Съвет на
Европейския съюз

Брюксел, 12 януари 2017 г.
(OR. en)

5034/17

Междуинституционално досие:
2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-н Jordi AYET PUIGARNAU, директор
Дата на получаване:	12 януари 2017 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2017) 8 final
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО

Приложено се изпраща на делегациите документ COM(2017) 8 final.

Приложение: COM(2017) 8 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 10.1.2017 г.
COM(2017) 8 final

2017/0002 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

В член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС), въведен с Договора от Лисабон, се установява принципът, че всеки има право на защита на неговите лични данни. Освен това в член 16, параграф 2 от ДФЕС Договорът от Лисабон въвежда специално правно основание за приемането на разпоредби относно защитата на личните данни. В член 8 от Хартата на основните права на Европейския съюз защитата на личните данни е залегнала като основно право.

Правото на защита на личните данни се прилага също спрямо обработването на лични данни от институциите, органите, службите и агенциите на ЕС. Регламент (ЕО) № 45/2001[1], основният действащ законодателен акт на ЕС относно защитата на личните данни от страна на институциите на ЕС, бе приет през 2001 г. с две предвидени цели: да бъде защитено основното право на защита на данните и да се гарантира свободният поток на лични данни навсякъде в Съюза. Той бе допълнен с Решение № 1247/2002/ЕО[2].

На 27 април 2016 г. Европейският парламент и Съветът приеха Общ регламент относно защитата на данните (Регламент (ЕС) 2016/679), който ще започне да се прилага на 25 май 2018 г. Посоченият регламент изисква адаптирането на Регламент (ЕО) № 45/2001 към принципите и правилата, установени в Регламент (ЕС) 2016/679, с цел да се осигури силна и съгласувана рамка за защита на данните в Съюза и да се даде възможност за едновременното прилагане на двата инструмента[3].

Привеждането, доколкото е възможно, на правилата относно защитата на данните от страна на институциите, органите, службите и агенциите на Съюза в съответствие с правилата относно защитата на данните, приети за държавите членки, е в съответствие със съгласувания подход към защитата на личните данни навсякъде в Съюза. Когато разпоредбите на предложението се основават на една и съща концепция с разпоредбите на Регламент (ЕС) 2016/679, уместно е тълкуването на тези две разпоредби да бъде еднозначно, особено защото структурата на предложението следва да се схваща като еквивалентна на структурата на Регламент (ЕС) 2016/679[4].

При преразглеждането на Регламент (ЕО) № 45/2001 са взети също предвид и резултатите от проучвания и консултации със заинтересованите страни, както и оценката на прилагането му през последните 15 години.

---

1 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г.).

2 Решение № 1247/2002/ЕО от 1 юли 2002 г. относно статута и общите условия, регулиращи изпълнението на задълженията на Европейския надзорен орган по защита на данните' (ОВ L 183, 12.7.2002 г., стр. 1)..

3 Вж. член 98 и съображение 17 от Регламент (ЕС) № 20016/679.

4 Вж. Съд на Европейския съюз, 9 март 2010 г., *Комисия/Германия*, дело C-518/07, ECLI:EU:C:2010:125, точки 26 и 28.

Настоящата инициатива не е по линия на Програмата за пригодност и резултатност на регулаторната рамка (REFIT).

- **Съгласуваност със съществуващите разпоредби в тази област на политиката**

Предложението има за цел да се приведат разпоредбите на Регламент (ЕО) № 45/2001 в съответствие с принципите и правилата, установени в Регламент (ЕС) 2016/679, с цел да се осигури силна и съгласувана рамка за защита на данните в Съюза. В предложението също така са включени съответните правила, установени в Регламент (ЕО) № XXXX/XX [Регламент за неприкосновеността на личния живот в сектора на електронните съобщения], по отношение на защитата на крайните устройства на крайните потребители.

- **Съгласуваност с другите политики на Съюза**

Не е приложимо.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

- **Правно основание**

Защитата на физическите лица във връзка с обработването на техните лични данни е основно право, установено в член 8, параграф 1 от Хартата на основните права на Европейския съюз.

Настоящото предложение се основава на член 16 от ДФЕС, който е правното основание за приемане на разпоредби в областта на защитата на данните. Посоченият член дава възможност за приемането на разпоредби за защита на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза при изпълнение на техните дейности, които попадат в обхвата на правото на Съюза. Той също така дава възможност за приемането на разпоредби, свързани със свободното движение на лични данни, включително лични данни, обработвани от посочените институции, органи, служби и агенции.

