Унија".

Главниот правен инструмент на Европската Унија за заштита на податоците е Директивата 95/46/ЕЗ на Европскиот парламент и на Советот од 24 октомври 1995 година за заштита на поединците во однос на обработката на личните податоци и на слободниот пренос на таквите податоци (*Директива за заштита на податоците*)[11]. Донесена е во 1995 година, во време кога неколку држави-членки веќе имале усвоено национални закони за заштита на податоците. Слободното движење на стоки, капитал, услуги и луѓе во рамките на внатрешниот пазар било условено со слободниот пренос на податоци, кој би можел да се оствари само доколку државите- членки се повикаат на единствен висок степен на заштита на податоците.

Бидејќи целта на усвојувањето на Директивата за заштита на податоците била да се усогласи[12] законодавството во врска со заштитата на податоците на национално ниво, за неа е својствен оној степен на специфичност што може да се спореди

11 Директива за заштита на податоците, Сл. весник на ЕУ 1995 L 281, стр. 31.

12 Види, на пример, Директива за заштита на податоците, Уводни изјави бр. 1, 4, 7 и 8.

со (тогашните) национални законодавства за заштита на податоците. За Судот на правдата на Европската Унија, „Директивата 95/46 има за цел […] да осигури дека степенот на заштитата на правата и слободите на поединците во однос на обработката на личните податоци мора да биде еднаков во сите држави-членки. […] Приближувањето на националното законодавство што се применува во оваа област не смее да доведе до намалување на заштитата која се гарантира со него, туку, напротив, тоа мора да биде насочено кон обезбедување повисок степен на заштита во Европската Унија. Според тоа, […] усогласувањето на националните законодавства не е ограничено на најнизок степен на усогласување, туку доведува до усогласување кое начелно е сеопфатно."[13] Оттука, државите-членки на Европската Унија имаат само ограничен маневарски простор при спроведувањето на директивата.

Директивата за заштита на податоците е изработена со цел да ги потврди и да ги прошири начелата за правото на приватност кои веќе се содржани во Конвенцијата бр. 108. Фактот дека сите 15 држави-членки на Европската Унија во 1995 година биле и договорни страни на Конвенцијата бр. 108 ја отфрла можноста за усвојување на противречни правила во овие два правни инструмента. Сепак, во Директивата за заштита на податоците, оставена е можноста за додавање на инструменти на заштита, која е предвидена во членот 11 на Конвенцијата бр. 108. Поточно, воспоставувањето на независен надзор како инструмент за подобра усогласеност со правилата за заштита на податоците се покажало како важен придонес за ефикасното функционирање на европското законодавство за заштита на податоците. (Во 2001 година тој инструмент беше преземен во правото на Советот на Европа со Дополнителниот протокол кон Конвенцијата бр. 108).

Територијалната примена на Директивата за заштита на податоците ги надминува границите на 28-те држави-членки на Европската Унија, вклучувајќи ги и државите што не се членки на Унијата, а кои се дел од Европската економска област (ЕЕО)[14] – односно Исланд, Лихтенштајн и Норвешка.

Судот на правдата на Европската Унија со седиште во Луксембург е надлежен да утврди дали некоја држава-членка ги исполнила своите обврски од Директивата за заштита на податоците и донесува првична одлука во врска со валидноста и толкувањето на Директивата, со цел да осигури нејзина делотворна и еднаква

13 СПЕУ, заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 24 ноември 2011 година, параграфи 28-29.

14 Договор за Европската економска област, Сл. весник на ЕУ 1994 L 1, кој стапи на сила на 1 јануари 1994 година.

примена во државите-членки. Важен исклучок од применливоста на Директивата за заштита на податоците претставува таканаречениот исклучок за домашна употреба, односно обработката на личните податоци што се врши од страна на физички лица исклучиво заради лични цели или за целите на домот[15]. Таквата обработка начелно се смета за дел од слободите на поединецот.

Во согласност со примарното право на Европската Унија кое било важечко во времето на усвојувањето на Директивата за заштита на податоците, предметната област на примена на директивата е ограничена на прашања поврзани со внатрешниот пазар. Надвор од опфатот на примена првенствено се прашањата поврзани со соработката на полицијата и кривичното правосудство. Заштитата на податоците во овие области произлегува од различни правни инструменти, кои детално се опишани во поглавјето 7.

Бидејќи Директивата за заштита на податоците се однесува само на државите-членки на Европската Унија, бил неопходен дополнителен правен иструмент со цел да се воспостави заштита на податоците при обработка на личните податоци од страна на институциите и телата на Европската Унија. Таквата задача ја исполнува Регулативата (ЕЗ) Бр. 45/2001 за заштита на поединците во врска со обработката на личните податоци од страна на институциите и телата на Заедницата и со слободното движење на такви податоци (*Регулатива за заштита на податоците во институциите на Европската Унија*).[16]

Покрај тоа, дури и во областите кои се опфатени со Директивата за заштита на податоците, често се потребни подетални одредби за заштита на податоците со цел да се постигне потребната јасност во одмерувањето на други легитимни интереси. Два примера за тоа се Директивата 2002/58/ЕЗ во врска со обработката на личните податоци и заштитата на приватноста во секторот за електронски комуникации (*Директива за приватност и електронски комуникации*)[17] и Директивата 2006/24/ЕЗ за задржување на податоци што се создадени или обработени во врска со обезбедувањето јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи и изменување на Директивата 2002/58/ЕЗ (*Директива за*

15 Директива за заштита на податоците, член 3 став 2 втора алинеја.

16 Регулатива (ЕЗ) Бр. 45/2001 на Европскиот парламент и на Советот од 18 декември 2000 година за заштита на поединците во врска со обработката на личните податоци од страна на институциите и телата на Заедницата и со слободното движење на такви податоци, Сл. весник на ЕУ 2001 L 8.

17 Директива 2002/58/ЕЗ на Европскиот парламент и на Советот од 12 јули 2002 година во врска со обработката на личните податоци и заштитата на приватноста во секторот за електронски комуникации (*Директива за приватност и електронски комуникации*), Сл. весник на ЕУ 2002 L 201.

задржување на податоци, прогласена за неважечка на 8 април 2014 година)[18]. Други примери ќе се разгледуваат во поглавјето 8. Таквите одредби мора да бидат во согласност со Директивата за заштита на податоците.

Повелбата за основните права на Европската Унија

Првичните договори за Европските Заедници воопшто не содржеле упатства за човековите права или за нивната заштита. Сепак, со појавата на предмети покренати пред Европскиот суд на правдата (ЕСП) коишто содржеле наводи за повреди на човековите права во области што биле во рамките на полето на примена на правото на Европската Унија, судот развил нов пристап. За да им гарантира заштита на поединците, основните права ги вградил во таканаречените општи начела на европското право. Според Судот на правдата на Европската Унија, овие општи начела ја одразуваат содржината на заштитата на човековите права што е вградена во националните устави и во договорите за човекови права, особено во Европската конвенција за човековите права. Судот сметал дека тоа ќе ја гарантира усогласеноста на правото на Европската Унија со овие начела.

Препознавајќи дека нејзините политики може да влијаат на човековите права и обидувајќи се да поттикне кај граѓаните чувство на „блискост“ со Европската Унија, во 2000 година Европската Унија ја донесе Повелбата за основните права на Европската Унија (Повелба). Оваа повелба опфаќа цела низа граѓански, политички, економски и социјални права на европските граѓани, синтетизирајќи ги уставните традиции и меѓународните обврски кои се заеднички за државите-членки. Правата кои се опишани во Повелбата се поделени на шест категории: достоинство, слободи, еднаквост, солидарност, граѓански права и правда.

Иако на почетокот била само политички документ, Повелбата станала правно обврзувачка[19] како примарно право на Европската Унија (види го членот 6 став 1 од ДЕУ) со стапувањето на сила на Договорот од Лисабон на 1 декември 2009 година[20].

18 Директива 2006/24/ЕЗ на Европскиот парламент и на Советот од 15 март 2006 година за задржување на податоци што се создадени или обработени во врска со обезбедувањето јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи и изменување на Директивата 2002/58/ЕЗ, *(Директива за задржување на податоци),* Сл. весник 2006 L 105, прогласена за неважечка на 8 април 2014 година.

19 ЕУ (2012), Повелба за основните права на Европската Унија, Сл. весник на ЕУ 2012 C 326.

20 Види ги прочистените верзии на Европските Заедници (2012), Договор за Европската Унија, Сл. весник 2012 C 326; и на Европските Заедници (2012), ДФЕУ, Сл. весник 2012 C 326.

Примарното право на Европската Унија исто така содржи општа надлежност на Унијата за донесување закони кои се однесуваат на заштитата на податоците (член 16 од ДФЕУ).

Повелбата не го гарантира само почитувањето на личниот и семејниот живот (член 7), туку го утврдува и правото на заштита на податоците (член 8), изречно покренувајќи го степенот на тој вид заштита до оној што го уживаат основните права во законодавството на Европската Унија. Институциите на Европската Унија како и државите-членки мораат да го почитуваат и да го гарантираат ова право, кое исто така се применува за државите-членки кога го спроведуваат правото на Унијата (член 51 на Повелбата). Членот 8 на Повелбата, кој е формулиран неколку години по Директивата за заштита на податоците, треба да се сфати како отелотворување на претходно воспоставеното законодавство на Европската Унија за заштита на податоците. Затоа, покрај тоа што Повелбата во членот 8 став 1 изречно го споменува правото на заштита на податоците, упатува и на главните начела на заштита на податоците во членот 8 став 2. Конечно, членот 8 став 3 на Повелбата осигурува дека независен орган ќе врши контрола на спроведувањето на овие начела.

Изгледи

Во јануари 2012 година, Европската комисија предложила пакет-реформи за заштита на податоците, држејќи до тоа дека треба да се модернизираат актуелните правила за заштита на податоците во контекст на брзиот технолошки напредок и глобализацијата. Пакетот-реформи се состои од предлог за Општа регулатива за заштита на податоците[21] со која би се заменила Директивата за заштита на податоците, како и од нова Општа директива за заштита на податоците[22] со која би се обезбедила заштита на податоците во областите на полициската и судската соработка во кривичните предмети. Во времето на објавувањето на овој прирачник сè уште беа во тек расправите во врска со пакетот-реформи.

21 Европска комисија (2012), *Предлог за Регулатива на Европскиот парламент и на Советот за заштита на поединците во врска со обработката на личните податоци и со слободното движење на такви податоци (Општа регулатива за заштита на податоците)*, COM(2012) 11 конечно, Брисел, 25 јануари 2012 година.

22 Европска комисија (2012), *Предлог за Директива на Европскиот парламент и на Советот за заштита на поединците во врска со обработката на личните податоци од страна на надлежни органи со цел спречување, истрага, откривање или гонење на кривични дела или извршување на казните, како и за слободното движење на такви податоци (Општа директива за заштита на податоците)*, COM(2012) 10 конечно, Брисел, 25 јануари 2012 година.

1.2. Постигнување урамнотеженост на правата

Клучни точки

- Правото на заштита на податоците не е апсолутно право. Тоа мора да се доведе во рамнотежа со другите права.

Основното право на заштита на личните податоци според членот 8 на Повелбата „сепак, не е апсолутно право, туку тоа треба да се разгледува во врска со неговата функција во општеството“[23]. Така, членот 52 став 1 на Повелбата ја допушта можноста за наметнување на ограничувања при остварувањето на правата како што се оние утврдени во членовите 7 и 8 на Повелбата, доколку таквите ограничувања се пропишани со закон, ако ја почитуваат суштината на тие права и слободи и ако се неопходни во согласност со начелото на пропорционалност и ако вистински ги исполнуваат целите од општ интерес кои се признаени од Европската Унија или потребата за заштита на правата и слободите на другите[24].

Во системот на Европската конвенција за човековите права, заштитата на податоците е загарантирана со членот 8 (право на почитување на личниот и семејниот живот) и, исто како во системот на Повелбата, ова право мора да се применува со почитување на опфатот на примената на други конкурентни права. Во согласност со членот 8 став 2 на Конвенцијата, „Јавната власт не смее да се меша во остварувањето на ова право, освен ако тоа мешање е предвидено со закон и ако е нужно во едно демократско општество […] за заштитата на правата и слободите на другите“.

Според тоа, и Европскиот суд за човековите права и Судот на правдата на Европската Унија повеќе пати нагласија дека при применувањето и толкувањето на членот 8 на Конвенцијата и членот 8 на Повелбата неопходно е правото да се остварува во рамнотежа со други права[25]. Неколку значајни примери ќе покажат како може да се постигне таа рамнотежа.

23 Види, на пример, СПЕУ, заеднички предмети C-92/09 и C-93/09, *Volker and Markus Schecke GbR u Hartmut Eifert v. Land Hessen*, 9 ноември 2010 година, параграф 48.

24 *На истото место*, параграф 50.

25 ЕСЧП, *Von Hannover v. Germany (бр. 2)* [GC], Бр. 40660/08 и 60641/08, 7 февруари 2012 година; СПЕУ, заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros*

1.2.1. Слобода на изразување

Едно од правата кое може да дојде во судир со правото на заштита на податоците е правото на слобода на изразување.

Слободата на изразување е заштитена со членот 11 на Повелбата („Слобода на изразување и информирање"). Тоа право ја вклучува и „слободата на мислење и примање и испраќање на информации и идеи без мешање од страна на некој државен орган и без оглед на границите". Членот 11 одговара на членот 10 од Европската конвенција за човековите права. Во согласност со членот 52 став 3 на Повелбата, доколку Повелбата содржи права што одговараат на правата кои се загарантирани со Европската конвенција за човековите права, „значењето и опфатот на примена на тие права се исти како оние што се предвидени со споменатата конвенција". Според тоа, ограничувањата кои законски можат да му се наметнат на правото што е загарантирано со членот 11 на Повелбата не смеат да ги надминат тие што се предвидени во членот 10 став 2 од Европската конвенција за човековите права или, со други зборови, тие мора да бидат пропишани со закон и мора да бидат нужни во едно демократско општество „заради заштитата […] на угледот или правата на другите". Со овој концепт е опфатено и правото на заштита на податоците.

Односот меѓу заштитата на личните податоци и слободата на изразување е регулиран со членот 9 на Директивата за заштита на податоците, насловен „Обработка на лични податоци и слобода на изразување"[26]. Според тој член, државите-членки се должни да обезбедат низа отстапки или ограничувања во поглед на заштитата на податоците, а оттука и, во поглед на основното право на приватност, кое е наведено во поглавјата II, IV и VI на Директивата. Тие отстапки мора да бидат направени исклучиво за новинарски цели или за целите на уметничкото или книжевното изразување, кои потпаѓаат под опфатот на примената на основното право на слобода на изразување, доколку се неопходни за усогласување на правото на приватност со правилата со кои се регулира слободата на изразување.

---

de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 ноември 2011 година, параграф 48; СПЕУ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 јануари 2008 година, параграф 68. Види исто така и Совет на Европа (2013), судска практика на Европскиот суд за човековите права поврзана со заштитата на личните податоци, DP (2013) судска практика, достапна на: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_ FINAL.pdf.

26 Директива за заштита на податоците, член 9.

Пример: Во предметот *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy u Satamedia Oy*[27] од Судот на правдата на Европската Унија било побарано толкување на членот 9 на Директивата за заштита на податоците и дефинирање на односот меѓу заштитата на податоците и слободата на печатот. Судот требало да го испита случајот со објавување на даночните податоци на околу 1.2 милиони физички лица кои претпријатијата *Markkinapörssi* и *Satamedia* законски ги добиле од финските даночни власти. Поточно, Судот требало да провери дали обработката на личните податоци, кои даночните власти ги ставиле на располагање со цел да им овозможат на корисниците на мобилната телефонија да примаат даночни податоци во врска со други физички лица, треба да се смета како дејство што било извршено исклучиво за новинарски цели. Откако заклучил дека дејствата на *Satakunnan* се состоеле од „обработка на лични податоци" во смисла на членот 3 став 1 на Директивата за заштита на податоците, Судот се зафатил со толкување на членот 9 на Директивата. Судот најпрвин ја забележал важноста на правото на слобода на изразување во секое демократско општество и сметал дека поимите кои се поврзани со таа слобода, како што е новинарството, требало да се толкуваат широко. Потоа, тој оценил дека за да се постигне рамнотежа меѓу двете основни права, отстапките и ограничувањата на правото на заштита на податоците мора да се применуваат само во случај кога тоа е сосема неопходно. Во такви околности, Судот сметал дека дејствата како оние извршени од страна на *Markkinapörssi* и на *Satamedia*, кои се однесувале на податоци од документи од јавен домен според националното законодавство, би можеле да се класифицираат како „новинарски дејства" ако нивниот предмет е откривање информации, мислења и идеи на јавноста, независно од медиумот што бил искористен за нивен пренос. Судот исто така пресудил дека таквите дејства не се ограничени на медиумските друштва и можат да се преземат со цел да се оствари профит. Сепак, Судот на правдата на Европската Унија на националниот суд му ја препуштил одлуката во врска со тоа дали било така во конкретниот случај.

Во поглед на усогласувањето на правото на заштита на податоците со правото на слобода на изразување, Европскиот суд за човековите права донел неколку пресуди кои служат како патоказ.

27 СПЕУ, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy u Satamedia Oy,* 16 декември 2008 година, *параграфи* 56, 61 и 62.

Пример: Во предметот *Axel Springer AG v. Germany*[28], Европскиот суд за човековите права сметал дека домашниот суд со забраната што му ја наметнал на сопственикот на весник кој сакал да објави статија за апсењето и осудата на добро познат глумец го повредил членот 10 на Европската конвенција за човековите права. Европскиот суд за човековите права повторно се повикал на критериумите што ги утврдил во својата судска практика во врска со постигнувањето урамнотеженост на правото на слобода на изразување со правото на почитување на приватниот живот:

- прво, дали настанот на кој се однесувала објавената статија бил од општ интерес: апсењето и осудата на лице бил јавен факт на судот и затоа бил од јавен интерес;

- второ, дали засегнатото лице било јавна личност: засегнатото лице било глумец кој бил доволно добро познат за да се смета за јавна личност;

- трето, како биле добиени информациите и дали биле веродостојни: информациите ги обезбедило Јавното обвинителство, а точноста на информациите кои биле содржани во двете публикации не била предмет на спор меѓу странките.

Затоа, Европскиот суд за човековите права донел одлука дека ограничувањата на објавата кои ѝ биле наметнати на компанијата не биле оправдано сразмерни со легитимната цел на заштитата на приватниот живот на жалителот. Судот заклучил дека имало повреда на членот 10 на Европската конвенција за човековите права.

Пример: Во предметот *Von Hannover v. Germany (Бр. 2)*[29], Европскиот суд за човековите права не утврдил повреда на правото на почитување на приватниот живот според членот 8 на Европската конвенција за човековите права, кога на принцезата Каролина од Монако ѝ била одбиена судската забрана против објавувањето на фотографија од неа и од нејзиниот сопруг која била снимена за време на одморот со скијање. Фотографијата била објавена заедно со статија во која, меѓу другото, се известувало за лошата здравствена состојба на принцот Рение. Европскиот суд за човековите права заклучил

28 ЕСЧП, *Axel Springer AG v. Germany [GC],* Бр. 39954/08, 7 февруари 2012 година, параграфи 90 и 91.

29 ЕСЧП, *Von Hannover v. Germany (No. 2)* [GC], Бр. 40660/08 и 60641/08, 7 февруари 2012 година, параграфи 118 и 124.

дека домашните судови внимателно го одмериле правото на слобода на изразување на издавачките куќи со правото на жалителот на почитување на неговиот приватен живот. Домашните судови ја карактеризирале болеста на принцот Рение како настан на современото општество, што не би можело да се смета за неразумно, па Европскиот суд на правдата можел да прифати дека фотографијата, разгледана во контекст на статијата, барем до одреден степен придонела за дебата од општ интерес. Судот заклучил дека немало повреда на членот 8 на Европската конвенција за човековите права.

Во судската практика на Европскиот суд за човековите права еден од суштинските критериуми кои се однесувале на урамнотежувањето на овие права е тоа дали предметното изразување ќе придонесе за расправа од општ јавен интерес.

Пример: Во предметот *Mosley v. the United Kingdom*[30], еден национален неделник објавил интимни фотографии од жалителот. Тој се пожалил на наводна повреда на членот 8 од Конвенцијата затоа што не бил во можност да побара судска забрана пред да бидат објавени предметните фотографии поради непостоењето на барање за доставување на претходно известување од страна на весникот во случај на објавување на материјал што би можел да повреди нечие право на приватност. Иако објавувањето на таквиот материјал повеќе било за забавни отколку за образовни цели, несомнено се подразбирала заштитата загарантирана со членот 10 на Конвенцијата, која би можела да се надоврзе на барањата на членот 8 на Конвенцијата според кој информациите биле од приватна и интимна природа и не постоел јавен интерес за нивно објавување. Меѓутоа, би требало да се посвети особено внимание при испитувањето на ограничувањата кои би можеле да се сметаат за облик на цензура пред објава. Имајќи го предвид обесхрабрувачкиот ефект со кој барањето за претходно известување ризикува да создаде значително сомневање во однос на ефективноста на какво било барање за претходно известување и со големата слобода на сопствена процена во оваа област, Судот заклучил дека членот 8 не налага законски обврзувачко барање за претходно известување. Според тоа, Судот заклучил дека немало повреда на членот 8.

30 ЕСЧП, предмет *Mosley v. the United Kingdom*, Бр. 48009/08, 10 мај 2011 година, параграфи 129 и 130.

Пример: Во предметот *Biriuk v. Lithuania*[31], жалителката побарала надомест на штета од еден дневен весник затоа што објавил статија во која пишувало дека таа била ХИВ позитивна. Таквата информација наводно ја потврдиле докторите во локалната болница. Европскиот суд за човековите права сметал дека предметната статија не придонесувала за расправа од општ интерес и повторил дека заштитата на личните податоци, а пред сè на медицински податоци, била од суштинско значење за остварувањето на правото на лицето на почитување на неговиот приватен и семеен живот, кое е гарантирано со членот 8 на Конвенцијата. Судот му придал особена важност на фактот дека во случајот, според извештајот во весникот, медицинскиот персонал на болницата дал информации во врска со заразеноста на жалителката со вирусот ХИВ со што очигледно ја прекршил својата обврска за чување на лекарска тајна. Според тоа, државата не го осигурила правото на жалителката на почитување на нејзиниот приватен живот. Судот заклучил дека имало повреда на членот 8.

1.2.2. Пристап до документи**

Според членот 11 на Повелбата и членот 10 на ЕКЧП, со слободата на информирање се штити правото не само на давање туку и на *примање* информации. Сè повеќе се согледува колку е значајно транспарентното работење на владата за функционирањето на едно демократско општество. Поради тоа, во последните две децении, правото на пристап до документи на државните органи е признаено како важно право на секој граѓанин на Унијата и на секое физичко или правно лице кое живее или има регистрирано седиште во некоја држава-членка.

Според правото на Советот на Европа, може да се упати на начелата кои се предвидени во Препораката за пристап до службени документи, која ги инспирирала авторите на Конвенцијата за пристап до службени документи (*Конвенција бр. 205*)[32]. **Според правото на Европската Унија**, правото на пристап до документи е загарантирано со Регулативата 1049/2001 во врска со јавниот пристап до документи на Европскиот парламент, на Советот и на Комисијата

31 ЕСЧП, предмет *Biriuk v. Lithuania,* Бр. 23373/03, 25 ноември 2008 година.

** Во законодавството на Република Македонија се користи и терминот *информации од јавен карактер*, а се однесува на истата цел, односно на пристапот до документите на органите на јавната власт со цел да се обезбеди транспарентното работење на државната власт *(заб. на ред.).*

32 СЕ, Комитет на министри (2002), Препорака Rec(2002) до државите-членки за пристап до службени документи, 21 февруари 2002 год.; СЕ, Конвенција за пристап до службени документи, ЗДСЕ Бр. 205, 18 јуни 2009 год. Конвенцијата сè уште не стапила на сила.

(*Регулатива за пристап до документи*)[33]. Со членот 42 на Повелбата и членот 15 став 3 од Договорот за функционирањето на Европската Унија, тоа право е проширено на пристап „до документи на институции, тела, канцеларии и агенции на Унијата, независно од нивниот облик". Во согласност со членот 52 став 2 на Повелбата, правото на пристап до документи исто така може да се оствари во рамките на условите и ограничувањата кои се предвидени во членот 15 став 3 од Договорот за функционирањето на Европската Унија. Тоа право би можело да дојде во судир со правото на заштита на податоците ако со пристапот до некој документ се откријат лични податоци на друго лице. Затоа, може да биде потребно да се урамнотежат барањата за пристап до документи или до информации на државни органи со правото на заштита на податоците на лица чии податоци се содржани во побараните документи.

Пример: Во предметот *European Commission v. Bavarian Lager*[34], Судот на правдата на Европската Унија ја дефинирал опфатноста на заштитата на личните податоци во смисла на пристапот до документи на институциите на Европската Унија и односот меѓу Регулативите бр. 1049/2001 (*Регулатива за пристап до документи*) и 45/2001 (*Регулатива за заштита на податоците*). Претпријатието „*Bavarian Lager*", основано во 1992 година, увезувало флаширано германско пиво во Обединетото Кралство, првенствено наменето за пивниците и баровите. Меѓутоа, наишло на тешкотии затоа што британското законодавство *de facto* ги ставало во поповолна положба националните производители. Како одговор на жалбата на „*Bavarian Lager*", Европската комисија одлучила да поведе постапка против Обединетото Кралство поради неисполнување на неговите обврски, што довело до измена на оспорените одредби и нивно усогласување со правото на Европската Унија. Потоа „*Bavarian Lager*" побарало од Комисијата, меѓу другите документи, копија од записникот за еден состанок на кој учествувале претставници на Комисијата, британските државни органи и *Confédération des Brasseurs du Marché Commun* (CBMC). Комисијата се согласила да открие одредени документи кои се однесувале на состанокот, но изоставила пет имиња кои се појавиле во записникот затоа што две лица изречно се противеле на тоа да биде откриен нивниот идентитет, а Комисијата не била во можност да ги контактира другите три лица. Со одлука од 18 март 2004 година, Комисијата одбила нова жалба

33 Регулатива (ЕЗ) Бр. 1049/2001 на Европскиот парламент и на Советот од 30 мај 2001 година во врска со јавниот пристап до документи на Европскиот парламент, на Советот и на Комисијата, Сл. весник 2001 L 145.

34 СПЕУ, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 јуни 2010 год., параграфи 60, 63, 76, 78 и 79.

со која претпријатието *„Bavarian Lager“* го барало целосниот записник од состанокот, повикувајќи се првенствено на заштитата на приватниот живот на тие лица која е загарантирана со Директивата за заштита на податоците. Бидејќи не било задоволно со ваквото стојалиште, *„Bavarian Lager“* поднело тужба пред првостепениот суд, кој со пресуда од 8 ноември 2007 година ја поништил одлуката на Комисијата (предмет T-194/04, *Bavarian Lager v. Commission*), особено сметајќи дека самото внесување на имињата на односните лица во списокот на лица кои присуствувале на состанокот во име на установата која ја претставувале, не претставува нарушување на приватниот живот и не ги доведува приватните животи на тие лица во никаква опасност.

На жалба на Комисијата, Судот на правдата на Европската Унија ја поништил пресудата на првостепениот суд. Судот сметал дека со Регулативата за пристап до документи се воспоставува „конкретен и зајакнат систем на заштита на лица чии лични податоци, во одредени случаи, би можеле да бидат објавени“. Според Судот, во случај кога со барање што е засновано на Регулативата за пристап до документи се бара пристап до документи кои содржат лични податоци, во целост се применуваат одредбите од Регулативата за заштита на податоците. Потоа Судот заклучил дека Комисијата со право ја одбила жалбата за пристап до целосниот записник од состанокот од октомври 1996 год. Во недостиг од согласноста на петте учесници на тој состанок, Комисијата во доволна мера ја исполнила својата должност за отвореност со тоа што доставила верзија на предметниот документ во која ги изоставила нивните имиња.

Покрај тоа, според Судот, „бидејќи претпријатието *Bavarian Lager* не дало изречно и легитимно оправдување за своето барање ниту, пак, дало некаков уверлив аргумент со кој би ја покажало потребата за доставување на таквите лични податоци, Комисијата не можела да ги одмери различните интереси на засегнатите учесници ниту, пак, можела да провери дали постоела причина за претпоставка дека би можеле да се повредат легитимните интереси на субјектите на податоците“, како што налага Регулативата за заштита на податоците.

Според оваа пресуда, за мешање во правото на заштита на податоците во врска со пристапот до документи треба да постои конкретна и оправдана причина.

Правото на пристап до документи не може автоматски да го укине правото на заштита на податоците[35].

Посебен аспект на барањето за пристап бил даден во следната пресуда на Европскиот суд за човековите права.

Пример: Во предметот *Társaság a Szabadságjogokért v. Hungary*[36], жалителот, невладина организација за човекови права, од Уставниот суд побарал пристап до информации за случај што бил во тек. Без претходно да се советува со парламентарецот кој ја поднел тужбата, Уставниот суд го одбил барањето за пристап со образложение дека жалбите кои се поднесени до него би можеле да им се стават на располагање на трети лица само со одобрение на подносителот. Домашните судови го потврдиле ова одбивање со образложение дека заштитата на таквите лични податоци не може да биде надвладеана од други законити интереси, вклучувајќи ја достапноста на јавни информации. Жалителот бил во служба на „општествен чувар", чии активности барале слична заштита како онаа што ја уживаат медиумите. Во врска со слободата на печатот, Европскиот суд за човековите права бил доследен во своето стојалиште дека јавноста има право да добива информации од општ интерес. Информациите кои ги барал жалителот биле „готови и достапни" и не барале прибирање на податоци. Во такви околности, државата имала обврска да не го загрозува преносот на информациите кои ги барал жалителот. Накусо, Европскиот суд за човековите права сметал дека пречките со кои се попречува пристапот до информации од јавен интерес би можеле да ги обесхрабрат лицата кои работат во медиумите или во сродните области во вршењето на нивната суштинска улога на „јавен чувар". Судот заклучил дека имало повреда на членот 10.

Според правото на Европската Унија, јасно е утврдена важноста на транспарентноста. Начелото на транспарентност е предвидено во членовите 1 и 10 од Договорот за Европската Унија и во членот 15 став 1 од Договорот за функциони-

35 На оваа тема погледни ги деталните расправи во Европски супервизор за заштита на податоците (ЕСЗП) (2011), *Јавен пристап до документи кои содржат лични податоци по пресудата на претпријатието B*avarian Lager, Брисел, 24 март 2011 година, достапни на: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/ Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ЕСЧП, *Társaság a Szabadságjogokért v. Hungary*, Бр. 37374/05, 14 април 2009 год.; види параграфи 27, 36–38.

рањето на Европската Унија[37]. Според уводната изјава бр. 2 на Регулативата (ЕЗ) Бр. 1049/2001, тоа начело им овозможува на граѓаните поактивно да учествуваат во процесот на одлучување, гарантирајќи дека администрацијата ужива поголема легитимност и е поефективна и одговорна пред граѓаните во демократскиот систем[38].

Според ова образложение, Регулативата на Советот (ЕЗ) Бр. 1290/2005 за финансирањето на заедничката земјоделска политика и Регулативата на Комисијата (ЕЗ) Бр. 259/2008 која ги пропишува деталните правила за нејзината примена бараат објава на информации за корисниците на одредени средства на Европската Унија во земјоделскиот сектор и за износите што ги примил секој корисник[39]. Објавувањето на таквите податоци би требало да придонесе за јавна контрола на администрацијата во поглед на соодветното користење на јавни средства. Неколку корисници ја оспориле пропорционалноста на таквото објавување.

Пример: Во предметот *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*[40], Судот на правдата на Европската Унија морал да донесе пресуда во врска со пропорционалноста на објавувањето на имињата на корисниците на земјоделските субвенции на Европската Унија и на износот што го примил секој од нив, како што налагало законодавството на Европската Унија.

Напоменувајќи дека правото на заштита на податоците не е апсолутно право, Судот сметал дека објавувањето на податоците со имињата на корисниците на два европски фонда за земјоделска помош и на вкупниот износ што тие го примиле на интернет-страница начелно претставува мешање во нивниот приватен живот, а особено во заштитата на нивните лични податоци.

37 ЕУ (2012 година), Прочистени верзии на Договорот за Европската Унија и на Договорот за функционирањето на Европската Унија, Сл. весник 2012 C 326.

38 СПЕУ, C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communities*, 6 март 2003 год., параграф 39; и СПЕУ, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 јуни 2010 год., параграф 54.

39 Регулатива на Советот (ЕЗ) Бр. 1290/2005 од 21 јуни 2005 година за финансирање на заедничката земјоделска политика, Сл. весник 2005 L 209; и Регулатива на Комисијата (ЕЗ) Бр. 259/2008 од 18 март 2008 год. која ги пропишува деталните правила за примена на Регулативата на Советот (ЕЗ) Бр. 1290/2005 во врска со објавување информации за корисниците на средства на Европскиот земјоделски гарантен фонд (ЕЗГФ) и на Европскиот земјоделски фонд за рурален развој (ЕЗФРР), Сл. весник 2008 L 76.

40 СПЕУ, заеднички предмети C-92/09 и C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 ноември 2010, параграфи 47–52, 58, 66–67, 75, 86 и 92.

Судот сметал дека таквото мешање во членовите 7 и 8 на Повелбата било законски предвидено и исполнувало цел од општ интерес која била признаена од Европската Унија, а која, имено, го вклучувала зголемувањето на транспарентноста на користењето на фондовите на Заедницата. Меѓутоа, Судот на правдата на Европската Унија бил на мислење дека објавувањето на имињата на физички лица кои се корисници на земјоделската помош на Европската Унија од овие два фонда и вкупниот износ што тие го примиле претставувало несразмерна мерка и не било оправдано ако се земе предвид членот 52 став 1 на Повелбата. Судот затоа го прогласил законодавството на Европската Унија во врска со објавувањето информации за корисниците на европските земјоделски фондови за делумно неважечко.

1.2.3. Слобода на уметноста и науката

Друго право на постигнување урамнотеженост со правото на почитување на приватниот живот и со заштитата на податоците е слободата на уметноста и на науката, која изречно е заштитена со членот 13 на Повелбата. Тоа право во прв ред е изведено од правото на слобода на мислење и на изразување и треба да се остварува со земање предвид на членот 1 на Повелбата (човеково достоинство). Европскиот суд за човековите права смета дека слободата на уметноста е заштитена со членот 10 на Европската конвенција за човековите права[41]. Правото загарантирано со членот 13 на Повелбата исто така може да подлежи на ограничувањата од членот 10 на Конвенцијата[42].

Пример: Во предметот *Vereinigung bildender Künstler v. Austria*[43], австриските судови му забраниле на здружението-жалител да продолжи да изложува слика со фотографија од главите на различни јавни фигури во сексуални пози. Еден австриски парламентарец, чија фотографија била искористена во сликата, повел постапка против здружението-жалител, барајќи забрана на изложување на сликата. Домашниот суд го прифатил неговото барање и ја изрекол забраната. Европскиот суд за човековите права повторил дека членот 10 на Европската конвенција за човековите права се применувал за ширење идеи кои ја навредувале, ја шокирале или ја вознемирувале државата или кој било дел од населението. Тие што создаваат, изведуваат, шират или изложуваат

41 ЕСЧП, *Müller and Others v. Switzerland*, Бр. 10737/84, 24 мај 1988 година.

42 Објаснувања кои се однесуваат на Повелбата за основните права, Сл. весник 2007 година С 303.

43 ЕСЧП, *Vereinigung bildender Künstler v. Austria*, Бр. 68345/01, 25 јануари 2007 година; види ги особено параграфите 26 и 34.

уметнички дела придонесуваат за размената на идеи и мислења, па државата е должна да не им ја ускратува непотребно слободата на изразување. Бидејќи сликата била колаж во кој биле искористени фотографии само од главите на лицата, а нивните тела биле насликани на нереалистичен и претеран начин, чија цел очигледно ниту било да се прикаже ниту да се навести стварноста, Европскиот суд за човековите права понатаму изјавил дека „сликата тешко би можела да се сфати како опишување на детали од приватниот живот [на насликаниот], туку таа повеќе се однесувала на неговата јавна положба како политичар" и на тоа дека „во тоа својство [насликаниот] требало да покаже поголема толеранција на критика". Одмерувајќи ги различните интереси што биле засегнати, Европскиот суд на правдата заклучил дека неограничената забрана за натамошно изложување на сликата била несразмерна. Судот заклучил дека имало повреда на членот 10 на Конвенцијата.

Во врска со науката, европското законодавство за заштита на податоците ја зема предвид посебната вредност што таа ја има за општеството. Од таа причина, општите ограничувања на употребата на личните податоци се намалени. И Директивата за заштита на податоците и Конвенцијата бр. 108 допуштаат задржување податоци за научно истражување кога тие повеќе не се потребни за првичната цел заради која биле прибрани. Покрај тоа, подоцнежната употреба на лични податоци за научно истражување не се смета за несоодветна цел. Задача на националното право е да создаде подетални одредби, вклучувајќи ги и потребните мерки на заштита, за да го усогласи интересот за научно истражување со правото на заштита на податоците (види ги исто така поглавјата 3.3.3. и 8.4.) .

1.2.4. Заштита на сопственоста

Правото на заштита на сопственоста е предвидено во членот 1 од Првиот протокол кон Европската конвенција за човековите права како и во членот 17 став 1 на Повелбата. Важен аспект на правото на сопственост е заштитата на интелектуалната сопственост, која изречно се споменува во членот 17 став 2 на Повелбата. Во правниот поредок на Европската Унија постојат неколку директиви кои се насочени кон ефикасната заштита на интелектуалната сопственост, а особено на авторското право. Интелектуалната сопственост не ја опфаќа само сопственоста на литературните и уметничките дела туку и патентите, трговските марки и сродните права.

Од судската практика на Судот на правдата на Европската Унија јасно произлегува дека заштитата на основното право на сопственост мора да се урамнотежи со заштитата на другите основни права, а особено со правото на заштита на податоците[44]. Имало случаи каде што институциите за заштита на авторските права барале од давателите на интернет-услуги да го откријат идентитетот на корисници на платформи за споделување на датотеки на интернет. Таквите платформи често им овозможуваат на корисниците на интернет бесплатно да преземаат музички записи и покрај тоа што тие се заштитени со авторското право.

Пример: Предметот *Promusicae v. Telefónica de España*[45] се однесувал на противењето на еден шпански давател на услуги за пристап на интернет, „*Telefónica*“, на една непрофитна организација на музички продуценти и издавачи на музички и аудиовизуелни снимки под називот „*Promusicae*“, да ѝ ги открие личните податоци на одредени лица на кои им дал услуги за пристап на интернет. Организацијата „*Promusicae*“ барала откривање на информациите за да може да поведе граѓанска постапка против тие лица за кои тврдела дека користеле програма за размена на датотеки што овозможувала пристап до фонограми, чие право на користење го имале членови на „*Promusicae*“.

Шпанскиот суд го проследил предметот до Судот на правдата на Европската Унија, барајќи одговор на прашањето дали таквите лични податоци, во согласност со правото на Заедницата, мораат да бидат проследени во рамките на граѓанска постапка за да се осигури делотворна заштита на авторското право. Тој се повикал на Директивите 2000/31, 2001/29 и 2004/48, кои исто така биле толкувани во контекст на членовите 17 и 47 на Повелбата. Судот заклучил дека овие три директиви, како и Директивата за приватност и електронски комуникации (2002/58/ЕЗ), не ги спречуваат државите-членки да пропишат обврска за откривање на лични податоци во смисла на граѓанската постапка за да обезбедат ефикасна заштита на авторското право.

Судот на правдата на Европската Унија истакнал дека од таа причина тој предмет го покренал прашањето за потребата од усогласување на барањата за заштита на различните основни права, односно правото на почитување на приватниот живот, со правата на заштита на сопственоста и на реална жалба.

44 ЕСЧП, *Ashby Donald and others v. France,* Бр. 36769/08, 10 јануари 2013 год.

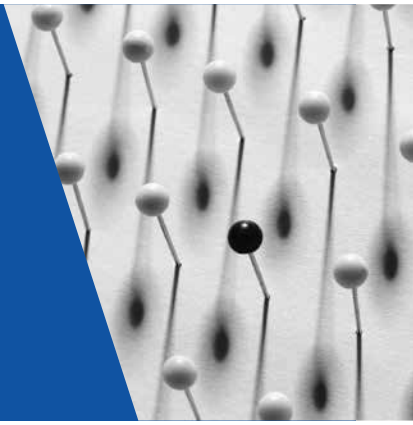
45 СПЕУ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU,* 29 јануари 2008 година, параграфи 54 и 60.

Судот заклучил дека „државите-членки при пренесувањето во правниот поредок (транспонирањето) на горенаведените директиви мораат да се потпрат на она нивно толкување што ќе овозможи да се постигне правична рамнотежа меѓу различните основни права кои се заштитени со правниот поредок на Заедницата. Понатаму, при спроведување на мерките за пренесување во правниот поредок на тие директиви, државните органи и судовите на државите-членки не само што мораат да го толкуваат своето национално право во согласност со тие директиви туку треба и да осигурат дека не се потпираат на нивно толкување кое би било во судир со тие основни права или со другите општи начела на правото на Заедницата, како што е начелото на пропорционалност"[46].

46 *На истото место*, стр. 65 и 68; види исто така СПЕУ, C-360/10, *SABAM v. Netlog N.V.*, 16 февруари 2012 година.

2

Терминологијата во врска со заштитата на податоците



Европска Унија	Обработени прашања	Совет на Европа
Лични податоци		
Директива за заштита на податоците, член 2 точка (а) СПЕУ, заеднички случаи C-92/09 и C-93/09, *Volker and Markus Schecke GbR (C-92/09) u Hartmut Eifert (C-93/09) v. Land Hessen*, 9 ноември 2010 година СПЕУ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 јануари 2008 година	Правна дефиниција	Конвенција бр. 108, член 2 точка (а) ЕСЧП, *Bernh Larsen Holding AS u Others v. Norway*, Бр. 24117/08, 14 март 2013 година
Директива за заштита на податоците, член 8 став 1 СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 година	Посебни категории на лични податоци (чувствителни податоци)	Конвенција бр. 108, член 6
Директива за заштита на податоците, член 6 став 1 точка (д)	Анонимизирани и псевдонимизирани податоци	Конвенција бр. 108, член 5 точка (д) Конвенција бр. 108, Појаснувачки извештај, член 42
Обработка на податоци		
Директива за заштита на податоците, член 2 точка (б) СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 година	Дефиниции	Конвенција бр. 108, член 2 точка (в)

Корисници на податоци		
Директива за заштита на податоците, член 2 точка (г)	Контролор	Конвенција бр. 108, член 2 точка (г) Препорака за профилирањето, член 1 точка (е) *
Директива за заштита на податоците, член 2 точка (д) СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 година	Обработувач	Препорака за профилирањето, член 1 точка (ж)
Директива за заштита на податоците, член 2 точка (е)	Корисник	Конвенција бр. 108, Дополнителен протокол, член 2 став 1
Директива за заштита на податоците, член 2 точка (ѓ)	Трета страна	
Согласност		
Директива за заштита на податоците, член 2 точка (ж) СПЕУ, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 мај 2011 година	Дефиниција и услови за валидна согласност	Препорака за медицински податоци, член 6, и разни последователни препораки

*Напомена: *Совет на Европа, Комитет на министри (2010), Препорака Rec(2010)13 до државите- членки за заштита на поединците во однос на автоматската обработка на лични податоци во контекст на профилирањето (*Препорака за профилирањето*), 23 ноември 2010 год.*

2.1. Лични податоци

Клучни точки

- Податоците се сметаат за лични податоци доколку се однесуваат на лице кое е идентификувано или кое може да се идентификува, односно на субјектот на податоците.
- Лицето може да се идентификува ако без несразмерно голем напор е можно да се добијат дополнителни информации за него, со што се овозможува идентификација на субјектот на податоците.
- Автентикација подразбира докажување дека некое лице има определен идентитет и/или е овластено за извршување одредени дејства.

- Постојат посебни категории на податоци, таканаречени чувствителни податоци, наведени во Конвенцијата бр. 108 и во Директивата за заштита на податоците, кои бараат зголемена заштита и затоа подлежат на посебен правен режим.
- Податоците се анонимизирани ако повеќе не содржат никакви идентификатори, а се псевдонимизирани ако идентификаторите се кодирани.
- За разлика од анонимизираните податоци, псевдонимизираните податоци се лични податоци.

2.1.1. Главни аспекти на поимот за лични податоци

Според правото на Европската Унија и **правото на Советот на Европа,** „личните податоци" се дефинираат како информации кои се однесуваат на физичко лице што е идентификувано или може да се идентификува[47], односно информации за лице чиј идентитет е или јасно утврден или барем може да се утврди со прибирање на дополнителни информации.

Доколку податоците за таквото лице се обработуваат, тоа лице се нарекува „субјект на податоците".

Лице

Правото на заштита на податоците произлегло од правото на почитување на приватниот живот. Концептот за приватен живот се однесува на луѓето. Според тоа, физичките лица се примарните корисници на заштитата на податоците. Понатаму, според Мислењето на Работната група за членот 29, само *живо суштество* е заштитено со европското законодавство за заштита на податоците[48].

Судската практика на Европскиот суд за човековите права во врска со членот 8 на Европската конвенција за човековите права покажува дека може да биде

47 Директива за заштита на податоците, член 2 точка (а); Конвенција бр. 108, член 2 точка (а).

48 Работна група за членот 29 (2007), *Мислење 4/2007 во врска со поимот за лични податоци*, РГ 136, 20 јуни 2007 год., стр. 22.

тешко целосно да се одвојат работите кои се однесуваат на приватниот и на професионалниот живот[49].

Пример: Во предметот *Amann v. Switzerland*[50], властите следеле деловен телефонски повик до жалителот. Врз основа на тој повик, властите повеле истрага против жалителот и пополниле картичка за него за потребите на националниот индекс на сигурносни картички. Иако следењето на комуникациите се однесувало на деловен телефонски повик, Европскиот суд за човековите права сметал дека чувањето податоци во врска со овој повик се однесувало на приватниот живот на жалителот. Судот истакнал дека поимот „приватен живот" не смее да се толкува рестриктивно, особено поради тоа што почитувањето на приватниот живот го содржи и правото на воспоставување и развивање односи со други луѓе. Покрај тоа, не постоела никаква начелна причина за да се оправда исклучувањето на активности од професионална или деловна природа од поимот „приватен живот". Таквото широко толкување одговарало на тоа на Конвенцијата бр. 108. Судот понатаму утврдил дека мешањето во случајот на жалителот не било во согласност со законот, бидејќи домашното право не содржело конкретни и детални одредби за собирањето, евидентирањето и чувањето на информациите. Оттука, Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Понатаму, доколку и работите од професионалниот живот можат да подлежат на заштита на податоците, се поставува прашањето зошто им се нуди заштита само на физички лица. Правата содржани во Европската конвенција за човековите права им се гарантираат на сите, а не само на физичките лица.

Постои судска практика на Европскиот суд за човековите права со пресуда во врска со жалбите на правни лица поради наводната повреда на нивното право на заштита од употреба на нивните податоци во согласност со членот 8 на Конвенцијата. Но, Судот го разгледувал случајот од перспектива на правото на почитување на домот и преписката, а не на приватниот живот:

49 Види, на пример: ЕСЧП, *Rotaru v. Romania* [GC], бр. 28341/95, 4 мај 2000 год., параграф 43; ЕСЧП, *Niemietz v. Germany*, 13710/88, 16 декември 1992 год., параграф 29.

50 ЕСЧП, *Amann v. Switzerland* [GC], бр. 27798/95, 16 февруари 2000 год., параграф 65.

Пример: Во предметот *Bernh Larsen Holding AS and Others v. Norway*[51] се работело за жалба од страна на три норвешки компании за одлуката на даночните власти со која им било наложено на даночните ревизори да им достават копии од сите податоци на компјутерскиот сервер кој трите компании заеднички го користеле.

Европскиот суд за човековите права утврдил дека таквата обврска наметната на компаниите-жалители претставувала мешање во нивните права на почитување на „домот" и на „преписката" за целите на членот 8 на Конвенцијата. Меѓутоа, Судот заклучил дека даночните власти располагале со делотворни и соодветни заштитни мерки од злоупотреба: компаниите-жалители биле добро известени однапред, биле присутни и во можност да учествуваат во постапката на лице место, а материјалот требало да биде уништен по завршувањето на даночната ревизија. Во такви околности била воспоставена правична рамнотежа меѓу правото на компаниите-жалители на почитување на „домот" и на „преписката" и нивниот интерес за заштита на приватноста на лицата кои работеле за нив, од една страна, и јавниот интерес за обезбедување ефикасна контрола за потребите на утврдување на данокот, од друга страна. Според тоа, Судот утврдил дека немало повреда на членот 8.

Според Конвенцијата бр. 108, заштитата на податоците се занимава, пред сè, со заштитата на физички лица. Меѓутоа, договорните страни во рамките на домашното законодавство можат да ја прошират заштитата на податоците и на правни лица, како што се деловни компании и здруженија. **Законодавството на Европската Унија за заштита на податоците** начелно не ја опфаќа заштитата на правните лица во поглед на обработката на податоците што се однесуваат на нив. Националните законодавци слободно можат да го регулираат тоа прашање[52].

Пример: Во предметот *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*[53], Судот на правдата на Европската Унија, повикувајќи се на објавата на лични податоци кои се однесувале на корисниците на земјоделска помош, сметал дека „правни лица имаат право да бараат заштита според членовите 7 и 8 на Повелбата во врска со

51 ЕСЧП, *Bernh Larsen Holding AS and Others v. Norway*, бр. 24117/08, 14 март 2013 год. Сепак, види, исто така, и ЕСЧП, *Liberty and Others v. the United Kingdom*, бр. 58243/00, 1 јули 2008 год.

52 Директива за заштита на податоците, Уводна изјава 24.

53 СПЕУ, Заеднички случаи C-92/09 и C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 ноември 2010 год., параграф 53.

таква идентификација само ако службеното име на правното лице идентификува едно или повеќе физички лица.[…] Правото на почитување на приватниот живот во однос на обработката на лични податоци, признаено во членовите 7 и 8 на Повелбата, се однесува на која било информација во врска со идентификуван поединец или поединец што може да се идентификува […]"[54].

Можност за идентификување лице

Според правото на Европската Унија како и **правото на Советот на Европа**, информациите содржат податоци за некое лице ако:

- поединецот се идентификува со тие информации; или
- поединецот, и покрај тоа што не е идентификуван, е опишан преку тие информации на начин што овозможува со натамошно истражување да се открие кој е субјектот на податоците.

И двата вида информации се заштитени на ист начин со европското законодавство за заштита на податоците. Европскиот суд за човековите права во неколку наврати изјавил дека поимот „лични податоци" според Европската конвенција за човековите права е ист како и во Конвенцијата бр. 108, посебно во поглед на условот којшто се однесува на идентификувани лица или на лица што можат да се идентификуваат[55].

Правните дефиниции за личните податоци не појаснуваат дополнително кога едно лице се смета за идентификувано[56]. Очигледно, идентификацијата бара елементи кои го опишуваат лицето на таков начин што тој или таа се разликува од сите други лица и е препознатлив како поединец. Името на некое лице е одличен пример за такви елементи на описот. Во исклучителни случаи, други идентификатори можат да имаат сличен ефект како името. На пример, за јавните личности може да биде доволно да се спомене функцијата на лицето, како што е претседател на Европската комисија.

54 *На истото место,* параграф 52.

55 Види ЕСЧП, *Amann v. Switzerland* [GC], Бр. 27798/95, 16 февруари 2000 год., параграф. 65 *и други*.

56 Види, исто така, и ЕСЧП, *Odièvre v. France* [GC], Бр. 42326/98, 13 февруари 2003 год..; и ЕСЧП, *Godelli v. Italy*, Бр. 33783/09, 25 септември 2012 год.

Пример: Во предметот *Promusicae*[57], Судот на правдата на Европската Унија изјавил дека „е неоспорно дека доставувањето имиња и адреси на одредени корисници на [одредена платформа за споделување датотеки на интернет] кои ги побарала организацијата 'Promusicae' вклучува ставање на располагање лични податоци, односно информации во врска со физички лица што се идентификувани или можат да се идентификуваат, во согласност со дефиницијата од членот 2 точка (а) на Директивата 95/46 […]. Таквото доставување информации кои, како што изнела *'Promusicae'*, а *'Telefónica'* не оспорила, биле зачувани од *'Telefónica'*, претставува обработка на лични податоци во смисла на првиот параграф од членот 2 на Директивата 2002/58, во врска со членот 2 точка (б) на Директивата 95/46".

Бидејќи многу имиња не се единствени, за да се утврди идентитетот на лицето може да се потребни дополнителни идентификатори со цел да се осигури дека лицето не е заменето со некое друго лице. Често се користат датумот и местото на раѓање. Покрај тоа, во некои земји се внесени персонализирани броеви, со цел подобро да се прави разлика помеѓу граѓаните. Биометриските податоци, како што се отпечатоци од прсти, дигитални фотографии или скенирање на ирисот на окото, стануваат сè поважни за идентификација на лицата во технолошката ера.

Меѓутоа, предуслов за применливоста на европското законодавство за заштита на податоците не е прецизната идентификација на субјектот на податоците. Доволно е засегнатото лице да може да се идентификува. Се смета дека едно лице може да се идентификува ако информациите за него содржат елементи на идентификација преку кои лицето може да се идентификува, директно или индиректно[58]. Според Уводната изјава бр. 26 на Директивата за заштита на податоците, од пресудно значење е дали им се достапни разумни средства за идентификација на веројатните корисници на информациите и дали тие ќе ги употребат. Тоа вклучува и трети лица како корисници (види го поглавјето 2.3.2.).

Пример: Локална власт одлучува да собира податоци за автомобили кои пребрзо возат по локалните улици. Ги фотографира автомобилите, автоматски снимајќи ги времето и локацијата, со цел да ги предаде податоците на надлежниот орган за тој да може да ги казни оние штоги прекршиле

57 СПЕУ, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 јануари 2008 год., параграф 45.

58 Директива за заштита на податоците, член 2 точка (а).

ограничувањата на брзината. Субјект на податоците поднесува жалба, тврдејќи дека локалната власт нема законска основа, според законот за заштита на податоците, за такво собирање на податоци. Локалната власт смета дека не собира лични податоци, велејќи дека регистарските таблички се податоци за анонимни лица. Локалната власт нема законско овластување за пристап во општиот регистар на возила за да го дознае идентитетот на сопственикот на автомобилот или на возачот.

Овој аргумент не се совпаѓа со Уводната изјава бр. 26 на Директивата за заштита на податоците. Со оглед на тоа што очигледната цел на собирањето на податоците е да се идентификуваат и казнат прекршителите, извесно е дека ќе следи обид за идентификација. Иако локалните власти немаат директен пристап до средства за идентификација, тие ќе ги пренесат податоците до надлежниот орган, полицијата, кој располага со такви средства. Од Уводната изјава бр.26, исто така, јасно произлегува сценарио од кое може да се предвиди дека натамошните корисници на податоците, не само нивниот непосреден корисник, може да се обидат да го идентификуваат поединецот. Во смисла на Уводната изјава бр.26, постапката на локалната власт е еднаква на собирање податоци за лица кои може да се идентификуваат и, затоа, според законодавството за заштита на податоците за неа е неопходна законска основа.

Според правото на Советот на Европа, можноста за идентификување е дефинирана на сличен начин. Членот 1 став 2 од Препораката за податоците за плаќања[59], на пример, вели дека лицето нема да се смета за „лице што може да се идентификува" доколку за идентификувањето бидат потребни неразумно многу време, финансиски средства или работна сила.

Автентикација

Автентикацијата е постапка со која едно лице може да докаже дека тој или таа поседува одреден идентитет и/или е овластено за одредени работи како, на пример, да влезе во безбедносна област, или да подигне пари од банкарска сметка. Автентикацијата може да се постигне со помош на споредување на биометриските податоци, како што се слика или отпечатоци од прсти во пасош, со податоците од лицето кое се претставува, на пример, пред имиграциска контрола; или со барање

59 СЕ, Комитет на министри (1990), Препорака бр. R Rec(90) 19 за заштита на личните податоци кои се користат при плаќање и при други сродни постапки, 13 септември 1990 год.

информации кои треба да му се познати само на лице со определен идентитет или овластување, како што се личен идентификациски број (PIN) или лозинка; или со барање да се приложи определен токен, кој треба да биде исклучиво во сопственост на лицето со определен идентитет или овластување, како што е посебна чип-картичка или клуч од банкарски сеф. Освен лозинки или чип-картички, понекогаш заедно со личните идентификациски броеви, електронските потписи се средство што е особено погодно за идентификација и автентикација на лице при електронските комуникации.

Природа на податоците

Некоја информација може да биде личен податок, под услов да се однесува на лице.

Пример: Оцената на претпоставениот за работата на работникот, што се чува во личното досие на работникот, е личен податок за вработениот, и покрај тоа што може да одразува само, делумно или целосно, лично мислење на претпоставениот, како што е: „работникот не е посветен на својата работа", а не цврсти факти, како, на пример: „работникот бил отсутен од работа пет недели во текот на последните шест месеци".

Личните податоци опфаќаат информации кои се однесуваат на приватниот живот на некое лице, како и информации за неговиот или нејзиниот професионален или јавен живот.

Во предметот *Amann*[60], Европскиот суд за човековите права го толкувал поимот „лични податоци" без да го ограничи на прашања од приватната сфера на поединецот (види во поглавјето 2.1.1.). Ова значење на поимот „лични податоци" е, исто така, важно и за Директивата за заштита на податоците:

Пример: Во предметот *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*[61], Судот на правдата на Европската Унија изјавил дека „во таа смисла не е важно тоа што објавените податоци се однесувале на работи од професионална природа […]. Европскиот суд за човековите права,

60 Види ЕСЧП, *Amann v. Switzerland,* Бр. 27798/95, 16 февруари 2000 год, параграф 65.

61 Заеднички случаи C-92/09 и C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen,* 9 ноември 2010 год., параграф 59.

повикувајќи се на толкувањето на членот 8 на Конвенцијата, по ова прашање зазел став дека поимот 'приватен живот' не смее да се толкува рестриктивно и дека не постои начелна причина која би го оправдала исклучувањето на работи од професионална […] природа од поимот за приватен живот".

Податоците се однесуваат на лица и ако содржината на информациите индиректно открива податоци за некое лице. Во некои случаи, кога постои тесна врска помеѓу предмет или настан – на пример, мобилен телефон, автомобил, несреќа – од една страна, и лице – на пример, негов сопственик, корисник, жртва – од друга страна, информациите за предметот или за настанот треба, исто така, да се сметаат за лични податоци.

Пример: Во предметот *Uzun v. Germany*[62], жалителот и уште еден човек биле ставени под надзор со помош на ГСП-уред (глобален систем за позиционирање) вграден во автомобилот на другиот човек поради сомненија за нивно учество во бомбашки напади. Во овој случај, Европскиот суд за човековите права сметал дека надгледувањето на жалителот преку глобален систем за позиционирање претставувало мешање во неговиот приватен живот, кој е заштитен со членот 8 на Конвенцијата. Сепак, надзорот преку ГСП бил во согласност со законот и пропорционален со законитата цел на истрагата на неколку обиди за убиство и затоа бил неопходен во едно демократско општество. Судот заклучил дека немало повреда на членот 8 на Европската конвенција за човековите права.

Облик на прикажување на податоците

Обликот во кој се чуваат или се користат личните податоци не е релевантен за применливоста на законодавството за заштита на податоците. Писмената или усната комуникација можат да содржат лични податоци како и слики[63], вклучувајќи и снимки[64] или звук од затворено телевизиско коло (ЗТК)[65]. Електронски сни-

62 ЕСЧП, *Uzun v. Germany*, Бр. 35623/05, 2 септември 2010 год.

63 ЕСЧП, *Von Hannover v. Germany*, Бр. 59320/00, 24 јуни 2004 год.; ЕСЧП, *Sciacca v. Italy*, Бр. 50774/99, 11 јануари 2005 год.

64 ЕСЧП, *Peck v. the United Kingdom*, Бр. 44647/98, 28 јануари 2003 год.; ЕСЧП, *Köpke v. Germany*, Бр. 420/07, 5 октомври 2010 год.

65 Директива за заштита на податоците, Уводни изјави 16 и 17; ЕСЧП, *P.G. and J.H. v. the United Kingdom*, Бр. 44787/98, 25 септември 2001 год., параграфи 59 и 60; ЕСЧП, *Wisse v. France*, Бр. 71611/01, 20 декември 2005 год.

мените информации, како и информациите на хартија, можат да бидат лични податоци; дури и примероци на клетки од човечко ткиво можат да бидат лични податоци, бидејќи содржат ДНК на лицето.

2.1.2. Посебни категории на лични податоци

Според правото на Европската Унија како и **правото на Советот на Европа,** постојат посебни категории на лични податоци кои, поради својата природа, во текот на обработката можат да претставуваат ризик за субјектите на податоците и поради тоа имаат потреба од дополнителна заштита. Затоа, обработката на овие посебни категории на лични податоци („чувствителни податоци“) треба да се дозволи само со примена на посебни заштитни мерки.

При дефинирањето на чувствителните податоци и Конвенцијата бр. 108 (член 6) и Директивата за заштита на податоците (член 8) ги наведуваат следниве категории:

- лични податоци кои откриваат расно или етничко потекло;
- лични податоци кои откриваат политички ставови, верски или други убедувања; и
- лични податоци во врска со здравјето или сексуалниот живот

Пример: Во предметот *Bodil Lindqvist*[66], Судот на правдата на Европската Унија изјавил дека „повикувањето на фактот дека лицето си го повредило стапалото и има скратено работно време поради медицински причини претставува личен податок во врска со здравјето во смисла на членот 8 став 1 на Директивата 95/46“.

Директивата за заштита на податоците дополнително го наведува „членството во синдикати“ како чувствителен податок, бидејќи оваа информација може да биде силен показател за политичко убедување или припадност.

Конвенцијата бр. 108 исто така за чувствителни ги смета и личните податоци што се однесуваат на кривични осуди.

66 СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 год., параграф 51.

Членот 8 став 7 на Директивата за заштита на податоците ги овластува државите-членки на Европската Унија „да ги утврдат условите под кои може да се обработи еден национален идентификациски број или некој друг идентификатор за општа употреба".

2.1.3. Анонимизирани и псевдонимизирани податоци

Во согласност со начелото за ограничено задржување на податоците, кое е содржано во Директивата за заштита на податоците, како и во Конвенцијата бр. 108 (за кое подетално се расправа поглавјето 3), податоците мора да се чуваат „во облик што дозволува субјектите на податоците да можат да се идентификуваат не подолго отколку што е потребно за намените за кои податоците биле собрани или за кои се дополнително обработени"[67]. Според тоа, податоците ќе треба да бидат анонимизирани ако контролорот сака да ги чува откако ќе застарат и веќе нема да служат за нивната првична намена.

Анонимизирани податоци

Податоците се анонимизирани ако сите елементи на идентификација биле елиминирани од збирката на лични податоци. Не смее да се остави ниту еден елемент во информациите кој би можел, со примена на разумен напор, да послужи за повторно идентификување на засегнатото лице или лица[68]. Кога податоците се успешно анонимизирани, тие веќе не се сметаат за лични податоци.

Ако личните податоци веќе не служат за нивната првична намена, но треба да се чуваат во персонализиран облик за историски, статистички и научни цели, Директивата за заштита на податоците и Конвенцијата бр. 108 ја дозволуваат оваа можност, под услов да се применат соодветни заштитни мерки против нивна злоупотреба[69].

Псевдонимизирани податоци

Личните информации содржат идентификатори како што се име, датум на раѓање, пол и адреса. Кога личните информации се псевдонимизирани, идентификаторите

67 Директива за заштита на податоците, член 6 став 1 точка (д); и Конвенција бр. 108, член 5 точка (д).

68 *На истото место*, Уводна изјава бр. 26.

69 *На истото место*, член 6 став 1 точка (д); и Конвенција бр. 108, член 5 точка (д).

се заменуваат со псевдоним. Псевдонимизацијата се постигнува, на пример, со помош на кодирање на идентификаторите во личните податоци.

Псевдонимизираните податоци не се изречно споменати во правните дефиниции ниту на Конвенцијата бр. 108 ниту на Директивата за заштита на податоците. Сепак, Појаснувачкиот извештај кон Конвенцијата бр. 108 во членот 42 наведува дека „[ ] барањето [...] во врска со временските рокови за чување на податоците во облик кој е поврзан со името не значи дека податоците по извесно време треба да бидат неповратно одвоени од името на лицето на кое се однесуваат, туку само дека не би требало да биде можно веднаш да се поврзат податоците и идентификаторите". Тоа може да се постигне со псевдонимизирање на податоците. На секој што не го поседува клучот за декриптирање ќе му биде тешко да ги идентификува псевдонимизираните податоци. Врската со идентитетот сè уште постои во облик на псевдонимот со клуч за декриптирање. Оние што имаат право да го користат таквиот клуч можат, на едноставен начин, повторно да го идентификуваат лицето. Особено е важно да се спречи користење на клучеви за декриптирање од страна на неовластени лица.

Бидејќи псевдонимизирањето на податоците е едно од најважните средства за постигнување на опсежна заштита на податоците, ако не е можно целосно да се воздржи од користење на лични податоци, логиката и ефектот на таквата постапка мора да бидат подетално објаснети.

Пример: Реченицата „Чарлс Спенсер, роден на 3 април 1967 година, е татко на четири деца, две момчиња и две девојчиња" може, на пример, да биде псевдонимизирана на следниов начин:

„Ч.С. 1967 е татко на четири деца, две момчиња и две девојчиња"; или

„324 е татко на четири деца, две момчиња и две девојчиња"; или

„YESz320l е татко на четири деца, две момчиња и две девојчиња".

Корисниците кои пристапуваат до овие псевдонимизирани податоци обично не ќе можат да го идентификуваат „Чарлс Спенсер, роден на 3 април 1967 г." од „324" или „YESz3201". Затоа е поверојатно дека псевдонимизираните податоци се заштитени од злоупотреба.

Сепак, првиот пример е помалку безбеден. Ако реченицата „Ч.С. 1967 е татко на четири деца, две момчиња и две девојчиња“ се користи во малото село каде што живее Чарлс Спенсер, г. Спенсер може лесно да биде препознаен. Методот на псевдонимизација влијае на ефикасноста на заштитата на личните податоци.

Личните податоци со кодирани идентификатори се користат во многу случаи како начин да се задржи во тајност идентитетот на лицата. Тоа е особено корисно кога контролорите на податоците треба да се осигурат дека се занимаваат со истите субјекти на податоците, но не им се потребни или не смеат да ги имаат вистинските идентитети на тие лица. Таков случај е, на пример, кога еден истражувач го проучува текот на болеста кај пациенти чиј идентитет е познат само на болницата каде што тие се лекуваат и од која истражувачот добива псевдонимизирани историјати на болести. Затоа псевдонимизацијата е силно оружје во арсеналот на технологијата за зајакнување на приватноста. Таа може да биде важен елемент при спроведувањето на заштитата на приватноста со помош на техниката. Тоа значи дека заштитата на податоците треба да биде вградена во структурата на напредните системи за обработка на податоци.

2.2. Обработка на податоци

Клучни точки

- Поимот „обработка“ се однесува пред сè на автоматската обработка.
- Според правото на Европската Унија, поимот „обработка“ се однесува и на рачната обработка во структурирани системи за архивирање.
- Според правото на Советот на Европа, значењето на поимот „обработка“ може да биде проширено во рамките на националното законодавство за да опфаќа и рачна обработка.

Заштитата на податоците според Конвенцијата бр. 108 и Директивата за заштита на податоците првенствено се фокусира на автоматската обработка на податоци.

Меѓутоа, **според правото на Советот на Европа**, дефиницијата за автоматска обработка на податоците допушта дека меѓу автоматските постапки може да се јави потреба од одредени фази на рачна употреба на личните податоци. Слично на

тоа, **според правото на Европската Унија**, автоматската обработка на податоци се дефинира како „операција што се врши врз личните податоци, целосно или делумно автоматски“[70].

Пример: Во предметот *Bodil Lindqvist*[71], Судот на правдата на Европската Унија сметал дека:

„чинот на упатување на интернет-страница на различни лица и нивно идентификување по име или на друг начин, на пример, со наведување на нивните телефонски броеви или информации во врска со условите за работа или хоби, претставува 'целосно или делумно автоматска обработка на личните податоци' во рамките на значењето на членот 3 став 1 на Директивата 95/46“.

Рачната обработка на податоците исто така бара заштита на податоците.

Заштитата на податоците **според правото на Европската Унија** во никој случај не е ограничена на автоматската обработка на податоци. Според тоа, во согласност со правото на Европската Унија, заштитата на податоците се однесува на обработката на личните податоци во рачен систем за архивирање, односно во посебно структурирана хартиена датотека[72]. Причината за ваквото проширување на опфатот на заштитата на податоците е тоа што:

- хартиените датотеки можат да бидат структурирани на начин кој овозможува брзо и лесно пронаоѓање информации; и

- чувањето на личните податоци во структурирани хартиени датотеки ја олеснува можноста да се заобиколат законските ограничувања кои важат за автоматската обработка на податоците[73].

Според правото на Советот на Европа, Конвенцијата бр. 108 првенствено ја регулира обработката на податоците во автоматизирани бази на податоци[74]. Но, таа, исто така, овозможува и проширување на заштитата за да опфаќа

70 Конвенција бр. 108, член 2 точка (в); и Директива за заштита на податоците, член 2 точка (б) и член 3 став 1.

71 СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003, параграф 27.

72 Директива за заштита на податоците, член 3 став 1.

73 *На истото место*, Уводна изјава бр. 27.

74 Конвенција бр. 108, член 2 точка (б).

рачна обработка во рамките на домашното право. Многу договорни страни на Конвенцијата бр. 108 ја искористиле оваа можност и за таа цел упатиле изјави до генералниот секретар на Советот на Европа[75]. Проширувањето на заштитата на податоците според една таква изјава мора да се однесува на секоја рачна обработка на податоци и не може да се ограничи на обработката во рачни системи за архивирање[76].

Што се однесува до природата на вклучените операции на обработка, **и во правото на Европската Унија и во правото на Советот на Европа**, сеопфатно е содржан поимот за обработка: „обработка на 'лични податоци' [...] е секоја операција [...], како што се: собирање, евидентирање, организирање, складирање, адаптирање или менување, вадење, консултирање, користење, откривање со пренесување, ширење или на некој друг начин ставање на податоците на располагање, нивно подредување или комбинирање, блокирање, бришење или уништување"[77] извршена врз личните податоци. Поимот „обработка" исто така вклучува и постапки во кои одговорноста за податоците преминува од еден на друг контролор.

Пример: Работодавците ги собираат и ги обработуваат податоците за вработените, вклучувајќи ги и информациите за нивните плати. Правната основа за законитост на таквиот чин е договорот за работа.

Работодавците ќе мора да ги проследат податоците за платата на нивниот персонал до даночните власти. Ова проследување на податоците исто така ќе претставува „обработка" во смисла на значењето на овој поим во Конвенцијата бр. 108 и во Директивата. Сепак, правната основа за таквото откривање не е договорот за работа. Мора да постои дополнителна правна основа за операциите на обработка кои резултираат со пренос на податоците за платата од работодавецот до даночните власти. Таквата правна основа обично е содржана во одредбите на националните даночни закони. Без таквите одредби преносот на податоци би претставувал незаконска обработка.

75 Види ги изјавите упатени според Конвенцијата бр. 108, член 3 став 2 точка (в).

76 Види ги изјавите упатени според Конвенцијата бр .108, член 3 став 2.

77 Директива за заштита на податоците, член 2 точка (б). Слично, види и Конвенција бр. 108, член 2 точка (в).

2.3. Корисниците на лични податоци

Клучни точки

- Оној што ќе одлучи да обработува лични податоци на други лица, во согласност со законодавството за заштита на податоците, се нарекува „контролор"; ако повеќе лица заеднички ја донесат таа одлука, може да се наречат „здружени контролори".
- „Обработувач" е посебен правен субјект кој обработува лични податоци во име на контролорот.
- Обработувачот станува контролор доколку ги користи податоците за сопствени цели, не следејќи инструкции од контролор.
- Оној што прима податоци од контролор се нарекува „корисник".
- „Трета страна" е физичко или правно лице кое не постапува според инструкциите на контролорот (и не е субјект на податоците).
- „Корисник на трета страна" е лице или субјект кој е правно одвоен од контролорот, но добива лични податоци од контролорот.

2.3.1. Контролори и обработувачи

Најважната последица од вршењето на функцијата контролор или обработувач е правната одговорност за исполнување на соодветните обврски што произлегуваат од законодавството за заштита на податоците. Затоа, само оние што можат да се сметаат за одговорни според применливото право можат да ја вршат таа функција. Во приватниот сектор, тоа обично е физичко или правно лице, а во јавниот сектор, надлежен орган. Други субјекти, како што се органи или институции без правен субјективитет, можат да бидат контролори или обработувачи само кога тоа е пропишано со посебни законски одредби.

Пример: Кога одделението за маркетинг на компанијата *„Sunshine"* планира да обработи податоци заради истражување на пазарот, компанијата *„Sunshine"*, а не одделението за маркетинг, ќе биде контролорот на таквата обработка. Одделението за маркетинг не може да биде контролор, бидејќи нема посебен правен идентитет.

Кога се работи за групации, матичната компанија и секоја подружница, како посебни правни лица, се сметаат за посебни контролори или обработувачи. Како последица на ваквиот посебен правен статус, преносот на податоци помеѓу членовите на една групација ќе бара посебна правна основа. Не постои привилегија која би овозможила размена на личните податоци како такви меѓу одделните правни субјекти во рамките на групацијата.

Во таа смисла треба да се спомене и улогата на приватните лица. **Според правото на Европската Унија**, кога приватни лица вршат обработка на податоци за други, во рамките на активности кои се исклучиво од лична или домашна природа, за нив не важат одредбите на Директивата за заштита на податоците. Тие не се сметаат за контролори[78].

Сепак, судската практика налага примена на законодавството за заштита на податоците кога приватното лице, користејќи интернет, објавува податоци за други лица.

Пример: Во случајот *Bodil Lindqvist*[79] Судот на правдата на Европската Унија сметал дека:

„чинот на упатување, на интернет-страница, на различни лица и нивно идентификување по име или на друг начин […] претставува 'целосно или делумно автоматска обработка на личните податоци' во рамките на значењето на членот 3 став 1 на Директивата 95/46"[80].

Таквата обработка на личните податоци не спаѓа во исклучиво лични или домашни активности, кои се надвор од опфатот на Директивата за заштита на податоците, бидејќи таквиот исклучок „мора […] да се толкува како да се однесува само на активности кои се спроведуваат во рамките на приватниот или семејниот живот на поединците, што очигледно не е случај при обработката на лични податоци која вклучува објава на интернет, со што тие податоци им се достапни на неограничен број на луѓе"[81].

78 Директива за заштита на податоците, Уводна изјава бр. 12 и член 3 став 2 последна алинеја.

79 СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 год.

80 *На истото место*, параграф 27.

81 *На истото место*, параграф 47.

Контролор

Според правото на Европската Унија, контролорот се дефинира како некој што „самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци“[82]. Одлуката на контролорот утврдува зошто и како податоците ќе бидат обработени. **Според правото на Советот на Европа**, дефиницијата за „контролор“ дополнително наведува дека контролорот одлучува кои категории на лични податоци треба да се чуваат[83].

Во дефиницијата за контролор во Конвенцијата бр. 108 се споменува уште еден аспект на контролата кој бара разгледување. Оваа дефиниција се однесува на прашањето кој може законито да обработува определени податоци за одредена цел. Меѓутоа, кога се одвиваат наводно незаконити операции на обработка и треба да се пронајде одговорниот контролор, се смета дека контролор е физичко или правно лице, како што е компанија или надлежен орган, кое одлучило дека податоците треба да се обработат, без оглед на тоа дали било правно овластено да одлучи такво нешто или не[84]. Затоа, барањето за бришење секогаш мора да се поднесе до „фактичкиот“ контролор.

Заедничка контрола

Дефиницијата за „контролор“ во Директивата за заштита на податоците наведува дека можат да постојат и неколку засебни правни субјекти кои заедно или со други вршат функција на контролор. Тоа значи дека заедно одлучуваат да обработуваат податоци со заедничка цел[85]. Меѓутоа, тоа е правно можно само во случаи кога постои посебна правна основа која дозволува заедничка обработка на податоци со заедничка цел.

Пример: Општ пример за заедничка контрола е базата на податоци за клиентите што заеднички ја водат неколку кредитни институции. Кога некој аплицира за кредит во банка која е една од заедничките контролори, банките ја проверуваат базата на податоци поради полесно донесување одлука врз основа на применливи информации за кредитната способност на барателот.

82 Директива за заштита на податоците, член 2 точка (г).

83 Конвенција бр. 108, член 2 точка (г).

84 Види и Работна група за членот 29 (2010), *Мислење 1/2010 за поимите „контролор“ и „обработувач“*, РГ 169, Брисел, 16 февруари 2010 год., стр. 15.

85 Директива за заштита на податоците, член 2 точка (г).

Прописите не наведуваат изречно дали заедничката контрола налага заедничката цел да биде иста за секој од контролорите или е доволно нивните цели само делумно да се поклопуваат. Сепак, на европско ниво сè уште нема релевантна судска практика, а исто така не се јасни последиците во врска со одговорноста. Работната група за членот 29 се залага за поширок толкување на поимот за заедничка контрола, со цел да се допушти некаква флексибилност за да се одговори на сè поголемата сложеност на моменталната ситуација во врска со обработката на податоците[86]. Еден предмет во кој било вклучено Друштвото за светски интербанкарски финансиски телекомуникации (SWIFT) го покажува ставот на Работната група.

Пример: Во таканаречениот предмет за SWIFT, Европските банкарски институции го ангажирале Друштвото за светски интербанкарски финансиски телекомуникации, првично како обработувач, за пренос на податоци во текот на банкарските трансакции. Такви податоци за банкарски трансакции, кои се чувале во еден компјутерски услужен центар во Соединетите Американски Држави (САД), Друштвото му открило на американското Министерство за финансии, без тоа да му биде изречно наредено од европските банкарски институции кои го ангажирале. Работната група за членот 29, при проценатa на законитоста на оваа ситуација, дошла до заклучок дека европските банкарски институции кои го ангажирале SWIFT, како и самото Друштво, морало да се сметаат за заеднички контролори кои биле одговорни пред европските клиенти за откривање на нивните податоци пред американските државни органи[87]. Друштвото за светски интербанкарски финансиски телекомуникации, со донесување на одлуката за откривање, ја презело - незаконски – улогата на контролор; банкарските институции очигледно не ја исполниле својата обврска за надзор на нивниот обработувач и затоа не може да бидат целосно ослободени од нивната одговорност како контролори. Ваквата состојба резултира со заедничка контрола.

86 Работна група за членот 29 (2010), *Мислење 1/2010 за поимите „контолор“ и „обработувач“* , РГ 169, Брисел, 16 февруари 2010 год., стр. 19.

87 Работна група за членот 29 (2006), *Мислење 10/2006 за обработката на лични податоци од страна на Друштвото за светски интербанкарски финансиски телекомуникации (SWIFT),* РГ 128, Брисел, 22 ноември 2006 год.

Обработувач

Според правото на Европската Унија, обработувачот се дефинира како лице кое обработува лични податоци во име на контролорот[88]. Активностите што му се доверени на обработувачот можат да бидат ограничени на многу конкретна задача или контекст, или можат да бидат прилично општи и сеопфатни.

Според правото на Советот на Европа, значењето на поимот обработувач е исто како и според правото на Европската Унија.

Покрај тоа што обработуваат податоци за други, обработувачите исто така се и контролори на податоците во однос на обработката на податоците што ја вршат за сопствени цели како, на пример, управување со своите вработени, продажба и сметки.

Примери: Компанијата *„Everready"* е специјализирана за обработка на податоци за управување со податоци за човечки ресурси за други компании. Во оваа функција, *„Everready"* е обработувач.

Меѓутоа, кога *„Everready"* ги обработува податоците за своите вработени, таа е контролор на операциите на обработка на податоците, бидејќи со тоа ги исполнува своите обврски како работодавец.

Односот меѓу контролорот и обработувачот

Како што видовме, контролорот е дефиниран како оној што ги утврдува целите и начините на обработка.

Пример: Директорот на компанијата *„Sunshine"* одлучува дека компанијата *„Moonlight"*, која е специјализирана за анализа на пазарот, треба да спроведе анализа на пазарот со податоците за клиентите на *„Sunshine"*. Според тоа, иако задачата за утврдување на начинот на обработка ѝ е доверена на *„Moonlight"*, компанијата *„Sunshine"* е контролор, а *„Moonlight"* е само обработувач бидејќи, според договорот, *„Moonlight"* може да ги користи податоците за клиентите од компанијата *„Sunshine"* само за целите што ќе ги утврди *„Sunshine"*.

88 Директива за заштита на податоците, член 2 точка (д).

Доколку овластувањето за утврдување на начините на обработка е доверено на обработувач, контролорот мора сепак да биде во можност да влијае на одлуките на обработувачот во однос на начинот на обработка. Целосната одговорност сè уште му припаѓа на контролорот, кој мора да врши надзор на обработувачите со цел да осигури дека нивните одлуки се во согласност со законодавството за заштита на податоците. Затоа, договорот со кој му се забранува на контролорот да се меша во одлуките на обработувачот веројатно би се толкувал на начин што ќе доведе до заедничка контрола, каде двете страни ја делат законската одговорност на контролорот.

Понатаму, во случај кога обработувачот не ги почитува ограничувањата за употреба на податоците на начин што е пропишан од страна на контролорот, обработувачот ќе стане контролор барем до степенот на непочитување на упатствата на контролорот. Тоа, најверојатно, обработувачот ќе го претвори во контролор кој постапува незаконито, а првобитниот контролор ќе треба да објасни како било можно обработувачот да ги прекрши неговите наредби. Навистина, Работната група за членот 29 често претпоставува заедничка контрола во такви случаи, бидејќи тоа доведува до најдобра заштита на интересите на субјектите на податоците[89]. Значајна последица од заедничката контрола би требало да биде заедничката и солидарна одговорност за штетите, со што на субјектите на податоците ќе им се овозможат поголем број на правни средства.

Прашањето околу поделбата на одговорноста може да се појават и кога контролорот е мало претпријатие, а обработувачот е голема корпорација која може да ги диктира условите на своите услуги. Сепак, во такви околности, Работната група за членот 29 смета дека стандардот за одговорност не смее да се спушти поради економската нееднаквост и дека мора да се задржи смислата на поимот контролор[90].

Поради јасност и транспарентност, деталите околу односот меѓу контролорот и обработувачот треба да се утврдат со писмен договор[91]. Непостоењето на та-

89 Работна група за членот 29 (2010), *Мислење 1/2010 за поимите „контролор" и „обработувач"*, РГ 169, Брисел, 16 февруари 2010 год., стр. 25; и Работна група за членот 29 (2006), *Мислење 10/2006 за обработката на лични податоци од страна на Друштвото за светски интербанкарски финансиски телекомуникации (SWIFT)*, РГ 128, Брисел, 22 ноември 2006 год.

90 Работна група за членот 29 (2010), *Мислење 1/2010 за поимите „контролор" и „обработувач"*, РГ 169, Брисел, 16 февруари 2010 год., стр. 26.

91 Директива за заштита на податоците, член 17 точки (3) и (4).

ков договор е повреда на обврската на контролорот да обезбеди писмена документација за заедничките одговорности, што може да доведе до казнување[92].

Обработувачите можат да им препуштат определени задачи на дополнителни под-обработувачи. Тоа е законски дозволено и конкретно зависи од договорните одредби меѓу контролорот и обработувачот, вклучувајќи го и тоа дали овластувањето на контролорот е неопходно во секој поединечен случај или е доволно само информирање.

Според правото на Советот на Европа, во целост е применливо толкувањето на поимите контролор и обработувач, како што се објаснети погоре, на што укажуваат препораките донесени во согласност со Конвенцијата бр. 108[93].

2.3.2. Корисници и трети страни

Разликата помеѓу овие две категории лица или субјекти, која беше внесена со Директивата за заштита на податоците, е начелна во нивниот однос со контролорот и, следствено, во нивното овластување за пристап до личните податоци кои се чуваат од страна на контролорот.

„Третата страна" правно се разликува од контролорот. Затоа, за откривање на податоци на трета страна, секогаш ќе биде потребна посебна правна основа. Според членот 2 точка (ѓ) на Директивата за заштита на податоците, трета страна е „секое физичко или правно лице, јавен орган, агенција или секое друго тело освен субјектот на податоците, контролорот, обработувачот и лицата кои, под директно овластување на контролорот или обработувачот, се овластени да ги обработуваат податоците". Тоа значи дека лицата што работат за организација која е правно различна од контролорот – дури и ако ѝ припаѓа на истата групација или холдинг – ќе бидат (или ќе припаѓаат на) „трета страна". Од друга страна, филијалите на една банка која обработува сметки на клиентите под директна надлежност на нивното седиште не се сметаат за „трети страни"[94].

„Корисник" е поширок поим од „трета страна". Во смисла на членот 2 точка (е) на Директивата за заштита на податоците, корисник значи „физичко или правно лице,

92 Работна група за членот 29 (2010), *Мислење 1/2010 за поимите „контролор" и „обработувач"*, РГ 169, Брисел, 16 февруари 2010 год., стр. 27.

93 Види, на пример, Препорака за профилирањето, член 1.

94 Работна група за членот 29 (2010), *Мислење 1/2010 за поимот „контролор" и „обработувач"*, РГ 169, Брисел, 16 февруари 2010 год., стр. 31.

јавен орган, агенција или секое друго тело на кое му се откриваат податоците, без оглед дали е трета страна или не". Корисник може да биде лице надвор од функцијата на контролорот или обработувачот – тогаш тој ќе биде трета страна – или некој во рамките на функцијата на контролорот или обработувачот, како, на пример, вработен или друг оддел во рамките на истата компанија или тело.

Разликата помеѓу корисниците и третите страни е важна само поради условите за законито откривање на податоците. Вработените на контролорот или обработувачот можат без дополнително правно барање да бидат корисници на личните податоци ако се вклучени во операциите на обработка на контролорот или обработувачот. Од друга страна, третата страна, која е правно одвоена од контролорот или обработувачот, не е овластена да користи лични податоци што ги обработил контролорот, освен ако во конкретниот случај постојат конкретни правни основи. Затоа, на „третите страни како корисници" на податоци, секогаш ќе им треба правна основа за законито примање на личните податоци.

Пример: Еден вработен на обработувачот, кој користи лични податоци во рамките на задачите што му ги доверил работодавецот, е корисник на податоците, но не и трета страна, бидејќи ги користи податоците во име и според упатствата на обработувачот.

Меѓутоа, ако истиот вработен одлучи да ги користи податоците до кои има пристап како вработен на обработувачот за неговите сопствени цели и ги продаде на друга компанија, тогаш вработениот постапил како трета страна. Тој повеќе не ги следи наредбите на обработувачот (работодавецот). Како трета страна, на вработениот ќе му биде потребна правна основа за стекнување со и продажба на податоците. Во конкретниов пример, вработениот очигледно нема таква правна основа, па овие постапки се сметаат за незаконити.

2.4. Согласност

Клучни точки

- Согласноста, како правна основа за обработка на личните податоци, мора да биде слободно дадена, заснована на информираност и конкретна.

- Согласноста мора да биде дадена недвосмислено. Согласноста може да се даде или експлицитно или имплицитно, и тоа на начин кој не доведува до сомнеж дека субјектот на податоците се согласува со обработката на неговите податоци.
- За обработка на чувствителни податоци врз основа на согласност, потребна е изречна согласност.
- Согласноста може да се повлече во секое време.

Согласност е „секое слободно дадено, конкретно и информирано навестување на желбите на субјектот на податоците"[95]. Тоа е, во голем број случаи, правната основа за законита обработка на податоците (види го поглавјето 4.1).

2.4.1. Елементите на валидната согласност***

Правото на Европската Унија предвидува три елементи за да биде валидна согласноста, чија цел е да се гарантира дека субјектите на податоците навистина се согласиле на употреба на нивните податоци:

- Субјектот на податоците не смее да биде под притисок при давање на согласноста;
- Субјектот на податоците мора да биде соодветно информиран за целта и за последиците од давањето согласност; и
- Опфатот на согласноста мора да биде доволно конкретен.

Само ако се исполнети сите овие услови согласноста ќе биде валидна во смисла на законодавството за заштита на податоците.

Конвенцијата бр. 108 не содржи дефиниција за согласност; тоа му е препуштено на домашното право. Сепак, **според правото на Советот на Европа**, елементите на валидната согласност одговараат на оние што ги споменавме претходно, како што е предвидено со препораките кои се подготвени во согласност со Конвенцијата

95 Директива за заштита на податоците, член 2 точка (ж).

*** Се мисли на правно релевантна согласност *(заб. на ред.)*

бр. 108[96]. Барањата за согласност се исти како и оние за валидна изјава за намерата според европското граѓанското право.

Дополнителни барања според граѓанското право за валидна согласност, како што е деловната способност, обично се применуваат и во контекст на заштита на податоците, бидејќи таквите барања се основни законски предуслови. Невалидната согласност на лицата што немаат деловна способност ќе резултира со отсуство на правна основа за обработка на податоците во врска со тие лица.

Согласноста може да се даде експлицитно[97] или имплицитно. Експлицитната согласност не доведува до сомнеж за намерите на субјектот на податоците и таа може да се даде усно или писмено; а втората се утврдува врз основа на околностите. Секоја согласност мора да биде дадена недвосмислено[98]. Ова значи дека не треба да постои основано сомневање дека субјектот на податоците сакал да ја изрази својата согласност за да дозволи обработка на неговите податоци. Така, на пример, само од нечија неактивност не може да се заклучи дека лицето дало недвосмислена согласност. Ако податоците што треба да бидат обработени се чувствителни, експлицитната согласност е задолжителна и мора да биде недвосмислена.

Доброволна согласност

Постоењето на доброволна согласност важи само „ако субјектот на податоците има вистински избор и не постои ризик од измама, заплашување, принуда или значителни негативни последици ако тој/таа не се согласи“[99].

На пример: На многу аеродроми патниците треба да поминат низ скенери за тело за да можат да пристапат до областа за качување во авионот[100]. Со оглед на тоа што податоците за патниците се обработуваат во текот на скенирањето, обработката мора да е во согласност со една од правните основи според членот 7 на Директивата за заштита на податоците (види го поглавјето 4.1.1.). Минувањето низ скенери за тело понекогаш на патниците

96 Види, на пример, Конвенција бр. 108, Препорака за статистичките податоци, точка 6.

97 Директива за заштита на податоците, член 8 став 2.

98 *На истото место*, член 7 точка (а) и член 26 став 1.

99 Види, исто така, Работна група за членот 29 (2011), *Мислење 15/2011 за поимот согласност*, РГ 187, Брисел, 13 јули 2011 год., стр. 12.

100 Овој пример е земен од *На истото место*, стр. 15.

им се претставува како избор, што подразбира дека нивната согласност може да ја оправда обработката. Меѓутоа, патниците можат да се плашат дека нивното одбивање да поминат низ скенери за тело ќе создаде сомнеж или ќе предизвика дополнителни контроли, како што е претрес на телото. Многу патници се согласуваат на скенирањето, бидејќи со тоа избегнуваат можни проблеми или одложувања. Таквата согласност не се смета за доброволна во доволна мера.

Затоа, солидна законска основа може да постои само во законодавниот акт, врз основа на членот 7 точка (д) на Директивата за заштита на податоците, што резултира со обврска за патниците да соработуваат поради превладувачки јавен интерес. Но, таквото законодавство сепак може да обезбеди избор помеѓу скенирање и претрес, но само како дел од дополнителните мерки на граничната контрола, кои се нужни во определени околности. Ова е тоа што Европската комисија го утврди во двете регулативи од 2011 година кои се однесуваат на безбедносните скенери[101].

Доброволната согласност може, исто така, да биде загрозена во случаи на подреденост, кога постои значителна економска или друга нееднаквост помеѓу контролорот, кој бара согласност и субјектот на податоците, кој дава согласност[102].

Пример: Голема компанија планира да направи регистар со имиња на сите вработени, нивната функција во компанијата и нивните деловни адреси, само за да се подобри внатрешната комуникација во компанијата. Раководителот на одделот за човечки ресурси предлага да се додаде слика во регистарот од секој вработен за да можат, на пример, полесно да се препознаат колегите на состаноци. Претставниците на вработените бараат тоа да се направи само со посебна согласност на секој вработен.

101 Регулатива на Комисијата (ЕУ) бр. 1141/2011 од 10 ноември 2011 год. за измена на Регулативата (ЕЗ) бр. 272/2009 за дополнување на заедничките основни стандарди за безбедноста во цивилното воздухопловство во врска со употребата на безбедносни скенери на аеродромите на ЕУ, Сл. весник 2011 Л 293 и Регулатива за спроведување на Комисијата (ЕУ) бр. 1147/2011 од 11 ноември 2011 год. за измена на Регулативата (ЕУ) бр. 185/2010 за спроведување на заедничките основни стандарди за безбедноста во цивилното воздухопловство во врска со употребата на безбедносни скенери на аеродромите на ЕУ, Сл. весник 2011 L 294.

102 Види, исто така, Работна група за членот 29 (2001), *Мислење 8/2001за обработката на личните податоци во контекст на вработувањето*, РГ 48, Брисел, 13 септември 2001 год.; и Работна група за членот 29 (2005), *Работен документ за заедничкото толкување на член 26 (1) на Директивата 95/46/ЕЗ од 24 октомври 1995 год.*, РГ 114, Брисел, 25 ноември 2005 год.

Во таква ситуација, согласноста на вработениот треба да се признае како правна основа за обработка на фотографиите во регистарот, бидејќи е јасно дека објавувањето на фотографиите во регистарот само по себе нема да има негативни последици и, згора на тоа, веројатно е дека вработениот нема да се соочи со негативни реакции од страна на работодавецот ако тој не се согласува неговата фотографија да биде објавена во регистарот.

Меѓутоа, тоа не значи дека согласноста никогаш не може да биде валидна во околности кога недавањето согласност би имало негативни последици. Ако, на пример, недавањето согласност за корисничка картичка во супермаркет резултира само со недобивање попусти на одредени производи, согласноста сè уште е валидна правна основа за обработка на личните податоци на оние купувачи што се согласиле да добијат таква картичка. Во тој случај нема подреденост меѓу компанијата и купувачот, а последиците од недавањето согласност не се доволно сериозни за да го попречат слободниот избор на субјектот на податоците.

Од друга страна, секогаш кога доволно важни производи или услуги можат да се добијат само и исклучиво ако определени лични податоци им се откријат на трети страни, согласноста на субјектот на податоците за објавување на неговите податоци обично не може да се смета за слободна одлука и затоа е невалидна во согласност со законодавството за заштита на податоците.

Пример: Ако патниците на една авиокомпанија изразат согласност таа да ја пренесе таканаречената евиденција на патнички имиња (ЕПИ), односно податоци за нивниот идентитет, навиките за исхрана или здравствените проблеми, на имиграциските власти на определена странска земја, таа не може да се смета за валидна согласност според законодавството за заштита на податоците бидејќи патниците немаат избор доколку сакаат да ја посетат таа земја. За да може таквите податоци да бидат законито пренесени, потребна е поинаква правна основа од согласноста: најверојатно посебен закон.

Согласност заснована на информираност

Субјектот на податоците мора да има доволно информации пред да донесе одлука. Дали дадените информации се доволни или не може да се утврди единствено од-случај-до-случај. Согласноста заснована на информираност обично содржи

прецизен и лесно разбирлив опис на предметот за кој е потребна согласност, како и наведување на последиците од согласувањето или несогласувањето. Јазикот што се користи за информирање треба да биде прилагоден за веројатните корисници на информациите.

Информациите, исто така, мора да му бидат лесно достапни на субјектот на податоците. Достапноста и видливоста на информациите се важни елементи. Во електронска средина, слоевитите информативни известувања можат да бидат добро решение бидејќи, освен до скратената верзија, субјектот на податоците може да пристапи и до проширената верзија на информациите.

Посебна согласност

За да биде валидна, согласноста мора да биде и посебна. Тоа оди рака под рака со квалитетот на информациите што се дадени во врска со предметот на согласноста. Во таа смисла, важни се разумните очекувања на субјектот на податоците. Од субјектот на податоците мора повторно да се побара согласност ако треба да се додадат или да се изменат операциите на обработка на начин кој од оправдани причини не можел да се предвиди кога согласноста првично била дадена.

Пример: Во предметот *„Deutsche Telekom AG“*[103], Судот на правдата на Европската Унија се занимавал со прашањето дали на давателот на телекомуникациски услуги, кој морал да пренесе лични податоци за претплатниците, според членот 12 на *Директивата за приватност и електронски комуникации*[104], му била потребна повторна согласност од субјектот на податоците, бидејќи корисниците не биле наведени во времето кога првично била дадена согласноста.

Судот сметал дека според тој член не била потребна нова согласност пред проследувањето на податоците затоа што субјектите на податоците, според таа одредба, имале можност да дадат согласност само за целта на обработката, односно за објавување на нивните податоци, и не можеле да одбираат помеѓу различни регистри во кои би можеле да бидат објавени податоците.

103 СПЕУ, C-543/09, *Deutsche Telekom AG v. Germany*, 5 мај 2011 год.; види, особено, параграфи 53 и 54.

104 Директива 2002/58/ЕЗ на Европскиот парламент и на Советот од 12 јули 2002 год. за обработка на лични податоци и за заштита на приватноста во секторот за електронски комуникации, Сл. весник 2002 L 201 (*Директива за приватност и електронски комуникации*).

Како што истакнал Судот, „од контекстуалното и систематско толкување на членот 12 на Директивата за приватност и електронски комуникации произлегува дека согласноста според членот 12 став 2 се однесува на целта на објавувањето на личните податоци во јавен регистар, но не и на идентитетот на конкретниот давател на услуги со регистри“[105]. Покрај тоа, „самото објавување на личните податоци во јавен регистар заради определена цел може да му причини штета на претплатникот“[106], а не конкретниот автор на таквата објава.