- **Субсидиарност (при неизключителна компетентност)**

Предметът на настоящия регламент попада в областта на изключителната компетентност на Съюза, тъй като само Съюзът може да приеме разпоредби, които уреждат обработването на лични данни от институции на Съюза.

- **Пропорционалност**

Съгласно принципа на пропорционалност за постигането на основните цели за гарантиране на еквивалентно ниво на защита на физическите лица във връзка с обработването на лични данни и свободния поток на лични данни навсякъде в Съюза е необходимо и целесъобразно да се установят правила относно обработването на лични данни от институциите, органите, службите и агенциите на Съюза. С настоящия регламент не се надхвърля необходимото за постигането на поставените цели в съответствие с разпоредбите на член 5, параграф 4 от Договора за Европейския съюз,

- **Избор на инструмент**

Смята се, че регламентът е подходящият правен инструмент за определяне на рамката относно защитата на физическите лица по отношение на обработването на лични данни от институциите, органите, службите и агенциите на Съюза, както и на свободното движение на тези данни. С него на физическите лица се предоставят гарантирани от закона права и се определят задълженията на администраторите в институциите, органите, службите и агенциите на Съюза по отношение на обработването на данни. В него също така се предвижда и независим надзорен орган — Европейският надзорен орган по защита на данните, който да отговаря за наблюдението на обработването на лични данни от институциите, органите, службите и агенциите на Съюза.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

Комисията извърши консултации със заинтересованите страни през 2010 г. и 2011 г., както и оценка на въздействието в контекста на подготовката на пакета за реформа на защитата на данните, в която се дава информация относно предложените изменения на Регламент (ЕО) № 45/2001. В този контекст Комисията проведе анкета сред координаторите за защита на данните в Комисията (КЗД)[5].

По отношение на практическото прилагане на Регламент (ЕО) № 45/2001 от институциите, органите, службите и агенциите на Съюза беше събрана информация от Европейския надзорен орган по защита на данните (ЕНОЗД), други институции, органи, служби и агенции на Съюза, други генерални дирекции на Комисията, а също и от външен изпълнител. На мрежата на длъжностните лица по защита на данните (ДЛЗД) бе изпратен въпросник[6].

Длъжностните лица по защита на данните от редица институции, органи, служби и агенции на Съюза проведоха семинари относно реформата на Регламент № 45/2001 на 9 юли 2015 г., 22 октомври 2015 г., 19 януари 2016 г. и 15 март 2016 г.

През 2013 г. Комисията реши да извърши проучване за оценка на прилагането досега на Регламент (ЕО) № 45/2001, което бе възложено на външен изпълнител. Окончателните резултати от проучването за оценка (окончателен доклад, пет проучвания на конкретни случаи и анализ на всеки член поотделно) бяха предоставени на Комисията на 8 юни 2015 г.[7]

---

5 Вж. на: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

6 Вж. Общ доклад на Европейския надзорен орган по защита на данните ‘Measuring compliance with Regulation (EC) 45/2001 in EU institutions (‘Survey 2013’)’ (Измерване на спазването на Регламент (ЕО) № 45/2001 в институциите на ЕС (Анкета— 2013 г.) и ‘Opinion 3/2015 ‘Europe’s big opportunity: EDPS recommendations on the EU’s options for data protection reform’ (Становище 3/2015 „Големите възможности на Европа: препоръки на ЕНОЗД относно възможностите на ЕС за реформа в областта на защитата на данните“).

7 JUST/2013/FRAC/FW/0157/A4 в контекста на рамков договор за многократно предоставяне на услуги; JUST/2011/EVAL/01 (RS 2013/05) — Evaluation Study on Regulation (EC) 45/2001 (Проучване за оценка относно Регламент (ЕО) № 45/2001), Ernst and Young, достъпен на адрес: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087.

Оценката показа, че системата за управление, чиято структура се гради на длъжностните лица по защита на данните и ЕНОЗД, е ефективна. В нея бе установено, че разпределението на правомощията между длъжностните лица по защита на данните и ЕНОЗД е ясно и добре балансирано, като те разполагат с подходящ набор от правомощия. Трудности обаче биха могли да възникнат от липса на авторитет поради недостатъчна подкрепа за длъжностните лица по защита на данните от тяхното ръководство.

В проучването за оценка бе посочено, че Регламент (ЕО) № 45/2001 може да се прилага по-добре чрез използването на санкции от страна на ЕНОЗД. Увеличеното използване на правомощията на надзорния орган по регламента би могло да доведе до по-добро прилагане на правилата за защита на данните. Друго заключение беше, че администраторите на данни следва да възприемат подход за управление на риска, както и да извършват оценки на риска преди извършването на операции по обработване на данни с цел по-добро прилагане на изискванията за запазването и сигурността на данните.