2.4.2. Правото на повлекување на согласноста во секое време

Во Директивата за заштита на податоците не се спомнува општо право на повлекување на согласноста во секое време. Сепак, општо се претпоставува дека такво право постои и дека субјектот на податоците мора да биде во можност да го остварува по своја волја. Не треба да се бара образложување на причините за повлекување на согласноста или на ризикот од негативни последици, освен укинување на сите придобивки што произлегувале од претходно договорената употреба на податоците.

Пример: Клиентот се согласува да добива промотивни пораки на адреса што му ја дал на контролорот на податоците. Доколку клиентот ја повлече согласноста, контролорот мора веднаш да престане со испраќање на промотивните пораки. Не смеат да се наметнат никакви казнени мерки како, на пример, плаќање надоместоци.

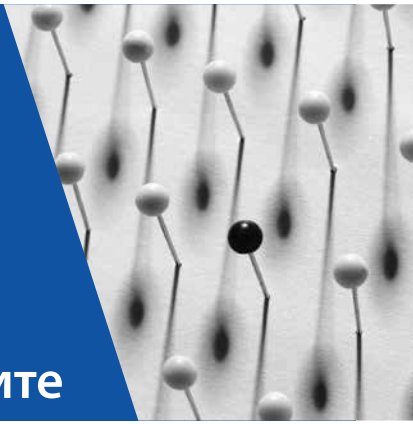
Ако клиентот добивал попуст од 5% на цената на хотелска соба во замена за согласноста за користење на неговите податоци за испраќање на промотивни пораки, подоцнежното повлекување на согласноста за примање на промотивни пораки не би смеело да резултира со обврска да го врати износот на таквиот попуст.

105 СПЕУ, C-543/09, *Deutsche Telekom AG v. Germany*, 5 мај 2011; види, особено, параграф 61.

106 *На истото место*, види, особено, параграф 62.

3

Главните начела на европското законодавство за заштита на податоците



Европска Унија	Обработени прашања	Совет на Европа
Директива за заштита на податоците , член 6 став 1 точки (а) и (б) СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 година СПЕУ, заеднички предмети C-92/09 и C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 ноември 2010 година	Начело за законита обработка	Конвенција бр. 108, член 5 точки (а) и (б) ЕСЧП, *Rotaru v. Romania* [GC], Бр. 28341/95, 4 мај 2000 год. ЕСЧП, *Taylor-Sabori v. the United Kingdom*, Бр. 47114/99, 22 октомври 2002 година ЕСЧП, *Peck v. the United Kingdom*, Бр. 44647/98, 28 јануари 2003 година ЕСЧП, *Khelili v. Switzerland*, Бр. 16188/07, 18 октомври 2011 година ЕСЧП, *Leander v. Sweden*, Бр. 9248/81, 26 март 1987 година
Директива за заштита на податоците, член 6 став 1 точка (б)	Начело за определување и ограничување на целта	Конвенција бр. 108, член 5 точка (б)
	Начела за квалитет на податоците:	

Директива за заштита на податоците, член 6 став 1 точка (в)	Релевантност на податоците	Конвенција бр. 108, член 5 точка (в)
Директива за заштита на податоците, член 6 став 1 точка (г)	Точност на податоците	Конвенција бр. 108, член 5 точка (г)
Директива за заштита на податоците, член 6 став 1 точка (д)	Ограничено задржување на податоци	Конвенција бр. 108, член 5 точка (д)
Директива за заштита на податоците, член 6 став 1 точка (д)	Исклучок за научно истражување и статистика	Конвенција бр. 108, член 9 став 3
Директива за заштита на податоците, член 6 став 1 точка (а)	Начело за правична обработка	Конвенција бр. 108, член 5 точка (а) ЕСЧП, *Haralambie v. Romania*, бр. 21737/03, 27 октомври 2009 година ЕСЧП, *K.H. and Others v. Slovakia*, бр. 32881/04, 28 април 2009 година
Директива за заштита на податоците, член 6 став 2	Начело за одговорност	

Начелата предвидени во членот 5 на Конвенцијата бр. 108 ја сочинуваат суштината на европското законодавство за заштита на податоците. Тие исто така се појавуваат и во членот 6 на Директивата за заштита на податоците како појдовна точка за подетални одредби во следните членови на директивата. Целокупното подоцнежно законодавство за заштита на податоците на ниво на Советот на Европа или на Европската Унија мора да биде во согласност со овие начела и тие мора да бидат земени предвид при толкувањето на таквото законодавство. Сите исклучоци и ограничувања во поглед на тие главни начела можат да бидат предвидени на национално ниво[107]; тие мора да бидат законски пропишани, да бидат насочени кон легитимна цел и да бидат нужни во едно демократско општество. Сите три услови мора да бидат исполнети.

107 Конвенција бр. 108, член 9 став 2; Директива за заштита на податоците, член 13 став 2.

3.1. Начелото за законита обработка

Клучни точки

- За да се разбере начелото за законита обработка, треба да се упати на условите за законско ограничување на правото на заштита на податоците во смисла на членот 52 ставот 1 на Повелбата и барањата за оправдано мешање во согласност со членот 8 ставот 2 на Европската конвенција за човековите права.
- Според тоа, обработката на лични податоци е законита само ако е:
  - во согласност со законот;
  - насочена кон легитимна цел;
  - нужна во едно демократско општество за да се постигне легитимната цел.

Според законодавството за заштита на податоците на Европската Унија и на Советот на Европа, начелото за законита обработка е првото наведено начело. Речиси на еднаков начин тоа е опишано во членот 5 на Конвенцијата бр.108 и во членот 6 на Директивата за заштита на податоците.

Ниедна од тие одредби не содржи дефиниција за тоа што претставува „законита обработка". За да се разбере овој правен поим, потребно е да се упати на поимот за оправдано мешање според Европската конвенција за човековите права онака како што тој се толкува во судската практика на Европскиот суд за човековите права и на условите за законско ограничување во согласност со членот 52 на Повелбата.

3.1.1. Барањата за оправдано мешање според Европската конвенција за човековите права

Обработката на личните податоци може да претставува мешање во правото на почитување на приватниот живот на субјектот на податоците. Меѓутоа, правото на почитување на приватниот живот не претставува апсолутно право, туку тоа мора да се урамнотежи и да се усогласи со други легитимни интереси, било да се на други лица (приватни интереси) или на општеството во целина (јавни интереси).

Мешањето од страна на државата е оправдано под следните услови:

Да биде во согласност со законот

Според судската практика на Европскиот суд за човековите права, мешањето е во согласност со законот ако се темели на одредба од националното законодавство, кое има одредени карактеристики. Законот мора да биде „достапен за засегнатите лица, а неговите ефекти мора да бидат предвидливи“[108]. Прописот е предвидлив „ако е формулиран со доволна прецизност за да му овозможи на секој поединец – ако е потребно со соодветен совет – да го регулира своето однесување“[109]. „Степенот на прецизност што се бара од 'законот' во тој поглед ќе зависи од конкретниот случај“[110].

Пример: Во предметот *Rotaru v. Romania*[111], Европскиот суд за човековите права утврдил повреда на членот 8 на Европската конвенција за човековите права затоа што според романското законодавство било допуштено прибирање, снимање и архивирање во тајни датотеки на информации кои влијаеле на националната безбедност без да бидат утврдени границите за користење на тие овластувања, кои останале дискрециско право на државните органи. На пример, со националното законодавство не биле дефинирани видот на информација што смеела да се обработува, категориите на луѓе над кои смееле да се вршат мерки на надзор, околностите во кои смеат да се преземаат такви мерки или постапката што требало да се користи. Поради овие недостатоци, Судот заклучил дека националното законодавство не го исполнило барањето за предвидливост според членот 8 на Европската конвенција за човековите права и дека тој член бил повреден.

108 ЕСЧП, *Amann v. Switzerland* [GC], Бр. 27798/95, 16 февруари 2000 год., параграф 50; исто така види ЕСЧП, *Kopp v. Switzerland,* Бр. 23224/94, 25 март 1998 год., параграф 55 и ЕСЧП, *Iordachi and Others v. Moldova,* Бр. 25198/02, 10 февруари 2009 год., параграф 50.

109 ЕСЧП, *Amann v. Switzerland* [GC], Бр. 27798/95, 16 февруари 2000 год., параграф 56; исто така види ЕСЧП, *Malone v. the United Kingdom,* Бр. 8691/79, 2 август 1984 год., параграф 66; ЕСЧП, *Silver and Others v. the United Kingdom,* бр. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 год., параграф 88.

110 ЕСЧП, *The Sunday Times v. the United Kingdom,* бр. 6538/74, 26 април 1979 год., параграф 49; исто така види ЕСЧП, *Silver and Others v. the United Kingdom,* бр. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 год., параграф 88.

111 ЕСЧП, *Rotaru v. Romania* [GC], Бр. 28341/95, 4 мај 2000 год., параграф 57; види и ЕСЧП, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Бр. 62540/00, 28 јуни 2007 год.; ЕСЧП, *Shimovolos v. Russia,* Бр. 30194/09, 21 јуни 2011 год.; и ЕСЧП, *Vetter v. France,* Бр. 59842/00, 31 мај 2005 год..

Пример: Во предметот *Taylor-Sabori v. the United Kingdom*[112], жалителот бил подложен на надзор од страна на полицијата. Користејќи „клон" на пејџерот на жалителот, полицијата била во можност да ги следи пораките што му биле испраќани. Потоа жалителот бил уапсен и обвинет за заговор за набавка на контролирана дрога. Еден дел од обвинението против него бил заснован на записите од пораките на пејџерот кои биле транскрибирани од страна на полицијата. Меѓутоа, во времето на судењето на жалителот, во британското законодавство не постоела одредба за регулирање на следењето на комуникациите пренесени преку приватен телекомуникациски систем. Затоа, мешањето во неговото право не било „во согласност со законот". Европскиот суд за човековите права заклучил дека имало повреда на членот 8 на Конвенцијата.

Да биде насочено кон легитимна цел

Легитимна цел може да биде или еден од споменатите јавни интереси или правата и слободите на други лица.

Пример: Во предметот *Peck v. the United Kingdom* [113], жалителот се обидел да изврши самоубиство на улица со сечење на вените, притоа незнаејќи дека ЗТК-камера го снимила за време на обидот. Откако бил спасен од страна на полицијата, која ги гледала снимките од ЗТК-камерите, полициското орган ја проследил ЗТК-снимката до медиумите, кои ја објавиле без да го прикријат лицето на жалителот. Европскиот суд за човековите права заклучил дека надлежните органи немале релевантни или доволно причини кои би го оправдале директното откривање на снимката пред јавноста без претходно добиена согласност на жалителот или со прикривање на неговиот идентитет. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Да биде нужно во едно демократско општество

Европскиот суд за човековите права истакнал дека „поимот за нужност подразбира дека мешањето е одговор на итна општествена потреба и особено дека тоа е пропорционално на легитимната цел што се следи"[114].

112 ЕСЧП, *Taylor-Sabori v. the United Kingdom*, Бр. 47114/99, 22 октомври 2002 год.

113 ЕСЧП, *Peck v. the United Kingdom*, Бр. 44647/98, 28 јануари 2003 год., особено параграф 85.

114 ЕСЧП, *Leander v. Sweden*, Бр. 9248/81, 26 март 1987 год., параграф 58.

Пример: Во предметот *Khelili v. Switzerland*[115], полицијата за време на една проверка утврдила дека жалителката со себе носела визит-картички на кои пишувало: „Симпатична, згодна жена во своите доцни триесетти би сакала да запознае маж за повремено дружење со пијачка или излегување. Телефонски број [...]". Жалителката се жалела дека полицијата, откако ги пронашла кај неа визит-картичките, во својата евиденција ја запишала како проститутка, иако таа упорно тврдела дека не се занимава со тоа. Жалителката побарала бришење на зборот „проститутка" од компјутерската евиденција на полицијата. Европскиот суд за човековите права во принцип потврдил дека задржувањето на личните податоци на поединецот, поради можноста тоа лице да стори друго кривично дело, во одредени околности би можело да биде пропорционално. Меѓутоа, во случајот на жалителката, тврдењето за незаконска проституција се чинело дека е премногу нејасно и општо, не било поткрепено со конкретни факти затоа што таа никогаш не била осудена за незаконска проституција и затоа не би можело да се смета дека одговара на „итна општествена потреба" во рамките на значењето на членот 8 на Конвенцијата. Сметајќи дека надлежните органи се одговорни за докажување на точноста на зачуваните податоци за жалителката и за сериозноста на мешањето во нејзините права, Судот пресудил дека долгогодишното задржување на зборот „проститутка" во полициската евиденција не било нужно во едно демократско општество. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Пример: Во предметот *Leander v. Sweden*[116], Европскиот суд за човековите права пресудил дека тајната проверка на лицата кои се пријавувале за вработување на работни места што биле важни за националната безбедност, сама по себе не била спротивна на барањето за нужност во едно демократско општество. Посебните заштитни мерки кои биле пропишани во националното законодавство за заштита на интересите на субјектот на податоците – како на пример, контролите кои ги вршат парламентот и државниот секретар довеле до заклучокот на Европскиот суд за човековите права дека шведскиот систем за лична контрола ги исполнувал условите од членот 8 став 2 на Конвенцијата. Имајќи ја предвид големата слобода на сопствена процена со која располагала, тужената држава со право сметала дека во случајот на жалителот интересите на националната безбедност надвладувале над индивидуалните интереси. Судот утврдил дека немало повреда на членот 8 на Конвенцијата.

115 ЕСЧП, *Khelili v. Switzerland,* Бр. 16188/07, 18 октомври 2011 год.

116 ЕСЧП, *Leander v. Sweden,* Бр. 9248/81, 26 март 1987 год., стр. 59 и 67.

3.1.2. Условите за законито ограничување според Повелбата на Европската Унија

Структурата и текстот на Повелбата се разликуваат од структурата и текстот на Европската конвенција за човековите права. Во Повелбата не се споменува мешање во загарантираните права, но во неа е содржана одредба за ограничување(-ња) на остварувањето на правата и слободите кои се признаени во Повелбата.

Според членот 52 став 1, ограничувањата на остварувањето на правата и слободите кои се признаени во Повелбата и, според тоа, на остварувањето на правото на заштита на лични податоци, како што е обработката на лични податоци, се допуштени само под следните услови:

- ако се пропишани со закон;
- ако ја почитуваат суштината на правото на заштита на податоците;
- ако се неопходни и подлежат на начелото на пропорционалност;
- ако ги исполнуваат целите од општ интерес кои се признаени од Унијата или потребата за заштита на правата и слободите на другите.

Примери: Во предметот *Volker and Markus Schecke*[117], Судот на правдата на Европската Унија заклучил дека со наметнувањето на обврската за објавување на личните податоци на секое физичко лице што било корисник на помош од [одредени земјоделски фондови] без да се прави разлика врз основа на релевантни критериуми, како што е временскиот период во кој лицата ја примале таквата помош, зачестеноста на помошта или нејзиниот вид и износ. Советот и Комисијата ги пречекориле ограничувањата кои биле пропишани со начелото на пропорционалност.

Од таа причина, Судот на правдата на Европската Унија заклучил дека е нужно одредени одредби на Регулативата на Советот (ЕЗ) Бр. 1290/2005 да

117 СПЕУ, заеднички предмети C-92/09 и C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 ноември 2010 год., параграфи 89 и 86.

се прогласат за неважечки, а Регулативата Бр. 259/2008 да се прогласи за неважечка во целост[118].

И покрај различниот текст, условите за законска обработка содржани во членот 52 став 1 на Повелбата потсетуваат на членот 8 став 2 на Конвенцијата. Всушност, условите кои се набројани во членот 52 став 1 на Повелбата мора да се сметаат како усогласени со оние од членот 8 став 2 на Конвенцијата, бидејќи во првата реченица на членот 52 став 3 на Повелбата се вели: „Доколку оваа повелба содржи права кои кореспондираат со правата гарантирани со Конвенцијата за заштита на човековите права и основни слободи, значењето и опфатот на тие права ќе бидат исти како и на правата пропишани со Конвенцијата".

Меѓутоа, според последната реченица на членот 52 став 3,„тоа нема да претставува пречка за да може Унијата да обезбедува поширока заштита со своите закони". Во контекст на споредувањето на членот 8 став 2 на Конвенцијата и првата реченица на членот 52 став 3, тоа единствено може да значи дека условите за оправдано мешање во согласност со членот 8 став 2 на Конвенцијата се минимални барања за законито ограничување на правото на заштита на податоците во согласност со Повелбата. Според тоа, за законита обработка на личните податоци во согласност со правото на Европската Унија, потребно е, во најмала рака, да бидат исполнети условите од членот 8 став 2 на Конвенцијата. Меѓутоа правото на Европската Унија би можело да пропише дополнителни барања за посебни случаи.

Соодветствувањето на начелото за законита обработка според правото на Европската Унија со релевантните одредби на Европската конвенција за човековите права дополнително е унапредено со членот 6 ставот 3 на Договорот за Европската Унија, каде се вели дека „основните права, како што се гарантираните со Европската конвенција за заштита на човековите права и основните слободи […], ги сочинуваат општите начела на правото на Унијата".

118 Регулатива на Советот (ЕЗ) Бр. 1290/2005 од 21 јуни 2005 год. за финансирање на заедничката земјоделска политика, Сл. весник 2005 L 209; Регулатива на Комисијата (ЕЗ) Бр. 259/2008 од 18 март 2008 год. во врска со деталните правила за примена на Регулативата на Советот (ЕЗ) Бр. 1290/2005 во врска со објавата на информации за корисниците на средства од Европскиот земјоделски гарантен фонд (EAGF) и од Европскиот земјоделски фонд за рурален развој (EAFRD), Сл. весник Ј 2008 L 76.

3.2. Начелото за определување и за ограничување на целта

Клучни точки

- Целта на обработката на податоците мора јасно да се дефинира пред да започне обработката.
- Според правото на Европската Унија, целта на обработката мора да биде изречно утврдена. Според правото на Советот на Европа, тоа прашање е препуштено на националното законодавство.
- Обработката за неопределени цели не е во согласност со законодавството за заштита на податоците.
- За натамошна употреба на податоците за други цели, потребна е дополнителна правна основа ако новата цел на обработката не е усогласена со првичната.
- Преносот на податоци до трети страни е нова цел за која е потребна дополнителна правна основа.

Во суштина, начелото за определување и ограничување на целта значи дека легитимноста на обработката на личните податоци зависи од целта на обработката[119]. Целта мора да ја определи и соопшти контролорот пред да започне обработката[120]. **Според правото на Европската Унија**, тоа треба да се направи или по пат на изјава, односно со известување, до соодветниот надзорен орган или, барем, по пат на интерна документација која контролорот мора да им ја даде на располагање на надзорните органи заради преглед и на субјектот на податоците заради увид.

Обработката на лични податоци за неопределени и/или неограничени цели е незаконита.

Секоја нова цел за обработка на податоци мора да има сопствена правна основа и не може да се заснова на фактот дека податоците првично биле добиени или

119 Конвенција бр. 108, член 5 точка (б); Директива за заштита на податоците, член 6 став 1 точка (б).

120 Исто така види го Мислењето *03/2013* на Работната група за членот 29 (2013), *за ограничувањето на целта*, РГ 203, Брисел, 2 април 2013 година.

обработени за друга легитимна цел. Од друга страна, законската обработка е ограничена на својата првично определена цел, па секоја нова цел на обработката ќе бара нова посебна правна основа. Откривањето на податоците на трети лица мора да се разгледа со особена внимателност, бидејќи тоа обично претставува нова цел и од таа причина бара правна основа која е различна од таа за прибирање на податоци.

Пример: Една авионска компанија прибира податоци од своите патници заради непречено одвивање на резервациите и на летот. На компанијата ѝ се потребни податоци за: броевите на седиштата на патниците; посебни физички попреченост, како што се потребите на лицата во инвалидска количка; и посебни барања во однос на храната, како што се „кошер“ и „халал“ храна. Ако од авионските компании се побара да ѝ ги пренесат податоците, кои се содржани во евиденцијата со имињата на патниците, на имиграциската служба на одредишниот аеродром, тие податоци потоа ќе се употребат за целта на имиграциската контрола, која се разликува од првичната цел на прибирањето на податоците. Од таа причина, за пренос на тие податоци на имиграциска служба потребна е нова и посебна правна основа.

При разгледувањето на опфатноста и ограничувањата на определена цел, Конвенцијата бр. 108 и Директивата за заштита на податоците се повикуваат на начелото за споивост: употребата на податоци за споиви цели е дозволена врз основа на првичната правна основа. Меѓутоа, значењето на зборот „споиво“ во тој контекст не е дефинирано, па тој треба да се толкува на основа од-случај-до-случај.

Пример: Продажбата на податоците за клиентите на компанијата „Sunshine“, кои ги добила во текот на управувањето на односите со корисниците (УОК), на компанијата „Moonlight“, која се занимава со директен маркетинг, која сака да ги употреби тие податоци како помош во маркетиншките кампањи на трети компании, претставува нова цел, која е споива со УОК, односно со првичната цел на компанијата „Sunshine“ за прибирање на податоците за клиентите. Затоа, продажбата на податоците на компанијата „Moonlight“ изискува своја сопствена правна основа.

За разлика од тоа, употребата на податоците од УОК од страна на компанијата „Sunshine“ за сопствените маркетиншки цели, односно за испраќање на

маркетиншки податоци за своите производи до своите клиенти, во основа е прифатена како споива цел.

Во Директивата за заштита на податоците изречно е наведено дека „дополнителната обработка на податоците за историски, статистички или научни цели не се смета за неспоива, под услов државите-членки да обезбедат соодветни заштитни мерки“[121].

Примери: Компанијата „Sunshine“ прибрала и зачувала податоци од УОК во врска со нејзините клиенти. Натамошната употреба на тие податоци од страна на компанијата „Sunshine“ за статистички анализи на однесувањето на нејзините клиенти е дозволена, бидејќи статистиката е споива цел. Не е потребна дополнителна правна основа, како што е согласноста на субјектите на податоците.

Ако истите податоци се проследуваат до трето лице, компанијата „Starlight“, исклучиво за статистички цели, преносот би бил допуштен без дополнителна правна основа, но само под услов да постојат соодветни заштитни мерки, како што е прикривањето на идентитетот на субјектот на податоците, бидејќи идентитетот најчесто не е потребен за статистички цели.

3.3. Начелата за квалитет на податоците

Клучни точки

- Контролорот мора да ги применува начелата за квалитет на податоците во сите постапки за обработка.
- Врз основа на начелото за ограничено задржување на податоците неопходно е податоците да се избришат веднаш кога повеќе нема да бидат потребни за целите за кои биле прибрани.

121 Пример за такви национални одредби е австрискиот Закон за заштита на податоците (*Datenschutzgesetz*), Сојузен службен весник бр. 165/1999, параграф 46, достапен на англиски јазик на: www.dsk.gv.at/DocView. axd?CobId=41936.

- Исклучоци од начелото за ограничено задржување мора да бидат пропишани со закон и изискуваат посебни заштитни мерки за заштитата на субјектите на податоците.

3.3.1. Начелото за релевантност на податоците

Може да се обработуваат само податоци кои се „соодветни, релевантни и не се прекумерни во однос на целта за која се прибираат и/или понатаму се обработуваат“[122]. Категориите на податоци кои се избрани за обработка мора да бидат нужни за да се постигне наведената општа цел на операцијата на обработка, а контролорот треба строго да го ограничи прибирањето на податоци за оние информации што се директно релевантни за конкретната цел кон која е насочена обработката.

Во современото општество, начелото за релевантност на податоците има дополнителен аспект: со користење на посебна технологија со која се унапредува приватноста, понекогаш е можно во целост да се избегне користењето на лични податоци, или да се користат псевдонимизирани податоци, со што се постигнува решение кое ја поддржува приватноста. Тоа е особено соодветно во поголеми системи за обработка.

Пример: Градски совет на редовните корисници на системот на градскиот јавен превоз им нуди чип-картичка за одреден паричен надомест. На површината на картичката е испечатено името на корисникот, кое исто така е зачувано во електронски облик во чипот. При секое користење на автобус или трамвај, чип-картичката треба да се стави пред вградениот уред за читање, на пример, во автобуси и во трамваи. Податоците што ги отчитува уредот електронски се проверуваат во базата на податоци која ги содржи имињата на луѓето што купиле патен билет.

Овој систем не го почитува начелото за релевантност на оптимален начин: проверката во однос на тоа дали некое лице смее да ги користи средствата за јавен превоз би можела да се изврши без да се споредуваат личните податоци од чип-картичката со оние од базата на податоци. Доволно би било, на пример, во чипот на картичката да има посебна електронска слика, како што е баркод, со кој, кога картичката ќе се постави пред уредот за читање, би се

122 Конвенција бр. 108, член 5 точка (в); и Директива за заштита на податоците, член 6 став 1 точка (в).

потврдило дали картичката е валидна или не. Таквиот систем не би бележел кој и во кое време користел некое превозно средство. Не би се прибирале лични податоци, што претставува оптимално решение во смисла на начелото за релевантност, бидејќи од тоа начело произлегува обврската за прибирање на колку што е можно помалку податоци.

3.3.2. Начелото за точност на податоците

Контролорот кој располага со лични податоци не смее да ги користи таквите податоци без да преземе чекори со кои во доволна мера може да се осигури дека податоците се точни и актуелни.

Обврската за осигурување на точноста на податоците треба да се разгледува во контекст на целта на обработката на податоците.

Пример: Компанија што се занимава со продажба на мебел на свој купувач му зела податоци за неговиот идентитет и адреса на живеење за да му подготви фактура. По шест месеци, истата компанија сака да започне кампања и да ги контактира поранешните купувачи. За таа цел, компанијата сака да пристапи во националниот регистар на жители, кој најверојатно содржи ажурирани адреси, затоа што жителите се законски обврзани на регистарот да му ја соопштат својата моментална адреса. Пристапот до податоците од овој регистар е ограничен на лица и субјекти кои ќе наведат оправдана причина за тоа.

Во оваа ситуација, компанијата не може да го искористи аргументот дека мора да чува точни и ажурирани податоци за да докаже дека има право да прибере нови податоци со адресите на сите свои поранешни купувачи од регистарот на жители. Податоците се прибрани во текот на подготвувањето на фактурите. За таа цел, релевантна е адресата во времето на продажбата. Нема правна основа за прибирање на нови податоци за адресите, бидејќи маркетингот не претставува интерес кој го надвладува правото на заштита на податоците и затоа не може да го оправда пристапот во податоците од регистарот.

Исто така може да се појават случаи во кои ажурирањето на зачуваните податоци е забрането со закон, бидејќи основната цел на зачувувањето на податоците е документирање на настани.

Пример: Записникот за медицинска операција не смее да се измени, односно да се „ажурира", дури и ако подоцна се покаже дека наодите што се споменати во записникот се погрешни. Во тој случај во записникот може да се додадат само забелешки кои треба да бидат јасно означени како дополнително внесени податоци.

Од друга страна, има ситуации во кои редовната проверка на точноста на податоците, вклучувајќи го и ажурирањето, претставува апсолутна нужност поради можната штета што може да ја претрпи субјектот на податоците ако податоците останат неточни.

Пример: Ако некое лице сака да склучи договор со банкарска институција, банката обично ќе ја провери кредитната способност на потенцијалниот клиент. За таа цел, постојат посебни бази на податоци што содржат податоци за кредитната историја на приватни лица. Ако во таквата база на податоци се наведени неточни или застарени податоци за некое лице, тоа лице може да се соочи со сериозни проблеми. Затоа, тие што се одговорни за таквите бази на податоци мораат да направат посебни напори за почитување на начелото за точност.

Покрај тоа, податоците кои не се однесуваат на факти, туку на сомневања, како што се кривичните истраги, можат да се прибираат и да се чуваат сè додека контролорот има правна основа за прибирање на такви информации и сè додека неговото сомневање е доволно оправдано.

3.3.3. Начелото за ограничено задржување на податоците

Со членот 6 став 1 точка (д) на Директивата за заштита на податоците, како и со членот 5 точка (д) на Конвенцијата бр. 108, предвидено е дека државите-членки треба да осигурат да мора личните податоци „да се водат во облик што

дозволува субјектите на податоците да можат да се идентификуваат не подолго отколку што е потребно за намените за кои податоците биле собрани или за кои се дополнително обработени". Затоа, податоците мора да се избришат откако ќе бидат исполнети тие цели.

Во предметот *S. and Marper*, Европскиот суд за човековите права заклучил дека клучните начела на релевантните иструменти на Советот на Европа, како и правото и практиката на другите договорни страни, налагаат задржувањето на податоците да биде сразмерно со целта на прибирањето и да биде временски ограничено, а особено во полицискиот сектор[123].

Меѓутоа, временското ограничување на чувањето на личните податоци се однесува само на податоците кои се чуваат во облик што овозможува да се идентификуваат субјектите на податоците. Затоа, законитото чување на податоците кои повеќе не се потребни би можело да се постигне со нивна анонимизација или псевдонимизација.

Чувањето податоци заради нивна идна употреба за научни, историски или статистички цели изречно е изземено од начелото за ограничено задржување на податоците во Директивата за заштита на податоците[124]. Меѓутоа, таквото континуирано чување и таквата употреба на лични податоци мора да бидат придружени со посебни заштитни мерки на националното законодавство.

3.4. Начелото за правична обработка

Клучни точки

- Правичната обработка значи транспарентност на обработката, а особено во поглед на субјектите на податоците.
- Контролорите мораат да ги известат субјектите на податоците пред обработката на нивните податоци, барем за целта на обработката и за идентитетот и адресата на контролорот.
- Освен ако тоа не е посебно допуштено со закон, личните податоци не смеат да се обработуваат тајно и скришно.

123 ЕСЧП, *S. and Marper v. the United Kingdom*, бр. 30562/04 и 30566/04, 4 декември 2008 год.; исто така види, на пример: ЕСЧП, *M.M. v. the United Kingdom*, Бр. 24029/07, 13 ноември 2012 година.

124 Директива за заштита на податоците, член 6 став 1 точка (д).

- Субјектите на податоците имаат право на пристап до своите податоци независно од местото на нивна обработка.

Начелото за правична обработка првенствено го регулира односот меѓу контролорот и субјектот на податоците.

3.4.1. Транспарентност

Со ова начело на контролорот му се наметнува обврската за известување на субјектите на податоците за начинот на којшто се користат нивните податоци.

Пример: Во предметот *Haralambie v. Romania*[125] жалителот побарал пристап до досието кое тајната служба го чувала за него, но неговото барање било одобрено дури по пет години. Европскиот суд за човековите права повторил дека од суштинска важност за лицата за кои државните органи чуваат лични досиеја е да можат да пристапат до нив. Државните органи биле должни да осигурат ефикасна постапка за добивање пристап до таквите информации. Европскиот суд за човековите права сметал дека ниту количината на пренесените досиеја ниту недостатоците во системот за архивирање не оправдувале петгодишно доцнење во одобрувањето на барањето на жалителот за пристап до неговото досие. Државните органи не му обезбедиле на жалителот ефикасна и лесно применлива постапка за да му овозможат да добие пристап до неговото лично досие во разумен рок. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Операциите на обработка мора да им се објаснат на субјектите на податоците на едноставен и разбирлив начин кој ќе осигури дека тие разбираат што ќе се случи со нивните податоци. Субјектот на податоците исто така има право, на негово барање, да дознае од контролорот дали неговите податоци се обработуваат, и, ако тоа е случај, кои податоци.

3.4.2. Воспоставување доверба

Контролорите би требало да ги известат субјектите на податоците и јавноста дека ќе ги обработат податоците на законит и транспарентен начин. Операциите на

125 ЕСЧП, *Haralambie v. Romania*, Бр. 21737/03, 27 октомври 2009 година.

обработка не смеат да се извршуваат тајно и не би смееле да имаат непредвидливи негативни последици. Контролорите би требало да осигурат информираност на купувачите, клиентите или граѓаните за употребата на нивните податоци. Покрај тоа, контролорите мораат, колку што е можно, да постапуваат на начин кој повеќе одговара на желбите на субјектот на податоците, особено ако неговата согласност ја сочинува правната основа за обработката на податоците.

Пример: Во предметот *K.H. and Others v. Slovakia*[126], жалителките биле осум жени од ромско етничко потекло кои во текот на бременоста и породувањето се лекувале во две болници во Источна Словачка. Потоа, ниедна од нив не можела повторно да зачне и покрај многубројните обиди. Националните судови им наложиле на болниците да им дозволат на жалителките и на нивните застапници увид во нивните здравствени картони и да препишат делови од нив, но го отфрлиле нивното барање да ги фотокопираат документите, наводно со цел да ја спречат нивната злоупотреба. Од позитивните обврски на државата во согласност со членот 8 на Конвенцијата, нужно произлегувала должноста на субјектите на податоците да им се дадат на располагање копии од досиејата со нивните податоци. Државата требало да ги определи начините на копирање на досиејата со лични податоци или, кога тоа е соодветно, да наведе од кои релевантни причини одбива да го стори тоа. Во случајот на жалителките, националните судови забраната за копирање на здравствените картони првенствено ја оправдувале со потребата да ги заштитат релевантните информации од злоупотреба. Меѓутоа, Европскиот суд за човековите права не можел да сфати како жалителките, кои во секој случај добиле пристап до нивната целокупна медицинска документација, би можеле да ги злоупотребат информациите што се однесувале на нив. Покрај тоа, ризикот од таквата злоупотреба можел да се спречи на понаков начин наместо со забрана за копирање на досиејата од страна на жалителките, како на пример со ограничување на бројот на луѓето што имаат право на пристап до досиејата. Државата не успеала да го покаже постоењето на доволно релевантни причини поради кои на жалителките им бил забранет ефективниот пристап до информации во врска со нивното здравје. Судот заклучил дека имало повреда на членот 8.

Што се однесува до интернет-услугите, карактеристиките на системите за обработка на податоци мораат да им овозможат на субјектите на податоците да разберат што се случува со нивните податоци.

126 ЕСЧП, *K.H. and Others v. Slovakia*, Бр. 32881/04, 28 април 2009 година.

Правичната обработка исто така значи дека контролорите се подготвени да преминат преку задолжителните и законски пропишаните минимални барања за услуги дадени на субјектите на податоците ако тоа го налагаат легитимните интереси на субјектот на податоците.

3.5. Начелото за одговорност

Клучни точки

- Одговорноста значи дека контролорите во своите операции на обработка на податоците мораат активно да ги спроведуваат мерките со кои се промовира и се гарантира заштитата на податоците.
- Контролорите се одговорни за усогласувањето на своите операции на обработка со законодавството за заштита на податоците.
- Контролорите би требало да можат во секое време на субјектите на податоците, на јавноста и на надзорните органи да им ја докажат усогласеноста со одредбите за заштита на податоците.

Во 2013 година Организацијата за економска соработка и развој (OECP) усвоила насоки за приватност со кои се нагласува дека контролорите имаат важна улога во осигурувањето на функционирањето на заштитата на податоците во практиката. Во таквите насоки е развиено начелото за одговорност според кое „контролорот на податоците треба да биде одговорен за усогласувањето со мерките со кои се спроведуваат погоре споменатите [материјални] начела“[127].

Додека Конвенцијата бр. 108 не упатува на одговорноста на контролорите, начелно препуштајќи му ја таа тема на националното законодавство, во членот 6 став 2 на Директивата за заштита на податоците е наведено дека контролорот мора да осигури усогласеност со начелата кои се однесуваат на квалитетот на податоците вклучени во ставот 1.

127 OECP (2013), *Насоки со кои се уредува заштитата на приватноста и прекуграничниот пренос на лични податоци*, член 14.

Пример: Пример од законодавството со кој се нагласува начелото за одговорност е измената[128] на Директивата за приватност и електронски комуникации (2002/58/ЕЗ). Според членот 4 во неговиот изменет облик, директивата наметнува обврска за спроведување на безбедносна политика, а поточно за „осигурување на спроведувањето на безбедносна политика во поглед на обработката на лични податоци". Па така, што се однесува до одредбите за безбедност на таа директива, законодавецот одлучил дека е неопходно да се внесе изречно барање за постоење и спроведување на безбедносна политика.

Според мислењето на Работната група за членот 29[129], суштината на одговорноста е обврската на контролорот:

- да воспоставува мерки со кои – во нормални околности – би се гарантирало почитувањето на правилата за заштита на податоците во смисла на операциите на обработка;
- да има подготвено документација со која на субјектите на податоците и на надзорните органи може да им докаже кои мерки биле преземени за да се постигне усогласеност со правилата за заштита на податоците.

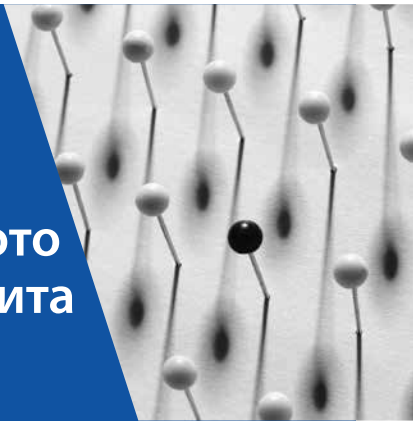
Според тоа, начелото за одговорност бара од контролорот способност активно да ја докажува усогласеноста наместо да чека субјектите на податоците или надзорните органи да му укажат на недостатоците.

128 Директива 2009/136/ЕЗ на Европскиот парламент и на Советот од 25 ноември 2009 година за измена на Директивата 2002/22/ЕЗ за универзална услуга и права на корисниците во врска со електронски комуникациски мрежи и услуги, Директива 2002/58/ЕЗ за обработка на лични податоци и заштита на приватноста во секторот за електронски комуникации и Регулатива (ЕЗ) Бр. 2006/2004 за соработка помеѓу националните органи одговорни за спроведување на законодавството за заштита на корисниците, Сл. весник 2009 L 337, стр. 11.

129 Работна група за членот 29, *Мислење 3/2010 во врска со начелото за одговорност*, РГ 173, Брисел, 13 јули 2010 год.

4

Правилата на европското законодавство за заштита на податоците



Европска Унија	Обработени прашања	Совет на Европа
Правила за законита обработка на нечувствителни податоци		
Директива за заштита на податоците, член 7 точка (а)	Согласност	Препорака за профилирањето членови 3.4. точка (б) и 3.6.
Директива за заштита на податоците, член 7 точка (б)	(Пред)договорен однос	Препорака за профилирањето, член 3.4. точка (б)
Директива за заштита на податоците, член 7 точка (в)	Законски должности на контролорот	Препорака за профилирањето, член 3.4. точка (а)
Директива за заштита на податоците, член 7 точка (г)	Суштински интереси на субјектот на податоците	Препорака за профилирањето, член 3.4. точка (б)
Директива за заштита на податоците, член 7 точка (д) и член 8 став 4 СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 година	Јавен интерес и вршење службено овластување	Препорака за профилирањето, член 3.4. точка(б)
Директива за заштита на податоците, член 7 точка (ѓ), член 8 став 2 и член 8 став 3 СПЕУ, заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de EstablecimientosFinancierosdeCrédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 ноември 2011 год.	Легитимни интереси на другите	Препорака за профилирањето, член 3.4. точка (б)
Правила за законита обработка на чувствителни податоци		
Директива за заштита на податоците, член 8 став 1	Општа забрана за обработка	Конвенција бр. 108, член 6

Директива за заштита на податоците, член 8 став 2.–4.	Исклучоци од општата забрана	Конвенција бр. 108, член 6
Директива за заштита на податоците, член 8 став 5	Обработка на податоци за (кривични) пресуди	Конвенција бр. 108, член 6
Директива за заштита на податоците, член 8 став 7	Обработка на идентификациски броеви	
Правила за безбедност на обработката		
Директива за заштита на податоците, член 17	Обврска да се осигури безбедна обработка	Конвенција бр. 108, член 7 ЕСЧП, *I.v.Finland*, Бр. 20511/03, 17 јули 2008 год.
Директива за приватност и електронски комуникации, член 4 став 2	Известувања во случај на повреда на заштитата на податоците	
Директива за заштита на податоците, член 16	Обврска за доверливост	
Правила за транспарентност на обработката		
	Општа транспарентност	Конвенција бр. 108, член 8 точка (а)
Директива за заштита на податоците, членови 10 и 11	Информации	Конвенција бр. 108, член 8 точка (а)
Директива за заштита на податоците, членови 10 и 11	Исклучоци од обврската за информирање	Конвенција бр. 108, член 9
Директива за заштита на податоците, членови 18 и 19	Известување	Препорака за профилирањето, член 9.2. точка (а)
Правила за унапредување на усогласеноста		
Директива за заштита на податоците, член 20	Претходна проверка	
Директива за заштита на податоците, член 18 став 2	Службеници за заштита на личните податоци	Препорака за профилирањето, член 8.3.
Директива за заштита на податоците, член 27	Правила на однесување	

Начелата се нужно од општа природа. Нивната примена во конкретни ситуации допушта извесна можност за толкување и за избор на средства. Според **правото на Советот на Европа**, задача на договорните страни на Конвенцијата бр. 108 е да определат што е допуштено за толкување во нивното национално право. Ситуацијата е поинаква во **правото на Европската Унија** за воспоставување на заштитата на податоците во внатрешниот пазар, се сметало дека е неопходно да постојат подетални правила на ниво на Европската Унија со цел да се усогласи степенот на заштита на податоците во националните законодавства на државите-членки. Со Директивата за заштита на податоците, според начелата кои се наведени во нејзиниот член 6, се воспоставува збир на детални правила кои треба верно да се спроведуваат во националното законодавство. Затоа, следните напомени за деталните правила за заштита на податоците на европско ниво претежно се однесуваат на правото на Европската Унија.

4.1. Правилата за законита обработка

Клучни точки

- Личните податоци можат законито да се обработуваат ако:
- обработката се заснова на согласноста на субјектот на податоците;
- обработката на податоците е нужна поради суштинските интереси на субјектот на податоците;
- причина за обработка се легитимните интереси на другите, но само ако тие не се надвладеани од интересите за заштита на основните права на субјектите на податоците.
- Законитата обработка на чувствителните лични податоци подлежи на посебен, построг режим.

Директивата за заштита на податоците содржи две збирки на правила за законита обработка на податоци: една за нечувствителни податоци во членот 7 и една за чувствителни податоци во членот 8.

4.1.1. Законита обработка на нечувствителни податоци

Поглавјето II на Директивата 95/46, насловено „Општи правила во врска со законитоста на обработката на лични податоци" предвидува дека мора, врз основа на исклучоците кои се дозволени со членот 13, секоја обработка на лични податоци, како прво, да биде во согласност со начелата во врска со квалитетот на податоците кои се содржани во членот 6 на Директивата за заштита на податоците и, како второ, со еден од критериумите за законитост на обработката на податоците кои се наведени во членот 7[130]. Со тоа се објаснуваат случаите во кои е законито да се обработуваат нечувствителните лични податоци.

Согласност

Според правото на Советот на Европа, согласноста не се споменува во членот 8 на Европската конвенција за човековите права или во Конвенцијата бр. 108. Меѓутоа, таа се споменува во судската практика на Европскиот суд за човековите права и во неколку препораки на Советот на Европа. **Според правото на Европската Унија**, согласноста како основа за законита обработка на податоците јасно е утврдена во членот 7 точка (а) на Директивата за заштита на податоците, а исто така изречно е спомената во членот 8 на Повелбата.

Договорен однос

Друга основа за законита обработка на лични податоци **според правото на Европската Унија**, која е наведена во членот 7 точка (б) на Директивата за заштита на податоците, е дека „обработката е неопходна заради спроведување на договор чијашто страна е субјектот на податоците". Оваа одредба исто така се однесува и на преддоговорните односи. На пример: некоја страна сака да склучи договор, но тоа сè уште не го сторила најверојатно поради тоа што е потребно да се направат уште некои проверки. Ако некоја страна за таа цел мора да обработи податоци, таквата обработка е законита сè додека се спроведува „со цел да се преземат чекори по барање на субјектот на податоците пред склучувањето на договорот".

130 СПЕУ, заеднички предмети C-465/00, C-138/01 и C-139/01. *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*, 20 мај 2003 година, параграф 65; СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 год., параграф 48; СПЕУ, заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 ноември 2011 год., параграф 26.

Што се однесува до правото на Советот на Европа, „заштитата на правата и слободите на другите“ се споменува во членот 8 став 2 на Европската конвенција за човековите права како причина за законито мешање во правото за заштита на податоците.

Законски должности на контролорот

Во **правото на Европската Унија** изречно се споменува еден друг критериум за законитост на обработката на податоците, имено, ако „обработката е потребна за усогласување со законската обврска на која подлежи контролорот“ (член 7 точка (в) на Директивата за заштита на податоците). Оваа одредба се однесува на контролорите кои работат во приватниот сектор, додека правните обврски на контролорите од јавниот сектор потпаѓаат под членот 7 точка (д) на Директивата. Има многу случаи во кои контролорите од приватниот сектор се законски обврзани да обработуваат податоци за други; на пр. лекарите и болниците имаат законска обврска да чуваат податоци за лекувањето на пациентите во текот на неколку години, работодавците мораат да обработуваат податоци за своите вработени за потребите на социјалното осигурување и на одаточувањето, а претпријатијата мораат да обработуваат податоци за своите клиенти за целите на одаточувањето.

Со оглед на тоа дека авионските компании се должни на странските органи за имиграциска контрола да им пренесуваат податоци за патниците, се поставува прашањето дали законските обврски во согласност со *странски закон* би можеле да претставуваат легитимна основа за обработка на податоците според правото на Европската Унија (ова прашање подетално е разгледано во поглавјето 6.2.).

Правните обврски на контролорот претставуваат основа за законита обработка на податоците и **според правото на Советот на Европа.** Како што е претходно наведено, законските обврски на контролор од приватниот сектор се само еден посебен случај за легитимни интереси на други, како што е наведено во членот 8 став 2 на Европската конвенција за човековите права. Според тоа, горенаведениот пример е релевантен и за правото на Советот на Европа.

Суштински интереси на субјектот на податоците

Според правото на Европската унија, членот 7 точка (г) на Директивата за заштита на податоците пропишува дека обработката на личните податоци е законита ако „е неопходна за да се заштитат суштинските интереси на субјектот

на податоците". Таквите интереси, кои се тесно поврзани со преживувањето на субјектот на податоците, може да бидат основа за легитимна употреба, на пример, на здравствени податоци или на податоци за исчезнати лица.

Според правото на Советот на Европа, суштинските интереси на субјектот на податоците не се споменуваат во членот 8 на Европскиот суд за човековите права како причина за законито мешање во правото на заштита на податоците. Меѓутоа, во некои од препораките на Советот на Европа, кои во одредени области ја надополнуваат Конвенцијата бр. 108, суштинските интереси на субјектот на податоците изречно се наведени како основа за законита обработка на податоците[131]. Се чини дека суштинските интереси на субјектот на податоците се вбројуваат во причините со кои се оправдува обработката на податоци: заштитата на основните права не смее никогаш да ги загрозува суштинските интереси на лицето кое е заштитено.

Јавен интерес и вршење службено овластување

Со оглед на тоа дека јавните дејности можат да се организираат на многу начини, членот 7 точка (д) на Директивата за заштита на податоците пропишува дека личните податоци можат законито да се обработат ако „обработката е неопходна за реализирање на задачите што се извршуваат заради јавен интерес или за вршење на службено овластување доделено на контролорот или на трета страна на која ѝ се откриени податоците […]"[132].

Пример: Во предметот *Huber v. Germany*[133], г. Хубер, австриски државјанин со живеалиште во Германија, побарал од Сојузната служба за миграција и бегалци да ги избрише податоците за него во Централниот регистар на странци (AZR). Тој регистар, кој ги содржи личните податоци на државјани на Европската Унија кои не се германски државјани, но живеат во Германија подолго од три месеци, се користи за статистички цели како и од страна на полициските и правосудните органи кога ги истражуваат и ги гонат криминалните активности или оние што ја загрозуваат јавната безбедност. Судот што го проследил предметот го поставил прашањето дали обработката на лични податоци која ја врши регистар како што е Централниот регистар за странци, до кој имаат пристап и други државни органи, е во согласност

131 Препорака за профилирањето, член 3.4. точка (б).

132 Види ја Директивата за заштита на податоците, Уводна изјава бр. 32.

133 СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 год.

со правото на Европската Унија, ако се земе предвид дека не постои таков регистар за германски државјани.

Судот на правдата на Европската Унија смета, како прво, дека според членот 7 точка (д) на Директивата, личните податоци може законито да се обработуваат само ако тоа е неопходно за реализирање на задачата што се извршува заради јавен интерес или при вршење службено овластување.

Според мислењето на Судот, „имајќи ја предвид целта за обезбедување на еднаков степен на заштита во сите држави-членки, поимот за нужност од членот 7 точка (д) на Директивата 95/46 […] не може да има значење кое се разликува во секоја од државите-членки. Оттука произлегува дека станува збор за поим кој има свое самостојно значење во правото на Заедницата и кој мора да се толкува така што целосно ќе ја одразува целта на таа директива, како што е наведено во нејзиниот член 1 став 1“[134].

Судот напоменува дека правото на слободно движење на граѓанин на Унијата на територијата на држава-членка на која не е државјанин не е безусловно, туку тоа може да подлежи на ограничувања и услови што се утврдени со Договорот и со мерките кои се усвоени заради негово спроведување. Според тоа, ако начелно е легитимно за држава-членка да користи регистар како што е AZR за да ги поддржи државните органи кои се одговорни за примена на законодавството кое се однесува на правото на престој, таквиот регистар не смее да содржи информации кои не се потребни за таа одредена цел. Судот заклучил дека таквиот систем за обработка на лични податоци е во согласност со правото на Европската Унија ако ги содржи само оние податоци што се потребни за примена на тоа законодавство и ако поради неговата централизирана природа примената на тоа законодавство е поделотворна. Националниот суд мора да утврди дали таквите услови се исполнети во овој конкретен случај. Ако тие не се исполнети, зачувувањето и обработката на лични податоци во регистар како што е AZR за статистички цели, по ниедна основа, не може да се смета за нужна во смисла на членот 7 точка (д) на Директивата 95/46/ЕЗ[135].

Конечно, што се однесува до прашањето за употреба на податоците кои се содржани во регистарот за целите на сузбивање на криминалот, Судот смета дека таа цел „нужно го вклучува гонењето на сторени кривични дела и

134 *На истото место*, параграф 52.

135 *На истото место*, ставови 54, 58, 59, 66-68.

прекршоци, независно од националноста на нивните сторители". Предметниот регистар не содржи лични податоци поврзани со државјаните на засегнатата држава-членка, а таа разлика во постапувањето претставува дискриминација што е забранета со членот 18 од Договорот за функционирањето на Европската Унија. Според тоа, таа одредба, според толкувањето на Судот, „ја исклучува можноста државата-членка, за целите на сузбивање на криминалот, да воспостави систем за обработка на лични податоци посебно за жителите на Унијата кои не се државјани на таа држава-членка"[136].

Користењето на лични податоци од страна на органите од јавниот сектор исто така е предмет на членот 8 на Европската конвенција за човековите права.

Легитимни интереси на контролорот или на трето лице

Субјектот на податоците не е единственото лице кое има легитимни интереси. Членот 7 точка (ѓ) на Директивата за заштита на податоците пропишува дека личните податоци можат законито да се обработат ако тоа „е неопходно за целите на легитимните интереси што ги спроведува контролорот или третата страна или страните на кои им се откриени податоците, освен ако ваквите интереси се надгласани со интересите или со основните права и слободи на субјектот на податоците […]".

Следната пресуда Судот на правдата на Европската Унија ја донел изречно врз основа на членот 7 точка (ѓ) на Директивата:

Пример: Во предметот *ASNEF and FECEMD*[137], Судот на правдата на Европската Унија појаснил дека националното законодавство не смее да додава услови покрај тие што се наведени во членот 7 точка (ѓ) на Директивата за законита обработка на податоци. Тоа се однесувало на ситуација во која еден шпански закон за заштита на податоците содржел одредба врз основа на која други приватни страни можеле да тврдат дека имаат легитимен интерес за обработка на лични податоци само ако таквите информации веќе се појавиле во јавни извори.

136 *На истото место*, стр. 78 и 81.

137 СПЕУ, заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 ноември 2011 година.

Судот најпрвин напоменал дека целта на Директивата 95/46/ЕЗ е да осигури еднаков степен на заштита на правата и слободите на поединците во врска со обработката на лични податоци во сите држави-членки. Покрај тоа, приближувањето на националните закони што се применуваат во таа област не смее да доведе до намалување на заштитата што ја гарантираат. Напротив, мора да се настојува со нив да се осигури највисоко ниво на заштита во Европската Унија[138]. Според тоа, Судот на правдата на Европската Унија заклучил дека „од целта за осигурување на еднаков степен на заштита во сите држави-членки произлегува дека со членот 7 на Директивата 95/46 се наведува исцрпна и ограничена листа на случаи во кои обработката на лични податоци може да се смета како законита". Покрај тоа, „државите-членки не можат да додаваат нови начела кои се однесуваат на законитоста на обработката на лични податоци во членот 7 на Директивата 95/46 или да наметнуваат нови барања кои имаат за цел да се измени опфатот на примена на едно од шесте начела содржани во членот 7"[139]. Судот потврдил дека во поглед на урамнотежувањето кое е потребно во согласност со членот 7 точка (ѓ) на Директивата 95/46/ЕЗ, „можно е да се земе предвид фактот дека сериозноста на повредата на основните права на субјектот на податоците што произлегува од обработката може да се разликува во зависност од тоа дали податоците за кои станува збор веќе се појавиле во јавни извори".

Меѓутоа, според „членот 7 точка (ѓ) на Директивата, не е можно држава-членка, на категорички и општ начин, да ја исклучува можноста за обработка на определени категории на лични податоци, без притоа да овозможи меѓусебно урамнотежување на предметните спротивставени права и интереси во конкретен случај".

Имајќи го предвид горенаведеното, Судот заклучил дека „членот 7 точка (ѓ) на Директивата 95/46 треба да се толкува како да ги исклучува националните правила кои, во отсуство на согласност од страна на субјектот на податоците и со цел да овозможат таквата обработка на личните податоци на субјектот на податоците која е неопходна за да се исполнат легитимните интереси на контролорот на податоците или на третата страна или на страните на кои им се откриени податоците, не само што налагаат почитување на основните права и слободи на субјектот на податоците туку и појавување на податоците

138 *На истото место*, параграф 28. Види ја Директивата за заштита на податоците, Уводни изјави бр. 8 и 10.

139 СПЕУ, *заеднички случаи C-468/10 и C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 ноември 2011 год., параграфи 30 и 32.

во јавни извори, притоа исклучувајќи ја, на категорички и општ начин, секоја обработка на податоците кои не се појавуваат во такви извори“[140].

Слични формулации можат да се најдат во препораките на Советот на Европа. Препораката за профилирањето потврдува дека обработката на личните податоци за цели на профилирањето е законита ако е потребна заради легитимните интереси на другите, „освен ако таквите интереси се надвладеани со основните права и слободи на субјектот на податоците“[141].

4.1.2. Законита обработка на чувствителни податоци

Во согласност со **правото на Советот на Европа**, националното законодавство е одговорно за утврдување на соодветна заштита за користење на чувствителни податоци, додека во согласност со **правото на Европската Унија**, во членот 8 на Директивата за заштита на податоците е содржан детален режим за обработка на видови податоци кои откриваат: расно или етничко потекло, политички мислења, верски или филозофски убедувања, членство во синдикат или информации во врска со здравјето или сексуалниот живот. Обработката на чувствителни податоци начелно е забранета[142]. Меѓутоа, постои исцрпна листа на исклучоци од таа забрана, која може да се најде во членот 8 став 2 и 3 на Директивата. Тие исклучоци ги содржат изречната согласност на субјектот на податоците, суштинските интереси на субјектот на податоците, легитимните интереси на други лица и јавните интереси.

За разлика од обработката на нечувствителни податоци, договорниот однос со субјектот на податоците не се смета за општа основа за законитата обработка на чувствителни податоци. Затоа, ако чувствителните податоци се обработуваат во смисла на договор со субјектот на податоците, за употреба на тие податоци е потребна посебна изречна согласност на субјектот на податоците, заедно со согласноста за склучување на договорот. Меѓутоа, изречното барање од страна на субјектот на податоците за стоки или услуги со кои нужно се откриваат чувствителни податоци треба да се смета за подеднакво важно како изречната согласност.

140 *На истото место*, параграфи 40, 44, 48 и 49.

141 Обврска за профилирање, член 3.4. точка (б).

142 Директива за заштита на податоците, член 8 став (1).

Пример: Ако патник при резервација на летот побара од авиокомпанијата инвалидска количка и „кошер“ храна, авиокомпанијата смее да ги употреби тие податоци дури и ако патникот не потпишал посебна клаузула за согласност во која се вели дека тој се согласува со употребата на неговите податоци со кои се откриваат информации во врска со неговото здравје и неговите верски убедувања.

Изречна согласност на субјектот на податоците

Првиот услов за законита обработка на кои било податоци, без оглед на тоа дали се нечувствителни или чувствителни, е согласноста на субјектот на податоците. Во случајот на чувствителни податоци, таквата согласност мора да биде изречна. Меѓутоа, со националното законодавство може да е пропишано дека давањето согласност за употреба на чувствителни податоци не е доволна правна основа за допуштање на нивната обработка[143], ако на пример, во исклучителни случаи, обработката вклучува невообичаени ризици за субјектот на податоците.

Во посебен случај, дури и имплицитната согласност се прифаќа како правна основа за обработка на чувствителни податоци: во членот 8 став 2 точка (д) на Директивата е предвидено дека обработката не е забранета ако се однесува на податоци за кои е очигледно дека ги објавил субјектот на податоците. Таа одредба јасно претпоставува дека постапувањето на субјектот на податоците, со кое ги објавува своите податоци, мора да се толкува како да ја подразбира согласноста на субјектот на податоците за употреба на тие податоци.

Суштински интереси на субјектот на податоците

Исто како нечувствителните податоци, и чувствителните податоци можат да се обработуваат поради суштинските интереси на субјектот на податоците[144].

За да биде законита обработката на чувствителни податоци на таа основа, потребно е да се утврди дека било невозможно да се побара одлука од субјектот на податоците, затоа што, на пример, не било при свест или било отсутно и недостапно.

143 *На истото место*, член 8 став 2 точка (а).

144 *На истото место*, член 8 став 2 точка (в).

Легитимни интереси на другите

Како во случајот на нечувствителните податоци, легитимните интереси на другите лица можат да послужат и како основа за обработка на чувствителни податоци. Меѓутоа, за чувствителни податоци, во согласност со членот 8 став 2 на Директивата за заштита на податоците, тоа се однесува само на следните случаи:

- ако обработката е потребна поради суштинските интереси на друго лице[145] во случај кога субјектот на податоците физички или правно не е способно да ја даде својата согласност;

- ако чувствителните податоци се релевантни во областа на трудовото право, како што се, на пример, здравствените податоци во контекст на особено опасно работно место или податоците за верските убедувања во контекст на празниците[146];

- ако фондации, здруженија или други непрофитни организации со политичка, филозофска, верска или синдикална цел обработуваат податоци за своите членови или спонзори или за други заинтересирани страни (таквите податоци се чувствителни бидејќи голема е веројатноста да ги откриваат верските или политичките убедувања на засегнатите поединци)[147];

- ако чувствителните податоци се употребуваат во смисла на правни постапки пред суд или пред управен орган за поднесување, спроведување или одбрана на правни барања[148].

- Покрај тоа, според членот 8 став 3 на Директивата за заштита на податоците, ако здравствените податоци се користат од страна на здравствените работници за здравствен преглед и за лекување, исклучокот се однесува и на управувањето со таквите услуги. Како посебна заштитна мерка, лицата се сметаат за „здравствени работници“ само ако подлежат на посебни професионални обврски за доверливост.

145 *На истото место.*

146 *На истото место*, член 8 став 2 точка (б).

147 *На истото место*, член 8 став 2 точка (г).

148 *На истото место*, член 8 став 2 точка (д).

Јавен интерес

Покрај тоа, во согласност со членот 8 став 4 на Директивата за заштита на податоците, државите-членки можат да предвидат дополнителни цели за кои може да се обработуваат чувствителни податоци, ако:

- податоците се обработуваат поради значаен јавен интерес;
- тоа е пропишано со национално законодавство или со одлука на надзорен орган;
- националното законодавство или одлуката на надзорен орган ги содржи потребните заштитни мерки за ефикасна заштита на интересите на субјектите на податоците[149].

Добар пример се електронските системи на здравствени картони, кои се внесуваат во многу држави-членки. Таквите системи овозможуваат здравствените податоци, кои се прибрани од страна на здравствените работници во текот на лекувањето на пациентот, да им се стават на располагање на други здравствени работници на тој пациент на широка основа, а најчесто на национална.

Работната група за членот 29 заклучила дека воспоставувањето на таквите системи не би било можно во согласност со постојните законски правила за обработка на податоци за пациенти која се темели на членот 8 ставот 3 на Директивата за заштита на податоците. Меѓутоа, ако се претпостави дека постоењето на такви електронски системи на здравствени картони претставува значаен јавен интерес, тогаш тие би биле засновани на членот 8 став 4 на Директивата, кој налага постоење на изречна правна основа за нивно воспоставување што ги содржи и потребните заштитни мерки за безбедно работење на системот[150].

149 *На истото место*, член 8 став 4.

150 Работна група за членот 29 (2007), *Работен документ за обработката на лични податоци во врска со здравјето во електронските здравствени картони (EHR)*, РГ 131, Брисел, 15 февруари 2007 година.

4.2. Правилата за безбедност на обработката

Клучни точки

- Правилата за безбедност на обработката ја подразбираат обврската на контролорот и на обработувачот да спроведуваат соодветни технички и организациски мерки заради спречување на неовластено мешање во операциите на обработка на податоците.
- Потребното ниво на безбедност на податоците се определува со:
  - безбедносните карактеристики кои се достапни на пазарот за определен вид обработка;
  - трошоците;
  - чувствителноста на податоците кои се обработуваат.
- Безбедната обработка на податоците е дополнително заштитена со општата должност на сите лица, контролори и обработувачи, да ја осигурат доверливоста на податоците.

Според тоа, обврската на контролорите и обработувачите да ги применуваат соодветните мерки за осигурување безбедност на податоците е содржана во **законодавството на Советот на Европа за заштита на податоците** како и во **законодавството на Европската Унија за заштита на податоците**.

4.2.1. Елементи на безбедноста на податоците

Според релевантните одредби на **правото на Европската Унија**:

> *„Државите-членки утврдуваат дека контролорот мора да ги спроведе соодветните технички и организациски мерки за заштита на личните податоци од случајно и од незаконско уништување или од нивно случајно губење, преправање, неовластено откривање или пристап, особено кога*

обработката вклучува пренос на податоци преку мрежа и заштита од какви било незаконски облици на обработка"[151].

Слична одредба постои и **според правото на Советот на Европа**:

„Мора да се преземат соодветни безбедносни мерки за заштита на личните податоци кои се зачувани во автоматизирани податочни датотеки од случајно или неовластено уништување или случајно губење, како и од неовластен пристап, препрaвање или ширење"[152].

Често пати постојат и индустриски, национални и меѓународни стандарди кои се утврдени за безбедна обработка на податоци. На пример, Европскиот печат за приватност (ЕПП) е проект на Трансевропската телекомуникациска мрежа (ТТМ) на Европската Унија кој ги истражува можностите за сертифицирање на производите, особено на софтверот, во согласност со европското законодавство за заштита на податоците. Европската агенција за мрежна и информациска безбедност (ЕАМИБ) е основана заради зголемување на способноста на Европската Унија, на државите-членки на Европската Унија и на деловната заедница за спречување, решавање и одговарање на проблеми со мрежната и информациската безбедност[153]. Европската агенција за мрежна и информациска безбедност редовно објавува анализи во врска со актуелните безбедносни закани и советува за нивно решавање.

Безбедноста на податоците не се постигнува само со примена на правилната опрема – хардвер и софтвер. Таа исто така налага соодветни внатрешни организациски правила. Таквите внатрешни правила во идеален случај се занимаваат со следните прашања:

- Редовно информирање на сите вработени за правилата за безбедност на податоците и нивните обврски во согласност со законодавството за заштита на податоците, особено во поглед на нивната обврска за доверливост;

- јасна поделба на одговорностите и јасен приказ на компетенциите во поглед на обработката на податоците, а особено во поглед на одлуките за обработка на лични податоци и за пренос на податоците до трети лица;

151 Директива за заштита на податоците, член 17 став 1.

152 Конвенција бр. 108, член 7.

153 Регулатива (ЕЗ) Бр. 460/2004 на Европскиот парламент и на Советот од 10 март 2004 година за основање на Европската агенција за мрежна и информациска безбедност, Сл. весник 2004 L 77.

- употреба на лични податоци само според упатствата на надлежно лице или според општо утврдени правила;

- заштита на пристапот до локации и до хардверот и софтверот на контролорот или обработувачот, вклучувајќи проверки на овластувањето за пристап;

- осигурување дека овластувањето за пристап до лични податоци е доделено од надлежно лице и дека бара соодветна документација;

- автоматизирани записници за пристап до лични податоци по електронски пат и редовна проверка на таквите записници од страна на интерната надзорна служба;

- внимателно документирање на други облици на откривање, освен на автоматизиран пристап до податоци, со цел да се докаже дека не дошло до никакви незаконски преноси на податоци.

Понудата на соодветна обука и курсеви за безбедност на податоците за членови на персоналот исто така претставува важен елемент на делотворните мерки на претпазливост. Исто така е потребно да се определат постапки со кои ќе се провери дали соодветните мерки постојат само на хартија или се спроведуваат и функционираат во практиката (како што се внатрешните и надворешните ревизии).

Мерките за подобрување на нивото на безбедност на контролор или на обработувач вклучуваат; инструменти како што се службениците за заштита на лични податоци, едукација на вработените во врска со безбедноста, редовни ревизии, пенетрациски тестови и печати за квалитет.

Пример: Во предметот *I. v. Finland*[154], жалителката не успеала да докаже дека други вработени во болницата во која работела незаконски пристапиле до нејзините здравствени картони. Затоа, нејзината тужба поради повреда на нејзиното право на заштита на податоците била одбиена од страна на домашните судови. Европскиот суд за човековите права заклучил дека имало повреда на членот 8 на Конвенцијата, бидејќи системот на болницата за евиденција на здравствените картони „не овозможувал ретроактивно разјаснување на употребата на картоните на пациентите затоа што ги при-

154 ЕСЧП, *I. v. Finland*, Бр. 20511/03, 17 јули 2008 година.

кажувал само петте последни увида, а тие информации се бришеле откако датотеките ќе се врателе во архивата". Од пресудно значење за Судот бил фактот дека системот за евиденција на болниците очигледно не бил во согласност со законските барања на националното законодавство, на кој домашните судови не му придале доволна важност.

Известувања во случај на повреда на податоците

Во законодавството за заштита на податоците на неколку држави-членки е внесен нов инструмент за справување со нарушувањата на безбедноста на податоците: обврската на давателите на електронски комуникациски услуги да ги известуваат потенцијалните жртви и надзорните органи во случај на повреда на податоците. За давателите на телекомуникациски услуги тоа е обврзувачко во согласност со правото на Европската Унија[155]. Со известувањата на субјектите на податоците во случај на повреда на податоците, треба да се избегне штетата: со известувањата во случај на повреда на податоците и за нивните можни последици се намалува ризикот од негативни последици за субјектите на податоците. Во случаи на тешка небрежност и давателите на услуги можат парично да се казнат.

Потребно ќе биде однапред да се воспостават внатрешни постапки за делотворно управување и известување за повреди на безбедноста, бидејќи временскиот рок за обврската за известување на субјектите на податоците и/или надзорниот орган, според националното законодавство, обично е прилично краток.

4.2.2. Доверливост

Според правото на Европската Унија, безбедната обработка на податоците дополнително е заштитена со општата обврска на сите лица, контролори или обработувачи да ја обезбедат доверливоста на податоците.

155 Види ја Директивата 2002/58/ЕЗ на Европскиот парламент и на Советот од 12 јули 2002 година во врска со обработката на личните податоци и заштитата на приватноста во електронскиот комуникациски сектор, (*Директива за приватност и електронски комуникации*), Сл. весник 2002 L 201, член 4 став 3, како што е изменета со Директивата 2009/136/ЕЗ на Европскиот парламент и на Советот од 25 ноември 2009 година со која се изменува Директивата 2002/22/ЕЗ за универзална услуга и права на корисниците во врска со електронските комуникациски мрежи и услуги; види ја исто така Директивата 2002/58/ЕЗ во врска со обработката на личните податоци и заштитата на приватноста во електронскиот комуникациски сектор, како и Регулативата (ЕЗ) Бр. 2006/2004 за соработка помеѓу националните органи одговорни за спроведување на законодавството за заштита на потрошувачите, Сл. весник 2009 L 337.

Пример: Вработена во осигурителна компанија на работа прима телефонски повик од лице кое тврди дека е клиент и бара информации во врска со неговиот договор за осигурување.

Со оглед на тоа дека вработената е должна да ги чува во тајност податоците на клиентите, таа мора да примени барем минимални мерки за безбедност пред откривање на лични податоци. Таа можела да го стори тоа, на пример, така што ќе му понуди на клиентот возвраќање на повикот на телефонскиот број кој бил забележан во неговото досие.

Членот 16 на Директивата за заштита на податоците се однесува на доверливоста само во рамките на односот меѓу контролорот и обработувачот. Прашањето дали контролорите се должни да ги чуваат податоците во тајност, во смисла дека не смеат да им ги откриваат на трети лица, е уредено во членовите 7 и 8 на Директивата.

Обврската за доверливост не се однесува на ситуации во кои податоците ги дознава лице во својство на поединец, а не во својство на вработено лице на контролорот или обработувачот. Во тој случај не се применува членот 16 на Директивата за заштита на податоците бидејќи, всушност, употребата на лични податоци од страна на поединци во целост се иззема од областа на примена на Директивата каде што таквата употреба е во границите на таканаречениот исклучок за домашна употреба[156]. Исклучок за домашна употреба претставува употребата на лични податоци „од страна на физичко лице во текот на активности исклучиво заради лични активности или активности во домот[157]. Меѓутоа, по одлуката на Судот на правдата на Европската Унија во предметот *Bodil Lindqvist*[158], таквиот исклучок треба да се толкува ограничено, особено во поглед на откривањето на податоците. Поточно, исклучокот за домашна употреба не се проширува на објавувањето лични податоци на неограничен број корисници на интернет (за повеќе детали во врска со овој предмет, види ги поглавјата 2.1.2., 2.2., 2.3.1. и 6.1.).

Според правото на Советот на Европа, обврската за доверливост се подразбира во поимот за безбедност на податоците содржана во членот 7 на Конвенцијата бр. 108 во кој се обработува безбедноста на податоците.

156 Директива за заштита на податоците, член 3 став 2 втора алинеја.

157 *На истото место.*

158 СПЕУ, C-101/01, *Lindqvist*, 6 ноември 2003 година.

За обработувачите доверливоста значи дека тие смеат да употребуваат лични податоци што им биле доверени од страна на контролорот само во согласност со упатствата што им ги дал контролорот. За вработените на еден контролор или обработувач, доверливоста значи дека тие смеат да употребуваат лични податоци само во согласност со упатствата на нивните надлежни претпоставени лица.

Обврската за доверливост мора да биде содржана во секој договор меѓу контролорите и нивните обработувачи. Покрај тоа, контролорите и обработувачите мораат да преземат посебни мерки за утврдување на законска обврска за доверливост за нивните вработени. Тоа обично се постигнува со вклучување на одредби за доверливост во договорот за вработување на вработеното лице.

Повредата на професионалните обврски за доверливост е казнива според кривичното право во многу држави-членки на Европската Унија и договорни страни на Конвенцијата бр. 108.

4.3. Правилата за транспарентност на обработката

Клучни точки

- Пред почетокот на обработката на личните податоци, контролорот мора барем да го информира субјектот на податоците за идентитетот на контролорот и за целта на обработката на податоците, освен ако тоа лице веќе ја поседува таа информација.
- Ако податоците се прибираат од страна на трети лица, обврската за давање информации не се применува во случај кога:
  - обработката на податоците е пропишана со закон;
  - давањето информации се покаже како невозможно или бара несразмерни напори.
- Пред почетокот на обработката на личните податоци, контролорот мора, дополнително:
  - да го извести надзорниот орган за својата намера да спроведе операција на обработка;

- да наложи интерна документација на обработката од страна на независен службеник за заштита на личните податоци, ако со националното законодавство е пропишана таква постапка.

Начелото за правична обработка бара транспарентност на обработката. За таа цел, со **правото на Советот на Европа** е пропишано дека секое лице мора да е во можност да го утврди постоењето на датотеки за обработка на податоците, нивната цел и одговорниот контролор[159]. На националното законодавство му е препуштено утврдувањето на начинот на кој би требало да се постигне тоа. **Правото на Европската Унија** е поконкретно, па ја осигурува транспарентноста за субјектот на податоците преку обврската на контролорот да го информира тоа лице, а за општата јавност преку известувања.

Во националното законодавство на двата правни система може да постојат исклучоци и ограничувања од обврските за транспарентност на контролорот ако таквото ограничување претставува мерка која е неопходна за заштита на одредени јавни интереси или за заштита на субјектот на податоците или на правата и слободите на други лица, сè додека тоа е нужно во едно демократско општество[160]. Таквите исклучоци можат, на пример, да бидат потребни во смисла на кривичните истраги, но можат да бидат оправдани и во други околности.

4.3.1. Информација

Во согласност со правото на Советот на Европа како и во согласност со правото на Европската Унија, контролорите што ги водат постапките за обработка се должни однапред да го информираат субјектот на податоците за својата намера за обработка[161]. Таа обврска не треба да се почитува дури откако ќе биде поднесено барање од страна на субјектот на податоците, туку контролорот тоа мора да го стори проактивно, без оглед на тоа дали субјектот на податоците покажал интерес за информирањето или не.

Содржина на информацијата

Информацијата мора да ја содржи целта на обработката, како и идентитетот и податоците за контакт на контролорот[162]. Според Директивата за заштита

159 Конвенција бр. 108, член 8 точка (а).

160 *На истото место*, член 9 став 2; и Директива за заштита на податоците, член 13 став 1.

161 Конвенција бр. 108, член 8 точка (а); и Директива за заштита на податоците, членови 10 и 11.

162 Конвенција бр. 108, член 8 точка (а); и Директива за заштита на податоците, член 10 точки (а) и (б).

на податоците, потребно е да се дадат дополнителни информации ако „тие се неопходни, имајќи ги предвид посебните околности под кои се прибираат податоците, за да се гарантира правична обработка во однос на субјектот на податоците". Во членовите 10 и 11 на Директивата се утврдени, меѓу другото, категориите на податоците кои се обработуваат и корисниците на таквите податоци, како и постоењето на правото на пристап до и правото на исправка на податоците. Ако податоците се прибираат од страна на субјектот на податоците, треба да се дадат информации во врска со тоа дали давањето одговори на прашањата е задолжително или доброволно, како и за можните последици на недавањето одговор[163].

Од аспект на **правото на Советот на Европа**, давањето такви информации може да се смета за добра практика во рамките на начелото за правична обработка, а со тоа и за составен дел на правото на Советот на Европа.

Во согласност со начелото за правична обработка, информациите треба да бидат лесно разбирливи за субјектите на податоците. Мора да се употребува јазик што е соодветен за корисниците. Нивото и видот на употребениот јазик мора да се разликуваат во зависност од тоа дали информациите се наменети, на пример, за возрасни лица или за деца, за јавноста или за научни и стручни лица.

Некои субјекти на податоците ќе сакаат само накратко да бидат информирани за тоа како и зошто се обработуваат нивните податоци, додека други лица ќе бараат детално објаснување. Начинот на кој може да се урамнотежи тој аспект на правично информирање е разгледан во мислењето на Работната група за членот 29, која се залага за идејата за таканаречените слоевити известувања[164], овозможувајќи им на субјектите на податоците да одлучат каков степен на исцрпност на информацијата претпочитаат.

Време на давање информација

Директивата за заштита на податоците содржи малку поразлични одредби за времето на давање на информацијата, во зависност од тоа дали податоците се прибрани од субјектот на податоците (член 10) или од трета страна (член 11). Ако податоците се прибираат од субјектот на податоците, информацијата треба да се обезбеди најдоцна во времето на прибирањето. Ако податоците се прибирани

163 Директива за заштита на податоците, член 10 точка (в).

164 Работна група за членот 29 (2004), *Мислење 10/2004 за поусогласени одредби за информирање*, РГ 100, Брисел, 25 ноември 2004 година.

од трети лица, информацијата треба да се обезбеди најдоцна или во времето на евидентирањето на податоците од страна на контролорот или пред тие да бидат откриени на трето лице за првпат.

Исклучоци од обврската за информирање

Според правото на Европската Унија, постои општ исклучок од обврската за информирање на субјектот на податоците доколку тој е запознаен со работите[165]. Тоа се однесува на оние ситуации во кои субјектот на податоците, според околностите на случајот, веќе е запознаен со тоа дека контролор ги обработува неговите податоци за определена цел.

Во членот 11 на Директивата, кој се однесува на обврската за информирање на субјектот на податоците ако податоците не се добиени од него, исто така се вели дека таквата обврска не постои, особено во случаите на обработка за статистички цели или за целите на научното и историското истражување, ако:

- давањето на таквите информации е невозможно;
- бара несразмерен напор;
- евидентирањето или откривањето на податоците е изречно утврдено со закон.[166]

Само во членот 11 став 2 на Директивата за заштита на податоците се вели дека субјектите на податоците не треба да се информираат за постапките за обработка ако тие се пропишани со закон. Со оглед на општата правна претпоставка дека законот им е познат на лицата на кои се однесува, може да се смета дека ако податоците се прибрани од субјектот на податоците во согласност со членот 10 на Директивата, тоа лице е информирано. Но, со оглед на тоа дека познавањето на законот е само претпоставка, со членот 10 е пропишано дека начелото за правична обработка налага информирање на субјектот на податоците дури и ако обработката е пропишана со закон, а особено затоа што информирањето на субјектот на податоците не претставува посебно оптоварување доколку податоците се прибрани директно од тоа лице.

Што се однесува до правото на Советот на Европа, Конвенцијата бр. 108 изречно ги предвидува исклучоците од нејзиниот член 8. Сепак, исклучоците наведени во

165 Директива за заштита на податоците, членови 10 и 11 став 1.

166 *На истото место*, Уводна изјава бр. 40 и член 11 став 2.

членовите 10 и 11 на Директивата за заштита на податоците може да се сметаат за примери на добра практика за исклучоците од членот 9 на Конвенцијата бр. 108.

Различни начини на давање информација

Идеален начин на информирање би било поединечно обраќање до секој субјект на податоците, по писмен или устен пат. Ако податоците се прибираат од субјектот на податоците, давањето информации би требало да оди рака под рака со прибирањето. Меѓутоа, информациите исто така може да бидат дадени и по пат на нивно соодветно објавување, особено ако податоците се прибираат од страна на трети лица, имајќи ги предвид очигледните практични тешкотии за лично контактирање на субјектите на податоците.

Еден од најделотворните начини на давање информации е по пат на соодветни информациски клаузули на интернет-страницата на контролорот, како што е политиката за приватност на веб-страница. Меѓутоа, голем дел од населението не користи интернет, па тоа би требало да биде вклучено во политиката на информирање на некоја компанија или јавен орган.

4.3.2. Известување

Според националното законодавство, контролорите можат да бидат обврзани да го известат надлежниот надзорен орган за нивните постапки за обработка, заради нивно објавување. Евентуално, националното законодавство може да пропишува дека контролорите можат да вработат службеник за обработка на личните податоци, кој пред сè е одговорен за водење регистар во врска со постапките за обработка кои ги спроведува контролорот[167]. Тој интерен регистар треба да ѝ се стави на располагање на јавноста на нејзино барање.

Пример: Во едно известување и во документацијата на секој интерен службеник за заштита на лични податоци мора да бидат опишани главните карактеристики на предметната операција на обработка. Тоа вклучува информации за контролорот, за целите на обработката, за правната основа на обработката, за категориите на податоците кои се обработуваат, за евентуални трети лица кои се корисници на податоците и за тоа дали постои намера за прекугранично пренос на податоците, и ако постои, каков е.

167 *На истото место*, член 18 став 2 втора алинеја.

Надзорниот орган мора да ги објави известувањата во облик на посебен регистар. За да се исполни целта на овој регистар, пристапот до него треба да биде едноставен и бесплатен. Истото важи и за документацијата за која е задолжен службеникот за заштита на личните податоци на контролорот.

Исклучоците од обврските за известување на надлежниот надзорен орган или за вработување на интерен службеник за заштита на податоците можат да бидат пропишани со национално законодавство во врска со постапките за обработка кои не претставуваат посебен ризик за субјектите на податоците. Тие исклучоци се наведени во членот 18 став 2 на Директивата за заштита на податоците[168].

4.4. Правилата за унапредување на усогласеноста

Клучни точки

- Развивајќи го начелото за одговорност, Директивата за заштита на податоците споменува неколку инструменти за унапредување на усогласеноста:
  - претходна проверка на планирани постапки за обработка од страна на национален надзорен орган;
  - службеници за заштита на податоците кои на контролорот му ги нудат своите посебни стручни знаења во областа на заштитата на податоците;
  - правила на однесување со кои поточно се утврдуваат постојните правила за заштита на податоците за примена во некоја општествена гранка, а особено во деловното работење.
- Правото на Советот на Европа предвидува слични инструменти за унапредување на усогласеноста во неговата Препорака за профилирање.

4.4.1. Претходна проверка

Во согласност со членот 20 на Директивата за заштита на податоците, надзорниот орган мора да ги провери постапките за обработка за кои е веројатно дека

168 *На истото место*, член 18 став 2 прва алинеја.

претставуваат посебни ризици за правата и за слободите на субјектите на податоците – било да е тоа поради целта или поради околностите на обработката – пред почетокот на обработката. Со националното законодавство мора да се определи кои постапки за обработка можат да подлежат на претходна проверка. Таквата проверка може да доведе до забрана на операцијата на обработка или до налог за измена на карактеристиките во предложениот план на операциите на обработка. Целта на членот 20 на Директивата е да осигури дека воопшто нема да дојде до непотребно ризична обработка, бидејќи надзорниот орган е овластен да ги забрани таквите постапки. За да биде делотворен таквиот механизам, надзорниот орган навистина мора да биде известен. Со цел да се осигури дека контролорите ја исполнуваат својата обврска за известување, надзорните органи мора да имаат овластување за примена на средства за присилба, како што е изрекувањето парични казни за контролорите.

Пример: Ако едно претпријатие врши постапки за обработка кои, според националното законодавство, подлежат на претходна проверка, тогаш тоа мора да поднесе документација за планираните постапки за обработка до надзорниот орган. Претпријатието не смее да започне постапки за обработка пред да добие позитивен одговор од страна на надлежниот орган.

Во некои држави-членки, со националното законодавство алтернативно е пропишано дека постапките за обработка можат да започнат ако надзорниот орган не реагирал во определен временски рок, на пример, од три месеци.

4.4.2. Службеници за заштита на личните податоци

Директивата за заштита на податоците остава можност во националното законодавство да се пропише дека контролорите можат да именуваат службеник кој ќе дејствува како службеник за заштита на личните податоци[169]. Целта е да се осигури дека постапките за обработка нема да ги загрозуваат правата и слободите на субјектите на податоците[170].

Пример: Во Германија, во согласност со членот 4ѓ став 1 на Сојузниот закон за заштита на податоците (*Bundesdatenschutzgesetz*), претпријатијата во приватна

169 *На истото место*, член 18 став 2 втора алинеја.

170 *На истото место*.

сопственост мораат да именуваат интерен службеник за заштита на личните податоци ако постојано вработат десет или повеќе лица за автоматизирана обработка на личните податоци.

За да се постигне таа цел, службеникот треба да има извесен степен на независност во организацијата на контролорот, како што е изречно истакнато во Директивата. Со цел да се поддржи делотворното фукнционирање на неговата служба, потребни се силни работнички права со кои вработените ќе се заштитат од некои евентуалности како што е неоправдан отказ.

Заради унапредување на усогласеноста со националното законодавство за заштита на податоците, поимот за интерен службеник за заштита на личните податоци е усвоен и во некои од препораките на Советот на Европа[171].

4.4.3. Правилата на однесување

Заради унапредување на усогласеноста, деловните и другите сектори можат да составаат детални правила со кои ќе ги регулираат своите вообичаени постапки за обработка, кодификувајќи ја притоа најдобрата практика. Стручното знаење на членовите на тој сектор ќе помогне во пронаоѓањето на практични решенија кои најверојатно ќе бидат прифатени. Според тоа, државите-членки, како и Европската комисија, се поттикнуваат да го унапредуваат создавањето правила на однесување со цел да се придонесе за правилно спроведување на националните одредби кои државите-членки ги усвојуваат во согласност со директивата, земајќи ги предвид посебните карактеристики на различните сектори[172].

Со цел да се осигури дека таквите правила на однесување се во согласност со националните одредби кои се усвоени во согласност со Директивата за заштита на податоците, државите-членки мораат да воспостават постапка за евалуација на правилата. Во таа постапка обично е потребно да се вклучат националниот орган, трговски здруженија и други тела кои претставуваат други категории на контролори[173].

Предлозите за правила на Заедницата и измените или проширувањата на постојните правила на Заедницата може да се достават до Работната група за членот

171 Види, на пример, Препораки за профилирањето, член 8.3.

172 Види ја Директивата за заштита на податоците, член 27 став 1.

173 *На истото место*, член 27 став 2.

29 заради евалуација. Откако Работната група ќе ги одобри, Европската комисија може да се погрижи за соодветно објавување на таквите правила[174].

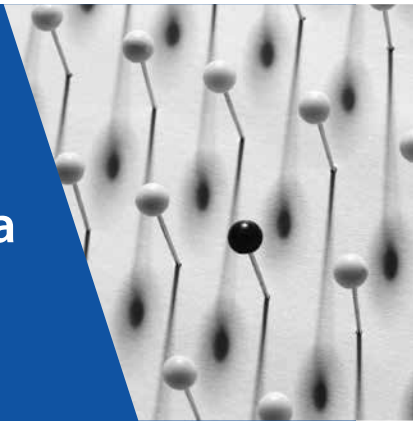
Пример: Европската федерација за директен и интерактивен маркетинг (FEDMA) развила Европски кодекс на практиката на употребата на личните податоци во директен маркетинг. Кодексот бил успешно доставен до Работната група за членот 29. Во 2010 година на Кодексот му е додаден прилог кој се однесува на електронските маркетиншки комуникации[175].

174 *На истото место,* член 27 став 3.

175 Работна група за членот 29 (2010), *Мислење 4/2010 за Европскиот кодекс на однесување на FEDMA за употреба на личните податоци во директен маркетинг,* РГ 174, Брисел, 13 јули 2010 год.

5

Правата на субјектот на податоците и нивното спроведување



Европска Унија	Обработени прашања	Совет на Европа
Право на пристап		
Директива за заштита на податоците, член 12 СПЕУ, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, 7 мај 2009 год.	Право на пристап до сопствените податоци	Конвенција бр. 108, член 8 точка (б)
	Право на исправка, бришење или блокирање	Конвенција бр. 108, член 8 точка (в) ЕСЧП, *Cemalettin Canli v. Turkey*, Бр. 22427/04, 18 ноември 2008 год. ЕСЧП, *Segerstedt-Wiberg and Others v. Sweden*, Бр. 62332/00, 6 јуни 2006 год. ЕСЧП, *Ciubotaru v. Moldova*, Бр. 27138/04, 27 април 2010 год.
Право на приговор		
Директива за заштита на податоците, член 14 став 1 точка (а)	Право на приговор на субјектот на податоците поради неговата конкретна ситуација	Препорака за профилирањето, член 5.3.

Директива за заштита на податоците, член 14 став 1 точка (б)	Право на приговор против натамошната употреба на податоците за цели на директен маркетинг	Препорака за директен маркетинг, член 4.1.
Директива за заштита на податоците, член 15	Право на приговор против автоматизирани одлуки	Директива за профилирањето, член 5.5.
Независен надзор		
Повелба, член 8 став 3 Директива за заштита на податоците, член 28 Институции на ЕУ Регулатива за заштита на податоците, Поглавје V Регулатива за заштита на податоците СПЕУ, C-518/07, *European Commission v. Federal Republic of Germany*, 9 март 2010 год. СПЕУ, C-614/10, *European Commission v. Republic of Austria*, 16 октомври 2012 год. СПЕУ, C-288/12, *European Commission v. Hungary*, 8 април 2014 год.	Национални надзорни органи	Конвенција бр. 108, Дополнителен протокол, член 1
Правни средства и санкции		
Директива за заштита на податоците, член 12	Барање до контролорот	Конвенција бр. 108, член 8 точка (б)
Директива за заштита на податоците, член 28 став 4 Институции на ЕУ, Регулатива за заштита на податоците, член 32 став 2	Барања поднесени до надзорен орган	Конвенција бр. 108, Дополнителен протокол, член 1 став 2 точка (б)
Повелба, член 47	Судови (општо)	Европска конвенција за човековите права, член 13
Директива за заштита на податоците, член 28 став 3	Национални судови	Конвенција бр. 108, Дополнителен протокол, член 1 став 4
ДФЕУ, член 263 став 4 Институции на ЕУ, Регулатива за заштита на податоците, член 32 став 1 ДФЕУ, член 267	СПЕУ	
	ЕСЧП	Европска конвенција за човековите права, член 34

Правни средства и санкции

Повелба, член 47 Директива за заштита на податоците, членови 22 и 23 СПЕУ, C-14/83, *Sabine von Colson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10 април1984 год. СПЕУ, C-152/84, *M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority*, 26 февруари 1986 год.	За повреди на националното законодавство за заштита на податоците	Европска конвенција за човековите права, член 13 (само за држави-членки на Советот на Европа) Конвенција бр. 108, член 10 ЕСЧП, *K.U. v. Finland*, Бр. 2872/02, 2 декември 2008 год. ЕСЧП, *Biriuk v. Lithuania*, Бр. 23373/03, 25 ноември 2008 год.
Институции на ЕУ, Регулатива за заштита на податоците, членови 34 и 49 СПЕУ, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 29 јуни 2010 год.	За повреди на правото на ЕУ од страна на институции и тела на ЕУ	

Делотворноста на правните прописи воопшто, а особено на правата на субјектите на податоците, во значителна мера зависи од постоењето на соодветни механизми за нивно спроведување. Во европското законодавство за заштита на податоците, субјектот на податоците мора да има право на заштита на своите податоци врз основа на националното законодавство. Со националното законодавство треба да се воспостават и независни надзорни органи кои ќе им помогнат на субјектите на податоците во остварувањето на нивните права и ќе ја надгледуваат обработката на личните податоци. Покрај тоа, правото на реална жалба, кое се гарантира со Европската конвенција за човековите права и со Повелбата, значи дека правните средства мораат да бидат достапни до секое лице.

5.1. Правата на субјектите на податоците

Клучни точки

- Секој има право во согласност со националното законодавство да побара од контролорот да го информира дали се врши обработка на неговите податоци.
- Во согласност со националното законодавство субјектите на податоците имаат право на:

- пристап до сопствените податоци од контролор кој ги обработува таквите податоци;
- исправка (или блокирање, како што е соодветно) од страна на контролорот кој ги обработува нивните податоци, ако податоците се неточни;
- бришење или блокирање на своите податоци, во зависност од случајот, од страна на контролор ако контролорот незаконски ги обработува податоците.

- Покрај тоа, субјектите на податоците имаат право на приговор до контролорите во врска со:
  - автоматизирани одлуки (кои се донесени врз основа на лични податоци што се обработени само автоматски);
  - обработка на своите податоци ако тоа доведува до несразмерни резултати;
  - употреба на своите податоци за цели на директен маркетинг.

5.1.1. Правото на пристап

Според правото на Европската Унија, во членот 12 на Директивата за заштита на податоците, содржани се елементите на правото на субјектот на податоците на пристап до податоците, вклучувајќи го правото да добие од контролорот „потврда за тоа дали податоците што се однесуваат на него се обработуваат и информации барем во врска со целите на обработката, категориите на односните податоци, како и на корисниците или категориите на корисниците на кои им се откриваат податоците", како и „исправка, бришење или блокирање на податоците, чијашто обработка не е усогласена со одредбите од оваа Директива, особено поради нецелосната или неточна природа на податоците".

Во правото на Советот на Европа постојат истите права кои мора да бидат пропишани со домашен закон (член 8 на Конвенцијата бр. 108). Во неколку препораки на Советот на Европа се користи поимот 'пристап' заедно со опис на различните видови на правото на пристап и предлог за нивно спроведување во домашното законодавство на ист начин како што е наведено во параграфот погоре.

Во согласност со членот 9 на Конвенцијата бр. 108 и членот 13 на Директивата за заштита на податоците, обврската на контролорите да одговорат на барањето на

субјектот на податоците може да се ограничи како последица на превладувачките правни интереси на другите. Превладувачките правни интереси можат да ги вклучуваат правните интереси како што се националната безбедност, јавната безбедност и кривичниот прогон, како и приватните интереси кои се поважни од интересите за заштита на податоците. Исклучоците или ограничувањата мора да бидат неопходни во едно демократско општество и да бидат сразмерни со целта кон која се насочени. Во многу исклучителни случаи, како на пример поради медицински индикации, заштитата на субјектот на податоците може сама по себе да налага ограничување на транспарентноста. Тоа особено се однесува на ограничувањето на правото на пристап на секој субјект на податоците.

Секогаш кога податоците се обработуваат исклучиво за целите на научното истражување или за статистички цели, Директивата за заштита на податоците овозможува ограничување на правата на пристап со националното законодавство. Меѓутоа, мора да постојат соодветни законски гаранции. Поточно, треба да се осигури дека нема да бидат преземени никакви мерки или одлуки во однос на кој било конкретен поединец во смисла на таквата обработка на податоците и дека „не постои очигледен ризик од повреда на приватноста на субјектот на податоците“[176]. Слични одредби се содржани во членот 9 став 3 на Конвенцијата бр. 108.

Право на пристап до сопствените податоци

Според правото на Советот на Европа, правото на пристап до сопствените податоци изречно е потврдено со членот 8 на Конвенцијата бр. 108. Европскиот суд за човековите права постојано тврдел дека постои право на пристап до информации во врска со сопствените податоци кои ги чуваат или ги користат други лица и дека тоа право произлегува од потребата за почитување на приватниот живот[177]. Во предметот *Leander*[178], Европскиот суд за човековите права заклучил дека правото на пристап до лични податоци кои се чуваат од страна на државни органи сепак може да биде ограничено во определени околности.

Според правото на Европската Унија, правото на пристап до сопствените податоци изречно е потврдено со членот 12 од Директивата за заштита на податоците и како основно право во членот 8 став 2 на Повелбата.

176 Директива за заштита на податоците, член 13 став 2.

177 ЕСЧП, *Gaskin v. the United Kingdom*, Бр. 10454/83, 7 јули 1989 год.; ЕСЧП, *Odièvre v. France* [GC], Бр. 42326/98, 13 февруари 2003 год.; ЕСЧП, *K.H. and Others v. Slovakia*, Бр. 32881/04, 28 април 2009 год.; ЕСЧП, *Godelli v. Italy*, Бр. 33783/09, 25 септември 2012 год.

178 ЕСЧП, *Leander v. Sweden*, Бр. 9248/81, 26 март 1987 год.

Членот 12 точка (а) на Директивата пропишува дека државите-членки треба да му го гарантираат на секој субјект на податоците правото на пристап до неговите лични податоци и на добивање информации. Поточно, секој субјект на податоците има право да добие од контролорот потврда за тоа дали податоците што се однесуваат на него се обработуваат и информации барем во врска со следното:

- целите на обработката;
- категориите на односните податоци;
- податоците што се обработуваат;
- корисниците или категориите на корисниците на кои им се откриваат податоците;
- сите достапни информации за изворот на податоците што се обработуваат;
- во случај на автоматизирани одлуки, логиката што стои зад секоја автоматска обработка на податоците.

Во националното законодавство може да се вклучат дополнителни информации што треба да ги даде контролорот, како на пример наведувањето на правната основа за обработка на податоците.

Пример: Пристапувајќи до сопствените лични податоци, лицето може да утврди дали податоците се точни. Затоа, неопходно е субјектот на податоците да биде информиран за категориите на обработените податоци, како и за содржината на податоците. Од таа причина, не е доволно контролорот едноставно да му каже на субјектот на податоците дека се обработуваат неговото име, адреса, датум на раѓање и области на интерес. Контролорот мора да му открие на субјектот на податоците дека се обработуваат „име: N.N.; на адреса: 1040 Виена, Шварценбергплац 11, Австрија; датум на раѓање: 10.10.1974 година; и област на интерес (според тоа што го изјавил субјектот на податоците): класична музика". Последната точка дополнително содржи информации за изворот на податоците.

Соопштенијата до субјектот на податоците за податоците што се обработуваат и за сите достапни индормации за нивниот извор мора да бидат дадени во разбирлива

форма, што значи дека контролорот можеби ќе треба подетално да му објасни на субјектот на податоците што обработува. На пример, обично не е доволно во одговорот на барање за пристап само да се наведат техничките кратенки или медицинските поими, дури и ако се чуваат само такви кратенки или поими.

Ако се достапни, информациите за изворот на податоците кои ги обработува контролорот треба да бидат содржани во одговорот на барањето за пристап. Оваа одредба треба да се разгледува во смисла на начелата за правичност и одговорност. Контролорот не смее да уништи информации за изворот на податоците за да не мора да ги открие, а не смее ниту да ги занемари вообичаените стандардни и признаени потреби за документација во областа на неговото работење. Ако контролорот не чува никаква документација за изворот на податоците кои се обработуваат, тоа најчесто значи дека тој не ги исполнил своите обврски во врска со правото на пристап.

Ако се вршат автоматизирани евалуации, треба да се објасни општата логика на евалуацијата, вклучувајќи ги и определените критериуми кои биле разгледани при евалуацијата на субјектот на податоците.

Во Директивата не е јасно опишано дали правото на пристап до информации се однесува на минатото и, ако е тоа случај, на кој период во минатото. Во тој поглед, како што е нагласено во судската практика на Судот на правдата на Европската Унија, правото на пристап до сопствените податоци не смее непотребно временски да се ограничува. Исто така, на субјектите на податоците треба да им се даде разумна можност да добијат информации за поранешни операции на обработка.

Пример: Во предметот *Rijkeboer*[179], од Судот на правдата на Европската Унија било побарано да утврди дали, во согласност со членот 12 точка (а) на Директивата, правото на поединецот на пристап до информации во врска со корисниците или категориите на корисниците на лични податоци и во врска со содржината на проследените податоци може да се ограничи на една година пред неговото барање за пристап.