Проучването показа също, че действащите разпоредби от глава IV от Регламент (ЕО) № 45/2001 относно сектора на далекосъобщенията са остарели и че е необходимо привеждането в съответствие на посочената глава с Директивата за защитата на неприкосновеността на личния живот в сектора на електронните съобщения. В проучването за оценка се застъпва становището, че също така е необходимо да се изяснят някои основни определения от Регламент (ЕО) № 45/2001. Това включва идентифицирането на администраторите на данни в институциите, органите, службите и агенциите на Съюза, определението за получатели и разпростирането на задължението за поверителност към обработващите лични данни външни лица.

В проучването за оценка бе отбелязана също така необходимостта да бъде опростен режимът на уведомяване и предварителни проверки, за да се повиши ефикасността и да се намали административната тежест.

Оценителят проведе онлайн анкета в рамките на 64 институции, агенции, служби и органи на Съюза. На въпросите от анкетата отговориха 422 отговорни служители на администраторите на данни, 73 ДЛЗД, 118 КЗД и 109 респонденти в областта на информационните технологии. Оценителят извърши също така поредица от интервюта със заинтересовани страни. На 26 март 2015 г. оценителят и Комисията организираха заключителен семинар с участието на множество администратори на данни, ДЛЗД, КЗД, респонденти в областта на информационните технологии и представители на ЕНОЗД.

- **Събиране и използване на експертни становища**

Вж. препратка към проучването за оценка в предходната точка.

- **Оценка на въздействието**

Настоящото предложение ще има въздействие основно върху институциите, органите, службите и агенциите на Съюза. Това бе потвърдено от информацията, събрана от ЕНОЗД, други институции, органи, служби и агенции на Съюза, генерални дирекции на Комисията и външния изпълнител. Освен това въздействието на новите задължения, произтичащи от Регламент (ЕС) 2016/679, с който настоящият регламент следва да бъде

приведен в съответствие, беше оценено в контекста на подготвителната работа за него. Това прави специална оценка на въздействието за настоящия регламент ненужна.

- **Пригодност и опростяване на законодателството**

Не е приложимо.

- **Основни права**

Правото на защита на личните данни е установено в член 8 от Хартата на основните права на Европейския съюз („Хартата“), член 16 от ДФЕС и член 8 от Европейската конвенция за правата на човека. Както бе подчертано от Съда на Европейския съюз[8], правото на защита на личните данни не е абсолютно право, а трябва да се разглежда във връзка с функцията му в обществото[9]. Защитата на данните е също така тясно свързана със зачитането на личния и семейния живот, защитен с член 7 от Хартата.

Настоящото предложение определя правила относно защитата на физическите лица по отношение на обработването на лични данни от институциите, органите, службите и агенциите на Съюза, както и относно свободното движение на тези данни.

Други основни права, залегнали в Хартата, които потенциално могат да бъдат засегнати, са: свободата на изразяване (член 11); правото на собственост, и по-специално защитата на интелектуалната собственост (член 17, параграф 2); забраната на всякаква форма на дискриминация въз основа на раса, етнически произход, генетични характеристики, религия или убеждения, политически или други мнения, увреждане или сексуална ориентация (член 21); правата на детето (член 24); правото на висока степен на закрила на здравето (член 35); правото на достъп до документи (член 42); и правото на ефективни правни средства за защита и на справедлив съдебен процес (член 47*).*

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Вж. приложената финансова обосновка.

5. ДРУГИ ЕЛЕМЕНТИ

- **Планове за изпълнение и механизъм за наблюдение, оценка и докладване**

Не е приложимо.

---

[8] Съд на Европейския съюз, 9 ноември 2010 г., *Volker und Markus u Eifert*, съединени дела C-92/09 и C-93/09, ECLI:EU:C:2009:284, точка 48.

[9] В съответствие с член 52, параграф 1 от Хартата ограничения могат да бъдат налагани върху упражняването на правото на защита на данните, доколкото такива ограничения са предвидени по закон, зачитат основното съдържание на същите права и свободи и, при спазване на принципа на пропорционалност, са необходими и действително отговарят на признати от Европейския съюз цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

- **Обяснителни документи (за директивите)**

Не е приложимо.