За да утврди дали членот 12 точка (а) на Директивата допушта такво временско ограничување, Судот одлучи тој член да го толкува во смисла на целите на Директивата. Судот најпрвин истакнал дека правото на пристап е

179 СПЕУ, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 мај 2009 год.

неопходно за да му се овозможи на субјектот на податоците да го оствари своето право да добие исправка од контролорот, бришење или блокирање на неговите податоци (член 12 точка (б)), или известување до трети страни на кои им биле откриени податоците за исправката, бришењето или блокирањето (член 12 точка (в)). Правото на пристап е неопходно и за да му се овозможи на субјектот на податоците да го оствари своето право на приговор поради обработката на неговите лични податоци (член 14) или правото на тужба ако претрпи штета (членови 22 и 23).

Заради осигурување на практичното влијание на гореспоменатите одредби, Судот сметал дека „тоа право мора задолжително да се однесува на минатото. Во спротивно, субјектот на податоците не би можел ефективно да го оствари своето право на исправка, бришење или блокирање на податоците кои се сметаат за незаконити или неточни или на поведување судска постапка и добивање надомест за претрпена штета".

Правото на исправка, бришење и блокирање на податоците

„Секое лице мора да може да го оствари правото на пристап до податоците што се однесуваат на него, а кои се обработуваат, со цел да потврди, пред сè, дека податоците се точни и дека обработувањето е законито"[180]. Во согласност со овие начела, субјектите на податоците мора да имаат право според националното законодавство да добијат од контролорот исправка, бришење или блокирање на нивните податоци ако сметаат дека нивната обработка не е усогласена со одредбата на Директивата, особено поради нецелосната или неточна природа на податоците[181].

Пример: Во предметот *Cemalettin Canli v. Turkey*[182], Европскиот суд за човековите права утврдил повреда на членот 8 на Европската конвенција за човековите права во неточен полициски извештај во врска со кривична постапка.

Жалителот два пати бил вклучен во кривична постапка поради наводно членство во илегални организации, но никогаш не бил осуден. Кога бил

180 Директива за заштита на податоците, Уводна изјава 41.

181 *На истото место*, член 12 точка (б).

182 ЕСЧП, *Cemalettin Canli v. Turkey*, Бр. 22427/04, 18 ноември 2008 год., членови 33, 42 и 43; ЕСЧП, *Dalea v. France*, Бр. 964/07, 2 февруари 2010 год.

повторно уапсен и обвинет за друго кривично дело, полицијата поднела извештај до Кривичниот суд со наслов *„образец со информации за дополнителни кривични дела"*, во кој жалителот се појавувал како член на две илегални организации. Барањето на жалителот за измена на извештајот и на полициските записници било неуспешно. Европскиот суд за човековите права сметал дека информациите во полицискиот извештај потпаѓале во опфатноста на членот 8 на Европската конвенција за човековите права, бидејќи јавните информации исто така би можеле да потпаѓаат во опфатноста на 'приватен живот' ако биле систематски прибирани и зачувувани во датотеки на надлежните органи. Покрај тоа, полицискиот извештај бил неточен, а неговото составување и поднесување до Кривичниот суд не било во согласност со законот. Судот заклучил дека имало повреда на членот 8.

Пример: Во предметот *Segerstedt-Wiberg and Others v. Sweden*[183], жалителите биле поврзани со одредени либерални и комунистички политички партии. Тие се сомневале во тоа дека информации за нив биле чувани во безбедносните полициски досиеја. Европскиот суд за човековите права бил задоволен од фактот дека чувањето на односните податоци имало правна основа и било насочено кон легитимна цел. Во поглед на некои од жалителите, Европскиот суд за човековите права утврдил дека континуираното задржување на податоците претставувало несразмерно мешање во нивниот приватен живот. На пример, во случајот на г. Шмид, надлежните органи задржале информација дека во 1969 година наводно заговарал насилен отпор против полициската контрола за време на протести. Европскиот суд за човековите права утврдил дека тие информации не можеле да бидат од никаков интерес кој бил релевантен за националната безбедност, особено поради тоа што се однесувале на минатото. Европскиот суд за човековите права заклучил дека имало повреда на членот 8 на Конвенцијата во врска со четворица од петтемина жалители.

Во некои случаи доволно е субјектот на податоците едноставно да побара исправка, на пример, на правописни грешки во името, промена на адреса или на телефонски број. Меѓутоа, ако таквите барања се поврзани со правни прашања, како што е правниот идентитет на субјектот на податоците, или точното место на живеење заради достава на правни документи, барањата за исправка може да не бидат доволни, а контролорот може да биде овластен да побара доказ за

183 ЕСЧП, *Segerstedt-Wiberg and Others v. Sweden*, Бр. 62332/00, 6 јуни 2006, членови 89 и 90; исто така види, на пример: ЕСЧП, *M.K. v. France*, Бр. 19522/09, 18 април 2013 година.

наводните неточности. Со таквите барања на субјектот на податоците не смее да му се наметнува неразумен товар на докажување и на тој начин да се оневозможат субјектите на податоците да добијат исправка на нивните податоци. Европскиот суд за човековите права утврдил повреди на членот 8 на Европската конвенција за човековите права во неколку случаи во кои жалителот не бил во можност да ја оспори точноста на информациите што се чуваат во тајни регистри[184].

Пример: Во предметот *Ciubotaru v. Moldova*[185], жалителот не можел да го промени записот за своето етничко потекло во службената евиденција од молдавско на романско наводно поради тоа што не го поткрепил своето барање. Европскиот суд за човековите права сметал дека е прифатливо државите да побараат објективен доказ при запишувањето на етничкиот идентитет на поединецот. Ако таквото барање е засновано исклучиво на субјективни и непоткрепени основи, надлежните органи би можеле да го одбијат. Меѓутоа, барањето на жалителот не се засновало само на субјективното поимање на неговото етничко потекло туку тој ги навел своите врски со романската етничка група кои можеле објективно да се проверат, како на пример јазик, име, емпатија и друго. Меѓутоа, во согласност со домашното законодавство, од жалителот било побарано да обезбеди доказ дека неговите родители ѝ припаѓале на романската етничка група. Со оглед на историската ситуација во Молдавија, таквото барање би создало ненадминлива пречка за записот на етнички идентитет кој се разликувал од тој што бил запишан во врска со неговите родители од страна на советските власти. Бидејќи оневозможила да се провери тврдењето на жалителот во смисла на докази што можат објективно да се проверат, државата не ја исполнила својата позитивна обврска да го осигури почитувањето на неговиот приватен живот во ефективна смисла. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Во текот на граѓански спор или во постапка пред јавен орган во која се одлучува за точноста на податоците, субјектот на податоците може да побара во неговата податочна датотека да се внесе податок или забелешка со кои ќе се нагласи дека точноста е оспорена и дека се чека службена одлука. Во тој период, контролорот на податоците не смее да ги претставува податоците како сигурни или конечни, особено не на трети страни.

184 ЕСЧП, *Rotaru v. Romania*, Бр. 28341/95, 4 мај 2000 година.

185 ЕСЧП, *Ciubotaru v. Moldova*, Бр. 27138/04, 27 април 2010 година, членови 51 и 59.

Барањето на субјектот на податоците за бришење на податоците често е засновано на тврдење дека обработката на податоците нема законска основа. Такви тврдења обично се појавуваат ако согласноста е повлечена, или ако определени податоци повеќе не се потребни за исполнување на целта на собирањето на податоците. Товарот на докажување дека обработката на податоците е законита ќе го сноси контролорот на податоците, бидејќи тој е одговорен за законитоста на обработката. Според начелото за одговорност, контролорот мора во секое време да може да докаже дека постои цврста правна основа за обработка на податоците. Во спротивно обработката мора да биде прекината.

Ако обработката на податоците се оспорува поради тоа што податоците наводно не се точни или се незаконито обработени, субјектот на податоците, во согласност со начелото за правична обработка, може да побара блокирање на спорните податоци. Тоа значи дека податоците не се избришани, туку дека контролорот мора да се воздржи од употреба на податоците во текот на периодот на блокирањето. Тоа би било особено неопходно ако континуираната употреба на неточни или незаконски чувани податоци може да му наштети на субјектот на податоците. Со националното законодавство треба да се осигурат повеќе детали за тоа кога може да настане обврската за блокирање на употребата на податоците и начинот на кој треба да се исполни.

Субјектите на податоците имаат дополнително право да добијат од контролорот известување до трети страни за секое блокирање, исправка или бришење, ако ги примиле податоците пред операциите на обработка. Бидејќи контролорот требало да го документира откривањето на податоците на трета страна, треба да постои можност да се идентификуваат корисниците на податоците и да се побара бришење. Меѓутоа, ако податоците во меѓувреме биле објавени, на пример, на интернет, може да биде невозможно тие да се избришат во сите случаи, бидејќи не е возможно да се најдат корисниците на податоците. Во согласност со Директивата за заштита на податоците, задолжително треба да се контактираат корисниците на податоците поради исправка, бришење или блокирање на податоците, „освен ако не се покаже дека тоа е невозможно и дека вклучува несразмерен напор“[186].

5.1.2. Правото на приговор

Правото на приговор го вклучува правото на приговор поради автоматизирани индивидуални одлуки, правото на приговор поради конкретната ситуација на

186 Директива за заштита на податоците, член 12 точка (в), последна полуреченица.

субјектот на податоците и правото на приговор поради употребата на податоците за цели на директен маркетинг.

Правото на приговор против автоматизирани индивидуални одлуки

Автоматизирани одлуки се одлуки кои се донесени со употреба на лични податоци што се обработени исклучиво со автоматски средства. Ако за таквите одлуки е веројатно дека значително ќе влијаат на животите на некои поединци затоа што се однесуваат, на пример, на кредитната способност, ефектот на работа, однесувањето или доверливосат, неопходна е посебна заштита за да се избегнат несоодветни последици. Со Директивата за заштита на податоците, пропишано е дека автоматизираните одлуки не треба да определуваат прашања кои се важни за поединците и налага дека поединецот треба да има право на преиспитување на автоматизираната одлука[187].

Пример: Важен практичен пример на автоматизираното донесување одлуки е оценувањето на кредитната способност. Со цел побрзо да се донесе одлука во врска со кредитната способност на иден клиент, определени податоци, како што се занимањето и семејната состојба се прибираат од клиентот и се комбинираат со податоци за лицето добиени од други извори, како што се системите за кредитни информации. Тие податоци автоматски се внесуваат во алгоритамот за оценување што ја пресметува вкупната вредност која ја претставува кредитната способност на потенцијален клиент. На тој начин лице кое е вработено во компанијата за неколку секунди може да одлучи дали субјектот на податоците е прифатлив како клиент.

Сепак, според Директивата, државите-членки треба да предвидат дека лицето може да биде подложено на автоматизирана индивидуална одлука ако интересите на субјектот на податоците или не се загрозени затоа што одлуката била во полза на субјектот на податоците или се заштитени со други соодветни средства[188]. Правото на приговор против автоматизираните одлуки исто така е содржано во правото на **Советот на Европа**, како што може да се види во Препораката за профилирањето[189].

187 *На истото место*, член 15 став 1.

188 *На истото место*, член 15 став 2.

189 Препорака за профилирањето, член 5 став 5.

Правото на приговор на субјектот на податоците поради неговата конкретна ситуација

Не постои општо право на приговор на субјектите на податоците поради обработката на нивните податоци[190]. Меѓутоа, според членот 14 точка (а) на Директивата за заштита на податоците, субјектот на податоците има право да се жали врз присилна легитимна основа што се однесува на неговата конкретна ситуација. Слично право е признаено во Препораката за профилирањето на Советот на Европа[191]. Целта на таквите одредби е да се постигне најдобрата рамнотежа меѓу правата на субјектот на податоците на заштита на неговите права и легитимните права на другите во постапката на обработка на податоците на субјектот.

Пример: Една банка седум години чува податоци за своите клиенти кои не ги исполнувале кредитните обврски. Еден клиент чии податоци се чуваат во базата на податоци бара нов кредит. Се проверува базата на податоци, се оценува финансиската ситуација и на клиентот не му се одобрува кредит. Меѓутоа, клиентот може да поднесе приговор на евидентирањето на неговите лични податоци во базата на податоци и да побара бришење на податоците ако може да докаже дека неисполнувањето на кредитните обврски било само резултат на грешка која била исправена веднаш откако клиентот дознал за неа.

Резултатот на успешниот приговор е тоа дека контролорот веќе не смее да ги обработува односните податоци. Меѓутоа, операциите за обработка на податоците на субјектите на податоците пред приговорот и понатаму се законити.

Правото на приговор поради натамошната употреба на податоците за цели на директен маркетинг

Со членот 14 точка (б) на Директивата за заштита на податоците пропишано е посебно право на приговор против употребата на податоците на некое лице за целите на директен маркетинг. Такво право е утврдено и во Препораката на

190 Види исто така ЕСЧП, *M.S. v. Sweden*, Бр. 20837/92, 27 август 1997 год., каде биле поднесени медицински податоци без согласност или можност за приговор; или ЕСЧП, *Leander v. Sweden*, Бр. 9248/81, 26 март 1987 год.; или ЕСЧП, *Mosley v. the United Kingdom*, Бр. 48009/08, 10 мај 2011 год.

191 Препорака за профилирањето, член 5 став 3.

Советот на Европа за директен маркетинг[192]. Таков вид на приговор се поднесува пред да може податоците да им станат достапни на трети страни за целите на директен маркетинг. Затоа, субјектот на податоците мора да има можност да поднесе приговор пред преносот на податоците.

5.2. Независен надзор

Клучни точки

- За да се осигури делотворна заштита на податоците, со националното законодавство мора да бидат воспоставени независни надзорни органи.
- Националните надзорни органи мора да дејствуваат сосема независно, што мора да се гарантира со основачкото право и да дојде до израз во посебната организациска структура на надзорниот орган.
- Надзорните органи ги имаат, меѓу другото, следните посебни задачи:
  - да ја надгледуваат и унапредуваат заштитата на податоците на национално ниво;
  - да ги советуваат субјектите на податоците и контролорите, како и владата и целокупната јавност;
  - да прифаќаат жалби и да му помагаат на субјектот на податоците во врска со наводни повреди на правата на заштита на податоците;
  - да ги надгледуваат контролорите и обработувачите;
  - да интервенираат по потреба со
    - предупредувања, опомени, па дури и со парично казнување на контролорите и обработувачите,
    - да издаваат налози за исправка, блокирање или за бришење на податоците,
    - да наметнуваат забрани за обработка;
  - да поднесат предмет пред суд.

192 СЕ, Комитет на министри (1985 година), Препорака Rec(85)20 до државите-членки за заштитата на личните податоци кои се употребуваат за целите на директен маркетинг, 25 октомври 1985 година, член 4 став 1.

Според Директивата за заштита на податоците, независниот надзор е неопходен како значаен механизам за осигурување на делотворната заштита на податоците. Со Директивата е внесен инструмент за спроведување на заштитата на податоците, кој првично не постоел ниту во Конвенцијата бр. 108 ниту во Насоките на ОЕСР за заштита на приватноста.

Со оглед на тоа дека независниот надзор се покажал како незаменлив дел за развојот на ефективната заштита на податоците, во една нова одредба на ревидираните Насоки на Организацијата за економска соработка и развој за заштита на приватноста, која била усвоена во 2013 година, државите-членки се повикуваат на „создавање и одржување органи за спроведување на заштитата на приватноста со управа, извори и техничко знаење кои се нужни за ефикасно извршување на нивните овластувања и за објективно, непристрасно и доследно одлучување“[193].

Според правото на Советот на Европа, со Дополнителниот протокол кон Конвенцијата бр. 108 воспоставувањето на надзорни органи станало задолжително. Во тој инструмент, во членот 1, содржана е правната рамка за независни надзорни органи кои договорните страни мора да ги спроведат во своето домашно право. Во него се користат слични формулации за опис на задачите и овластувањата на органи кои се слични на тие од Директивата за заштита на податоците. Затоа, надзорните органи начелно би требало да функционираат на истиот начин и според правото на Европската Унија и според правото на Советот на Европа.

Според правото на Европската Унија, надлежностите и организациската структура на надзорните органи најпрвин биле утврдени во членот 28 став 1 на Директивата за заштита на податоците. Со Регулативата за заштита на податоците во институциите на Европската Унија[194] се воспоставува Европскиот супервизор за заштита на податоците како надзорен орган за обработка на податоците од страна на телата и институциите на Европската Унија. При утврдувањето на улогата и одговорностите на надзорниот орган, оваа регулатива се потпира на искуството што било стекнато од донесувањето на Директивата за заштита на податоците.

Независноста на органите за заштита на податоците е загарантирана со членот 16 став 2 на Договорот за функционирањето на Европската Унија и членот 8 став

193 ОЕСР (2013), *Насоки со кои се уредуваат заштитата на приватноста и прекуграничниот пренос на личните податоци*, параграф 19 точка (в).

194 Регулатива (ЕЗ) Бр. 45/2001 на Европскиот парламент и на Советот од 18 декември 2000 година за заштита на поединците во врска со обработката на личните податоци од страна на институциите и телата на Заедницата и со слободното движење на такви податоци, Сл. весник 2001 L 8, членови 41–48.

3 од Повелбата. Во оваа последно наведена одредба контролата од независен орган особено се смета за суштински елемент на основното право на заштита на податоците. Покрај тоа, според Директивата за заштита на податоците, државите-членки мора да воспостават надзорни органи за надгледување на примената на Директивата кои ќе постапуваат целосно независно[195]. Правото на кое се темели основањето на надзорното тело мора да содржи одредби со кои особено се гарантира независноста, а конкретната организациска структура на органот мора да ја покажува неговата независност.

Во 2010 година, Судот на правдата на Европската Унија за првпат се занимавал со прашањето околу опфатот на барањето за независност на надзорните органи за заштита на податоците[196]. Следните примери го покажуваат начинот на неговото размислување.

Пример: Во предметот *European Commission v. Germany*[197], Европската комисија побарала од Судот на правдата на Европската Унија да изјави дека Германија погрешно го пренела барањето за „целосна независност" на надзорните органи кои биле одговорни за осигурување на заштитата на податоците и на тој начин не успеала да ги исполни своите обврски според членот 28 став 1 на Директивата за заштита на податоците. Според стојалиштето на Комисијата, проблемот се состоел во тоа што Германија ги ставила под надзор на државата органите што биле одговорни за надгледување на обработката на личните податоци надвор од јавниот сектор во различните сојузни покраини (*Länder*). Проценета на суштината на таа постапка, според Судот, зависела од опфатот на барањето за независност кое било содржано во таа одредба, а со тоа и од неговото толкување.

Судот истакнал дека зборовите „целосно независно" во членот 28 став 1 од Директивата мора да се толкуваат врз основа на дословниот текст на таа одредба и на целите и систематиката на Директивата за заштита на податоците[198]. Судот нагласил дека надзорните органи се „чуварите" на правата во врска со обработката на личните податоци кои се загарантирани со

195 Директива за заштита на податоците, член 28 став 1, последна реченица; Конвенција бр. 108, Дополнителен протокол, член 1 став 3.

196 Види ЕАОП (2010), *Основни права: предизвици и достигнувања во 2010 година*, Годишен извештај за 2010 год., стр. 59. ЕАОП подетално го разгледа ова прашање во својот извештај за *Заштита на податоците во Европската унија: улогата на националните органи за заштита на податоците*, кој е објавен во мај 2010 год.

197 СПЕУ, C-518/07, *European Commission v. Federal Republic of Germany*, 9 март 2010 година, параграф 27.

198 *На истото место*, параграфи 17 и 29.

Директивата и, според тоа, нивното создавање во државите-членки се смета „за клучна компонента на заштитата на поединците во поглед на обработката на личните податоци“[199]. Судот заклучил дека „при извршувањето на своите обврски, надзорните органи мора да постапуваат објективно и непристрасно. За таа цел, тие мора да бидат ослободени од секакво надворешно влијание, вклучувајќи го и директното или индиректното влијание на државата или на покраините, а не само од влијанието на надгледуваните тела“[200].

Судот на правдата на Европската Унија исто така утврдил дека значењето на поимот „целосна независност“ треба да се толкува во смисла на независноста на Европскиот супервизор за заштита на податоците онака како што е дефинирана во Регулативата за заштита на податоците во Европската Унија. Како што истакнал Судот, во нејзиниот член 44 став 2 е објаснет поимот за независност со додавање дека во вршењето на своите должности Европскиот супервизор за заштита на податоците не смее да бара или да прима упатства од никого. Со тоа се исклучува можноста државата да врши надзор на независен надзорен орган за заштита на податоците[201].

Според тоа, Судот на правдата на Европската Унија сметал дека германските институции за заштита на податоците на ниво на сојузната држава што се надлежни за следење на обработката на личните податоци која ја вршат нејавни тела не биле доволно независни затоа што биле предмет на надзор од страна на државата.

Пример: Во предметот *European Commission v. Austria*[202], Судот на правдата на Европската Унија истакнал слични проблеми во врска со положбата на определени членови и на персоналот на австрискиот орган за заштита на податоците (Комисија за заштита на податоците, ДСК). Во овој предмет Судот заклучил дека австриското законодавство ја исклучувало можноста австрискиот орган за заштита на податоците да ги врши своите должности целосно независно во смисла на Директивата за заштита на податоците. Независноста на австрискиот орган за заштита на податоците не била осигурана во доволна мера бидејќи Сојузната канцеларија ѝ обезбедувала работна сила на ДСК, ја надгледувала ДСК и имала право во секое време да се информира за нејзината работа.

199 *На истото место*, параграф 23.

200 *На истото место*, параграф 25.

201 *На истото место*, параграф 27.

202 СПЕУ, C-614/10, *European Commission v. Republic of Austria*, 16 октомври 2012 год., параграфи 59 и 63.

Пример: Во предметот *European Commission v. Hungary*[203], Судот на правдата на Европската Унија истакнал дека „барањето […] да се осигури дека секој надзорен орган може да ги извршува задачите кои му се доверени целосно независно подразбира обврска за засегнатата држава-членка да го почитува целосното времетраење на мандатот на тој орган". Судот исто така сметал дека „со предвремено завршување на мандатот на надзорниот орган за заштита на личните податоци, Унгарија не успеала да ги исполни своите обврски од Директивата 95/46/ЕЗ […]".

Според националното законодавство, надзорните органи ги имаат следните овластувања и права[204]:

- да ги советуваат контролорите и субјектите на податоците за сите прашања во врска со заштитата на податоците;
- да ги истражуваат операциите на обработка и соодветно да преземаат дејства;
- да ги предупредуваат или опоменуваат контролорите;
- да наредат исправка, блокирање, бришење или уништување на податоците;
- да наметнат привремена или конечна забрана за обработка;
- да поднесат предмет пред суд.

За да ги извршува своите должност, надзорниот орган мора да има пристап до сите лични податоци и информации кои се неопходни за истрага, како и пристап до сите простории во кои контролорот чува суштински информации.

Има значајни разлики меѓу домашните надлежности кои се однесуваат на постапките и правната последица на наодите на надзорниот орган. Тие можат да варираат од препораки кои се слични на тие што ги дава народен правобранител до одлуки кои веднаш се спроведуваат. Според тоа, при анализа на делотворноста на правните средства во законодавството, нивните инструменти мора да се разгледаат во нивниот контекст.

203 СПЕУ, C-288/12, *European Commission v. Hungary*, 8 април 2014 год., параграфи 50 и 67.

204 Директива за заштита на податоците, член 28; види понатаму Конвенција бр. 108, Дополнителен протокол, член 1.

5.3. Правни средства и санкции

Клучни точки

- Според Конвенцијата бр. 108 и според Директивата за заштита на податоците, националното законодавство мора да предвидува соодветни правни средства и санкции за повреди на правото на заштита на податоците.
    - Во согласност со правото на Европската Унија, за правото на реална жалба потребно е со националното законодавство да се предвидат правни средства против повреди на правата на заштита на податоците, без оглед на можноста за обраќање до надзорен орган.
    - Националното законодавство мора да предвиди санкции кои се делотворни, еднакви, сразмерни и обесхрабрувачки.
- Пред да се обрати до суд, лицето треба да се обрати кај контролор. Исто така, прашањето дали лицето пред да се обрати до суд треба задолжително да се обрати до надзорен орган, треба да се уреди со националното законодавство.
- Субјектите на податоците може да поднесат пријава пред Европскиот суд за човековите права за повреди на правото на заштита на податоците, но само во крајни случаи и под определени услови.
- Покрај тоа, субјектите на податоците можат да се обратат до Судот на правдата на Европската Унија, но само во ограничен број случаи.

Правата во рамките на законодавството за заштита на податоците може да ги остварува само лицето чии права се загрозени; тоа е лице кое е, или барем тврди дека е, субјект на податоците. Таквите лица при остварувањето на нивните права можат да бидат застапувани од лица кои, според националното законодавство, ги исполнуваат потребните услови. Малолетниците мора да бидат застапувани од нивните родители или старатели. Пред надзорни органи лицето исто така може да биде застапувано од здруженија, чија законита цел е унапредување на правата на заштита на податоците.

5.3.1. Барања до контролорот

Правата кои се споменати во поглавјето 3.2. мораат прво да се остварат *vis-à-vis* контролорот. Директното обраќање до националниот надзорен орган или до суд не би помогнало бидејќи надзорниот орган би можел само да му советува на лицето прво да се обрати кај контролорот, а судот би утврдил дека жалбата е недопуштена. Формалните критериуми за правно релевантно барање до контролор, особено во поглед на тоа дали барањето треба да биде во писмена форма, треба да се уредат со националното законодавство.

На барањето мора да одговари телото на кое лицето му се обратило како на контролор, дури и ако тоа не е контролор. Во секој случај, до субјектот на податоците мора да се достави одговор во временскиот рок кој е утврден со националното законодавство, дури и ако во него само се вели дека за подносителот на барањето не се обработуваат никакви податоци. Во согласност со одредбите од членот 12 точка (а) на Директивата за заштита на податоците и членот 8 точка (б) на Конвенцијата бр. 108, барањето мора да се обработи „без прекумерно доцнење". Затоа, со националното законодавство треба да се пропише доволно краток период за одговор, кој сепак ќе му овозможи на контролорот соодветно да го обработи барањето.

Пред да одговори на барањето, телото до кое барателот се обратил како до контролор мора да го утврди идентитетот на подносителот на барањето со цел да утврди дали тој навистина е лицето кое тврди дека е и на тој начин да се избегне сериозна повреда на доверливоста. Ако условите за утврдување на идентитетот не се посебно уредени со националното законодавство, за нив одлучува контролорот. Меѓутоа, според начелото на правична обработка, контролорите не смеат да пропишуваат премногу тешки услови за потврдување на идентификувањето (и на автентичноста на барањето, како што е образложено во поглавје 2.1.1.).

Националното законодавство исто така треба да се занимава со прашањето дали контролорите, пред да одговорат на некое барање, смеат да побараат од подносителот на барањето да плати надомест: во членот 12 точка (а) на Директивата и членот 8 точка (б) на Конвенцијата бр. 108, пропишано е дека одговорот на барањето за пристап мора да се даде „без прекумерен […] трошок". Националното законодавство во многу европски земји пропишува дека на барањата кои се однесуваат на законодавството за заштита на податоците мора да се одговори бесплатно ако одговорот не предизвикува прекумерен и невообичаен напор. Од

друга страна, контролорите обично се заштитени со националното законодавство од злоупотреба на правото на добивање одговор на барање.

Ако лицето, институцијата или телото до кои подносителот на барањето се обратил како до контролор не одрече дека е контролор, тогаш во временскиот рок кој е пропишан со националното законодавство тој субјект мора:

- или да го одобри барањето и да го извести барателот за начинот на кој било исполнето барањето;

- или да го информира подносителот на барањето зошто не било исполнето неговото барање.

5.3.2. Барања поднесени до надзорниот орган

Ако лицето кое поднело барање за пристап или вложило приговор до контролор не добие навремен и задоволителен одговор, може да се обрати до националниот надзорен орган за заштита на податоците со барање за помош. Во текот на постапката пред надзорниот орган треба да се разјасни дали лицето, институцијата или телото до кои се обратил барателот навистина било должно да реагира на барањето и дали реакцијата била исправна и доволна. Надзорниот орган мора да го извести засегнатото лице за резултатот од постапката во која се обработува неговото барање[205]. Правните последици од резултатот на постапката пред национален надзорен орган зависат од националното законодавство: дали одлуките на органот можат законски да се спроведуваат, односно дали може да ги спроведува јавен орган или дали е неопходна жалба до суд ако контролорот не ги почитува одлуките (мислење, опомена и сл.) на надзорниот орган.

Во случај кога институциите или телата на Европската Унија наводно ги повредиле правата на заштита на податоците кои се загарантирани со членот 16 на Договорот за функционирањето на Европската Унија, субјектот на податоците може да поднесе жалба до Европскиот супервизор за заштита на податоците[206], кој е независен надзорен орган за заштита на податоците во согласност со Регулативата за заштита на податоците во институциите на Европската Унија со која се утврдуваат должностите и овластувањата на Европскиот супервизор за

205 Директива за заштита на податоците, член 28 став 4

206 Регулатива (ЕЗ) Бр. 45/2001 на Европскиот парламент и на Советот од 18 декември 2000 година за заштита на поединците во врска со обработката на личните податоци од страна на институциите и телата на Заедницата и со слободното движење на такви податоци, Сл. весник 2001 L 8.

заштита на податоците. Ако Европскиот супервизор за заштита на податоците не одговори во рок од шест месеци, се смета дека жалбата е одбиена.

Мора да постои можност за поднесување жалба до суд против одлуката на националниот надзорен орган. Тоа се однесува на субјектот на податоците како и на контролорите кои учествувале во постапката пред надзорен орган.

Пример: *Комесарот за информации на Обединетото Кралство* на 24 јули 2013 година донел одлука со која од полицијата на Хертфордшир барал престанок на користењето на систем за следење на регистарски таблички на возила за кој смета дека е незаконски. Податоците кои биле собрани од камерите биле складирани и во базите на податоци на локалната полиција и во централизирана база на податоци. Фотографиите од регистарските таблички се чувале две години, а фотографиите од автомобилите 90 дена. Се сметало дека таквата широка употреба на камерите и на другите видови на надзор не била сразмерна со проблемот кој се обидувала да го реши.

5.3.3. Барање поднесено до суд

Според Директивата за заштита на податоците, ако лицето кое поднело барање до контролор во согласност со законодавството за заштита на податоците не е задоволно со одговорот на контролорот, тогаш тоа лице мора да има право да поднесе жалба пред национален суд[207].

Прашањето дали пред да се обрати до суд лицето треба задолжително да се обрати до надзорниот орган треба да се уреди со националното законодавство. Меѓутоа, во повеќето случаи, препорачливо е за лицата кои ги остваруваат своите права на заштита на податоците најпрвин да се обратат до надзорниот орган бидејќи постапките во кои тие бараат помош би требало да бидат небирократски и бесплатни. Стручното знаење кое е документирано во одлуката на надзорниот орган (мислење, опомена и сл.) исто така може да му помогне на субјектот на податоците во остварувањето на неговите права пред судовите.

Според правото на Советот на Европа, повредите на правата за заштита на податоците кои наводно се случиле на национално ниво на некоја договорна

207 Директива за заштита на податоците, член 22.

страна на Европската конвенција за човековите права и кои истовремено претставуваат повреда на членот 8 на Конвенцијата можат дополнително да се обжалат пред Европскиот суд за човековите права откако ќе се исцрпат сите постојни домашни правни средства. Поднесувањето жалба пред Европскиот суд за човековите права поради повреда на членот 8 на Европската конвенција за човековите права мора да исполни и други критериуми за допуштеност (членовите 34–37 на Европската конвенција за човековите права)[208].

Иако жалбите до Европскиот суд за човековите права може да бидат насочени само против договорни страни, тие можат индиректно да се занимаваат и со постапки и пропусти на приватни лица, доколку некоја договорна страна не ги исполнила своите позитивни обврски според Европската конвенција за човековите права и не осигурала доволна заштита од повреди на правата за заштита на податоците во своето национално законодавство.

Пример: Во предметот *K.U. v. Finland*[209], жалителот, малолетник, се жалел дека за него е објавен оглас од сексуална природа на интернет-страница за запознавање. Давателот на услугите не го открил идентитетот на лицето кое ги објавило информациите поради обврската за доверливост според финското законодавство. Жалителот тврдел дека со финското законодавство не му била осигурана доволна заштита од таквите постапки на приватни лица кои на интернет објавувале инкриминирачки податоци за жалителот. Европскиот суд за човековите права сметал дека државите не само што биле должни да се воздржат од произволно мешање во приватните животи на поединците туку тие исто така подлежат на позитивни обврски кои вклучувале „усвојување мерки со цел да се осигури почитувањето на приватниот живот дури и во областа на меѓусебните односи на поединците". Во случајот на жалителот, неговата практична и делотворна заштита налагала преземање на делотворни мерки за идентификување и гонење на сторителот. Меѓутоа, државата не ја осигурила таквата заштита, а Судот заклучил дека имало повреда на членот 8 на Европската конвенција за човековите права.

Пример: Во предметот *Köpke v. Germany*[210], жалителката била осомничена за кражба на работното место и затоа била подложена на видеонадзор. Европскиот суд за човековите права заклучил дека „ништо не упатувало на

208 ЕКЧП, членови 34–37, достапни на: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 ЕСЧП, *K.U. v. Finland*, Бр. 2872/02, 2 декември 2008 година.

210 ЕСЧП, *Köpke v. Germany* (dec.), Бр. 420/07, 5 октомври 2010 год.

тоа дека домашните органи не успеале да воспостават правична рамнотежа, во рамките на својата слобода на сопствена процена, меѓу правото на жалителката на почитување на нејзиниот приватен живот според членот 8, од една страна, и интересот на нејзиниот работодавец за заштита на неговите права на сопственост и јавниот интерес за соодветно водење на судските постапки, од друга страна". Од таа причина, жалбата била прогласена за недопуштена.

Ако Европскиот суд за човековите права утврди дека некоја држава што е странка во постапката повредила некое од правата кои се заштитени со Европската конвенција за човековите права, тогаш таа држава е обврзана да ја изврши пресудата на Европскиот суд за човековите права. Со извршните мерки најпрвин треба да ѝ се стави крај на повредата и да се превенираат, колку што е можно, нејзините негативни последици за жалителот. За извршување на пресудите исто така може да бидат потребни општи мерки за спречување на повреди кои се слични на тие што ги утврдил Судот, било да е тоа со измени во законодавството, на судската практика или на некој друг начин.

Ако Европскиот суд за човековите права утврдил повреда на Европската конвенција за човековите права, членот 41 на Конвенцијата пропишува дека тој може да му досуди правичен надомест на жалителот на трошок на државата што е странка во постапката.

Според правото на Европската Унија,[211] жртвите на повреди на националното законодавство за заштита на податоците со кое се спроведува законодавството на Европската Унија за заштита на податоците во некои случаи можат да ги поднесат своите предмети пред Европскиот суд за човековите права. Има две можни сценарија за тоа како тврдењето на субјектот на податоците дека биле повредени неговите права може да доведе до постапка пред Судот на правдата на Европската Унија.

Според првото сценарио, субјектот на податоците би требало да биде директна жртва на некој административен или правен акт на Европската Унија со кој се повредува правото на поединецот на заштита на податоците. Според членот 263 став 4 на Договорот за функционирањето на Европската Унија:

211 ЕУ (2007), Договор од Лисабон со кој се изменуваат Договорот за Европската Унија и Договорот за воспоставување на Европската Заедница, потпишан во Лисабон на 13 декември 2007 год., Сл. весник 2007 С 306. Види ги, исто така, пречистените верзии на Договорот за Европската Унија, Сл. весник 2012 С 326 и на ДФЕУ, Сл. весник 2012 С 326.

„секое физичко или правно лице може [...] да поведе постапка против акт кој е упатен до него или кој директно и лично го засега, како и против правен акт кој директно го засега и не подразбира спроведување мерки".

Според тоа, жртвите на незаконската обработка на нивните податоци од страна на орган на Европската Унија можат да поднесат жалба директно до Општиот суд, кој претставува тело на Судот на правдата на Европската Унија кое е надлежно за донесување пресуда во предмети кои се однесуваат на Регулативата за заштита на податоците во институциите на Европската Унија. Исто така, постои можност за поднесување жалба директно до Судот на правдата на Европската Унија ако некоја правна одредба на Европската Унија директно влијаела на правната ситуација на поединецот.

Второто сценарио се однесува на надлежноста на Судот на правдата на Европската Унија (Суд на правдата) за донесување на прелиминарни одлуки во врска со членот 267 на Договорот за функционирањето на Европската Унија.

Во текот на домашната постапка, субјектите на податоците можат да побараат од националниот суд да побара појаснување од Судот на правдата во врска со толкувањето на договорите на Европската Унија, како и толкувањето на валидноста на актите на институциите, службите или агенциите на Европската Унија. Таквите појаснувања се познати како прелиминарни одлуки. Тоа не претставува директно правно средство за жалителот, но на националните судови им овозможува да обезбедат правилно толкување на правото на Европската Унија.

Ако една странка во постапка пред националните судови побара упатување на прашањето до Судот на правдата на Европската Унија, само националните судови кои постапуваат како највисока судска инстанца и против чии одлуки не постои правно средство се обврзани да одговорат на барањето.

Пример: Во предметот *Kärntner Landesregierung and Others*[212], австрискиот Уставен суд поднел прашања до Судот на правдата на Европската Унија во врска со валидноста на членовите 3 до 9 на Директивата 2006/24/ЕЗ (*Директива за задржување на податоците*) во смисла на членовите 7, 9 и 11 на Повелбата. Прашањата се однесувале и на тоа дали определени одредби од австрискиот Сојузен закон за телекомуникации со кој се пренесувала

212 СПЕУ, Заеднички случаи C-293/12 и C-594/12, *Digital Rights Ireland and Seitling and Others,* 8 април 2014 год.

Директивата за задржување на податоците биле неспоиви со аспектите на Директивата за заштита на податоците и на Регулативата за заштита на податоците во институциите на Европската Унија.

Господин Зајтлингер, еден од жалителите во постапката пред Уставниот суд, тврдел дека телефонот, интернетот и електронската пошта ги користи и за деловни и за приватни цели. Според тоа, информациите кои ги испраќа и ги прима минуваат низ јавна телекомуникациска мрежа. Според австрискиот Закон за телекомуникации од 2003 година, неговиот давател на телекомуникациски услуги законски е обврзан да собира и да складира податоци за неговото користење на мрежата. Господинот Зајтлингер сфатил дека таквото собирање и складирање на неговите лични податоци во никој случај не било неопходно за техничките цели на испраќање информации од точка А до точка Б на мрежата.

Покрај тоа, собирањето и складирањето на тие податоци воопшто не било неопходно за целите на наплатата. Господин Зајтлингер сигурно не се согласил за таква употреба на неговите лични податоци. Единствената причина за собирањето и складирањето на сите тие дополнителни податоци бил австрискиот Закон за телекомуникации од 2003 година.

Затоа, г. Зајтлингер покренал постапка пред австрискиот Уставен суд во која тврдел дека статутарните обврски на неговиот давател на телекомуникациски услуги ги повредувале неговите основни права според членот 8 на Повелбата на Европската Унија.

Судот на правдата на Европската Унија донесува одлука само во врска со составните делови на барањето за прелиминарно одлучување кое му било поднесено. Националниот суд останува надлежен за одлучување во изворниот предмет.

Начелно, Судот на правдата мора да одговори на поставените прашања. Тој не може да го одбие донесувањето на прелиминарна одлука поради тоа што тој одговор ниту би бил релевантен ниту навремен во поглед на изворниот предмет. Меѓутоа, тој може да го одбие донесувањето на прелиминарна одлука ако прашањето не потпаѓа под неговото подрачје на надлежност.

Конечно, ако правата на заштита на податоците, кои се загарантирани со членот 16 на Договорот за функционирањето на Европската Унија, наводно се повредени

од институција или тело на Европската Унија во текот на обработка на личните податоци, субјектот на податоците предметот може да го поднесе пред Општиот суд на Европската Унија (членот 32 став 1 и став 4 на Регулативата за заштита на податоците во институциите на Европската Унија). Истото се однесува на одлуките на Европскиот супервизор за заштита на податоците во врска со такви повреди (членот 32 став 3 на Регулативата за заштита на податоците во институциите на Европската Унија).

Општиот суд на Европската Унија е надлежен за донесување пресуда во предмети кои се однесуваат на Регулативата за заштита на податоците во институциите на Европската Унија. Меѓутоа, ако едно лице во својство на вработен во институција или тело на Европската Унија побара правно средство, тоа лице мора да се обрати до Европскиот трибунал за јавните служби.

Пример: Предметот *European Commission v. The Bavarian Lager Co. Ltd*[213]ги покажува правните средства што можат да се применат против дејства или одлуки на институции и тела на Европската Унија во врска со заштитата на податоците.

„Bavarian Lager" побарал од Европската комисија пристап до целосниот записник од состанокот што го одржала Комисијата и кој наводно се однесувал на правни прашања што биле значајни за компанијата. Комисијата го одбила барањето за пристап на компанијата поради превладувачките интереси за заштита на податоците[214]. Повикувајќи се на членот 32 од Регулативата за заштита на податоците во институциите на Европската Унија, „Bavarian Lager" поднел жалба пред Судот на правдата на Европската Унија, поточно пред Првостепениот суд (претходникот на Општиот суд). Во својата одлука во предметот T-194/04, *Bavarian Lager v. Commission*, Првостепениот суд ја поништил одлуката на Комисијата со која е одбиено барањето за пристап. Европската комисија се пожалила на таа одлука во Судот на правдата на Европската Унија. Судот на правдата (во Голем судски совет) донел пресуда со која ја укинал пресудата на Првостепениот суд и го потврдил одбивањето на барањето за пристап на Европската комисија.

213 СПЕУ, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 29 јуни 2010 год.

214 За анализа на аргументот, види: ЕСЗП (2011), *Јавен пристап до документи што содржат лични податоци по одлуката по предметот* Bavarian Lager , Брисел, ЕСЗП, достапно на: www.secure.edps.europa.eu/EDPSWEB/ webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_ Lager_EN.pdf.

5.3.4. Санкции

Според правото на Советот на Европа, со членот 10 од Конвенцијата бр. 108 е пропишано дека секоја од државите што се договорни страни мора да воспостави соодветни санкции и правни средства за повреди на одредбите на домашното законодавство со кои се реализираат основните начела за заштита на податоците кои се утврдени во Конвенцијата бр. 108[215]. **Според правото на Европската Унија**, со членот 24 на Директивата за заштита на податоците е пропишано дека државите-членки „донесуваат соодветни мерки како гаранција дека одредбите од оваа Директива се спроведуваат во целост и конкретно ги утврдуваат санкциите што треба да бидат наметнати во случај на повреда на донесените одредби […]".

Двата инструмента им овозможуваат на државите-членки широк простор за дискреција при одбирањето на соодветните санкции и правни средства. Ниеден правен иструмент не нуди конкретни насоки во врска со природата или за видот на соодветните санкции, ниту дава примери за санкции.

Меѓутоа:

> *„иако државите-членки на Европската Унија уживаат простор за дискреција при утврдувањето на тоа кои мерки се најсоодветни за заштита на правата на поединците што произлегуваат од правото на Европската Унија, во согласност со начелото за лојална соработка кое е утврдено во членот 4 став 3 на Договорот за Европската Унија, треба да се исполнат минималните барања за делотворност, еднаквост, пропорционалност и одвраќање"*[216].

Судот на правдата на Европската Унија во повеќе наврати тврдел дека националното законодавство нема целосна слобода за определување санкции.

Пример: Во предметот *Von Colson and Kamann v. Land Nordrhein-Westfalen*[217], Судот на правдата на Европската Унија истакнал дека сите држави-членки на кои се однесува некоја директива се обврзани во своите национални правни системи да ги усвојат сите потребни мерки со кои ќе се осигури нејзината

215 ЕСЧП, *I. v. Finland*, Бр. 20511/03, 17 јули 2008 год.; ЕСЧП, *K.U. v. Finland*, Бр. 2872/02, 2 декември 2008 год.

216 ЕАОП (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, 2/2012, Виена, 1 октомври 2012 год., стр. 27.

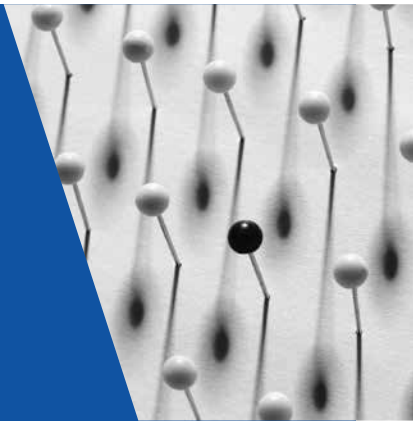
217 СПЕУ, C-14/83, *Sabine von Kolson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10 април 1984 год.

делотворност и целосна усогласеност со целта кон која е насочена. Судот сметал дека иако државите-членки се тие што треба да ги изберат начините и средствата со кои ќе се осигури дека некоја директива е спроведена, таа слобода не влијае на обврската на која подлежат. Поточно, делотворното правно средство мора да му овозможи на поединецот целосно остварување и спроведување на релевантното право. За да се постигне таа вистинска и делотворна заштита, правните средства мора да доведат до казнени постапки и/или постапки за надомест на штета чиј резултат се санкции со одвраќачко дејство.

Што се однесува до санкциите против повреди на правото на Европската Унија од страна на институции или тела на Унијата, поради посебната област на важење на Регулативата за заштита на податоците во институциите на Европската Унија, предвидени се санкции само во облик на дисциплинска мерка. Според членот 49 на Регулативата, „поради неизвршување на обврските од оваа Регулатива, било да е тоа намерно или поради небрежност од негова страна, службеник или друго службено лице на Европските Заедници ќе биде подложен на дисциплинска мерка […]".

6

Прекуграничен пренос на податоци



Европска Унија	Обработени прашања	Совет на Европа
Прекуграничен пренос на податоци		
Директива за заштита на податоците, член 25 став 1 од СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 год.	Дефиниција	Конвенција бр. 108, Дополнителен протокол, член 2 став 1
Слободен пренос на податоци		
Директива за заштита на податоците, член 1 став 2	Меѓу државите-членки на ЕУ	
	Меѓу договорните страни на Конвенцијата бр. 108	Конвенција бр. 108, член 12 став 2
Директива за заштита на податоците, член 25	Во трети земји со соодветно ниво на заштита на податоците	Конвенција бр. 108, Дополнителен протокол, член 2 став 1
Директива за заштита на податоците, член 26 став 1	Во трети земји во посебни случаи	Конвенција бр. 108, Дополнителен протокол, член 2 став 2 точка (а)
Ограничен пренос на податоци до трети земји		
Директива за заштита на податоците, член 26 став 2 Директива за заштита на податоците, член 26 став 4	Договорни клаузули	Конвенција бр. 108, Дополнителен протокол, член 2 став 2 точка (б) Водич за подготовката на договорните клаузули

Директива за заштита на податоците, член 26 став 2	Обврзувачки корпоративни правила	
Примери: Договор меѓу ЕУ и САД за ЕПИ Договор меѓу ЕУ и САД за SWIFT	Посебни меѓународни договори	

Покрај тоа што во Директивата за заштита на податоците е пропишан слободниот пренос на податоците меѓу државите-членки, таа содржи и одредби во врска со барањата за прекуграничен пренос на лични податоци до трети земји надвор од Европската Унија. Советот на Европа ја препознал важноста од спроведувањето на правила за прекуграничен пренос на податоци до трети земји и во 2001 година го усвоил Дополнителниот протокол кон Конвенцијата бр. 108. Со тој протокол се преземени главните регулаторни особености на прекугранични пренос на податоци од држави што се договорни страни на Конвенцијата и од држави-членки на Европската Унија.

6.1. Природата на прекугранични пренос на податоци

Клучни точки

- Прекугранични пренос на податоци е пренос на лични податоци до корисник кој е под странска надлежност.

Во членот 2 став 1 на Дополнителниот протокол кон Конвенцијата бр. 108, прекугранични пренос на податоци се опишува како пренос на лични податоци до корисник кој е под странска надлежност. Со членот 25 став 1 на Директивата за заштита на податоците се уредува „преносот во трети земји на личните податоци што се обработуваат или што се наменети за обработка по преносот […]". Таквиот пренос на податоци е дозволен само во согласност со правилата кои се наведени во членот 2 на Дополнителниот протокол кон Конвенцијата бр. 108 и, за државите-членки на Европската Унија, дополнително во членовите 25 и 26 на Директивата за заштита на податоците.

Пример: Во предметот *Bodil Lindqvist*[218], Судот на правдата на Европската Унија сметал дека „упатувањето на различни лица на интернет-страница и нивното идентификување по име или на друг начин, на пример со наведување на нивниот телефонски број или информации во врска со нивните работни услови или хобија, претставува 'обработка на лични податоци што може да биде целосно или делумно автоматска', во смисла на членот 3 став 1 на Директивата 95/46".

Потоа Судот истакнал дека со Директивата исто така се пропишуваат посебни правила чија цел е да им овозможат на државите-членки да го надгледуваат преносот на лични податоци до трети земји.