ГЛАВА I — ОБЩИ РАЗПОРЕДБИ

В член 1 се определят предметът на регламента и, както в член 1 от Регламент (ЕО) № 45/2001, двете цели на регламента: да бъде защитено основното право на защита на данните и да се гарантира свободният поток на лични данни навсякъде в Съюза. В него също така се предвиждат основните задачи на Европейския надзорен орган по защита на данните.

В член 2 се определя приложното поле на регламента: регламентът ще се прилага за обработването на данни чрез автоматизирани или други средства от всички институции и органи на Съюза дотолкова, доколкото това обработване се извършва при упражняване на дейности, които изцяло или частично попадат в обхвата на правото на Съюза. Материалното приложно поле на настоящия регламент е технологично неутрално. Защитата на личните данни следва се прилага за обработването на лични данни с автоматизирани средства, както и за ръчното им обработване, ако личните данни се съхраняват или са предназначени да се съхраняват в регистър с лични данни.

Член 3 съдържа определенията на термините, използвани в регламента. С изключение на определенията на „институции и органи на Съюза“, „администратор“, „потребител“ и „указател“, които са специфични за настоящия регламент, термините, използвани в настоящия регламент са определени в Регламент (ЕС) 2016/679, Регламент (ЕС) 0000/00 [нов Регламент за защитата на неприкосновеността на личния живот в сектора на електронните съобщения], Директива № 00/0000/ЕС [Директива за създаване на Европейски кодекс за електронните съобщения] и Директива 2008/63/ЕО на Комисията.

ГЛАВА II — ПРИНЦИПИ

В член 4 се определят принципите, отнасящи се до обработването на лични данни, които съответстват на принципите, посочени в член 5 от Регламент (ЕС) 2016/679. В сравнение с Регламент (ЕО) № 45/2001 в него са добавени новите принципи на прозрачност и на цялостност и поверителност.

Член 5 се основава на член 6 от Регламент (ЕС) 2016/679 и определя критериите за законосъобразно обработване, с изключение единствено на критерия на законния интерес на администратора, който не е приложим към публичния сектор, поради което не следва да се прилага по отношение на институциите и органите на Съюза. В член 5 се запазват критериите, които вече са установени съгласно член 5 от Регламент (ЕО) № 45/2001.

В член 6 се разясняват условията за обработване за друга съвместима цел в съответствие с член 6, параграф 4 от Регламент (ЕС) 2016/679. В сравнение с член 6 от Регламент (ЕО) № 45/2001 тази нова разпоредба осигурява повече гъвкавост и правна сигурност по отношение на допълнителното обработване за съвместими цели.

В член 7 се разясняват — в съответствие с член 7 от Регламент (ЕС) 2016/679 — условията, за да бъде съгласието валидно като правно основание за законосъобразно обработване.

В член 8 се посочват — в съответствие с член 8 от Регламент (ЕС) 2016/679 — допълнителни условия за законосъобразността на обработването на лични данни на деца във връзка с услуги на информационното общество, които им се предлагат пряко. В него минималната възраст на дете за валидно съгласие се определя на 13 години.

В член 9 се определят — в съответствие с член 8 от Регламент (ЕО) № 45/2001 — правила, предвиждащи специфично ниво на защита за предаването на лични данни на получатели, които са различни от институции и органи на Съюза, установени са в Съюза и попадат в обхвата на Регламент (ЕС) 2016/679 или Директива (ЕС) 2016/680. В него се пояснява, че когато администраторът е този, който предприема предаването, той следва да докаже необходимостта и пропорционалността на предаването.

В член 10 се определя — въз основа на член 9 от Регламент (ЕС) 2016/679 и като се доразвива член 10 от Регламент (ЕО) № 45/2001 — общата забрана за обработване на специални категории лични данни и изключенията от това общо правило.

В член 11 се определят — в съответствие с член 10 от Регламент (ЕС) 2016/679 и с член 10, параграф 5 от Регламент (ЕО) № 45/2001 — условията за обработването на лични данни, свързани с присъди и престъпления.

В член 12 се разясняват — в съответствие с член 11 от Регламент (ЕС) 2016/679 — задълженията на администратора да предоставя информация на субекта на данни, като се предвижда, че ако обработваните от администратора лични данни не му позволяват да идентифицира дадено физическо лице, администраторът на данни не е задължен да се сдобие с допълнителна информация, за да идентифицира субекта на данните с единствената цел да бъдат спазени разпоредбите на настоящия регламент. Администраторът обаче не следва да отказва да приеме допълнителна информация, подадена от субекта на данни, за да подпомогне упражняването на неговите права.

В член 13 се определят — въз основа на член 89, параграф 1 от Регламент (ЕС) 2016/679 — правилата относно гаранциите, свързани с обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели.

ГЛАВА III — ПРАВА НА СУБЕКТА НА ДАННИ

Раздел 1 — Прозрачност и условия

С член 14 се въвежда — въз основа на член 12 от Регламент (ЕС) 2016/679 — задължението на администраторите да осигуряват прозрачна, лесно достъпна и разбираема информация и процедури и механизми за упражняването на правата на субектите на данни, включително при необходимост средства за електронни искания, като се изисква да се предостави отговор на искането на субект на данни в рамките на определен срок, както и да се посочват причините за отказите. Тъй като при никакви обстоятелства не се очаква институциите и органите на Съюза да начисляват такси, свързани с административните разходи за предоставяне на информация, тази възможност не бе възприета от Регламент (ЕС) 2016/679 .

Раздел 2 — Информация и достъп до данни

В член 15 се посочват — въз основа на член 13 от Регламент (ЕС) 2016/679 и като се доразвива член 11 от Регламент (ЕО) № 45/2001 — задълженията на администратора

спрямо субекта на данни за предоставяне на информация, когато от субекта на данни се събират лични данни, като тези задължения включват предоставяне на информация на субекта на данни, включително относно срока на съхранение и правото на подаване на жалба, както и относно международното предаване на данни.

Освен това в член 16 се посочват — въз основа на член 14 от Регламент (ЕС) 2016/679 и като се доразвива член 12 от Регламент (ЕО) № 45/2001 — задълженията на администратора спрямо субекта на данни за предоставяне на информация, когато личните данни не са получени от субекта на данни, като тези задължения включват предоставяне на информация относно източника на данните. В него се запазват също възможните дерогации, предвидени в Регламент (ЕС) 2016/679, например липсата на подобно задължение, когато субектът на данни вече разполага с информацията, когато предоставянето на тази информация се окаже невъзможно или би било свързано с несъразмерно големи усилия на администратора, когато личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, което се урежда от правото на Съюза, или ако записването или разкриването са изрично предвидени от правото. Това може например да се прилага при процедурите на службите, компетентни по въпросите на социалната сигурност или здравеопазването.

В член 17 се предвижда — в съответствие с член 15 от Регламент (ЕС) 2016/679 и като се доразвива член 13 от Регламент (ЕО) № 45/2001 — правото на достъп на субекта на данни до неговите лични данни, като се добавят нови елементи, като например задължението за предоставянето на информация на субектите на данни относно срока на съхранение и относно правото им на коригиране и на изтриване на данни и правото им на подаване на жалба.

Раздел 3 — Коригиране и изтриване

Член 18 определя — като се основава на член 16 от Регламент (ЕС) 2016/679 и доразвива член 14 от Регламент (ЕО) № 45/2001 — правото на субекта на данни на коригиране.

В член 19 се определят — в съответствие с член 17 от Регламент (ЕС) 2016/679 и като се доразвива член 16, параграф 5 от Регламент (ЕО) № 45/2001 — правото на субекта на данни „да бъде забравен“ и правото му на изтриване на данни. В този член се предвиждат условията за упражняване на правото „да бъдеш забравен“, включително задължението на администратора, който публично е обявил данните, да уведоми третите страни за искането на субекта на данните да се изтрият всякакви връзки или копия или реплики на тези лични данни.

В член 20 се въвежда правото на ограничаване на обработването в определени случаи, като се избягва двусмисленият термин „блокиране“, използван в Регламент (ЕО) № 45/2001, и се гарантира съгласуваност с новата терминология от член 18 от Регламент (ЕС) 2016/679.

В член 21 се предвижда — в съответствие с член 19 от Регламент (ЕС) 2016/679 и като се доразвива член 17 от Регламент (ЕО) № 45/2001 — задължението на администратора да съобщи на получателите, на които личните данни са били разкрити, за всяко коригиране, изтриване или ограничаване на лични данни освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира също така субекта на данните относно тези получатели, ако субектът поиска това.

С член 22 се въвежда — в съответствие с член 20 от Регламент (ЕС) 2016/679 — правото на субекта на данни на преносимост на данните, т.е. правото да получи личните данни, които го засягат и които той е предоставил на администратор, или да прехвърли тези лични данни пряко на друг администратор, когато това е технически осъществимо. Като предварително условие и с цел да се подобри допълнително достъпът на физическите лица до техните лични данни, в посочения член се предвижда правото на субекта на данни да получава тези данни от администратора в структуриран, широко използван и машинночитаем формат. Това право се прилага само когато обработването се извършва въз основа на съгласието на субекта на данните или въз основа на договор, сключен от него.