Меѓутоа, со оглед на, прво, степенот на развиеност на интернетот во времето на подготвувањето на Директивата и, второ, отсуството на критериуми во неа кои се однесуваат на употребата на интернет, „не може да се претпостави дека законодавецот на Заедницата имал за цел изразот 'пренос [на податоци] до трета земја' да го покрие вчитувањето [...] на податоци на интернет-страница, дури и ако на тој начин податоците станат достапни за лица во трети земји кои имаат технички средства за пристапување до нив".

Во спротивно, доколку Директивата „се толкува така што ќе значи дека до пренос на податоци до трета земја доаѓа секогаш кога лични податоци се вчитуваат на интернет-страница, тој пренос нужно би бил пренос до сите трети земји во кои постојат технички средства што се потребни за пристап на интернет. На тој начин, посебниот режим кој е пропишан [со Директивата] нужно би се претворил во режим на општа примена, во поглед на активностите на интернет. Според тоа, доколку Комисијата утврдила [...] дека дури и само една трета земја не осигурила соодветна заштита, државите-членки би биле должни да спречат ставање на лични податоци на интернет".

Начелото според кое самата објава на (лични) податоци не треба да се смета за прекугранично пренесување податоци се применува и за јавни регистри на интернет или за масовни медиуми како што се (електронските) весници и телевизијата. Поимот „прекугранично пренесување податоци" се однесува само на комуникацијата која е насочена кон определени корисници.

218 СПЕУ, C-101/01, *Bodil Lindqvist*, 6 ноември 2003 год., параграфи 27, 68 и 69.

6.2. Слободен пренос на податоци меѓу државите-членки или договорните страни

Клучни точки

- Преносот на лични податоци во друга држава-членка на Европската економска област или во друга договорна страна на Конвенцијата бр. 108 не смее да се ограничи.

Според членот 12 став 2 на Конвенцијата бр. 108, **согласно со правото на Советот на Европа**, мора да постои слободен пренос на лични податоци меѓу државите што се договорни страни на Конвенцијата. Со домашното законодавство не смее да се ограничи извозот на лични податоци во договорна страна, освен ако:

- тоа е неопходно поради посебната природа на податоците[219];

- ограничувањето е неопходно со цел да се спречи избегнување на домашните правни одредби за прекугранично пренос на податоци во трети земји[220].

Според правото на Европската Унија, ограничувањето и забранувањето на слободниот пренос на податоци меѓу државите-членки од причини што се поврзани со заштитата на податоците се забранети со членот 1 став 2 на Директивата за заштита на податоците. Областа на слободниот пренос на податоци е проширена со Договорот за Европската економска област (ЕЕО)[221], со кој Исланд, Лихтенштајн и Норвешка се внесуваат во внатрешниот пазар.

Пример: Ако една подружница на меѓународна групација, со седиште во повеќе држави-членки на Европската Унија, меѓу кои и Словенија и Франција, пренесува лични податоци од Словенија во Франција, таквиот пренос на

219 Конвенција бр. 108, член 12 став 3 точка (а).

220 *На истото место*, член 12 став 3 точка (б).

221 Одлука на Советот и на Комисијата од 13 декември 1993 година во врска со склучувањето на Договорот за Европската економска област меѓу Европските Заедници, нивните држави-членки и Република Австрија, Република Финска, Република Исланд, Кнежеството Лихтенштајн, Кралството Норвешка, Кралството Шведска и Швајцарската Конфедерација, Сл. весник 1994 L 1.

податоци не смее да се ограничи или да се забрани со словенечкото национално законодавство.

Меѓутоа, ако истата словенечка подружница сака да ги пренесе истите лични податоци до матичната компанија во Соединетите Американски Држави, словенечкиот извозник на податоците мора да помине низ постапка која е пропишана во словенечкото законодавство за прекуграничен пренос на податоци во трети земји без соодветка заштита на податоците, освен ако матичната компанија ги усвоила начелата за приватност на безбедно пристаниште, доброволен кодекс на однесување за обезбедување на соодветно ниво на заштита на податоците (види го поглавјето 6.3.1.).

Меѓутоа, прекуграничниот пренос на податоци во држави-членки на Европската економска област за цели надвор од надлежностите на внатрешниот пазар, како што се кривичните истраги, не подлежи на одредбите на Директивата за заштита на податоците и затоа не е опфатен со начелото за слободен пренос на податоци. Што се однесува до правото на Советот на Европа, сите области се вклучени во опфатот на Конвенцијата бр. 108 и на Дополнителниот протокол кон Конвенцијата бр. 108, иако договорните страни можат да предвидат исклучоци. Сите членки на ЕЕО се членки и на Конвенцијата бр. 108.

6.3. Слободен пренос на податоци во трети земји

Клучни точки

- Преносот на лични податоци во трети земји не смее да се ограничува во согласност со националното законодавство за заштита на податоците, ако:
  - е утврдена соодветна заштита на податоците кај корисникот;
  - тоа е неопходно поради посебните интереси на субјектот на податоците или легитимните претежни интереси на други лица, особено важни јавни интереси.
- Соодветната заштита на податоците во трета земја значи дека главните начела на заштитата на податоците биле делотворно спроведени во националното законодавство на таа земја.

- Според правото на Европската Унија, Европската комисија ја проценува соодветноста на заштитата на податоците во трета земја. Според правото на Советот на Европа, домашното законодавство треба да го утврди начинот за процена на соодветноста.

6.3.1. Слободен пренос на податоци поради соодветна заштита

Според правото на Советот на Европа, со домашното законодавство може да се допушти слободен пренос на податоци до држави што не се договорни страни ако државата или организацијата корисник обезбеди соодветно ниво на заштита за планираниот пренос на податоци[222]. Со домашното законодавство се утврдува начинот на процена на нивото на заштита на податоците во странска земја и кој би требало да ја изврши таа процена.

Според правото на Европската унија, слободниот пренос на податоци во трети земји со соодветно ниво на заштита на податоците е пропишан во членот 25 став 1 на Директивата за заштита на податоците. Поради условот со кој предност ѝ се дава на соодветноста пред еднаквоста, постојат различни начини на спроведување на заштитата на податоците. Според членот 25 став 6 на Директивата, Европската комисија е надлежна да го процени нивото на заштита на податоците во странски држави врз основа на заклучоците во врска со соодветноста и се советува во врска со проценатa со Работната група за членот 29, која значително придонела за толкувањето на членовите 25 и 26[223].

Заклучокот на Европската комисија за соодветноста има обврзувачко дејство. Ако Европската комисија објави заклучок за соодветноста за определена земја во *Службениот весник на Европската Унија*, сите држави членки на ЕЕО и нивните органи се должни да ја почитуваат одлуката, што значи дека податоците можат да се пренесуваат до таа држава без постапка на проверка или со лиценцирање пред националните власти[224].

222 Конвенција бр. 108, Дополнителен протокол, член 2 став 1.

223 Види, на пример, Работна група за членот 29 (2003), *Работен документ за пренос на лични податоци во трети земји: примена на членот 26 став 2 на Директивата на Европската Унија за заштита на податоците на обврзувачките корпоративни правила за меѓународен пренос на податоци*, РГ 74, Брисел, 3 јуни 2003 год.; и Работна група за членот 29 (2005), *Работен документ за заедничко толкување на членот 26 став 1 на Директивата 95/46/ЕЗ од 24 октомври 1995 год.*, РГ 114, Брисел, 25 ноември 2005 год.

224 За најновата верзија на списокот на државите кои примиле заклучок за соодветноста, види ја почетната страница на Европската комисија, Генерален директорат за правосудство, достапна

Европската комисија може исто така да процени делови од правниот систем на некоја земја или да се ограничи на поединечни теми. Комисијата донела заклучок за соодветноста, на пример, само за канадското законодавство за приватни трговски друштва[225]. Има и неколку заклучоци за соодветноста во врска со преноси што се засновани на договори меѓу Европската Унија и странски држави. Тие одлуки се однесуваат исклучиво на еден вид пренос на податоци, како што е евиденцијата на патничките имиња кој авионските компании го пренесуваат до странски тела за гранична контрола кога авионот полетува од Европската Унија до определени прекуокеански дестинации (види го поглавјето 6.4.3.). Во поновата практика на преносот на податоци, која е заснована на посебни спогодби меѓу Европската Унија и трети земји, начелно не се користат заклучоци за соодветноста бидејќи се претпоставува дека самата спогодба обезбедува соодветно ниво на заштита на податоците[226].

Всушност, една од најзначајните одлуки за соодветноста воопшто не се однесува на збир на правни одредби[227]. Таа повеќе се однесува на правила, како што е кодексот на однесување, кои се познати како начела за приватност на безбедно пристаниште (Safe Harbour Privacy Principles). Тие начела биле разработени од страна на Европската Унија и Соединетите Американски Држави за деловните компании на САД. Членството во безбедното пристаниште се остварува со изјава за доброволно преземање обврски пред Министерството за трговија на САД и се документира во список што го објавува Министерството. Бидејќи еден од значајните елементи на соодветноста е делотворноста на спроведувањето на заштитата на податоците, со Спогодбата за безбедно пристаниште е предвиден и определен степен на надзор од страна на државата:

на следната адреса: http://ec.europa.eu/justice/ data-protection/document/international-transfers/adequacy/index_en.htm.

225 Европска комисија (2002), Одлука 2002/2/ЕЗ од 20 декември 2001 год. во согласност со Директивата 95/46/ЕЗ на Европскиот парламент и на Советот во врска со соодветната заштита на лични податоци која е пропишана со канадскиот Закон за заштита на лични податоци и електронски документи, Сл. весник 2002 L 2.

226 На пример, Спогодбата меѓу Соединетите Американски Држави и Европската Унија за употребата и преносот на Евиденцијата на патнички имиња во Министерството за домашна безбедност на САД (Сл. весник 2012 L 215, стр. 5–14) или Спогодбата меѓу Европската Унија и Соединетите Американски Држави за обработка и пренос на податоци за финансиски пораки кои од Европската Унија се праќаат во Соединетите Американски Држави за целите на Програмата за следење на финансирањето на тероризмот, Сл. весник 2010 L 8, стр. 11–16.

227 Европска комисија (2000), Одлука на Комисијата 2000/520/ЕЗ од 26 јули 2000 год. во согласност со Директивата 95/46/ЕЗ на Европскиот парламент и на Советот за соодветноста на заштитата која произлегува од начелата на приватност на безбедно пристаниште и е во врска со најчесто поставуваните прашања кои ги издало Министерството за трговија на САД, Сл. весник 2000 L 215.

Кон безбедното пристаниште може да пристапат само компаниите кои подлежат на надзор од страна на Сојузната комисија за трговија на САД.

6.3.2. Слободен пренос на податоци во посебни случаи

Според правото на Советот на Европа, со членот 2 став 2 на Дополнителниот протокол кон Конвенцијата бр. 108 се допушта пренос на лични податоци во трети земји во кои не постои соодветна заштита на податоците доколку преносот е пропишан со домашното законодавство и е неопходен за:

- посебни интереси на субјектот на податоците;
- легитимни претежни интереси на други лица, особено важни јавни интереси.

Според правото на Европската Унија, во членот 26 став 1 на Директивата за заштита на податоците се содржани одредби кои се слични на тие од Дополнителниот протокол кон Конвенцијата бр. 108.

Според Директивата, интересите на субјектот на податоците можат да го оправдаат слободниот пренос на податоци во трета земја ако:

- субјектот на податоците дал недвосмислена согласност за извозот на податоците;
- субјектот на податоците влегува – или се подготвува да влезе – во договорен однос кој јасно налага податоците да бидат пренесени до корисник во странство;
- бил склучен договор меѓу контролор на податоците и трета земја во интерес на субјектот на податоците;
- неопходен е пренос со цел да се заштитат суштинските интереси на субјектот на податоците.
- за преносот на податоци од јавни регистри; станува збор за претежни интереси на општата јавност кои се однесуваат на пристапот до информации кои се чуваат во јавни регистри.

Легитимните интереси на други лица можат да го оправдаат слободниот прекуграничен пренос на податоци[228]:

- поради значаен јавен интерес, освен прашањата за национална или јавна безбедност, бидејќи тие не се опфатени со Директивата за заштита на податоците;

- поради воспоставување, извршување или одбрана на правните барања.

Горенаведените случаи треба да се сфатат како исклучоци од правилото според кое за непречен пренос на податоци во други земји е потребно соодветно ниво на заштита на податоците во земјата што е корисник. Исклучоците треба секогаш да се толкуваат рестриктивно. Тоа во повеќе наврати било подвлечено од страна на Работната група за членот 29 во смисла на членот 26 став 1 на Директивата за заштита на податоците, особено ако согласноста е наводна основа за пренос на податоците[229]. Работната група за членот 29 заклучила дека општите правила за правното значење на согласноста исто така се применуваат за членот 26 став 1 на Директивата. Ако, на пример, во смисла на работните односи не е јасно дали согласноста што ја дале вработените навистина била слободна согласност, преносот на податоци не може да се заснова на членот 26 став 1 точка (а) на Директивата. Во такви случаи се применува членот 26 став 2, кој пропишува дека националните органи за заштита на податоците издаваат дозвола за пренос на податоци.

6.4. Ограничен пренос на податоци во трети земји

Клучни точки

- Пред извозот на податоци во трети земји со кој не е осигурано соодветно ниво на заштита на податоците, надзорниот орган може да побара од контролорот да му овозможи увид во податоците кои планира да ги извезува.

228 Директива за заштита на податоците, член 26 став 1 точка (г).

229 Види особено Работна група за член 29 (2005), *Работен документ за заедничко толкување на членот 26 став 1 на Директивата 95/46/ЕЗ од 24 октомври 1995 год.*, РГ 114, Брисел, 25 ноември 2005 год.

- Контролорот кој сака да ги извезува податоците мора да докаже две нешта во текот на проверката:
  - дека постои правна основа за пренос на податоците до корисникот; и
  - дека се преземаат мерки за соодветна заштита на податоците кај корисникот.
- Мерките за воспоставување на соодветна заштита на податоците кај корисникот може да вклучуваат:
  - договорни одредби меѓу контролорот што ги извезува податоците и странскиот корисник на податоците;
  - обврзувачки корпоративни правила кои обично се применуваат при пренос на податоци во рамките на меѓународна групација.
- Преносот на податоци до странски органи може да се уреди и со посебен меѓународен договор.

Според Директивата за заштита на податоците и Дополнителниот протокол кон Конвенцијата бр. 108, домашното законодавство може да воспостави режими за прекуграничен пренос на податоци во трети земји во кој не е осигурано соодветното ниво на заштита на податоците доколку контролорот презел посебни чекори за да ги осигури соодветните мерки на заштита на податоците кај корисникот и доколку тој може да му го докаже тоа на надлежен орган. Тој услов е изречно споменат само во Дополнителниот протокол кон Конвенцијата бр.108; меѓутоа, тоа се смета за стандардна постапка во согласност со Директивата за заштита на податоците.

6.4.1. Договорни клаузули

И во правото на **Советот на Европа** и во правото **на Европската Унија** се споменуваат договорни клаузули меѓу контролорот што ги извезува податоците и корисникот во трета земја како можен начин за осигурување на доволно ниво на заштита на податоците кај корисникот.

На ниво на **Европската Унија**, Европската комисија со помош на Работната група за членот 29 развила стандардни договорни клаузули кои биле официјално потврдени со одлука на Комисијата како доказ за соодветна заштита на пода-

тоците[230]. Поради тоа што одлуките на Комисијата во целост се обврзувачки во државите-членки, националните органи кои се одговорни за надзор на прекуграничниот пренос на податоци мора да ги преземаат таквите стандардни договорни клаузули во своите постапки[231]. Според тоа, ако контролорот кој ги извезува податоците и корисникот во трета земја ги договорат и ги потпишат таквите клаузули, тоа би требало да претставува доволен доказ за надзорниот орган дека постојат соодветни заштитни мерки.

Постоењето на стандардни договорни клаузули во правната рамка на Европската Унија не значи дека контролорите не смеат да составуваат други *ad hoc* договорни клаузули. Меѓутоа, со тие клаузули би требало да се осигури истото ниво на заштита кое се осигурува со стандардните договорни клаузули. Најважните карактеристики на стандардните договорни клаузули се:

- клаузула за корисник на трета страна со која на субјектите на податоците им се овозможува да остваруваат договорни права иако не се странки на договорот;

- согласност на корисник или увозник на податоците, во случај на спор што подлежи на постапка на национален надзорен орган и/или суд на контролорот што ги извезува податоците.

Достапни се два збира на стандардни клаузули за пренос меѓу два контролора, меѓу кои може да избере контролорот што ги извезува податоците[232]. За пренос на релацијата контролор-обработувач, постои само еден вид стандардни договорни клаузули[233].

230 Директива за заштита на податоците, член 26 став 4.

231 ДФЕУ, член 288.

232 Првиот збир е содржан во Прилогот кон Европската комисија (2001), Одлука на Комисијата 2001/497/ЕЗ од 15 јуни 2001 година во врска со стандардни договорни клаузули за пренос на лични податоци во трети земји, во согласност со Директивата 95/46/ЕЗ, Сл. весник 2001 L 181; Вториот збир е содржан во Прилогот кон Европската комисија (2004), Одлука на комисијата 2004/915/ЕЗ од 27 декември 2004 година со која се изменува Одлуката 2001/497/ЕЗ во поглед на внесувањето на алтернативен збир од стандардни договорни клаузули за пренос на лични податоци во трети земји, Сл. весник 2004 L 385.

233 Европска комисија (2010), Одлука на Комисијата 2010/87 од 5 февруари 2010 година во врска со стандардни договорни клаузули за пренос на лични податоци до обработувачи во трети земји во согласност со Директивата 95/46/ЕЗ на Европскиот парламент и на Советот, Сл. весник 2010 L 39.

Во контекст на **правото на Советот на Европа,** Советодавниот комитет за Конвенцијата бр. 108 составил водич за подготвувањето на договорните клаузули[234].

6.4.2. Обврзувачки корпоративни правила

Мултилатералните обврзувачки корпоративни правила (ОКП) многу често истовремено вклучуваат неколку европски органи за заштита на податоците[235]. За да се одобрат таквите правила, на главниот орган треба да му се испрати предлог за ОКП заедно со стандардизиран образец за пријава[236]. Од стандардизираниот образец за пријава може да се види кој е главниот орган. Потоа, тој орган ги известува сите надзорни органи во државите-членки на ЕЕО во кои групацијата има свои подружници, иако нивното учество во процесот за евалуација на обврзувачките корпоративни правила е на доброволна основа.

Иако не е задолжително, сите засегнати органи за заштита на податоците би требало да го инкорпорираат резултатот од евалуацијата во нивните формални постапки на лиценцирање.

6.4.3. Посебни меѓународни договори

Европската Унија склучила посебни договори за два вида пренос на податоци:

Евиденција на патнички имиња

Авионските компании во текот на постапката на резервација собираат податоци од Евиденцијата на патнички имиња (ЕПИ), која вклучува имиња, адреси, податоци за кредитните картички и броеви на седиштата на патниците во воздушниот сообраќај. Според законите на САД, авионските компании се должни тие податоци

234 СЕ, Советодавен комитет за Конвенцијата бр. 108 (2002), *Водич за подготовката на договорни клаузули со кои се уредува заштитата на податоците во текот на преносот на лични податоци до трети страни кои не се обврзани со соодветен степен на заштита на податоците.*

235 Содржината и структурата на соодветните обврзувачки корпоративни правила се објаснети во Работната група за член 29 (2008), *Работен документ за поставување на рамката за структурата на обврзувачките корпоративни правила,* РГ 154, Брисел, 24 јуни 2008 год.; и во Работната група за член 29 (2008), *Работен документ за изработка на табела со елементите и начелата од обврзувачките корпоративни правила*, РГ 153, Брисел, 24 јуни 2008 год.

236 Работна група за член 29 (2007), *Препорака 1/2007 за стандардната примена на одобрението на обврзувачките корпоративни правила за пренос на лични податоци,* РГ 133, Брисел, 10 јануари 2007 год.

да му ги стават на располагање на Министерството за домашна безбедност (*US Department od Homeland Security*, DHS) пред полетувањето на патниците. Тоа се однесува на летови до и од САД.

Со цел да се осигури соодветна заштита на податоците од Евиденцијата на патнички имиња во согласност со одредбите на Директивата 95/46/ЕЗ, во 2004 година е усвоен „ЕПИ-пакет"[237], кој ја вклучувал соодветноста на заштитата на обработката на податоците што ја спроведувало Министерството за домашна безбедност на САД.

По прогласувањето на ЕПИ-пакетот за неважечки од страна на Судот на правдата на Европската Унија[238], Европската Унија и Соединетите Американски Држави потпишале два посебни договора за следните цели: прво, да осигурат правна основа за откривање на податоците содржани во Евиденцијата на патничките имиња на органите на САД, и второ, да воспостават соодветна заштита на податоците во земјата што е корисник.

Првиот договор меѓу земјите на Европската Унија и Соединетите Американски Држави за начинот на кој тие разменуваат податоци и управуваат со нив е потпишан во 2012 година, но имал неколку недостатоци и истата година бил заменет со друг договор со кој се осигурувала поголема правна сигурност[239].

Новиот договор нуди значителни подобрувања. Со него се ограничуваат и се појаснуваат целите за кои можат да се користат информациите, како што се сериозен транснационален криминал и тероризам, а освен тоа се утврдува и временскиот период за задржување на податоците: по шест месеци податоците мора да се маскираат и да се деперсонализираат. Во случај на злоупотреба на

237 Одлука на Советот 2004/496/ЕЗ од 17 мај 2004 година во врска со склучувањето Договор меѓу Европската Заедница и Соединетите Американски Држави за обработка и пренос на податоците содржани во Евиденцијата на патнички имиња од страна на авионски превозници до Министерството за домашна безбедност на САД, Биро за царини и заштита на границите, Сл. весник 2004 L 183, стр. 83, и Одлука на Комисијата 2004/535/ЕЗ од 14 мај 2004 година во врска со соодветната заштита на личните податоци содржани во Евиденцијата на патнички имиња на патниците во воздушниот сообраќај до Бирото за царини и заштита на границите на САД, Сл. весник 2004 L 235, стр. 11-22.

238 СПЕУ, Заеднички случаи С-317/04 и С-318/04, *European Parliament v. Council of the European Union,* 30 мај 2006 година, параграфи. 57, 58 и 59, во кои Судот одлучил дека и одлуката за соодветност и договорот за обработка на податоците се надвор од опфатот на Директивата.

239 Одлука на Советот 2012/472/ЕУ од 26 април 2012 год. во врска со склучувањето на Договор меѓу Соединетите Американски Држави и Европската Унија за употребата и преносот на Евиденцијата на патнички имиња до Министерството за домашна безбедност на САД, Сл. весник 2012 L 215/4. Текстот на Договорот е приложен кон оваа Одлука, Сл. весник 2012 L 215, стр. 5-14.

неговите податоци, секое лице има право да поднесе жалба во управна и судска постапка во согласност со законодавството на САД. Исто така, тоа лице има право на пристап до сопствените податоци од Евиденцијата на патнички имиња и, ако информациите се неточни, да побара нивна исправка од страна на Министерството за домашна безбедност на САД, вклучувајќи ја и можноста за бришење.

Договорот кој стапи на сила на 1 јули 2012 година останува на сила седум години, до 2019 година.

Во декември 2011 година, Советот на Европската унија го одобрил склучувањето на еден ажуриран Договор меѓу Европската Унија и Австралија во врска со обработката и преносот на податоци од Евиденцијата на патнички имиња[240]. Договорот меѓу Европската Унија и Австралија во врска со податоците од ЕПИ претставува натамошен чекор на агендата на Европската Унија, која вклучува глобални насоки за ЕПИ[241], со кои се предвидува концепт за ЕПИ на Европската Унија[242] и склучување договори со трети земји[243].

Податоци за финансиски пораки

Друштвото за светски интербанкарски финансиски телекомуникации (SWIFT), со седиште во Белгија, кое го обработува најголемиот дел на глобалниот пренос на пари од европските банки, работело со „огледален" компјутерски центар (mirror centre) во Соединетите Американски Држави, па од него е побарано да му открие

240 Одлука на Советот 2012/381/ЕУ од 13 декември 2011 год. во врска со склучувањето на Договорот меѓу Европската Унија и Австралија за обработка и пренос на податоци содржани во Евиденцијата на патнички имиња (ЕПИ) од страна на авионски компании до австралиската Служба за царинска и гранична заштита, Сл. весник 2012 L 186/3. Текстот на Договорот со кој се заменува претходен договор од 2008 година е приложен кон оваа Одлука, Сл. весник 2012 L 186, стр. 4–16.

241 Види го особено Соопштението на Комисијата од 21 септември 2010 год. во врска со глобалниот пристап при преносот на податоците содржани во Евиденцијата на патнички имиња (ЕПИ) до трети земји, COM(2010) 492 конечно, Брисел, 21 септември 2010 год. Исто така види Работна група за членот 29 (2010), *Мислење 7/2010 во врска со Соопштението на Европската комисија за глобалниот пристап до пренос на податоци содржани во Евиденцијата на патнички имиња (ЕПИ) до трети земји*, РГ 178, Брисел, 12 ноември 2010 год.

242 Предлог за Директива на Европскиот парламент и на Советот за користењето податоците од ЕПИ за целите на спречувањето, откривањето, истрагата и гонењето на терористички кривични дела и тежок криминал,COM(2011) 32 конечно, Брисел, 2 февруари 2011 год. Во април 2011 год., Европскиот парламент побарал мислење од Европската агенција за основните права за тој предлог и за неговата усогласеност со Повелбата за основните права на Европската Унија. Види: ЕАОП (2011), *Мислење 1/2011 – Евиденција на патнички имиња,* Виена, 14 јуни 2011 год.

243 Европската Унија води преговори за нов договор за ЕПИ со Канада, со кој ќе се замени договорот од 2006 година кој е важечки во моментов.

податоци на Министерството за финансии на САД за целите на истрагата на тероризмот[244].

Според гледиштето на Европската Унија, не постоела доволна правна основа за откривање на тие, во суштина, европски податоци, кои требало да се пренесат во САД само поради тоа што таму се наоѓал еден од центрите на SWIFT за обработка на податоците.

Во 2010 година бил склучен посебен договор меѓу Европската Унија и САД, познат како Договор за SWIFT, со цел да се безбеди потребната правна основа и да се осигури соодветна заштита на податоците[245].
Според тој договор, финансиските податоци кои ги складирало SWIFT и понатаму се доставувале до Министерството за финансии на САД за целите на спречувањето, истрагата, откривањето или гонењето на тероризмот или на финансирањето терористички активности. Министерството за финансии на САД може да побара финансиски податоци од SWIFT, под услов барањето:

- колку што е можно појасно да ги означува финансиските податоци;
- јасно да ја поткрепува неопходноста од податоците;
- да биде формулирано колку што е можно попрецизно за да се сведе на минимална количина на побараните податоци;
- да не бара податоци во врска со Единствената европска платежна област (ЕЕПО).

244 Види, во таа смисла, Работна група за членот 29 (2011), *Мислење 14/2011 за прашања на заштитата на податоците кои се поврзани со спречувањето на перењето пари и финансирањето тероризам*, РГ 186, Брисел, 13 јуни 2011 год.; Работна група за членот 29 (2006), *Мислење 10/2006 за обработката на лични податоци од страна на Друштвото за светски интербанкарски финансиски телекомуникации (SWIFT),* РГ 128, Брисел, 22 ноември 2006 год.; Белгиска комисија за заштита на приватноста (*Commission de la protection de la vie privée*) (2008), *„Постапка за контрола и препорака поведена во однос на компанијата SWIFT scrl"*, Одлука, 9 декември 2008 год.

245 Одлука на Советот 2010/412/ЕУ од 13 јули 2010 год. за склучувањето на Договорот меѓу Европската Унија и Соединетите Американски Држави за обработка и пренос на податоци за финансиски пораки од Европската Унија до Соединетите Американски држави за целите на програмата за следење на финансирањето тероризам, Сл. весник 2010 L 195, стр. 3 и 4. Текстот на Договорот е приложен кон оваа Одлука, Сл. весник 2010 L 195, стр. 5-14.

Европол мора да добие примерок од секое барање на Министерството за финансии на САД и да провери дали се почитуваат начелата на Договорот за SWIFT[246]. Ако се потврди дека се почитуваат, SWIFT мора да ги достави финансиските податоци директно до Министерството за финансии на САД.

Министерството мора да ги складира финансиските податоци во физички безбедна средина така што до нив ќе можат да пристапат само аналитичари кои го истражуваат тероризмот или неговото финансирање, а таквите податоци не смеат да бидат меѓусебно поврзани со никоја друга база на податоци. Начелно, финансиските податоци применети од SWIFT мора да се избришат најдоцна по навршувањето на пет години од нивниот прием. Финансиските податоци кои се релевантни за определени истраги или за кривичен прогон можат да се задржат сè додека податоците се потребни за таквите истраги или гонења.

Министерството за финансии на САД може да пренесе информации од податоците кои се добиени од SWIFT до определени органи за спроведување на законите, за јавна безбедност или за борба против тероризмот, во или надвор од Соединетите Американски Држави, исклучиво заради целите на истрагата, откривањето, спречувањето или прогонот на тероризмот и на неговото финансирање. Ако натамошниот пренос на финансиски податоци вклучува граѓанин или државјанин на држава-членка на Европската Унија, секоја размена на податоците со органи на трета земја подлежи на претходна согласност на надлежните органи на засегнатата држава-членка. Може да се направат исклучоци ако размената на податоците е од суштинска важност за спречувањето на непосредна и сериозна закана за јавната безбедност.

Независните органи кои вршат надзор, вклучувајќи и лице кое е именувано од Европската комисија, ја надгледуваат усогласеноста со начелата на Договорот за SWIFT.

Субјектите на податоците имаат право да добијат потврда од надлежен орган на Европската Унија за заштита на податоците дека се почитуваат нивните права на заштита на податоците. Субјектите на податоците исто така имаат право на исправка, бришење или блокирање на своите податоци кои биле собрани и складирани од страна на Министерството за финансии на САД според Договорот за SWIFT. Меѓутоа, правата на пристап на субјектите на податоците можат да подлежат на определени правни ограничувања. Ако му е одбиен пристапот,

246 Заедничкото надзорно тело на Европол извршило надзор над активностите на Европол во оваа област, а резултатот од таквиот надзор е достапен на: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

субјектот на податоците мора да биде писмено известен за одбивањето и за неговото право на жалба во управна и судска постапка во Соединетите Американски Држави.

Договорот за SWIFT е со важност од пет години, односно до август 2015 година. Автоматски се продолжува за дополнителен период од една година, освен ако некоја од страните ја извести другата најмалку шест месеци претходно за својата намера да не го продолжи договорот.

7

Заштитата на податоците во контекст на полицијата и на кривичното правосудство

Европска Унија	Обработени прашања	Совет на Европа
	Општо	Конвенција бр. 108
	Полиција	Препорака на полицијата
		ЕСЧП, *B.B. v. France*, No. 5335/06, 17 декември 2009 год. ЕСЧП, *S. and Marper v. the United Kingdom*, бр. 30562/04 и 30566/04, 4 декември 2008 год. ЕСЧП, *Vetter v. France*, бр.59842/00, 31 мај 2005 год.
	Компјутерски криминал	Конвенција за компјутерски криминал
Заштитата на податоците во смисла на прекугранична соработка на полициските и правосудните органи		
Рамковна одлука за заштита на податоците	Општо	Конвенција бр. 108 Препорака на полицијата
Одлука од Прим	За посебни податоци: отпечатоци од прсти, ДНК, хулиганизам итн.	Конвенција бр.108 Препорака на полицијата
Одлука на Европол Одлука на Европравда Регулатива на Фронтекс	На посебни агенции	Конвенција бр. 108 Препорака на полицијата

Одлука Шенген II Одлука за ВИС Регулатива за Евродак Одлука за ЦИС	На посебни заеднички информациски системи	Конвенција бр. 108 Препорака на полицијата ЕСЧП, *Dalea v. France*, бр. 964/07, 2 февруари 2010 год.

За да се постигне урамнотеженост на интересите на поединецот за заштита на податоците и интересите на општеството за собирање податоци за целите на борбата против криминалот и во осигурувањето на националната и јавната безбедност, Советот на Европа и Европската Унија усвоиле посебни правни инструменти.

7.1. Правото на Советот на Европа за заштита на податоците во полициски и во кривично-правни предмети

Клучни точки

- Конвенцијата бр. 108 и Препораката на Советот на Европа за полицијата се однесуваат на заштитата на податоците во сите области на работата на полицијата.
- Конвенцијата за компјутерски криминал (*Конвенцијата од Будимпешта*) е обврзувачки меѓународен правен иструмент кој се занимава со криминал што е извршен против и преку електронски мрежи.

На ниво на Европа, Конвенцијата бр. 108 ги опфаќа сите области на обработка на лични податоци, а целта на нејзините одредби е општо да се уреди обработката на лични податоци. Според тоа, Конвенцијата бр. 108 се однесува на заштита на податоците во областа на полицијата и кривичното правосудство, но договорните страни можат да ја ограничат нејзината примена.

Правните задачи на органите на полицијата и на кривичното правосудство често налагаат обработка на лични податоци која може да има сериозни последици за засегнатите поединци. Препораката за полициските податоци, која Советот на Европа ја усвоил во 1987 година, им дава насоки на договорните страни за начинот

на кој треба да ги спроведуваат начелата на Конвенцијата бр. 108 во контекст на обработката на лични податоци од страна на полициските органи[247].

7.1.1. Препорака за полицијата

Ставот на Европскиот суд за човекови права е дека складирањето и задржувањето на лични податоци од страна на некои органи на полицијата или на националната безбедност претставува мешање во членот 8 став 1 од Европската конвенција за човекови права. Многу пресуди на Европскиот суд за човекови права се однесуваат на оправданоста на таквите мешања[248].

Пример: Во предметот *B.B. v. France*[249], Европскиот суд за човекови права одлучил дека внесувањето на осуден сексуален престапник во национална правосудна база на податоци потпаѓало под членот 8 од Европската конвенција за човековите права. Меѓутоа, со оглед на тоа што биле внесени доволно мерки за заштита на податоците, како што се правото на субјектот на податоците да побара бришење на податоците, ограниченото времетраење на складирањето на податоците и ограниченият пристап до таквите податоци, била постигната правична рамнотежа меѓу предметните приватни и јавни интереси кои биле спротивставени. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Пример: Во предметот *S. and Marper v. the United Kingdom*[250], двајцата жалители биле обвинети, но не и осудени, за кривични дела. Сепак, полицијата ги задржала и ги складирала нивните отпечатоци од прсти, ДНК-профили и примероци од клетки. Неограниченото задржување на биометриски податоци било законски дозволено ако лицето било осомничено за кривично дело, дури и ако осомниченият подоцна бил ослободен од обвинението или пуштен на слобода. Европскиот суд за човекови права сметал дека паушалното и неселективно задржување на лични податоци, кое не било временски ограничено и при кое ослободените поединци имале само

247 СЕ, Комитет на министри (1987), Препорака Rec(87)15 до државите-членки во врска со употребата на лични податоци во полициското сектор, 17 септември 1987 год.

248 Види, на пример, Европски суд за човекови права, *Leander v. Sweden*, бр. 9248/81, 26 март 1987 год.; Европски суд за човекови права, *M.M. v. the United Kingdom*, бр. 24029/07, 13 ноември 2012 год.; Европски суд за човекови права, *M.K. v. France*, бр. 19522/09, 18 април 2013 год.

249 ЕСЧП, *B.B. v. France*, бр. 5335/06, 17 декември 2009 год.

250 ЕСЧП, *S. and Marper v. the United Kingdom*, бр. 30562/04 и 30566/04, 4 декември 2008 год., параграфи 119 и 125.

ограничени можности да побараат бришење, претставувало несразмерно мешање во правото на жалителите на почитување на нивниот приватен живот. Судот заклучил дека имало повреда на членот 8 од Конвенцијата.

Многу други пресуди на Европскиот суд за човекови права се однесуваат на оправданоста на мешањето во правото на заштита на податоците со помош на надзор.

Пример: Во предметот *Allan v. the United Kingdom*[251], надлежните органи тајно снимале приватни разговори на затвореник со пријател во затворската соба за посети и со сообвинет во затворската ќелија. Европскиот суд за човекови права сметал дека употребата на уредите за аудио и видеоснимање во ќелијата на жалителот, во затворската соба за посети и на созатвореник претставувала мешање во правото на приватен живот на жалителот. Бидејќи во тоа време не постоел правен систем со кој би се регулирала употребата на уреди за тајно снимање од страна на полицијата, споменатото мешање не било во согласност со законот. Судот заклучил дека имало повреда на членот 8 од Конвенцијата.

Пример: Во предметот *Klass and Others v. Germany*[252], жалителите тврделе дека неколку германски законодавни акти со кои се дозволувал таен надзор на електронските пораки, поштата и телекомуникациите го повредувале членот 8 на Европската конвенција за човековите права, особено поради тоа што засегнатото лице не било известено за надзорните мерки и не можело да се обрати до судовите откако завршиле таквите мерки. Европскиот суд за човековите права сметал дека заканата со вршење надзор нужно ја попречувала слободата на комуникација меѓу корисниците на поштенските и телекомуникациските услуги. Меѓутоа, тој утврдил дека биле внесени доволно заштитни мерки против злоупотреба. Германското законодавство оправдано сметало дека таквите мерки биле неопходни во едно демократско општество во интерес на националната безбедност и поради спречување на нереди или криминал. Судот заклучил дека немало повреда на членот 8 од Конвенцијата.

251 ЕСЧП, *Allan v. the United Kingdom*, бр. 48539/99, 5 ноември 2002 год.

252 ЕСЧП, *Klass and Others v. Germany*, бр. 5029/71, 6 септември 1978 год.

Бидејќи обработката на податоците од страна на полициските органи може да има значително влијание на засегнатите лица, во таа област особено се неопходни детални правила за заштита на податоците кои се однесуваат на водењето на бази на податоци. Целта на Препораката на Советот на Европа за полицијата била да се реши прашањето со давање насоки за начинот на кој би требало да се собираат податоците за потребите на полицијата; за начинот на чување на податочните датотеки во таа област; за тоа на кого би требало да му се дозволи пристап до тие датотеки, вклучувајќи ги условите за пренос на податоците до странски полициски органи; за начинот на кој субјектите на податоците би требало да можат да ги остваруваат своите права на заштита на податоците; и за начинот на кој независните органи би требало да спроведуваат контрола. Земена е предвид и обврската да се осигури соодветна безбедност на податоците.

Препораката не предвидува отворено, неселективно собирање на податоци од страна на полициски органи. Со неа собирањето на лични податоци од страна на полициски органи се ограничува на количина која е неопходна за спречување на вистинска опасност или за сузбивање на определено кривично дело. Секое дополнително собирање на податоци би требало да се заснова на посебно национално законодавство. Обработката на чувствителните податоци би требало да се ограничи на количина која е апсолутно неопходна во смисла на определена истрага.

Ако личните податоци биле собрани без знаење на субјектот на податоците, тогаш тој треба да биде информиран за собирањето на податоците веднаш штом таквото откривање нема да ѝ пречи на истрагата. Собирањето на податоците кои се добиени со технички надзор или со други автоматски средства исто така треба да биде засновано на посебни правни одредби.

Пример: Во предметот *Vetter v. France*[253], анонимни сведоци го обвиниле жалителот за убиство. Бидејќи жалителот редовно го посетувал домот на еден негов пријател, полицијата во него поставила уреди за прислушување со дозвола на истражниот судија. Врз основа на снимените разговори, жалителот бил уапсен и кривично гонет за убиство. Тој побарал снимката да се прогласи за недопуштена како доказ, тврдејќи особено дека не била законски прибавена. Европскиот суд за човековите права требало да одлучи дали употребата на уредите за прислушување била „во согласност со законот". Поставувањето уреди за прислушување во приватни простории очигледно не спаѓало во

253 ЕСЧП, *Vetter v. France*, бр. 59842/00, 31 мај 2005 год.

опфатот на членот 100 *и на наредните членови* на Законот за кривичната постапка бидејќи тие одредби се однесувале на следењето на телефонските линии. Во членот 81 од Законот не е доволно јасно наведен опфатот или начинот на кој надлежните органи го користат своето дискрециско право при одобрувањето на следењето на приватни разговори. Според тоа, жалителот не уживал ни најмал степен на заштита на која граѓаните имале право во согласност со владеењето на правото во едно демократско општество. Судот заклучил дека имало повреда на членот 8 на Конвенцијата.

Во препораката е содржан заклучокот дека при складирањето на личните податоци треба да се прави јасна разлика меѓу: административните податоци и полициските податоци; различните видови на субјекти на податоците, како и осомничените, осудените лица, жртвите и сведоците; и меѓу податоците кои се сметаат за цврсти факти и оние што се темелат на сомневања или нагаѓања.

Полициските податоци треба строго да се ограничат во однос на целта. Тоа влијае на соопштувањето на полициските податоци на трети лица: преносот или соопштувањето на таквите податоци во рамките на полицискиот сектор би требало да зависат од тоа дали постои легитимен интерес за споделување на информациите. Преносот или соопштувањето на таквите податоци надвор од полицискиот сектор би требало да бидат дозволени само ако постои јасна правна обврска или овластување. Меѓународниот пренос или соопштување би требало да се ограничат на странски полициски органи и да се засновани на посебни правни одредби, како што се меѓународните договори, освен во случај кога тоа е потребно за да се спречи сериозна и непосредна опасност.

Обработката на податоците што ја врши полицијата мора да подлежи на независен надзор за да се осигури усогласеност со домашното законодавство за заштита на податоците. Субјектите на податоците мора да ги имаат сите права на пристап кои произлегуваат од Конвенцијата бр. 108. Ако правата на пристап на субјектите на податоците се ограничени во согласност со членот 9 на Конвенцијата бр. 108 во интерес на делотворните полициски истраги, според домашното законодавство субјектот на податоците мора да има право на жалба до националниот надзорен орган за заштита на податоците или до друго независно тело.

7.1.2. Конвенцијата од Будимпешта за компјутерски криминал

Бидејќи криминалните активности сè почесто користат електронски системи за обработка на податоци и им влијаат на таквите системи, за да се пресретне тој предизвик, потребни се нови кривично-правни одредби. Затоа, Советот на Европа усвоил меѓународен правен инструмент, односно Конвенција за компјутерски криминал – исто така позната како Конвенцијата од Будимпешта – за да го реши проблемот со кривичните дела сторени против и преку електронски мрежи[254]. Кон оваа Конвенција можат да пристапат и држави што не се членки на Советот на Европа и, до средината на 2013 година, четири држави надвор од Советот на Европа – Австралија, Доминиканската Република, Јапонија и Соединетите Американски Држави – биле договорни страни на Конвенцијата, а 12 други држави што не се членки ја потпишале или биле поканети да ѝ пристапат.

Конвенцијата за компјутерски криминал и понатаму е највлијателниот меѓународен договор кој се занимава со повреди на правото преку интернет или преку други информациски мрежи. Нејзините договорни страни мораат да ги ажурираат и да ги усогласат своите кривични закони против хакирања и други повреди на сигурноста, вклучувајќи ги и повредите на авторските права, компјутерски потпомогнатата измама, детската порнографија и други забранети компјутерски активности. Со конвенцијата се пропишани и процедурални овластувања кои го опфаќаат пребарувањето на компјутерските мрежи и следењето на комуникациите во смисла на борба против компјутерскиот криминал. Конечно, со неа е овозможена ефикасна меѓународна соработка. Дополнителен протокол кон Конвенцијата се занимава со инкриминација на расистичките и ксенофобичните пропаганди во компјутерските мрежи.

Иако Конвенцијата не претставува вистински инструмент за унапредување на заштитата на податоците, со неа се инкриминираат активности за кои е веројатно дека ќе го повредат правото на субјектот на податоците на заштита на неговите податоци. Таа, исто така, ги обврзува договорните страни при спроведувањето на конвенцијата да предвидат соодветна заштита на човековите права и слободи, вклучувајќи ги и правата кои се загарантирани со Европската конвенција за човековите права, како што е правото на заштита на податоците[255].

254 Совет на Европа, Комитет на министри (2001), Конвенција за компјутерски криминал, ЗДСЕ бр. 185, Будимпешта, 23 ноември 2001 год., стапена во сила од 1 јули 2004 год.

255 *На истото место*, член 15 став 1.

7.2. Правото на Европската Унија за заштита на податоците во полициски и во кривично-правни предмети

Клучни точки

- На ниво на Европската Унија, заштитата на податоците во полицискиот и во кривично-правниот сектор е уредена само во смисла на прекугранична соработка на полицијата и правосудните органи.
- За Европската полициска агенција (Европол) и за Европското тело за зајакнување на судската соработка (Европравда), тела на Европската Унија кои помагаат и го унапредуваат прекуграничното спроведување на законите, постојат посебни режими за заштита на податоците.
- Посебни режими за заштита на податоците постојат и за заедничките информациски системи кои се воспоставени на ниво на Европската Унија за прекугранична размена на информации меѓу надлежните полициски и правосудни органи. Значајни примери се Шенген 2, Визниот информациски систем (ВИС) и Евродак, централизиран систем кој содржи податоци за отпечатоци од прсти на државјани на трети земји кои бараат азил во некоја од државите-членки на Европската Унија.

Директивата за заштита на податоците не се однесува на областа на полицијата и кривичното правосудство. Во поглавјето 7.2.1. се опишани најважните правни инструменти во таа област.

7.2.1. Рамковна одлука за заштита на податоците

Целта на Рамковната одлука на Советот 2008/977/ЈНА за заштита на личните податоци што се обработуваат во рамките на полициската и правосудната соработка во кривични предмети (*Рамковна одлука за заштита на податоците*)[256]е да осигури заштита на личните податоци на физички лица кога нивните податоци се обработуваат за целите на спречувањето, истрагата, откривањето или прогонот на кривични дела или поради извршување на казните. Во име на државата-членка

256 Совет на Европската Унија (2008), Рамковна одлука на Советот 2008/977/ЈНА од 27 ноември 2008 год. за заштита на личните податоци што се обработуваат во рамките на полициската и правосудната обработка во кривични предмети (*Рамковна одлука за заштита на податоците*), Сл. весник 2008 L 350.

или на Европската Унија дејствуваат надлежни органи кои работат во областа на полицијата и кривичното правосудство. Тие органи се агенции или тела на Европската Унија, како и органи на државите-членки[257]. Применливоста на рамковната одлука е ограничена на осигурување на заштитата на податоците во прекуграничната соработка меѓу тие органи и не се проширува на националната безбедност.

Рамковната одлука за заштита на податоците во голема мера се потпира на начелата и дефинициите што се содржани во Конвенцијата бр. 108 и во Директивата за заштита на податоците.

Податоците смее да ги користи само надлежен орган и само за целта за која биле пренесени или ставени на располагање. Државата-членка што е корисник мора да ги почитува сите ограничувања на размената на податоците кои се пропишани во законодавството на државата-членка што ги пренесува податоците. Меѓутоа, државата што ги прима податоците смее да ги користи податоците за други цели во определени околности. Забележувањето и документирањето на преносот се посебни должности на надлежните органи поради помагање во појаснувањето на одговорностите што произлегуваат од жалбите. За натамошен пренос на податоци што се примени во текот на прекугранична соработка до трети страни, потребна е согласноста на државата-членка од која потекнуваат податоците, но постојат и исклучоци во итни случаи.

Надлежните органи мораат да ги преземат потребните мерки за да ги заштитат личните податоци од секаков вид на незаконита обработка.

Секоја држава-членка мора да осигури дека еден или повеќе независни национални надзорни органи се одговорни за советување и за следење на примената на одредбите кои се усвоени во согласност со Рамковната одлука за заштита на податоците. Тие мораат да ги сослушаат барањата кои се поднесени од кое било лице и кои се однесуваат на заштитата на неговите права и слободи во поглед на обработката на личните податоци од страна на надлежните органи.

Субјектот на податоците има право на информации во врска со обработката на неговите лични податоци и има право на пристап, исправка, бришење или блокирање. Ако остварувањето на тие права е одбиено од убедливи причини, субјектот на податоците мора да има право на жалба до надлежниот национален надзорен орган и/или до суд. Ако некое лице претрпи штета поради повреда

257 *На истото место*, член 2 (ж).

на националното законодавство со кое се спроведува Рамковната одлука за заштита на податоците, тоа лице има право на надомест од контролорот[258]. Начелно, субјектите на податоците мора да имаат пристап до правно средство за секакво прекршување на нивните права кои се загарантирани со националното законодавство со кое се спроведува Рамковната одлука за заштита на податоците[259].

Европската комисија предложи реформа која се состои од Општа регулатива за заштита на податоците[260] и од Општа директива за заштита на податоците[261]. Со таа нова директива ќе се замени моменталната Рамковна одлука за заштита на податоците и ќе се применат општите начела и правила за соработка на полицијата и на правосудните органи во кривични предмети.

7.2.2. Поспецифични правни инструменти за заштита на податоците во прекуграничната соработка на полицијата и на органите на кривичниот прогон

Освен со Рамковната одлука за заштита на податоците, размената на информации меѓу државите-членки во определени области е уредена и со низа други правни инструменти, како на пример Рамковната одлука на Советот 2009/315/ЈНА за организацијата и содржината на размената на информации содржани во криминалното досие меѓу државите-членки и Одлуката на Советот во врска со уредувањето на соработката меѓу единиците за финансиско разузнавање на државите-членки во врска со размената на информации[262].

258 *На истото место*, член 19.

259 *На истото место*, член 20.