Раздел 4 — Право на възражение и автоматизирано вземане на индивидуални решения

Член 23 — като се основава на член 21 от Регламент (ЕС) 2016/679 и доразвива член 18 от Регламент (ЕО) № 45/2001 — предвижда правата на субекта на данни на възражение.

Член 24 — в съответствие с член 22 от Регламент (ЕС) 2016/679 и като доразвива член 19 от Регламент (ЕО) № 45/2001 — се отнася до правото на субекта на данни да не бъде адресат на мярка, основаваща се единствено на автоматизирано обработване, включително профилиране.

Раздел 5 — Ограничения

В член 25 се разрешават ограничения на правата на субекта на данни, установени в членове 14—22 и в членове 34 и 38, както и на принципите, установени в член 4 (доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—22). Тези ограничения следва да бъдат определени в правни актове, приети въз основа на Договорите или на вътрешните правила на институциите и органите на Съюза. Ако евентуално подобно ограничение не е предвидено в правните актове, приети въз основа на Договорите или на вътрешните правила на институциите и органите на Съюза, институциите и органите могат да наложат във връзка с конкретна операция по обработване *ad hoc* ограничение, при условие че то зачита същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с оглед на защитата на една или повече от целите, които позволяват ограничения по отношение на правата на субектите на данни. Този подход е в съответствие с член 23 от Регламент (ЕС) 2016/679. Въпреки това — за разлика от член 23 от Регламент (ЕС) 2016/679 и в съответствие с член 20 от Регламент (ЕО) № 45/2001 — тази разпоредба не предвижда възможността да се ограничи правото на субекта на данни на възражение и правото му да не бъде адресат на решения, основаващи се единствено на автоматизирано обработване. Изискванията за ограниченията са в съответствие с Хартата на основните права и Европейската конвенция за правата на човека, така както те се тълкуват съответно от Съда на Европейския съюз и от Европейския съд по правата на човека.

ГЛАВА IV — АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Раздел 1 — Общи задължения

Член 26 се основава на член 24 от Регламент (ЕС) 2016/679 и въвежда „принципа на отчетност“, описвайки задължението за отговорност на администратора да спазва разпоредбите на настоящия регламент и да доказва тяхното спазване, включително като

приема съответни технически и организационни мерки и, когато е целесъобразно, вътрешни политики и механизми, за да гарантира спазването им. Член 24, параграф 3 от Регламент (ЕС) 2016/679 не бе запазен в тази разпоредба, тъй като институциите и органите на Съюза не следва да се придържат към кодекси на поведение или механизми за сертифициране.

В член 27 се определят — в съответствие с член 25 от Регламент (ЕС) 2016/679 — задълженията на администратора, произтичащи от принципите на защита на данните още при проектирането и по подразбиране.

Член 28 относно съвместните администратори се основава на член 26 от Регламент (ЕС) 2016/679, с цел изясняване на отговорностите на съвместните администратори — било то институции или органи на Съюза, или не — във връзка с техните вътрешни отношения и спрямо субекта на данни. Тази разпоредба урежда случая, когато всички съвместни администратори са обхванати от един и същ правен режим (настоящия регламент), и случая, когато някои от тях попадат в обхвата на настоящия регламент, а други — на друг правен инструмент (Регламент (ЕС) 2016/679, Директива (ЕС) 2016/680, Директива (ЕС) 2016/681 и други специфични режими за защита на данните от страна на институции или органи на Съюза).

Член 29 се основава на член 28 от Регламент (ЕС) 2016/679 и доразвива член 23 от Регламент (ЕО) № 45/2001 с цел изясняване на длъжността и задълженията на обработващите лични данни, включително като определя, че обработващият лични данни, който нарушава регламента, определяйки целите и средствата на обработването на данни, се счита за администратор по отношение на това обработване.

Член 30 относно обработването под ръководството на администратора и на обработващия лични данни се основава на член 29 от Регламент (ЕС) 2016/679, като установява забрана за обработващия лични данни или за всяко друго лице, действащо под ръководството на администратора или на обработващия лични данни и имащо достъп до лични данни, да обработва тези данни без указание на администратора, освен ако обработването се изисква от правото на Съюза или правото на държава членка.