260 Европска комисија (2012), *Предлог за Регулатива на Европскиот парламент и на Советот за заштита на поединците во однос на обработката на лични податоци и на слободното движење на такви податоци (Општа регулатива за заштита на податоците)*, COM(2012) 11 конечно, Брисел, 25 јануари 2012 год.

261 Европска комисија (2012), *Предлог за Директива на Европскиот парламент и на Советот за заштита на поединците во однос на обработката на лични податоци од страна на надлежни органи за целите на спречувањето, истрагата, откривањето или гонењето на кривичните дела или извршувањето на казните и слободното движење на таквите податоци (Општа директива за заштита на податоците)*, COM(2012) 10 конечно, Брисел, 25 јануари 2012 год.

262 Совет на Европската унија (2009), Рамковна одлука на Советот 2009/315/ЈНА од 26 февруари 2009 год. за организацијата и содржината на размената на информации содржани во криминалното досие меѓу државите-членки, Сл. весник 2009 L 93; Совет на Европската Унија (2000), Одлука на Советот 2000/642/ЈНА од 17 октомври 2000 год. во врска со уредувањето на соработката

Важно е да се напомене дека прекуграничната соработка[263] меѓу надлежните органи сè повеќе ја вклучува размената на имигрициски податоци. Таа правна област не спаѓа во полициските и кривично-правните предмети, но по многу нешта е релевантна за работата на полициските и правосудните органи. Истото важи и за податоците за стоките кои се увезуваат во Европската Унија или се извозуваат од неа. Укинувањето на внатрешните гранични контроли во Европската Унија го зголеми ризикот од измама, па државите-членки мораат да ја зајакнат соработката, особено со подобрување на прекуграничната размена на податоци со цел за поефикасно откривање и прогон на повредите на националното и царинското право на Европската Унија.

Одлуката од Прим

Важен пример за институционализирана прекугранична соработка преку размена на податоците кои се чуваат на национално ниво е Одлуката на Советот 2008/615/ЈНА за продлабочување на прекуграничната соработка, особено во сузбивањето на тероризмот и прекуграничниот криминал (*Одлуката од Прим*), со која Договорот од Прим е инкорпориран во правото на Европската Унија во 2008 година[264]. Договорот од Прим е договор за меѓународна полициска соработка, кој во 2005 година бил потпишан од: Австрија, Белгија, Франција, Германија, Луксембург, Холандија и Шпанија[265].

Целта на Одлуката од Прим е да им се помогне на државите-членки да ја подобрат размената на информации за спречување и сузбивање на криминал во три области: тероризам, прекуграничен криминал и незаконска миграција. За таа цел, во одлуката се предвидени одредби во поглед на:

- автоматизиран пристап до ДНК-профили, податоци за отпечатоци од прсти и определени национални податоци за регистрација на возила;

меѓу единиците за финансиско разузнавање на државите-членки во врска со размената на информации, Сл. весник 2000 L 271.

263 Европска комисија (2012), Соопштенија од Комисијата до Европскиот парламент и Советот – Зајакнување на полициската соработка во Европската Унија: Европскиот модел за размена на информации (EIXM), COM(2012) 735 конечно, Брисел, 7 декември 2012 год.

264 Совет на Европската Унија (2008), Одлука на Советот 2008/615/ЈНА од 23 јуни 2008 год. за продлабочување на прекуграничната соработка, особено во сузбивањето на тероризмот и прекуграничниот криминал, Сл. весник 2008 L 210.

265 Конвенција меѓу Кралство Белгија, Сојузна Република Германија, Кралство Шпанија, Република Франција, Големо Војводство Луксембург, Кралство Холандија и Република Австрија за продлабочување на прекуграничната соработка, особено во сузбивањето на тероризмот, прекуграничниот криминал и незаконската миграција; достапна на: http://register.consilium.europa.eu/pdf/en/05/st10/ st10900.en05.pdf.

- давањето податоци во врска со големи настани кои имаат прекугранично карактер;
- давањето информации со цел да се спречат терористички кривични дела;
- други мерки за продлабочување на прекуграничната полициска соработка.

Базите на податоци кои се стават на располагање според Одлуката од Прим се целосно уредени со националното законодавство, додека размената на податоци е дополнително уредена со одлуката и, од неодамна, со Рамковната одлука за заштита на податоците. Телата кои се надлежни за надзор на таквиот пренос на податоци се национални надзорни органи за заштита на податоците.

7.2.3. Заштитата на податоците во Европол и во Европравда

Европол

Европол, агенцијата за спроведување на правото на Европската Унија со седиште во Хаг, има национални одделенија за Европол (НОЕ) во секоја држава-членка. Европол е основан во 1998 година; неговиот моментален правен статус како институција на Европската Унија е заснован на Одлуката на Советот за основање на Европската полициска агенција (*Одлуката за Европол*)[266]. Целта на Европол е да помогне при спречувањето и истрагата на организираниот криминал, тероризмот и други облици на тежок криминал, како што е наведено во Прилогот кон Одлуката за Европол, кои се однесуваат на две или повеќе држави-членки.

За да ги постигне своите цели, Европол го воспоставил информацискиот систем на Европол, кој претставува база на податоци, врз чија основа државите-членки разменуваат сознанија и информации за кривични дела преку своите национални одделенија за Европол. Информацискиот систем на Европол може да се користи за ставање на располагање податоци кои се однесуваат на: лица кои се осомничени или осудени за кривично дело што е предмет на надлежност на Европол; или

266 Совет на Европската Унија (2009), Одлука на Советот од 6 април 2009 год. за основање на Европската полициска агенција, Сл. весник 2009 L 121 (Европол). Види го исто така предлогот на Комисијата со кој се пропишува правна рамка за нов Европол кој ќе го наследи и замени Европол, како што е утврдено со Одлуката на Советот 2009/371/ЈНА од 6 април 2009 год. за основање на Европската полициска управа (Европол), и КЕПОЛ, како што е утврдено со Одлука на Советот 2005/681/ЈНА за основање на Колеџот за европска полиција (КЕПОЛ), COM(2013) 173 конечно.

лица за кои постои оправдано сомнение дека ќе извршат такви дела. Европол и националните одделенија за Европол можат да внесуваат податоци директно во Информацискиот систем на Европол и да преземаат податоци од него. Податоците може да ги измени, исправи или избрише само странката која ги внела во системот.

Ако тоа е неопходно за извршување на неговите задачи, по пат на анализа на работните датотеки, Европол може да складира, да измени и да употреби податоци кои се однесуваат на кривични дела. Работните датотеки за анализа се создадени за целите на собирањето, обработката или употребата на податоците заради помагање во определени кривични истраги кои Европол ги спроведува заедно со државите-членки на Европската Унија.

Како одговор на новите промени, на 1 јануари 2013 година во Европол е основан Европскиот центар за компјутерски криминал[267]. Центарот има улога на средиште на Европската Унија за компјутерски криминал, кој придонесува за побрзо реагирање во случај на кривични дела на интернет, за развивање и примена на дигитални форензички решенија и ја прикажува најдобрата практика за истраги на компјутерски криминал. Центарот главно се занимава со компјутерски криминал кој:

- го вршат организирани групи со цел да остварат големи добивки од криминал, како што е измамата на интернет;
- ѝ нанесува голема штета на жртвата, како што е сексуалната експлоатација на деца на интернет;
- влијае на клучната инфраструктура и на информациските системи во Европската Унија.

Подобрен е режимот на заштита на податоците кој управува со активностите на Европол. Членот 27 на Одлуката за Европол пропишува дека се применуваат начелата кои се наведени во Конвенцијата бр. 108 и во Препораката за полициските податоци во врска со обработката на автоматизирани и неавтоматизирани податоци. Преносот на податоците меѓу Европол и државите-членки исто така мора да биде во согласност со правилата кои се содржани во Рамковната одлука за заштита на податоците.

267 Види исто така ЕСЗП (2012), *Мислење на Супервизорот за заштита на податоците во врска со соопштенијата од Европската комисија до Советот и до Европскиот парламент за основање на Европскиот центар за компјутерски криминал,* Брисел, 29 јуни 2012 год.

Независното заедничко надзорно тело при Европол (ЗНТ) ги прегледува и ги надгледува активностите на Европол со цел да осигури усогласеност со применливо законодавство за заштита на податоците, а особено со цел правата на поединците да не бидат повредени со обработка на личните податоци[268]. Секој поединец има право на пристап до сите лични податоци што Европол ги поседува за него, како и право да побара проверка, исправка или бришење на тие лични податоци. Ако лицето не е задоволно со некоја одлука на Европол во врска со остварувањето на тие права, може да се жали до Комитетот за жалби на Заедничкиото надзорно тело.

Ако дошло до штета поради правни или фактички грешки во податоците кои се складираат или се обработуваат во Европол, оштетената страна може да се жали само пред надлежен суд на државата-членка во која се случил настанот што ја предизвикал штетата[269]. Европол ќе ѝ ја надомести штетата на државата-членка ако до неа дошло поради тоа што Европол не ги исполнил своите правни обврски.

Европравда

Европравда е тело на Европската Унија основано во 2002 година со седиште во Хаг, кое ја унапредува судската соработка во истрагата и гонењето на тежок криминал од кој се засегнати барем две држави-членки[270]. Европравда е надлежна за:

- поттикнување и подобрување на координацијата на истрагите и прогонот меѓу надлежните органи на различните држави-членки;

- олеснување на извршувањето на барањата и одлуките кои се однесуваат на правосудната соработка.

Функциите во Европравда ги вршат национални членови. Секоја држава-членка именува по еден судија или јавен обвинител во Европравда, чиј статус подлежи на националното законодавство и кој располага со потребните стручни вештини

268 Одлука на Европол, член 34.

269 *На истото место*, член 52.

270 Совет на Европската Унија (2002), Одлука на Советот 2002/187/ЈНА од 28 февруари 2002 год. за основање на Европравда со цел за засилување на борбата против тежок криминал, Сл. весник 2002 L 63; Совет на Европската Унија (2003), Одлука на Советот 2003/659/ЈНА од 18 јуни 2003 год. за измена на Одлуката 2002/187/ЈНА за основање на Европравда со цел за засилување на борбата против тежок криминал, Сл. весник 2003 L 44; Совет на Европската Унија (2009), Одлука на Советот 2009/426/ЈНА од 16 декември 2008 год. за зајакнување на Европравда и за изменување на Одлуката 2002/187/ЈНА за основање на Европравда со цел за засилување на борбата против тежок криминал, Сл. весник 2009 L 138 (*Одлука за Европравда*).

за извршување на задачите кои се неопходни за поттикнување и подобрување на правосудната соработка. Покрај тоа, националните членови дејствуваат заеднички како колегиум за извршување на посебни задачи на Европравда.

Европравда може да обработува лични податоци ако тоа е потребно за да ги оствари своите цели. Меѓутоа, таа можност е ограничена на определени информации во врска со лица кои се осомничени дека сториле или учествувале во или биле осудени за кривично дело кое е предмет на надлежност на Европравда. Европравда може да обработува и определени информации во врска со сведоци или жртви на кривични дела кои потпаѓаат под неговата надлежност[271]. Во исклучителни околности и во текот на ограничен временски период, Европравда може да обработува повеќе лични податоци во врска со околностите на кривично дело ако таквите податоци се од непосредна важност за истрага што е во тек. Во рамките на својата област на надлежност, Европравда може да соработува со други институции, тела и агенции на Европската Унија и со нив да разменува лични податоци. Исто така, Европравда може да соработува и да разменува лични податоци и со трети земји и организации.

Во врска со заштитата на податоците, Европравда мора да гарантира ниво на заштита кое е барем еднакво со начелата на Конвенцијата бр. 108 на Советот на Европа и на нејзините подоцнежни измени.

При размена на податоците мора да се почитуваат посебните правила и ограничувања кои се внесени или со договор за соработка или со договори за работа во согласност со Одлуките на Советот за Европравда и со Правилата за заштита на податоците во Европравда[272].

Во Европравда е основано независно заедничко надзорно тело со задача да ја надгледува обработката на лични податоци која ја врши Европравда. Поединците можат да се жалат во заедничкото надзорно тело ако не се задоволни со одговорот на Европравда на барање за пристап, исправка, блокирање или бришење на лични податоци. Ако незаконито ги обработува личните податоци, Европравда ќе одговара во согласност со националното законодавство на државите-членки во местото на неговото седиште, Холандија, за штетата што му е причинета на субјектот на податоците.

271 Прочистена верзија на Одлуката на Советот 2002/187/ЈНА како што е изменета со Одлуката на Советот 2003/659/ЈНА и со Одлуката на Советот 2009/426/ЈНА, член 15 став 2.

272 Деловник за обработката и заштитата на личните податоци во Европравда, Сл. весник 2005 C 68/01, 19 март 2005 год., стр. 1.

7.2.4. Заштитата на податоците во заедничките информациски системи на ниво на Европската Унија

Покрај размена на податоците меѓу државите-членки и основањето на специјализирани органи на Европската Унија за сузбивање на прекугранично криминал, воспоставени се неколку заеднички информациски системи на ниво на Европската Унија кои служат како платформа за размена на податоци меѓу надлежните национални органи и органите на Европската Унија за посебните цели на спроведувањето на законот, вклучувајќи ги имиграциското и царинското право. Некои од овие системи се развиле од мултилатералните договори кои подоцна биле надополнети со правни инструменти и системи на Европската Унија, како што се Шенгенскиот информациски систем, Визниот информациски систем, Евродак, Евросур или Царинскиот информациски систем.

Европската агенција за големи информатички системи (ЕАГИС),[273] основана во 2012 година, е одговорна за долгорочното оперативно управување на втората генерација на Шенгенскиот информациски систем (ШИС II), Визниот информациски систем (ВИС) и со Евродак. Основната задача на Агенцијата е да осигури делотворно, сигурно и континуирано работење на информациските системи. Одговорна е и за усвојување на потребните мерки за сигурност на системите и на податоците.

Шенгенски информациски систем

Во 1985 година неколку држави-членки на поранешните Европски Заедници склучиле Договор со државите на Економската унија на Бенелукс, Германија и Франција за постепено укинување на контролата на нивните заеднички граници (*Шенгенски договор)* со цел да создадат простор за слободно движење на луѓе без да бидат попречени од гранични контроли во рамките на шенгенскиот простор[274]. Како противтежа на заканата за јавната безбедност која би можела да се произлезе од отворените граници, воспоставени се засилени гранични контроли

273 Регулатива (ЕУ) бр. 1077/2011 на Европскиот парламент и на Советот од 25 октомври 2011 год. за основање на Европската агенција за оперативно управување со големи информациски системи во областа на слободата, безбедноста и правдата, Сл. весник 2011 L 286.

274 Договор меѓу владите на државите на Економската Унија на Бенелукс, Сојузна Република Германија и Република Франција во врска со постепеното укинување на контролата на нивните заеднички граници, Сл. весник 2000 L 239.

на надворешните граници на шенгенската област, како и тесна соработка меѓу националната полиција и правосудните органи.

Како последица на пристапувањето на други држави кон Шенгенскиот договор, шенгенскиот систем конечно бил интегриран во правната рамка на Европската Унија со Договорот од Амстердам[275]. Таа одлука е спроведена во 1999 година. Најновата верзија на Шенгенскиот информациски систем, таканаречениот ШИС II, започна да функционира на 9 април 2013 година. Моментално со неа се служат сите држави-членки на Европската Унија, како и Исланд, Лихтенштајн, Норвешка и Швајцарија[276]. Европол и Европравда исто така имаат пристап до ШИС II.

ШИС II се состои од централен систем (Ц-ШИС), национален систем (Н-ШИС) во секоја држава-членка и од комуникациска инфраструктура меѓу централниот систем и националните системи. Ц-ШИС содржи определени податоци за лица и предмети кои се внесени од страна на државите-членки. Ц-ШИС се користи од страна на националните органи за гранична контрола, полициските, царинските, визните и правосудните органи во целокупната шенгенска област. Секоја од државите-членки управува со национална копија на Ц-ШИС, позната како Национален шенгенски информациски систем (Н-ШИС), која постојано се ажурира, а притоа се ажурира и Ц-ШИС. Националниот шенгенски информациски систем се прегледува и испраќа предупредување ако:

- лицето нема право да влезе или да остане во шенгенскиот простор;
- лицето или предметот се бара од страна на правосудните или полициските органи;
- лицето било пријавено за исчезнато;
- добрата, како што се банкноти, автомобили, камиони, огнено оружје и документи за идентификација, биле пријавени како украдени или изгубени.

275 Европски Заедници (1997), Договор од Амстердам за измена на Договорот за Европската Унија, договорите за основање на Европските Заедници и определени сродни акти, Сл. весник 1997 C 340.

276 Регулатива (ЕЗ) бр. 1987/2006 на Европскиот парламент и на Советот од 20 декември 2006 година за воспоставувањето, работењето и употребата на втората генерација на Шенгенски информациски систем, Сл. весник 2006 L 381 (*ШИС II*) и Совет на Европската Унија (2007), Одлука на Советот 2007/533/ЈНА од 12 јуни 2007 год. за воспоставувањето, работењето и употребата на втората генерација на Шенгенски информациски систем, (*ШИС II*), Сл. весник 2007 L 205.

Во случај на предупредување, треба да се започнат натамошни активности преку националните Шенгенски информациски системи.

ШИС II има нови функционалности, како што е можноста за внесување на биометриски податоци, како што се отпечатоците од прсти и фотографиите; или нови видови предупредувања, како што се украдени пловила, воздухоплови, контејнери или платежни средства; и засилени предупредувања за лица и објекти; копии од европските налози за апсење (ЕНА) за лица кои се бараат за апсење, нивно предавање или екстрадиција.

Во Одлуката на Советот 2007/533/ЈНА за воспоставувањето, работата и употребата на втората генерација на Шенгенскиот информациски систем (Одлука Шенген II), интегрирана е Конвенцијата бр. 108: „Личните податоци кои се обработуваат со примена на оваа одлука треба да бидат заштитени во согласност со Конвенцијата бр. 108 на Советот на Европа“[277]. Ако националните полициски органи ги користат личните податоци со примена на Одлуката Шенген II, одредбите на Конвенцијата бр. 108, како и Препораката за полициските податоци, мора да се внесат во националното законодавство.

Надлежниот национален надзорен орган во секоја држава-членка го надгледува националниот Н-ШИС. Поточно, тој мора да го провери квалитетот на податоците кои државите-членки ги внесуваат во Ц-ШИС преку Н-ШИС. Националниот надзорен орган мора да осигури ревизија на операциите за обработка на податоците во рамките на националниот Н-ШИС барем на секои четири години. Националните надзорни органи и Европскиот супервизор за заштита на податоците соработуваат и осигуруваат координиран надзор на ШИС, додека ЕСЗП е одговорен за надгледување на Ц-ШИС. Поради транспарентност, на секои две години до Европскиот парламент, Советот и ЕАГИС се испраќа заеднички извештај за активностите.

Правата на пристап на поединците кои се однесуваат на ШИС II може да се остваруваат со секоја држава-членка, бидејќи секој Н-ШИС е верна копија на Ц-ШИС.

Пример: Во предметот *Dalea v. France*[278], на жалителот му било одбиено барањето за виза поради посета на Франција бидејќи француските органи

277 Совет на Европската Унија (2007), Одлука на Советот 2007/533/ЈНА од 12 јуни 2007 год. за воспоставувањето, работењето и употребата втората генерација на Шенгенскиот информациски систем, Сл. весник 2007 L 205, член 57.

278 ЕСЧП, *Dalea v. France* (dec.), бр. 964/07, 2 февруари 2010 год.

пријавиле во Шенгенскиот информациски систем дека не смее да му се одобри влез. Жалителот неуспешно барал пристап и исправка или бришење на податоците пред француската Комисија за заштита на податоците и, на крајот, пред Државниот совет. Европскиот суд за човековите права сметал дека пријавата на жалителот во Шенгенскиот информациски систем била во согласност со законот и била насочена кон легитимната цел за заштита на националната безбедност. Всушност, бидејќи жалителот не покажал каква штета претрпел како последица на одбивањето на влезот во шенгенската област и бидејќи се применувале доволно мерки за негова заштита од произволни одлуки, мешањето во неговото право на почитување на приватниот живот било сразмерно. Според тоа, жалбата на жалителот според членот 8 била прогласена за недопуштена.

Визен информациски систем

Визниот информациски систем (ВИС) со кој исто така управува ЕАГИС е развиен како поддршка на спроведувањето на заедничката визна политика на Европската Унија[279]. Со помош на на ВИС, шенген-државите можат да разменуваат визни податоци преку систем кој ги поврзува конзулатите на шенген-државите што не се членки на Европската Унија со надворешните гранични премини на сите шенген-држави. Во ВИС се обработуваат податоци во врска со барањата за визи за краток престој за посета во или за транзит низ шенгенската област. Со помош на биометриски податоци, Визниот информациски систем им овозможува на граничните органи да проверат дали лицето кое ја предочило визата е нејзин вистински сопственик и да ги идентификуваат лицата кои немаат документи или имаат лажни документи.

Според Регулативата (ЕЗ) бр. 767/2008 на Европскиот парламент и на Советот во врска со Визниот информациски систем (ВИС) и размената на податоци меѓу државите-членки за визи за краток престој (*Регулатива за ВИС*), во ВИС смеат да се бележат само податоци за жалителот, за неговите визи, фотографии, отпечатоци од прсти, поврзувања со претходни барања и датотеки со барања на лица кои го

279 Совет на Европската Унија (2004), Одлука на Советот од 8 јуни 2004 година за воспоставување на Визниот информациски систем (ВИС), Сл. весник 2004 L 213; Регулатива (ЕЗ) бр. 767/2008 на Европскиот парламент и на Советот од 9 јули 2008 год. во врска со Визниот информациски систем (ВИС) и размената на податоци меѓу државите-членки за визи за краток престој, Сл. весник 2008 L 218 (*Регулатива за ВИС*); Совет на Европската Унија (2008), Одлука на Советот 2008/633/ЈНА од 23 јуни 2008 год. во врска со пристапот за проверка на Визниот информациски систем (ВИС) од страна на именувани органи на државите-членки и од страна на Европол за целите на спречувањето, откривањето и истрагата на терористички кривични дела и на други тешки кривични дела, Сл. весник 2008 L 218.

придружувале[280]. Пристапот до ВИС поради внесување, измена или бришење на податоци е ограничен исклучиво на органите на државите-членки кои се надлежни за издавање визи, додека пристапот заради увид во податоците е предвиден за органите кои се надлежни за издавање визи и на органите кои се надлежни за контрола на надворешните погранични премини, за имиграциска контрола и за азил. Во определени околности, националните надлежни полициски органи и Европол можат да побараат пристап до податоци кои се внесени во ВИС за целите на спречувањето, откривањето и истрагата на терористички и кривични дела[281].

Евродак

Називот „Евродак" се однесува на дактилограми или отпечатоци од прсти. Станува збор за централизиран систем кој ги содржи податоците за отпечатоците од прсти на државјани на трети држави кои бараат азил во некоја од државите-членки на Европската Унија[282]. Системот е во употреба од јануари 2003 година и служи како помош при определувањето на тоа која држава-членка би требала да биде одговорна за постапување по определено барање за азил според Регулативата на Советот (ЕЗ) бр. 343/2003 за утврдување на критериумите и механизмите за определување на државата-членка што е надлежна за постапување по барањето за азил кое било поднесено во една од државите-членки од страна на државјанин на трета држава (*Регулатива Даблин II*).[283] Личните податоци во Евродак можат да се користат само за целите на олеснувањето на примената на Регулативата Даблин II; употребата за која било друга цел е казнива.

Евродак се состои од централна единица со која управува ЕАГИС за складирање и споредување на отпечатоците од прсти и од систем за електронски пренос

280 Член 5 на Регулативата (ЕЗ) бр. 767/2008 на Европскиот парламент и на Советот од 9 јули 2008 година во врска со Визниот информациски систем (ВИС) и размената на податоци меѓу државите-членки за визи за краток престој (*Регулатива ВИС*), Сл. весник 2008 L 218.

281 Совет на Европската Унија (2008), Одлука на Советот 2008/633/ЈНА од 23 јуни 2008 година во врска со пристапот до Визниот информациски систем (ВИС) од страна на надлежните органи на државите-членки и Европол за целите на спречување, откривање и истрага на терористички кривични дела и други тешки кривични дела, Сл. весник 2008 L 218.

282 Регулатива на Советот (ЕЗ) бр. 2725/2000 од 11 декември 2000 година за уредување на системот Евродак за споредување на отпечатоци од прсти за ефикасна примена на Даблинската конвенција, Сл. весник 2000 L 316; Регулатива на Советот (ЕЗ) бр. 407/2002 од 28 февруари 2002 година која се однесува на одредени правила за имплементирање на Регулативата (ЕЗ) бр. 2725/2000 која се однесува на основање на Евродак за споредување на отпечатоците од прсти за ефикасна примена на Даблинската конвенција, Сл. весник 2002 L 62 (*Регулативи Евродак*).

283 Регулатива на Советот (ЕЗ) бр. 343/2003 од 18 февруари 2003 година за утврдување на критериумите и механизмите за определување на државата-членка што е надлежна за постапување по барањето за азил што било поднесено во една од државите-членки од страна на државјанин на трета држава, Сл. весник 2003 L 50 (*Регулатива Даблин II*).

на податоци меѓу државите-членки и централната база на податоци. Државите-членки ги преземаат и ги пренесуваат отпечатоците од прсти на секое лице што не е државјанин на Европската Унија или на лицата без државјанство на возраст од најмалку 14 години кои бараат азил на нивната територија или кои се фатени поради неовластено преминување на нивната надворешна граница. Исто така, државите-членки можат да ги преземат и да пренесат отпечатоците од прстите на лица кои не се државјани на Европската Унија или на лица без државјанство за кои било утврдено дека престојуваат на нивната територија без дозвола.

Податоците за отпечатоците од прсти се чувуваат во базата на податоци за Евродак само во псевдонимизиран облик. Во случај на совпаѓање, псевдонимот и името на првата држава-членка која ги пренела податоците за отпечатоците од прсти ѝ се откриваат на втората држава-членка. Потоа, втората држава-членка ќе ѝ се обрати на првата држава-членка, бидејќи, според Регулативата Даблин II, првата држава-членка е одговорна за обработка на барањето за азил.

Личните податоци кои се зачувани во системот Евродак и кои се однесуваат на барателите на азил се чуваат 10 години сметано од датумот на кој биле земени отпечатоците од прсти, освен ако субјектот на податоците добие државјанство на држава-членка на Европската Унија. Во тој случај, податоците мора веднаш да се избришат. Податоците кои се однесуваат на странски државјани што биле фатени поради неовластено преминување на надворешната граница се чуваат две години. Тие податоци мора да се избришат веднаш штом субјектот на податоците ќе добие дозвола за престој, ќе ја напушти територијата на Европската Унија или ќе добие државјанство на држава-членка.

Покрај сите држави-членки на Европската Унија, Евродак го користат и Исланд, Норвешка, Лихтенштајн и Швајцарија врз основа на меѓународни договори.

Евросур

Целта на Европскиот систем за надзор на границите (Евросур)[284] е да се зајакне контролата на надворешните граници на шенгенската област со откривање, спречување и сузбивање на незаконска имиграција и прекугранично криминал. Тој служи за подобрување на размената на информации и на оперативната соработка меѓу националните координативни центри и Фронтекс, агенцијата

284 Регулатива (ЕУ) бр. 1052/2013 на Европскиот парламент и на Советот од 22 октомври 2013 година за воспоставување на Европскиот систем за надзор на границите (Евросур), Сл. весник 2013 L 295.

на Европската Унија која е надлежна за развој и примена на нов концепт за интегрирано управување со границите[285]. Неговите општи цели се:

- да го намали бројот на незаконски мигранти што незабележано влегуваат во Европската Унија;
- да го намали бројот на смртни случаи на незаконски мигранти со спасување на повеќе животи на море;
- да ја зголеми внатрешната сигурност на Европската Унија во целина со помагање во спречувањето на прекугранично криминал[286].

Евросур започна со работа на 2 декември 2013 година во сите држави-членки со надворешни граници, а од 1 декември 2014 година ќе започне со работа и во други држави. Регулативата ќе се применува за надзор на копнени, надворешни морски и воздушни граници на државите-членки.

Царински информациски систем

Уште еден важен заеднички информациски систем што е воспоставен на ниво на Европската Унија е Царинскиот информациски систем (ЦИС)[287]. Во текот на воспоставувањето на внатрешниот пазар, укинати се сите контроли и формалности поврзани со стоките кои се движат на територијата на Европската Унија што довело до зголемен ризик од измама. Како противтежа на тој ризик била засилена соработката меѓу царинските управи на државите-членки. Целта на ЦИС

285 Регулатива (ЕУ) бр. 1168/2011 на Европскиот парламент и на Советот од 25 октомври 2011 година за изменување на Регулативата на Советот (ЕЗ) бр. 2007/2004 за воспоставување на Европската агенција за управување на оперативната соработка на надворешните граници на државите-членки на Европската Унија, Сл. весник 2011 L 394 (*Регулатива за Фронтекс*).

286 Види и: Европска комисија (2008), Соопштение на Комисијата до Европскиот парламент, Советот, Европскиот економски и социјален комитет и Комитетот на регионите: Испитување на основањето на Европскиот систем за надзор на границите (Евросур), COM(2008) 68 конечно, Брисел, 13 февруари 2008 год.; Европска комисија (2011), Процена на влијанието кое е придружено со Предлогот за Регулатива на Европскиот парламент и на Советот за воспоставување на Европски систем за надзор на границите (Евросур), Работен документ на службата на Комисијата, SEC(2011) 1536 конечно, Брисел,12 декември 2011 год., стр. 18.

287 Совет на Европската Унија (1995), Акт на Советот од 26 јули 1995 година за составување на Конвенцијата за употреба на информатичката технологија за царински цели, Сл. весник 1995 C 316, изменет од Советот на Европската Унија (2009), Регулатива бр. 515/97 од 13 март 1997 година во врска со меѓусебната помош меѓу управните органи на државите-членки и соработката меѓу овие органи и Комисијата за осигурување на правилна примена на законодавството во сферата на цариниите и земјоделието, Одлука на Советот 2009/917/ЈНА од 30 ноември 2009 година за употребата на информатичката технологија за царински цели, Сл. весник 2009 L 323 (*Одлука ЦИС*).

е да им помогне на државите-членки во спречувањето, истрагата и прогонот на сериозни повреди на царинските и земјоделските закони на ниво на одделните држави и на ниво на Европската Унија.

Информациите кои се содржани во ЦИС опфаќаат лични податоци кои се однесуваат на добрата, превозните средства, претпријатијата, лицата, стоките и готовината кои биле задржани, одземени или запленети. Таа информација може да се користи само за целите на следење, известување или извршување на определени инспекции или за стратешки или оперативни анализи во врска со лица кои се осомничени дека ги повредиле царинските одредби.

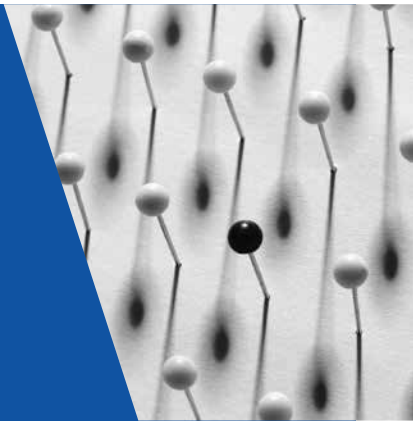
Пристапот до Царинскиот информациски систем им е дозволен на националните царински, даночни, земјоделски, јавноздравствени и полициски органи, како и на Европол и на Европравда.

Обработката на лични податоци мора да биде во согласност со посебните правила кои се утврдени со Регулативата бр. 515/97 и со Конвенцијата за ЦИС[288], како и со одредбите на Директивата за заштита на податоците, Регулативата за заштита на податоците во институциите на Европската Унија, Конвенцијата бр. 108 и Препораката за полициските податоци. Европскиот супервизор за заштита на податоците е одговорен за надгледување на усогласеноста на ЦИС со Регулативата (ЕЗ) бр. 45/2001 и барем еднаш годишно се состанува со сите национални органи за заштита на податоците кои се надлежни за прашањата за надзор во врска со ЦИС.

288 *На истото место.*

8

Други посебни европски закони за заштита на податоците



Европска Унија	Обработени прашања	Совет на Европа
Директива за заштита на податоците Директива за приватност и електронска комуникација	Електронски комуникации	Конвенција бр. 108 Препорака за телекомуникациски услуги
Директива за заштита на податоците, член 8 став 2 точка (б)	Работни односи	Конвенција бр. 108 Препорака за вработување
		ЕСЧП, *Copland v. the United Kingdom*, бр. 62617/00, 3 април 2007 год.
Директива за заштита на податоците, член 8 став 3	Медицински податоци	Конвенција бр. 108 Препорака за медицински податоци
		ЕСЧП, *Z. v. Finland*, бр. 22009/93, 25 февруари 1997 год.
Директива за клинички испитувања	Клинички испитувања	
Директива за заштита на податоците, член 6 став 1 точка (б) и (д), член 13 став 2	Статистика	Конвенција бр. 108 Препорака за статистички податоци
Регулатива (ЕЗ) бр. 223/2009 за европската статистика СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 год.	Службена статистика	Конвенција бр. 108 Препорака за статистички податоци

Директива 2004/39/ЕЗ за пазарите на финансиски инструменти Регулатива (ЕУ) бр. 648/2012 за пазари преку шалтер, централни други договорни страни и трговски репозитари Регулатива (ЕЗ) бр. 1060/2009 за агенции за кредитен рејтинг Директива 2007/64/ЕЗ за платежни услуги на внатрешниот пазар	Финансиски податоци	Конвенција бр. 108 Препорака 90(19) која се користи за исплати и за други сродни активности ЕСЧП, *Michaud v. France*, бр. 12323/11, 6 декември 2012 год.

Во неколку случаи, на европско ниво се усвоени посебни правни инструменти со кои во одредени ситуации подетално се применуваат општите правила на Конвенцијата бр. 108 или на Директивата за заштита на податоците.

8.1. Електронски комуникации

Клучни точки

- Посебните правила за заштита на податоците во областа на телекомуникациите, со особен нагласок на телефонските услуги, се содржани во Препораката на Советот на Европа од 1995 година.
- Обработката на личните податоци во врска со давањето на комуникациски услуги на ниво на Европската Унија е уредена со Директивата за приватност и за електронски комуникации.
- Доверливоста на електронските комуникации не се однесува само на содржината на комуникацијата туку и на податоците за сообраќајот, како на пример информации за тоа кој со кого комуницирал, кога и колку долго се одвивала комуникацијата, како и на податоците за локацијата, како што е локацијата од каде што се испратени податоците.

Кај комуникациските мрежи има сè поголема можност за неоправдано мешање во личната сфера на корисниците, поради тоа што постојат дополнителни технички можности за прислушување и следење на комуникацијата која се одвива на ваквите мрежи. Како последица на тоа, се сметало дека е неопходно да се внесат

посебни прописи за заштита на податоците со цел да се спречат определените ризици на кои се изложени корисниците на комуникациските услуги.

Во 1995 година Советот на Европа издал Препорака за заштита на податоците во областа на телекомуникацијата, која особено се однесувала на телефонските услуги[289].

Според оваа препорака, причината за собирањето и обработката на личните податоци во контекст на телекомуникациите треба да се ограничи на: приклучување на корисник на мрежата, овозможување на определена телекомуникациска услуга, наплатување, проверување, осигурување на оптимално техничко работење и развивање на мрежата и услугата.

Особено внимание е посветено и на користењето на комуникациските мрежи за испраќање пораки за директен маркетинг. Како општо правило, пораките за директен маркетинг не смеат да се праќаат кон некој претплатник кој изречно изјавил дека не сака да добива рекламни пораки. Уредите за автоматско повикување кои пренесуваат однапред снимени рекламни пораки можат да се користат само ако претплатникот ја дал својата изречна согласност за тоа. Со домашното законодавство треба да се пропишат детални правила во оваа област.

Што се однесува до **правната рамка на Европската Унија**, по првиот обид во 1997 година, Директивата за приватност и електронски комуникации е усвоена во 2002 година и е изменета во 2009 година со цел да се надополнат и да се прецизираат одредбите на Директивата за заштита на податоците за телекомуникацискиот сектор[290]. Примената на Директивата за приватност и електронски комуникации е ограничена на комуникациските услуги во јавните електронски мрежи.

Директивата за приватност и електронски комуникации разликува три главни категории на податоци кои се создаваат во текот на комуникацијата:

289 СЕ, Комитет на Министри (1995), Препорака Rec(95)4 за државите-членки во врска со заштитата на личните податоци во областа на телекомуникациските услуги, со посебен нагласок на телефонските услуги, 7 февруари 1995 год.

290 Директива 2002/58/ЕЗ на Европскиот парламент и на Советот од 12 јули 2002 година во врска со обработката на личните податоци и заштитата на приватноста во секторот за електронски комуникации, Сл. весник 2002 L 201 (*Директива за приватност и електронски комуникации*) изменета со Директивата 2009/136/ЕЗ на Европскиот парламент и на Советот од 25 ноември 2009 година за измена на Директивата 2002/22/ЕЗ за универзални услуги и права на корисниците во врска со мрежите и услугите за електронски комуникации, Директива 2002/58/ЕЗ во врска со обработката на личните податоци и заштитата на приватноста во секторот за електронски комуникации и Регулатива (ЕЗ) бр. 2006/2004 за соработката меѓу националните органи кои се одговорни за спроведувањето на законите за заштита на потрошувачите, Сл. весник 2009 L 337.

- податоците кои ја сочинуваат содржината на пораките кои се испратени за време на комуникацијата; овие податоци се строго доверливи;

- податоците кои се неопходни за воспоставување и за одржување на комуникацијата, таканаречените податоци за сообраќај, како што се информациите за партнерите во комуникацијата, времето и траењето на комуникацијата;

- во рамките на податоците за сообраќајот, постојат податоци кои се однесуваат конкретно на локацијата на уредот за комуникација, т.н. податоци за локацијата; овие податоци истовремено се податоци за *корисниците* на уредите за комуникација и се од особена важност за корисниците на мобилните комуникациски уреди;

Давателот на услуги може да ги користи податоците за сообраќајот само за цели на наплата и за техничко овозможување на услугата. Меѓутоа, со согласност на субјектот на податоците, овие податоци може да им се откријат на други контролори кои нудат услуги со додадена вредност, како што се давањето информации во врска со локацијата на корисникот во однос на следната постојка на подземната железница или аптека и временската прогноза за таа локација.

Другите видови пристап до податоци за комуникација во електронските мрежи, како што е пристапот со цел да се истражат злосторства, во согласност со членот 15 од Директивата за приватност и електронски комуникации, мора да ги исполнат барањата за оправдано мешање во правото за заштита на податоците како што е пропишано во членот 8 ставот 2 на Европската конвенција за човековите права и потврдено со членовите 8 и 52 на Повелбата.

Со измените на Директивата за приватност и електронски комуникации[291] од 2009 година, внесено е следното:

- Ограничувањата за испраќање на електронска пошта за цели на директен маркетинг биле проширени на услуги за кратки пораки (СМС), на услуги за мултимедијални пораки и на други видови слични апликации; електронската пошта во маркетиншки цели е забранета освен ако не е дадена претходна

291 Директива 2009/136/ЕЗ на Европскиот парламент и на Советот од 25 ноември 2009 година за изменување на Директивата 2002/22/ЕЗ за универзална услуга и права на корисниците во врска со електронски комуникациски мрежи и услуги, Директива 2002/58/ЕЗ во врска со обработката на личните податоци и заштитата на правото на приватност во секторот за електронски комуникации и Регулатива (ЕЗ) бр. 2006/2004 за соработка меѓу националните органи кои се одговорни за спроведување на законите за заштита на корисниците, Сл. весник 2009 L 337.

согласност. Без таква согласност маркетингот е допуштен само на електронската пошта на поранешните корисници, ако ја оставиле својата електронска адреса и не се противат на тоа.

- На државите-членки им била наметната обврската да обезбедат судски правни средства против повредите на забраната за несакана комуникација[292].

- Поставувањето на колачиња (cookies), софтвер кој ги следи и ги снима активностите на корисникот на компјутерот, повеќе не е дозволено без согласноста на корисникот на компјутерот. Со националното законодавство треба подетално да се уреди начинот на кој ќе се дава и ќе се добива согласноста со цел да се понуди доволна заштита[293].

Кога ќе настане повреда како резултат на неовластен пристап, загуба или уништување на податоци, веднаш мора да се информира надлежниот надзорен орган. Претплатниците мора да се информираат ако штетата која евентуално ја претрпеле е последица на повреда на податоците[294].

Директивата за задржување податоци[295] (прогласена за неважечка на 8 април 2014 година, види го примерот за случај подолу) ги обврзува давателите на комуникациски услуги да ги стават на располагање податоците за сообраќајот, особено за целите на борбата против тежок криминал, во период од најмалку шест месеци, но не подолго од 24 месеци, без оглед на тоа дали на давателот на услугата сè уште му се потребни тие податоци за цели на наплата или за техничко обезбедување на услугата.

Државите-членки на ЕУ ќе определат независни државни органи кои ќе бидат одговорни за надзор на сигурноста на задржаните податоци.

292 Види ја изменетата Директива, член 13.

293 *Види на истото место,* член 5; види и Работна група за член 29 (2012), *Мислење 04/2012 за исклучокот од согласноста за колачиња,* РГ 194, Брисел, 7 јуни 2012 год.

294 Види и Работна група за член 29 (2011), *Работен документ 01/2011 за актуелната рамка на ЕУ за повреда на личните податоци и препораките за иден развој на политиките,* РГ 184, Брисел, 5 април 2011 год.

295 Директива 2006/24/ЕЗ на Европскиот парламент и на Советот од 15 март 2006 година за задржување податоци што се создадени или обработени во врска со обезбедување на јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи и за изменување на Директивата 2002/58/ЕЗ, Сл. весник 2006 L 105.

Јасно е дека задржувањето на телекомуникациските податоци се вмешува во правото на заштита на податоците[296]. Во неколку судски постапки кои биле поведени во држави-членки на Европската Унија се разгледувало дали ова мешање е оправдано[297].

Пример: Во предметот *Digital Rights Ireland and Seitlinger and Others*[298], СПЕУ ја прогласил Директивата за задржување на податоци за неважечка. Според Судот,„обемното и особено сериозното мешање на Директивата во основните права за кои станува збор, не е доволно ограничено за да се осигури дека таквото мешање е ограничено само до апсолутно неопходниот степен".

Суштинско прашање во смисла на електронските комуникации е мешањето на државните органи. Средствата за надзор и за следење на комуникациите, како што се уредите за слушање и за прислушување, се допуштени само ако тоа е пропишано со закон и ако претставува неопходна мерка во демократското општество во интерес на: заштитата на државната безбедност, јавната безбедност, монетарните интереси на државата или во сузбивањето на кривични дела; или за заштита на субјектот на податоците или на правата и слободите на другите.

Пример: Во предметот *Malone v. the United Kingdom*[299], жалителот е обвинет за низа кривични дела поврзани со нечесно постапување со украдена стока. Во текот на судењето произлегло дека телефонскиот разговор на жалителот бил следен врз основа на налог што државниот секретар го издал за Министерството за внатрешни работи. Иако начинот на кој комуникацијата на жалителот била следена бил законит во смисла на домашното законодавство, Европскиот суд за човекови права сметал дека не постоеле законски правила кои го уредуваат опфатот и начинот на кој државните органи ги уживале своите дискрециски права во оваа област, па според тоа следењето кое произлегло од постојната практика која е во прашање „не било во согласност со законот". Судот сметал дека имало повреда на членот 8 од Европската конвенција за човекови права.

296 ЕСЗП (2011), *Мислење од 31 мај 2011 година за евалуацискиот извештај на Комисијата до Советот и до Европскиот парламент за Директивата за задржување податоци (Директива 2006/24/ЕЗ),* 31 мај 2011 год.

297 Германија, Сојузен уставен суд (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 март 2010 год.; Романија, Сојузен уставен суд (*Curtea Constituţională a României*), бр. 1258, 8 октомври 2009 год.; Република Чешка, Уставен суд (*Ústavní soud České republiky*), 94/2011 Coll., 22 март 2011 год.

298 СПЕУ, Заеднички предмети C-293/12 и C-594/12, *Digital Rights Ireland and Seitlinger and Others,* 8 април 2014 год., параграф 65.

299 ЕСЧП, *Malone v. the United Kingdom,* бр. 8691/79, 2 август 1984 год.

8.2. Податоци за вработување

Клучни точки

- Посебни правила за заштита на податоците во работните односи се содржани во Препораката на Советот на Европа за податоци за вработување.
- Во Директивата за заштита на податоците работните односи се споменуваат само во контекст на обработката на чувствителни податоци.
- Валидноста на согласноста, која мора да се даде доброволно, како правна основа за обработка на податоците за вработените може да биде неизвесна, ако се земе предвид економската нееднаквост меѓу работодавецот и вработениот. Мора внимателно да се проценат околностите во кои е дадена согласноста.

Не постои посебна правна рамка во Европската Унија која ја уредува обработката на податоците во контекст на вработувањето. Во Директивата за заштита на податоците, работните односи се споменуваат само во членот 8 став 2 на Директивата, кој се однесува на обработката на чувствителни податоци. Што се однесува до Советот на Европа, Препораката за податоци за вработување е издадена во 1989 година и во моментот се ажурира[300].

Преглед на најчестите проблеми во врска со заштитата на податоците во контекст на вработувањето може да се најде во еден работен документ на Работната група за членот 29[301]. Работната група ја анализирала значајноста на согласноста како правна основа за обработка на податоци за вработување[302]. Работната група утврдила дека економската неурамнотеженост меѓу работодавецот, кој бара согласност, и вработениот, кој дава согласност, често покренува сомнежи за тоа дали согласноста била дадена доброволно. Затоа, кога се проценува валидноста на согласноста во контекст на вработувањето треба внимателно да се разгледаат околностите под кои се дава согласност.

300 СЕ, Комитет на министри (1989), Препорака Rec(89)2 за државите-членки за заштитата на лични податоци кои се користат за цели на вработување, 18 јануари 1989 год. Види и Советодавен комитет за Конвенцијата бр. 108, Студија за Препораката бр. R (89) 2 за заштитата на лични податоци кои се користат за цели на вработување и за предлози за ревизија на гореспоменатата Препорака, 9 септември 2011 год.

301 Работна група за членот 29 (2001), *Мислење 8/2001 за обработката на лични податоци во контекст на вработувањето*, РГ 48, Брисел, 13 септември 2001 год.

302 Работна група за членот 29 (2005), *Работен документ за заедничко толкување на членот 26 став 1 на Директивата 95/46/ЕЗ од 24 октомври 1995 год.*, РГ 144, Брисел, 25 ноември 2005 год.

Чест проблем во врска со заштитата на податоците во денешната вообичаена работна средина е легитимната мера до која може да се следи електронската комуникација на вработените на работното место. Често се тврди дека овој проблем може лесно да се реши со забрана за приватна употреба на комуникациски средства на работното место. Но, таквата општа забрана би можела да биде и несразмерна и нереалистична. Следната пресуда на Европскиот суд за човековите права е особено значајна во овој контекст:

Пример: Во предметот *Copland v. UK*[303], тајно било следено користењето на телефонот, електронската пошта и интернетот на една вработена во колеџот, со цел да се утврди дали таа прекумерно ги користела просториите на колеџот за лични цели. Европскиот суд за човекови права бил на ставот дека телефонските повици кои се вршеле од деловните простории опфаќале теми од приватниот живот и допишувања. Затоа, таквите повици и таквата електронска пошта кои биле испраќани од работното место, како и информациите што биле добиени од следењето на личното користење на интернетот, биле заштитени со членот 8 од Европската конвенција за човековите права. Во случајот на жалителката не постоеле одредби со кои се уредувале околностите под кои работодавците би можеле да ја следат употребата на телефоните, електронската пошта и интернетот од страна на вработените. Според тоа, мешањето не било во согласност со законот. Судот заклучил дека имало повреда на членот 8 од Конвенцијата.

Според Препораката на Советот на Европа за вработување, личните податоци кои се собираат за целите на вработувањето треба да се добијат директно од вработениот.

Личните податоци кои се собираат за целите на вработување мора да се ограничат на информациите кои се неопходни за да се процени соодветноста на кандидатите и нивниот работен потенцијал.

Во препораката исто така изречно се споменуваат податоците во врска со проценатa на ефикасноста на работењето или потенцијалот на поединечни вработени. Таквите податоци мора да се засноваат на правични и чесни процени и не смеат да бидат формулирани на навредлив начин. Тоа го налагаат начелата за правична обработка и точност на податоците.

303 ЕСЧП, *Copland v. the United Kingdom*, бр. 62617/00, 3 април 2007 год.

Посебен аспект на законодавството за заштита на податоците во односот работодавец-вработен е улогата на претставниците на вработените. Таквите претставници можат да ги добијат личните податоци на вработените само ако тоа е неопходно за да можат да ги застапуваат интересите на вработените.

Чувствителните лични податоци кои се собрани за цели на вработување можат да се обработат само во определени случаи и во согласност со заштитните мерки кои се пропишани со домашното законодавство. Работодавците можат да ги прашаат вработените или кандидатите за работното место за нивната здравствена состојба или да ги подложат на здравствен преглед само ако тоа е неопходно за да се определи дали се соодветни за работното место, дали ги исполнуваат условите за превентивна медицина или за да се одобрат социјални надоместоци. Здравствените податоци смеат да се собираат само од засегнатото вработено лице, а не од други извори, освен ако за тоа е дадена изречна и информирана согласност или ако е пропишано со националното законодавство.

Во согласност со Препораката за вработување, вработените треба да бидат информирани за целта поради која се обработуваат нивните лични податоци, за видот на зачуваните лични податоци, за субјектите до кои редовно се пренесуваат податоците, за целта и правната основа на таквата комуникација. Исто така, работодавците треба однапред да ги информираат своите вработени кога внесуваат или прилагодуваат автоматизирани системи за обработка на личните податоци на вработените или за следење на движењето или за продуктивноста на вработените.

Вработените мора да имаат право на пристап до нивните податоци за вработување, како и право на нивна исправка или бришење. Понатаму, ако се обработуваат податоци за процена, вработените мора да имаат право да ја оспорат таа процена.

Меѓутоа, тие права можат да бидат привремено ограничени поради цели на внатрешни истраги. Ако на вработениот му се одбие пристап, исправка или бришење на личните податоци за вработување, во националното законодавство мора да се пропишат соодветни постапки со кои ќе се оспори таквото одбивање.

8.3. Медицински податоци

Клучна точка

- Медицинските податоци се чувствителни и поради тоа уживаат посебна заштита.

Личните податоци во врска со здравствената состојба на субјектот на податоците се сметаат за чувствителни податоци во согласност со членот 8 став 1 на Директивата за заштита на податоците и членот 6 на Конвенцијата бр. 108. Поради тоа, медицинските податоци подлежат на построг режим за обработка на податоци отколку нечувствителните податоци.

Пример: Во предметот *Z. v. Finland*[304], поранешниот сопруг на жалителката, кој бил заразен со ХИВ, извршил низа сексуални кривични дела. Подоцна бил осуден за убиство со умисла поради тоа што свесно ги изложил своите жртви на ризикот да се инфицираат со ХИВ. Националниот суд наложил целосната пресуда и документите за случајот да останат доверливи 10 години, и покрај барањата на жалителката за подолг период на доверливост. Таквите барања биле одбиени од Апелациониот суд, чија пресуда ги содржела целосните имиња и на жалителката и на нејзиниот поранешен сопруг. Европскиот суд за човековите права сметал дека мешањето не било неопходно во едно демократско општество, затоа што заштитата на медицинските податоци била од суштинско значење за остварување на правото на почитување на приватниот и семејниот живот, особено кога се работело за информација за ХИВ-инфекција, со оглед на тоа што таа состојба е стигматизирана во многу општества. Оттука, Судот заклучил дека одобрувањето на пристапот до идентитетот и до здравствената состојба на жалителот, како што е опишано во пресудата на Апелациониот суд, по истекот на временски период од 10 години по донесувањето на пресудата би го повредило членот 8 од Европската конвенција за човековите права.

Со членот 8 став 3 на Директивата за заштита на податоците е овозможена обработка на медицински податоци ако тоа е потребно за целите на превентивната

304 ЕСЧП, *Z. v. Finland*, бр. 22009/93, 25 февруари 1997 год., параграфи 94 и 112; види и ЕСЧП, *M.S. v. Sweden*, бр. 20837/92, 27 август 1997 год.; ЕСЧП, *L.L. v. France*, бр. 7508/02, 10 октомври 2006 год.; ЕСЧП, *I. v. Finland*, бр. 20511/03, 17 јули 2008 год.; ЕСЧП, *K.H. and others v. Slovakia*, бр. 32881/04, 28 април 2009 год.; ЕСЧП, *Szuluk v. the United Kingdom*, бр. 36936/05, 2 јуни 2009 год.

медицина, медицинската дијагноза, обезбедувањето на нега и лекување или управувањето со здравствените услуги. Меѓутоа, обработката е допуштена само ако ја врши здравствен работник кој подлежи на обврската за чување на професионална тајна или се врши од страна на друго лице кое подлежи на истата обврска[305].

Во Препораката на Советот на Европа за медицински податоци од 1997 година подетално се применуваат начелата на Конвенцијата бр. 108 во врска со обработката на податоци во областа на медицината[306]. Предложените правила се во согласност со оние од Директивата за заштита на податоците во поглед на легитимните цели за обработка на медицински податоци, неопходната обврска за чување на професионална тајна на лицата кои ги користат здравствените податоци и правата на субјектите на податоците на транспарентност и пристап, исправка и бришење. Понатаму, медицинските податоци кои законито се обработуваат од страна на здравствени работници не смеат да се пренесат на извршните власти ако не се осигурани со „соодветни заштитни мерки со кои се спречува откривање што не е во согласност со правото на почитување на [...] приватниот живот што е гарантирано со членот 8 од Европската конвенција за човекови права“[307].

Покрај тоа, Препораката за медицински податоци содржи посебни одредби за медицинските податоци за неродени деца и за инвалидизирани лица, како и за обработката на генетските податоци. Научното истражување е изречно признаено како причина за чување на податоците подолго отколку што е потребно, иако тоа обично бара анонимизација. Во членот 12 од Препораката за медицински податоци, предложени се детални прописи за ситуациите во кои на истражувачите им се потребни лични податоци, а анонимизираните податоци не се доволни.

Псевдонимизацијата може да претставува соодветен начин за исполнување на научните потреби и за истовремена заштита на интересите на засегнатите пациенти. Подетални објаснувања за концептот на псевдонимизација во смисла на заштитата на податоците се содржани во поглавјето 2.1.3.

На национално и на европско ниво се одвиваат интензивни дискусии во врска со иницијативите за чувањето податоци за медицинското лекување на пациен-

305 Види и ЕСЧП, *Biriuk v. Lithuania*, бр. 23373/03, 25 ноември 2008 год.

306 СЕ, Комитет на министри (1997), Препорака Rec(97)5 за државите-членки во врска со заштитата на медицински податоци, 13 февруари 1997 год.

307 ЕСЧП, бр. 1585/09, *Avilkina and Others v. Russia*, бр. 1585/09, 6 јуни 2013 год., параграф 53 (не е конечно).

тот во електронскиот здравствен картон[308]. Посебен аспект на постоењето на национални системи за електронски здравствени картони е нивната прекугранична достапност: тема која е од особено значење во рамките на Европската Унија во смисла на прекугранична здравствена заштита[309].

Друга тема на дискусија се новите одредби за клиничките испитувања, со други зборови, испитувањето на нови лекови на пациенти во документирана истражувачка средина; исто така, оваа тема е значително поврзана со заштитата на податоците. Клиничките испитувања на медицинските производи за хумана употреба се регулирани со Директивата 2001/20/ЕЗ на Европскиот парламент и на Советот од 4 април 2001 година за приближувањето на законите, регулативите и административните одредби на државите-членки во врска со спроведувањето на добрата клиничка практика во спроведувањето на клиничките испитувања на медицински производи за хумана употреба (*Директива за клинички испитувања*)[310]. Во декември 2012 година, Европската комисија предложила регулатива со која би се заменила Директивата за клинички испитувања со цел постапките за испитување да станат повоедначени и поефикасни[311].

На ниво на Европската Унија во тек се уште многу други законодавни и други иницијативи во врска со личните податоци во здравствениот сектор[312].

308 Работна група за член 29 (2007), *Работен документ за обработката на лични податоци во врска со здравјето во електронските здравствени картони (EHR)*, РГ 131, Брисел, 15 февруари 2007 год.

309 Директива 2011/24/ЕУ на Европскиот парламент и на Советот од 9 март 2011 година за примена на правата на пациентите во прекуграничната здравствена заштита, Сл. весник 2011 L 88.

310 Директива 2001/20/ЕЗ на Европскиот парламент и на Советот од 4 април 2001 година за приближувањето на законите, регулативите и административните одредби на државите-членки во врска со спроведувањето на добрата клиничка практика во спроведувањето на клиничките испитувања на медицински производи за хумана употреба, Сл. весник 2001 L 121.

311 Европска комисија (2012), *Предлог за Регулатива на Европскиот парламент и на Советот за клинички испитувања на медицински производи за хумана употреба, и за укинување на Директивата 2001/20/ЕЗ*, COM(2012) 369 конечно, Брисел, 17 јули 2012 год.

312 ЕСЗП (2013), *Мислење на Европскиот супервизор за заштита на податоци за информирањето на Комисијата за „ Акцискиот план за е-здравство за 2012–2020 година – Иновативна здравствена заштита за 21 век“*, Брисел, 27 март 2013 год.

8.4. Обработка на податоци за статистички цели

Клучни точки

- Податоците кои се собрани за статистички цели не смеат да се користат за никаква друга намена.
- Податоците кои се собрани законски за која било цел можат дополнително да се користат за статистички цели ако со националното законодавство се пропишани соодветни заштитни мерки кои ги применуваат корисниците. Се разбира, за таа цел треба да се предвиди анонимизација или псевдонимизација пред преносот до трети страни.

Во Директивата за заштита на податоците, обработката на податоци за статистички цели се споменува во контекст на можните исклучоци од начелата за заштита на податоците. Според членот 6 став 1 точка (б) од Директивата, во согласност со националното законодавство може да се отфрли начелото за ограничување на целта во корист на натамошна употреба на податоците за статистички цели, но со националното законодавство мора да бидат пропишани сите неопходни заштитни мерки. Според членот 13 став 2 од Директивата, можно е со националното законодавство да се ограничи правото на пристап ако податоците се обработуваат исклучиво за статистички цели; но и во тој случај мора да постојат соодветни заштитни мерки во согласност со националното законодавство. Во таа смисла, со Директивата за заштита на податоците, предвиден е посебен услов, според кој ниту еден од податоците кои се добиени или се создадени во текот на статистичкото истражување не смее да се користи за конкретни одлуки во врска со субјектите на податоците.

Иако податоците кои биле законски собрани од страна на контролор за која било цел може повторно да се искористат од негова страна за сопствени статистички цели – за таканаречена секундарна статистика – тие треба да се анонимизираат или да се псевдноимизираат, во зависност од случајот, пред да се пренесат до трета страна за статистички цели, освен ако субјектот на податоците дал своја согласност за тоа или ако тоа е посебно пропишано со националното законодавство. Ова произлегува од условот за соодветни заштитни мерки според членот 6 став 1 точка (б) од Директивата за заштита на податоците.

Најважни случаи за користење податоци за статистички цели се службените статистики, кои ги спроведуваат националните заводи за статистика и заводите за статистика на Европската Унија врз основа на националните законодавства и законодавствата на Европската Унија за службена статистика. Според тие законодавства, граѓаните и претпријатијата обично се обврзани да им ги откријат податоците на надлежните органи за статистика. Службениците кои работат во заводите за статистика подлежат на посебни обврски за чување на професионална тајна кои внимателно се следат затоа што тие се од суштинско значење за високото ниво на доверба кај граѓаните кое е неопходно ако податоците треба да им се дадат на располагање на надлежните органи за статистика.

Регулативата (ЕЗ) бр. 223/2009 за европска статистика (*Регулатива за европска статистика*) содржи суштински правила за заштита на податоците во службената статистика и, според тоа, би можела да се смета за релевантна за одредбите за службената статистика на национално ниво[313]. Во Регулативата се застапува начелото дека за службените статистички активности е потребна доволно прецизна правна основа[314].

Пример: Во предметот *Huber v. Germany*[315], Судот на правдата на Европската Унија утврдил дека прибирањето и чувањето на личните податоци што ги врши надлежниот орган за статистички цели, само по себе не претставува доволна причина за да се смета дека обработката е законита. Законодавството со кое се пропишува обработката на личните податоци исто така требало да го исполни условот за нужност, што во конкретниот предмет не било случај.

Во контекст на Советот на Европа, Препораката за статистички податоци што била донесена во 1997 година го опфаќа водењето статистика во јавните и во приватните сектори[316]. Со таа препорака се внесуваат начела кои се совпаѓаат

313 Регулатива (ЕЗ) бр. 223/2009 на Европскиот парламент и на Советот од 11 март 2009 година за Европската статистика и за укинување на Регулативата (ЕЗ, Евроатом) бр. 1101/2008 на Европскиот парламент и на Советот за доставувањето на доверливи статистички податоци до заводите за статистика на Европските Заедници, Регулатива на Советот (ЕЗ) бр. 322/97 за статистика на Заедницата, и Одлука на Советот 89/382/ЕЕЗ, Текст на Евроатом за основање на Комитет за статистички програми на Европските Заедници, Сл. весник 2009 L 87.

314 Ова начело треба подетално да се обработи во Кодексот на практиката на Евростат, кој, во согласност со членот 11 на Регулативата за европска статистика, дава етички насоки за начинот на водењето на службената статистика, вклучувајќи ја внимателната употреба на лични податоци; достапно на: http://epp.eurostat.ec.europa.eu/ portal/page/portal/about_eurostat/introduction.

315 СПЕУ, C-524/06, *Huber v. Germany*, 16 декември 2008 год.; види особено параграф 68.

316 СЕ, Комитет на министри (1997), Препорака Rec(97)18 за државите-членки во врска со заштитата на личните податоци кои се собираат и се обработуваат за статистички цели, 30 септември 1997 год.

со гравните правила на Директивата за заштита на податоците кои се опишани погоре. Во врска со следните прашања се наведени подетални правила.

Додека податоците кои ги собрал контролор за статистички цели не можат да се користат за ниту една друга цел, податоците кои се собрани за цели што не се од статистичка природа ќе бидат достапни за дополнителна статистичка употреба. Со Препораката за статистички податоци дури и се дозволува податоците да се пренесат на трети страни ако тоа е само за статистички цели. Во такви случаи страните би требало да го договорат и да го забележат обемот на легитимната дополнителна употреба за статистички цели. Бидејќи тоа не е замена за согласноста на субјектот на податоците, треба да се претпостави дека во националното законодавство мора да бидат пропишани дополнителни заштитни мерки со цел да се минимизираат ризиците за злоупотреба на лични податоци, како што е обврската за анонимизација или псевдонимизација на податоците пред преносот.

Луѓето кои професионално се занимаваат со статистички истражувања треба да се обврзат со посебни обврски за чување на професионална тајна – како што е вообичаено за службената статистика – врз основа на националното законодавство. Ова треба да се прошири за да ги вклучи и испитувачите ако се вработени за прибирање податоци од субјекти на податоци или од други лица.

Ако употребата на лични податоци за статистичко истражување не е пропишана со закон, субјектите на податоците би требало да ја дадат својата согласност за употреба на нивните податоци или би требало барем да им се даде можност за приговор со цел обработката да биде законита.

Ако испитувачите прибираат лични податоци за статистички цели, тие лица мора да бидат јасно информирани за тоа дали откривањето на личните податоци е задолжително во согласност со националното законодавство. Чувствителни податоци не смеат никогаш да се собираат на начин на кој поединецот би можел да се идентификува, освен ако тоа е изречно дозволено со националното законодавство.

Ако статистичкото истражување не може да се направи без анонимизирани податоци и ако личните податоци се навистина неопходни, податоците што се прибираат за оваа цел треба да се анонимизираат што е можно порано. Врз основа на резултатите од статистичкото истражување, во најмала рака, не смее да биде

можно да се идентификуваат субјектите на податоците, освен ако е очигледно дека тоа не претставува никаков ризик.

По завршувањето на статистичката анализа, употребените лични податоци треба или да се избришат или да се анонимизираат. Во тој случај, Препораката за статистички податоци предлага податоците за идентификација да се чуваат одделно од другите лични податоци. Тоа значи, на пример, дека податоците треба да се псевдонимизираат, а клучот за енкрипција или списокот со синонимите за идентификација треба да се чуваат одделно од псевдонимизираните податоци.

8.5. Финансиски податоци

Клучни точки

- Иако финансиските податоци не се чувствителни податоци во смисла на Конвенцијата бр.108 и на Директивата за заштита на податоците, за нивна обработка се потребни определени заштитни мерки со цел да се осигурат точноста и безбедноста на податоците.
- Системите за електронско плаќање треба да имаат вградена заштита на податоци, таканаречена приватност по мерка („*privacy by design*").
- Во оваа област се јавуваат одредени проблеми со заштитата на податоците поради потребата за воспоставување на соодветни механизми за автентикација.

Пример: Во предметот *Michaud v. France*[317], жалителот, француски адвокат, се спротивставил на својата обврска според француското право да пријави сомневања во врска со можни активности на своите клиенти за перење пари. Европскиот суд за човекови права сметал дека барањето од адвокатите да им даваат информации на управните органи во врска со друго лице до кои дошле преку разговор со него претставува мешање во правото на адвокатот на почитување на неговата преписка и приватниот живот во согласност со членот 8 од Европската конвенција за човековите права, бидејќи со тоа начело биле опфатени активностите од професионална или од деловна

317 ЕСЧП, *Michaud v. France,* бр. 12323/11, 6 декември 2012 год.; види и ЕСЧП, *Niemietz v. Germany,* бр. 13710/88, 16 декември 1992 год., параграф 29, и ЕСЧП, *Halford v. the United Kingdom,* бр. 20605/92, 25 јуни 1997 год., параграф 42.

природа. Меѓутоа, мешањето било во согласност со законот и било насочено кон легитимна цел, имено, спречување на неред и криминал. Поради тоа што адвокатите подлежат на обврската да пријават сомневања само во многу ограничени околности, Европскиот суд за човековите права сметал дека таа обврска била сразмерна и заклучил дека немало повреда на членот 8.

Примената на општата правна рамка за заштита на податоци, која е содржана во Конвенцијата бр.8, во контекст на плаќањата била разгледана од Советот на Европа во Препораката Rec(90)19 од 1990 година[318]. Во таа препорака е објаснет опфатот на законитото прибирање и употреба на податоци во контекст на плаќањата, особено со платежни картички. Понатаму, со неа на домашните законодавци им се предлагаат детални прописи за ограничувањата во поглед на проследувањето на податоците за плаќањата до трети лица, за временските ограничувања на чувањето на податоците, за транспарентост, безбедност на податоците и за прекугранично пренос на податоци, и, конечно, за надзорот и правните средства. Предложените решенија соодветствуваат на тоа што подоцна е пропишано како општа рамка на Европската Унија за заштита на податоците во Директивата за заштита на податоците.

Во тек е изработката на низа правни инструменти за регулирање на пазарите на финансиски инструменти и за активностите на кредитните институции и инвестициските фирми[319].

Останатите правни инструменти помагаат во сузбивањето на тргувањето со злоупотреба на привилегирани информации и манипулација со пазарот[320]. Најважните прашања во овие области кои влијаат на заштитата на податоците се:

318 СЕ, Комитет на министри (1990), Препорака бр. R(90)19 за заштита на личните податоци кои се користат за плаќање и за други сродни активности, 13 септември 1990 год.

319 Европска комисија (2011), *Предлог за Директива на Европскиот парламент и на Советот за пазарите за финансиски инструменти со кој се укинува Директивата 2004/39/ЕЗ на Европскиот парламент и на Советот*, COM(2011) 656 конечно, Брисел, 20 октомври 2011 год.; Европска комисија (2011), *Предлог за регулатива на Европскиот парламент и на Советот за пазарите за финансиски инструменти и за изменување на Регулативата [EMIR] за пазари преку шалтер, централни други договорни страни и трговски репозитари*, COM(2011) 652 конечно, Брисел, 20 октомври 2011 год.; Европска комисија (2011), *Предлог за Директива на Европскиот парламент и на Советот за пристап до активностите на кредитните институции и за разумен надзор на кредитните институции и инвестициските фирми и за изменување на Директивата 2002/87/ЕЗ на Европскиот парламент и на Советот за дополнителен надзор на кредитните институции, осигурителните компании и инвестициските фирми во финансиски конгломерат*, COM(2011) 453 конечно, Брисел, 20 јули 2011 год.

320 Европска комисија (2011), *Предлог за регулатива на Европскиот парламент и на Советот за тргувањето со злоупотреба на привилегирани информации и манипулација со пазарот (злоупотреба на пазарот)*, COM(2011) 651 конечно, Брисел, 20 октомври 2011 год.; Европска

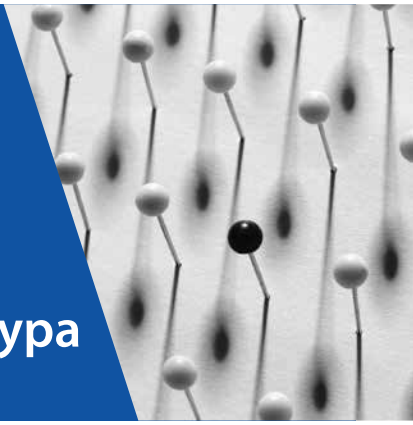
- задржувањето на записи за финансиски трансакции;
- преносот на лични податоци во трети земји;
- снимањето на телефонски разговори и на електронски комуникации, вклучувајќи го и овластувањето на надлежните органи да побараат записи за телефонскиот и податочниот сообраќај;
- откривањето на лични информации, вклучувајќи ја и објавата на санкции;
- овластувањата на надлежните органи за вршење надзор и истрага, влучувајќи и теренски проверки и влегување во приватни простории поради одземање на документи;
- механизмите за пријавување на прекршоци, односно програми за дојава; и
- соработката меѓу надлежните органи на државите-членки и Европското тело за хартии од вредност и пазари (ЕТХВП).

Има и други прашања во тие области што се посебно обработени, вклучувајќи го и собирањето податоци за финансиската состојба на субјектите на податоците[321] или за прекуграничното плаќање преку банкарски трансфер, кое неизбежно доведува до пренос на лични податоци[322].

комисија (2011), *Предлог за директива на Европскиот парламент и на Советот за кривични санкции за тргувањето со злоупотреба на привилегирани информации и манипулација со пазарот*, COM(2011) 654 конечно, Брисел, 20 октомври 2011 год.

321 Регулатива (ЕЗ) бр. 1060/2009 на Европскиот парламент и на Советот од 16 септември 2009 година за агенциите за кредитен рејтинг, Сл. весник 2009 L 302; Европска комисија, *Предлог за регулатива на Европскиот парламент и на Советот за изменување на Регулативата (ЕЗ) бр. 1060/2009 за агенциите за кредитен рејтинг*, COM(2010) 289 конечно, Брисел, 2 јуни 2010 год.

322 Директива 2007/64/ЕЗ на Европскиот парламент и на Советот од 13 ноември 2007 година за платежните услуги во внатрешниот пазар и за изменување на Директивите 97/7/ЕЗ, 2002/65/ЕЗ, 2005/60/ЕЗ и 2006/48/ЕЗ и за укинување на Директивата 97/5/ЕЗ, Сл. весник 2007 L 319.



Дополнителна литература

Поглавје 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Frei- heit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brussels, available at: www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Con- vention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.
Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220, available at: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Поглавје 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, pp. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, available at: www.ico.org.uk/ for_organisations/ data_protection/topic_guides/anonymisation.

Поглавја 3, 4 и 5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union europée- nne*, Saarbrucken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/ privacy_impact_assessment.

Поглавје 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Rein- venting data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Поглавје 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, availa- ble at: www.europol.europa.eu/sites/default/files/publications/europol_dpo_book- let_0.pdf.
Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Drewer, D. and Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, Vol. 13, No. 3, pp. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2, available at: www.asser. nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Поглавје 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

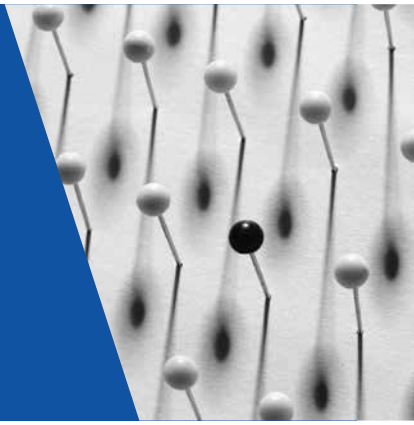
Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.



Судска практика

Избор од судската практика на Европскиот суд за човековите права

Пристап до лични податоци

Gaskin v. the United Kingdom, бр. 10454/83, 7 јули 1989 год.
Godelli v. Italy, бр. 33783/09, 25 септември 2012 год.
K.H. and Others v. Slovakia, бр. 32881/04, 28 април 2009 год.
Leander v. Sweden, бр. 9248/81, 26 март 1987 год.
Odièvre v. France [GC],бр. 42326/98, 13 февруари 2003 год.

Урамнотежување на заштитата на податоците со слободата на изразување

Axel Springer AG v. Germany [GC], бр. 39954/08, 7 февруари 2012 год.
Von Hannover v. Germany, бр. 59320/00, 24 јуни 2004 год.
Von Hannover v. Germany (No. 2) [GC], бр. 40660/08 и 60641/08, 7 февруари 2012 год.

Предизвици во електронската заштита на податоци

K.U. v. Finland, бр. 2872/02, 2 декември 2008 год.

Преписка

Amann v. Switzerland [GC], бр. 27798/95, 16 февруари 2000 год.

Bernh Larsen Holding AS and Others v. Norway, бр. 24117/08, 14 март 2013 год.
Cemalettin Canli v. Turkey, бр. 22427/04, 18 ноември 2008 год.
Dalea v. France, бр. 964/07, 2 февруари 2010 год.
Gaskin v. the United Kingdom, бр. 10454/83, 7 јули 1989 год.
Haralambie v. Romania, бр. 21737/03, 27 октомври 2009 год.
Khelili v. Switzerland, бр. 16188/07, 18 октомври 2011 год.
Leander v. Sweden, бр. 9248/81, 26 март 1987 год.
Malone v. the United Kingdom, бр. 8691/79, 2 август 1984 год.
McMichael v. the United Kingdom, бр. 16424/90, 24 февруари 1995 год.
M.G. v. the United Kingdom, бр. 39393/98, 24 септември 2002 год.
Rotaru v. Romania [GC],бр. 28341/95, 4 мај 2000 год.
S. and Marper v. the United Kingdom, бр. 30562/04 и 30566/04, 4 декември 2008 год.
Shimovolos v. Russia, бр. 30194/09, 21 јуни 2011 год.
Turek v. Slovakia, бр. 57986/00, 14 февруари 2006 год.

Бази на податоци со криминални досиеја

B.B. v. France, бр. 5335/06, 17 декември 2009 год.
M.M. v. the United Kingdom, бр. 24029/07, 13 ноември 2012 год.

Бази на податоци со ДНК

S. and Marper v. the United Kingdom, бр. 30562/04 и 30566/04, 4 декември 2008 год.

Податоци за ГСП уредите

Uzun v. Germany, бр. 35623/05, 2 септември 2010 год.

Здравствени податоци

Biriuk v. Lithuania, бр. 23373/03, 25 ноември 2008 год.
I. v. Finland, бр. 20511/03, 17 јули 2008 год.
L.L. v. France, бр. 7508/02, 10 октомври 2006 год.
M.S. v. Sweden, бр. 20837/92, 27 август 1997 год.
Szuluk v. the United Kingdom, бр. 36936/05, 2 јуни 2009 год.
Z. v. Finland, бр. 22009/93, 25 февруари 1997 год.

Идентитет

Ciubotaru v. Moldova, бр. 27138/04, 27 април 2010 год.

Godelli v. Italy, бр. 33783/09, 25 септември 2012 год.
Odièvre v. France [GC], бр. 42326/98, 13 февруари 2003 год.

Информации во врска со професионални активности

Michaud v. France, бр. 12323/11, 6 декември 2012 год.
Niemietz v. Germany, бр. 13710/88, 16 декември 1992 год.

Следење на комуникациите

Amann v. Switzerland [GC], бр. 27798/95, 16 февруари 2000 год.
Copland v. the United Kingdom, бр. 62617/00, 3 април 2007 год.
Cotlet v. Romania, бр. 38565/97, 3 јуни 2003 год.
Kruslin v. France, бр. 11801/85, 24 април 1990 год.
Lambert v. France, бр. 23618/94, 24 август 1998 год.
Liberty and Others v. the United Kingdom, бр. 58243/00, 1 јули 2008 год.
Malone v. the United Kingdom, бр. 8691/79, 2 август 1984 год.
Halford v. the United Kingdom, бр. 20605/92, 25 јуни 1997 год.
Szuluk v. the United Kingdom, бр. 36936/05, 2 јуни 2009 год.

Обврски за носителите на должност

B.B. v. France, бр. 5335/06, 17 декември 2009 год.
I. v. Finland, бр. 20511/03, 17 јули 2008 год.
Mosley v. the United Kingdom, бр. 48009/08, 10 мај 2011 год.

Фотографии

Sciacca v. Italy, бр. 50774/99, 11 јануари 2005 год.
Von Hannover v. Germany, бр. 59320/00, 24 јуни 2004 год.

Право на заборав

Segerstedt-Wiberg and Others v. Sweden, бр. 62332/00, 6 јуни 2006 год.

Право на приговор

Leander v. Sweden, бр. 9248/81, 26 март 1987 год.
Mosley v. the United Kingdom, бр. 48009/08, 10 мај 2011 год.

M.S. v. Sweden, бр. 20837/92, 27 август 1997 год.
Rotaru v. Romania [GC], бр. 28341/95, 4 мај 2000 год.

Чувствителни категории на податоци

I. v. Finland, бр. 20511/03, 17 јули 2008 год.
Michaud v. France, бр. 12323/11, 6 декември 2012 год.
S. and Marper v. the United Kingdom, бр.30562/04 и 30566/04, 4 декември 2008 год.

Надзор и спроведување (улога на различни чинители, вклучувајќи ги и органите за заштита на податоците)

I. v. Finland, бр. 20511/03, 17 јули 2008 год.
K.U. v. Finland, бр. 2872/02, 2 декември 2008 год.
Von Hannover v. Germany, бр. 59320/00, 24 јуни 2004 год.
Von Hannover v. Germany (No. 2) [GC], бр. 40660/08 и 60641/08, 7 февруари 2012 год.

Методи на надзор

Allan v. the United Kingdom, бр. 48539/99, 5 ноември 2002 год.
Association "21 Décembre 1989" and Others v. Romania, бр. 33810/07 и 18817/08, 24 мај 2011 год.
Bykov v. Russia [GC], бр. 4378/02, 10 март 2009 год.
Kennedy v. the United Kingdom, бр. 26839/05, 18 мај 2010 год.
Klass and Others v. Germany, бр. 5029/71, 6 септември 1978 год.
Rotaru v. Romania [GC], бр. 28341/95, 4 мај 2000 год.
Taylor-Sabori v. the United Kingdom, бр. 47114/99, 22 октомври 2002 год.
Uzun v. Germany, бр. 35623/05, 2 септември 2010 год.
Vetter v. France, бр. 59842/00, 31 мај 2005 год.

Видеонадзор

Köpke v. Germany, бр. 420/07, 5 октомври 2010 год.
Peck v. the United Kingdom, бр. 44647/98, 28 јануари 2003 год.

Гласовни примероци

P.G. and J.H. v. the United Kingdom, бр. 44787/98, 25 септември 2001 год.
Wisse v. France, бр. 71611/01, 20 декември 2005 год.

Избор од судската практика на Судот на правдата на Европската Унија

Судска практика поврзана со Директивата за заштита на податоците

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 декември 2008 год.

[Поимот за „новинарски дејства“ во рамките на значењето на членот 9 од Директивата за заштита на податоците]

Заеднички предмети C-92/09 и C-93/09, *Volker and Markus Schecke GbR and Hartmut Eif- ert v. Land Hessen*, 9 ноември 2010 год.

[Пропорционалноста на правната обврска за објавување на лични податоци за корисниците на одредени земјоделски фондови на Европската Унија]

C-101/01, *Bodil Lindqvist*, 6 ноември 2003 год.

[Законитоста на објавувањето податоци на интернет во врска со приватниот живот на други лица од страна на физичко лице]

C-131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Барање за прелиминарна одлука на судот *Audiencia Nacional* (Шпанија) поднесено на 9 март 2012 год., 25 мај 2012 год., во тек

[Обврски на давателите на услуги со интернет-пребарувачи, на барање на субјектот на податоците, да се воздржат од прикажување на лични податоци во резултатите од пребарувањето]

C-270/11, *European Commission v. Kingdom of Sweden*, 30 мај 2013 год.

[Казна за неспроведување на директива]

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 јануари 2008 год.

[Обврска на давателите на услуги за пристап до интернет да му го откријат на здружението за интелектуална сопственост идентитетот на корисниците на програмите за размена на датотеки „KaZaA“]

C-288/12, *European Commission v. Hungary*, 8 април 2014 год.

[Законитост на укинувањето на службата на националниот супервизор за заштита на податоците]

C-291/12, *Michael Schwarz v. Stadt Bochum*, Мислење на генералниот адвокат, 13 јуни 2013 год.

[Повреда на примарното право на Европската Унија со Регулативата (ЕЗ) 2252/2004 според која отпечатоците од прсти треба да се внесат во пасошите]

Заеднички предмети C-293/12 и C-594/12, *Digital Rights Ireland and Seitling and Others v. Ireland*, 8 април 2014 год.

[Повреда на примарното право на Европската Унија со Директивата за задржување на податоците]

C-360/10, *SABAM v. Netlog N.V.*, 16 февруари 2012 год.

[Обврска на давателите на услуги за друштвени мрежи за спречување на незаконското користење на музички и аудиовизуелни дела од страна на корисниците на интернет]

Заеднички предмети C-465/00, C-138/01 и C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*, 20 мај 2003 год.

[Пропорционалност на правната обврска за објавување на лични податоци во врска со платите на вработените во определени категории на институции поврзани со јавниот сектор]

Заеднички предмети C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 ноември 2011 година

[Правилно спроведување на членот 7 точка (ѓ) од Директивата за заштита на податоците – „легитимни интереси на други лица“ – во националното законодавство]

C-518/07, *European Commission v. Federal Republic of Germany*, 9 март 2010 год.

[Независност на националниот надзорен орган]

C-524/06, *Huber v. Bundesrepublik Deutschland*, 16 декември 2008 год.

[Законитост на чувањето на податоци за странски државјани во статистичкиот регистар]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 мај 2011 год.

[Нужност од обновена согласност]

C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijke- boer*, 7 мај 2009 год.

[Право на пристап на субјектот на податоците]

C-614/10, *European Commission v. Republic of Austria*, 16 октомври 2012 год.

[Независност на национален надзорен орган]

Судска практика поврзана со Регулативата за заштита на податоците во институциите на Европската Унија

C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 јуни 2010 год.

[Пристап до документи]

C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communi- ties*, 6 март 2003 год.

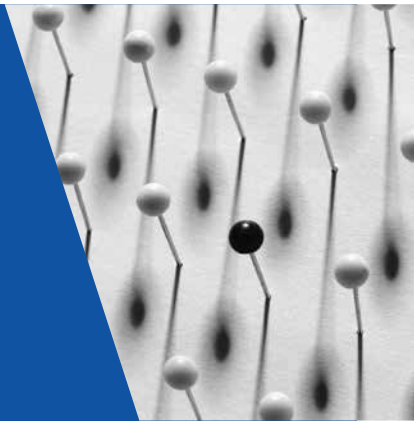
[Пристап до документи]

F-35/08, *Dimitrios Pachtitis v. European Commission*, 15 јуни 2010 год.

[Употреба на лични податоци во контекст на вработување во институциите на Европската Унија]

F-46/09, *V v. European Parliament*, 5 јули 2011год.

[Употреба на лични податоци во контекст на вработување во институции на Европската Унија]



Индекс на предмети

Судската практика на Судот на правдата на Европската Унија

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, заеднички предмети C-468/10 и C-469/10, 24 ноември 2011 год. 19, 23, 87, 90, 94, 95, 216

Bodil Lindqvist, C-101/01, 6 ноември 2003 год. 37, 47, 51, 54, 104, 145, 147, 215

College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, C-553/07, 7 мај 2009 год. 115, 121, 217

Deutsche Telekom AG v. Germany, C-543/09, 5 мај 2011год. 38, 65, 66, 216

Digital Rights Ireland and Seitlinger and Others, заеднички предмети C-293/12 и C-594/12,8 април 2014 год. 139, 192, 216

Dimitrios Pachtitis v. European Commission, F-35/08, 15 јуни 2010 год. 217

European Commission v. Federal Republic of Germany, C-518/07, 9 март 2010 год. 116, 130, 216

European Commission v. Hungary, C-288/12,
8 април 2014 год. 116, 132, 215
European Commission v. Kingdom of Sweden, C-270/11, 30 мај 2013 год. 215
European Commission v. Republic of Austria, C-614/10,
16 октомври 2012 год. 116, 131, 217
European Commission v. The Bavarian Lager Co. Ltd., C-28/08 P,
29 јуни 2010 год. 14, 29, 32, 117, 141, 217
European Parliament v. Council of the European Union, заеднички предмети
C-317/04 и C-318/04, 30 мај 2006 год. 157

Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, Барање за прелиминарна одлука на судот *Audiencia Nacional* (Шпанија) поднесено на
9 март 2012 год., 25 мај 2012 год., во тек 215

Huber v. Germany, C-524/06,
16 декември 2008 год. 67, 87, 90, 92, 187, 200, 216

Interporc Im- und Export GmbH v. Commission of the European Communities, C-41/00, 6 март 2003 год. 32, 217

M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority, C-152/84, 26 февруари 1986 год. 220
Michael Schwarz v. Stadt Bochum, C-291/12, Мислење на
генералниот адвокат, 13 јуни 2013 год. 216

Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, 29 јануари 2008 год. 14, 24, 35, 37, 43, 215

Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, заеднички предмети C-465/00, C-138/01 and C-139/01, 20 мај 2003 год. 90, 216

SABAM v. Netlog N.V., C-360/10, 16 февруари 2012 год. 36, 216

Sabine von Colson and Elisabeth Kamann v. Land Nordrhein-Westfalen, C-14/83, 10 април 1984 год. 117, 142

Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, 16 декември 2008 год. 13, 25, 215

V v. European Parliament, F-46/09, 5 јули 2011 год. 217
Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, заеднички предмети C-92/09 и C-93/09, 9 ноември 2010 год. 13, 23, 32, 37, 41, 45, 67, 73, 215

Судска практика на Европскиот суд за човековите права

Allan v. the United Kingdom, бр. 48539/99, 5 ноември 2002 год. 166, 214
Amann v. Switzerland [GC], бр. 27798/95, 16 февруари 2000 год. 40, 42, 45, 70, 211, 213
Ashby Donald and Others v. France, бр. 36769/08, 10 јануари 2013 год. 35
Association "21 Décembre 1989" and Others v. Romania, бр.33810/07 и 18817/08, 24 мај 2011 год. 214
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, бр. 62540/00, 28 јуни 2007 год. 70
Avilkina and Others v. Russia, бр. 1585/09, 6 јуни 2013 год. (не е конечна) 197
Axel Springer AG v. Germany [GC], бр. 39954/08, 7 февруари 2012 год. 13, 26, 211

B.B. v. France, бр. 5335/06, 17 декември 2009 год. 163, 165, 212, 213
Bernh Larsen Holding AS and Others v. Norway, бр. 24117/08, 14 март 2013 год. 37, 41, 212
Biriuk v. Lithuania, бр. 23373/03, 25 ноември 2008 год. 28, 117, 197, 212
Bykov v. Russia [GC], бр. 4378/02, 10 март 2009 год. 214

Cemalettin Canli v. Turkey, бр. 22427/04, 18 ноември 2008 год. 115, 122, 212
Ciubotaru v. Moldova, бр. 27138/04, 27 април 2010 год. 115, 124, 212
Copland v. the United Kingdom, бр. 62617/00, 3 април 2007 год. 15, 187, 194, 213

Cotlet v. Romania, бр. 38565/97, 3 јуни 2003 год. 213

Dalea v. France, бр. 964/07, 2 февруари 2010 год. 122, 164, 180, 212

Gaskin v. the United Kingdom, бр. 10454/83, 7 јули 1989 год. 119, 211, 212
Godelli v. Italy, бр. 33783/09, 25 септември 2012 год. 42, 119, 211, 213

Halford v. the United Kingdom, бр. 20605/92, 25 јуни 1997 год. 202, 213
Haralambie v. Romania, бр. 21737/03, 27 октомври 2009 год. 68, 82, 212

I. v. Finland, бр. 20511/03, 17 јули 2008 год. 16, 88, 102, 142, 196, 212, 213, 214
Iordachi and Others v. Moldova, бр. 25198/02,
10 февруари 2009 год. 70

K.H. and Others v. Slovakia, бр. 32881/04,
28 април 2009 год. 68, 83, 119, 196, 211
K.U. v. Finland, бр. 2872/02, 2 декември 2008 год. 16, 117, 137, 142, 211, 214
Kennedy v. the United Kingdom, Бр. 26839/05,
18 мај 2010 год. 214
Khelili v. Switzerland, бр. 16188/07, 18 октомври 2011 год. 67, 72, 212
Klass and Others v. Germany, Бр. 5029/71, 6 септември 1978 год. 15, 166, 214
Köpke v. Germany, бр. 420/07, 5 октомври 2010 год. 46, 137, 214
Kopp v. Switzerland, бр. 23224/94, 25 март 1998 год. 70
Kruslin v. France, бр. 11801/85, 24 април 1990 год. 213

L.L. v. France, бр. 7508/02, 10 октомври 2006 год. 196, 212
Lambert v. France, бр. 23618/94, 24 август 1998 год. 213
Leander v. Sweden, бр. 9248/81,
26 март 1987 год. 15, 67, 72, 119, 127, 165, 211, 212, 213
Liberty and Others v. The United Kingdom, бр. 58243/00, 1 јули 2008 год 41, 213

M.G. v. the United Kingdom, бр. 39393/98, 24 септември 2002 год. 212
M.K. v. France, бр. 19522/09, 18 април 2013 год. 123, 165
M.M. v. the United Kingdom, бр. 24029/07, 13 ноември 2012 год. 81, 165, 212

M.S. v. Sweden, бр. 20837/92, 27 август 1997 год. 127, 196, 212, 214
Malone v. the United Kingdom, бр. 8691/79, 2 август 1984 год. 15, 70, 192, 212, 213
McMichael v. the United Kingdom, бр. 16424/90,
24 февруари 1995 год.....212
Michaud v. France, бр. 12323/11, 6 декември 2012 год 188, 202, 213, 214
Mosley v. the United Kingdom,
бр. 48009/08, 10 май 2011 год. 13, 27, 127, 213
Müller and Others v. Switzerland,
бр. 10737/84, 24 май 1988 год. 33

Niemietz v. Germany, 13710/88, 16 декември 1992 год. 40, 202, 213

Odièvre v. France [GC], бр. 42326/98, 13 февруари 2003 год. 42, 119, 211, 213

P.G. and J.H. v. the United Kingdom, бр. 44787/98,
25 септември 2001 год. 46, 214
Peck v. the United Kingdom, бр. 44647/98, 28 януари 2003 год. 46, 67, 71, 214

Rotaru v. Romania [GC], бр. 28341/95,
4 май 2000 год. 40, 67, 70, 124, 212, 214

S. and Marper v. the United Kingdom, бр. 30562/04 и
30566/04, 4 декември 2008 год.....15, 81, 163, 165, 212, 214
Sciacca v. Italy, бр. 50774/99, 11 януари 2005 год.....46, 213
Segerstedt-Wiberg and Others v. Sweden, бр. 62332/00,
6 юни 2006 год. 115, 123, 213
Shimovolos v. Russia, бр. 30194/09, 21 юни 2011 год. 70, 212
Silver and Others v. the United Kingdom, бр. 5947/72, 6205/73,
7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 год.....70
Szuluk v. the United Kingdom, бр. 36936/05, 2 юни 2009 год. 196, 212, 213

Társaság a Szabadságjogokért v. Hungary, бр. 37374/05, 14 април 2009 год. 14, 31
Taylor-Sabori v. the United Kingdom, бр. 47114/99, 22 октомври 2002 год.....67, 71, 214
The Sunday Times v. the United Kingdom, бр. 6538/74, 26 април 1979 год. 70

Turek v. Slovakia, бр. 57986/00, 14 февруари 2006 год. 212

Uzun v. Germany, бр. 35623/05, 2 септември 2010 год. 15, 46, 212, 214

Vereinigung bildender Künstler v. Austria, бр. 68345/01,
25 јануари 2007 год. 13, 33
Vetter v. France, бр. 59842/00, 31 мај 2005 год. 70, 163, 167, 214
Von Hannover v. Germany (No. 2) [GC], бр. 40660/08 и
60641/08, 7 февруари 2012 год. 23, 26, 211, 214
Von Hannover v. Germany, бр. 59320/00, 24 јуни 2004 год 46, 211, 213, 214

Wisse v. France, бр. 71611/01, 20 декември 2005 год 46, 214

Z. v. Finland, бр. 22009/93, 25 февруари 1997 год. 187, 196, 212

Судска практика на националните судови

Германија, Сојузен уставен суд (*Bundesverfassungsgericht*),
1 BvR 256/08, 2 март 2010 год. 192

Романија, Сојузен уставен суд (*Curtea Constituțională a
României*), *бр. 1258*, 8 октомври 2009 год. 192

Република Чешка, Уставен суд (*Ústavní soud České
republiky*), *94/2011 Coll.*, 22 март 2011 год. 192

Голем дел од информациите за Европската агенција за основните права се достапни на интернет. До нив може да се пристапи преку интернет-страницата на Агенцијата: fra.europe.eu

Повеќе информации за Советот на Европа се достапни на интернет-страницата: hub.coe.int.

Повеќе информации за Европскиот суд за човекови права се достапни на интернет-страницата на Судот: echr.coe.int.

Порталот за пребарување HUDOC овозможува пристап до пресудите и одлуките на англиски и/или француски јазик, преводи на дополнителни јазици, месечен билтен со информации за судската практика, соопштенија за медиумите и други информации за работата на Судот.

Како да ги добиете публикациите на Европската Унија

Бесплатни публикации:

- еден примерок:
  преку книжарницата на Европската Унија (http://bookshop.europa.eu);
- повеќе од еден примерок или постери/географски карти:
  во претставништвата на Европската Унија (http://ec.europa.eu/represent_en.htm); од делегациите во земји што не се членки на Европската Унија (http://eeas.europa.eu/delegations/index_ en.htm);
  со контактирање на службата Europe Direct (http://europa.eu/europedirect/index_en.htm) или со повикување на 00 800 6 7 8 9 10 11 (бесплатен телефонски број од секаде во Европската Унија) (*).

Публикации што се наплаќаат:

- преку книжарницата на Европската Унија (http://bookshop.europa.eu);

Претплата за публикации:

- преку еден од продажните агенти во Канцеларијата за публикации на Европската Унија (http://publications.europa.eu/others/agents/index_en.htm).

(*) Информациите се бесплатни, како и повеќето повици (некои оператори, телефонски говорници или хотели може да ги наплатат повиците).

Како да ги добиете публикациите на Советот на Европа

Издавачката служба на Советот на Европа работи во сите релевантни области на организацијата, вклучувајќи човекови права, правна наука, здравство, етика, социјални работи, животна средина, образование, култура, спорт, млади и архитектонско наследство. Книги и електронски публикации од обемниот каталог може да се нарачаат онлајн (http://book.coe.int/).

Виртуелната читална им овозможува на корисниците бесплатно да консултираат извадоци од штотуку објавените дела или целосни текстови на одредени официјални документи.
Информации за, како и целосниот текст од конвенциите на Советот на Европа се достапни на веб-страницата на Канцеларијата за договорите (Treaty Office) на Советот на Европа: http://conventions.coe.int/.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Брзиот развој на информациските и комуникациските технологии со себе ја повлекува и сé поголемата потреба за силна заштита на личните податоци. Тоа право е заштитено и со инструментите на Европската унија (ЕУ) и на Советот на Европа (СЕ). Технолошкиот напредок ги проширува границите, на пример, на надзорот, следењето на комуникациите, и зачувувањето на податоците. Сето тоа претставува значаен предизвик за правото на заштита на податоците. Целта на овој прирачник е да ги запознае правниците кои не се специјализирани во областа на заштитата на податоците со оваа правна област. Прирачникот содржи преглед на применливите правни рамки на Европската унија и на Советот на Европа. Тој ја објаснува клучната судска практика на Европскиот суд за човекови права (ЕСЧП) и на Судот на правдата на Европската унија (СПЕУ) со резимирање на нивните главни судски пресуди. Во случај кога не постои таква судска практика, дава практични илустрации со хипотетички сценарија. Накратко, целта на овој прирачник е да придонесе за силно и одлучно почитување на правото на заштита на податоците.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 - 1040 Vienna - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

COUNCIL OF EUROPE
EUROPEAN COURT OF HUMAN RIGHTS
67075 Strasbourg Cedex - France
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

GERMAN FOUNDATION FOR INTERNATIONAL LEGAL COOPERATION (IRZ)
Ubierstr. 92, 53173 Bonn, Germany
Tel. +49 (0) 228 9555-0 - Fax +49 (0) 228 9555-100
info@irz.de

ГЕРМАНСКА ФОНДАЦИЈА ЗА МЕЃУНАРОДНА ПРАВНА СОРАБОТКА
IRZ

Stabilitätspakt für Südosteuropa
Gefördert durch Deutschland
Stability Pact for South Eastern Europe
Sponsored by Germany

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738:340.13(4)

ПРИРАЧНИК за европското законодавство за заштита на податоците / [превод од англиски јазик Наташа Андреевска-Томовска]. - Скопје : Макавеј, 2016. - 230 стр. ; 21 см

Превод на делото: Handbook on European data protection law. -
Фусноти кон текстот

ISBN 978-608-205-403-2

а) Заштита на лични податоци - Законодавство - Европа
COBISS.MK-ID 101024010

IRZ

Макавеј, 2016

ISBN 978-608-205-403-2