Член 31 се основава на член 30 от Регламент (ЕС) 2016/679 и въвежда задължението за администраторите на данни и обработващите лични данни да поддържат документация за операциите по обработване, за които отговарят, вместо да подават предварително уведомление до ЕНОЗД, изисквано по член 25 от Регламент (ЕО) № 45/2001, и до регистъра, воден от ДЛЗД. За разлика от Регламент (ЕС) 2016/679 в посочената разпоредба не се споменават представители, тъй като институциите няма да имат представители, а винаги ще имат ДЛЗД. Позоваванията на предаване на данни въз основа на дерогациите в конкретни случаи, посочени в Регламент (ЕС) 2016/679, не бяха запазени, тъй като тези видове предаване на данни не са предвидени в настоящия регламент. Задължението да се поддържа регистър на дейностите по обработване може да бъде централизирано на равнището на институция или орган на Съюза. В този случай институциите и органите на Съюза имат възможност да поддържат своите регистри на дейностите по обработване на лични данни под формата на публично достъпен регистър.

В член 32 се разясняват — въз основа на член 31 от Регламент (ЕС) 2016/679 — задълженията на институциите и органите на Съюза за сътрудничество с ЕНОЗД.

Раздел 2 — Сигурност на личните данни и поверителност на електронните съобщения

В член 33 — в съответствие с член 32 от Регламент (ЕС) 2016/679 и като се доразвива член 22 от Регламент (ЕО) № 45/2001 — администраторът се задължава да прилага подходящи мерки за сигурността на обработването, като това задължение се разширява, за да обхване и обработващите лични данни, независимо от договора с администратора.

Член 34 се основава на член 36 от Регламент (ЕО) № 45/2001 и гарантира поверителността на електронните съобщения в рамките на институциите и органите на Съюза.

Член 35 се основава на съществуващата практика на институциите и органите на Съюза и защитава информацията, свързана с крайните устройства на крайните потребители, осъществяващи достъп до обществено достъпни уебсайтове и мобилни приложения, предлагани от институциите и органите на Съюза, в съответствие с Регламент (ЕС) XXXX/XX [нов Регламент за защитата на неприкосновеността на личния живот в сектора на електронните съобщения], и по-специално член 8 от него.

Член 36 се основава на член 38 от Регламент (ЕО) № 45/2001 и защитава личните данни, съхранявани в обществено достъпни и обществено недостъпни указатели на институциите и органите на Съюза.

С членове 37 и 38 се въвежда — в съответствие с членове 33 и 34 от Регламент (ЕС) 2016/679 — задължение за уведомяване при нарушение на сигурността на личните данни.

Раздел 3 — Оценка на въздействието върху защитата на данните и предварителни консултации

Член 39 се основава на член 35 от Регламент (ЕС) 2016/679 и въвежда задължението на администраторите и обработващите лични данни да извършват преди операции по обработване, които има вероятност да породят висок риск за правата и свободите на физическите лица, оценка на въздействието върху защитата на данните. Това задължение ще се прилага по-специално в случай на систематична и подробна оценка на лични аспекти по отношение на физически лица, която се базира на автоматизирано обработване, включително профилиране, мащабно обработване на специални категории данни или систематично мащабно наблюдение на публично достъпна зона.

Член 40 се основава на член 36 от Регламент (ЕС) 2016/679 и се отнася до случаите, при които разрешението от ЕНОЗД и консултацията с него са задължителни преди обработването. В член 40, параграф 1 обаче се възпроизвежда текста на съображение 94 от Регламент (ЕС) 2016/679, като се цели изясняване на обхвата на задължението за консултиране.

Раздел 4 — Информация и законодателни консултации

В член 41 се предвижда задължение за институциите и органите на Съюза да информират ЕНОЗД при изготвянето на административни мерки и вътрешни правила, свързани с обработването на лични данни.

В член 42 се предвижда задължение за Комисията да се консултира с ЕНОЗД след приемането на предложения за законодателен акт и на препоръки или предложения до

Съвета съгласно член 218 от ДФЕС и при подготовката на делегирани актове или актове за изпълнение, които имат въздействие върху защитата на правата и свободите на физическите лица по отношение на обработването на лични данни. Когато тези актове имат особено значение за защита на правата и свободите на физическите лица по отношение на обработването на лични данни, Комисията може също така да се консултира с Европейския комитет по защита на данните. В тези случаи двата органа следва да координират работата си с оглед на съставянето на съвместно становище. За посочените по-горе случаи се установява срок от 8 седмици за даването на становище, като са възможни дерогации за спешни случаи и когато това е уместно, например когато Комисията подготвя делегирани актове и актове за изпълнение.

Раздел 5 — Задължение за реагиране на твърдения

В член 43 се установява задължението на администраторите и обработващите лични данни да реагират на твърдения, след като ЕНОЗД реши да отнесе въпрос до тях.

Раздел 6 — Длъжностно лице по защита на данните

Член 29 се основава на член 37, параграф 1, буква а) от Регламент (ЕС) 2016/679 и член 24 от Регламент (ЕО) № 45/2001 и предвижда задължително ДЛЗД за институциите и органите на Съюза.

Член 29 се основава на член 38 от Регламент (ЕС) 2016/679 и член 24 от Регламент (ЕО) № 45/2001 и определя длъжността на ДЛЗД.

Член 46 се основава на член 39 от Регламент (ЕС) 2016/679, на член 24 от Регламент (ЕО) № 46/2001 и на втора и трета точка от приложението към Регламент (ЕО) № 46/2001, като предвижда основните задачи на ДЛЗД.

ГЛАВА V — ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

В член 47 се доразвива член 9 от Регламент (ЕО) № 45/2001 и се установява — в съответствие с член 44 от Регламент (ЕС) 2016/679 — общият принцип, че спазването на другите разпоредби на настоящия регламент и на условията, установени в глава V, е задължително при всяко предаване на лични данни на трети държави или международни организации, включително във връзка с последващо предаване на лични данни от третата държава или от международната организация на друга трета държава или международна организация.

В член 48 се предвижда, че предаване на лични данни на трета държава или на международна организация може да се осъществи, ако Комисията реши в съответствие с член 45, параграф 3 от Регламент (ЕС) 2016/679, че в тази трета държава, територия, или един или повече конкретни сектори в тази трета държава, или в рамките на международната организация е гарантирано адекватно ниво на защита и че личните данни се предават единствено с оглед изпълнение на задачи, които са от компетенциите на администратора. Параграфи 2 и 3 от този член са заимствани от член 9 от Регламент (ЕО) № 45/2001, тъй като те представляват полезни елементи на наблюдението на нивото на защита на данните в трети държави и международни организации.

Член 49 се основава на член 46 от Регламент (ЕС) 2016/679 и изисква при предаването на данни на трети държави, когато Комисията не е приела решение относно

адекватното нивото на защита, да се предоставят подходящи гаранции, по-специално стандартни клаузи за защита на данните и договорни клаузи. Обработващите лични данни, различни от институциите и органите на Съюза, биха могли в съответствие с Регламент (ЕС) 2016/679 да използват задължителни фирмени правила, кодекси за поведение и механизми за сертифициране. Четвъртият параграф от този член относно задължението на институциите и органите на Съюза да информират ЕНОЗД за категориите случаи, в които са приложили този член, съответства на член 9, параграф 8 от Регламент (ЕО) № 45/2001 и е запазен поради специфичния си характер. Петият параграф се основава на принципа за запазване на валидността на съществуващите разрешения, установен в член 46, параграф 5 от Регламент (ЕС) 2016/679.

В член 50 се пояснява — в съответствие с член 48 от Регламент (ЕС) 2016/679 — че всяко решение на съдилищата или всяко решение на административните органи на трета държава, с което се изисква предаване или разкриване на лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само ако се основават на международно споразумение, като например договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза, без да се засягат другите основания за предаване на данни съгласно посочената глава от регламента.

Член 51 се основава на член 49 от Регламент (ЕС) 2016/679 и формулира и разяснява дерогациите за предаване на данни. Те се прилагат по-специално за предаването на данни, което се изисква и е необходимо за защитата на важен обществен интерес, например при международно предаване на данни, в което участват органи по защита на конкуренцията, данъчни или митнически власти или между служби по социална сигурност или служби по управление на рибарството. Петият параграф относно задължението да се информира ЕНОЗД за категориите случаи, в които е извършено предаване на данни въз основа на дерогации, съответства на настоящия член 9, параграф 8 от Регламент (ЕО) № 45/2001.

Член 52 се основава на член 50 от Регламент (ЕС) 2016/679 и изрично предвижда механизми за международно сътрудничество за защитата на личните данни между ЕНОЗД, в сътрудничество с Комисията и Европейския комитет по защита на данните, и надзорните органи на трети държави.

ГЛАВА VI — ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ

Член 53 доразвива член 41 от Регламент (ЕО) № 45/2001 и се отнася до създаването на ЕНОЗД.

Член 54 се основава на член 42 от Регламент (ЕО) № 45/2001 и на член 3 от Решение № 1247/2002/ЕО и определя правилата за назначаването на ЕНОЗД от Европейския парламент и Съвета. В него се посочва също така срокът на неговия мандат: пет години.

Член 55 се основава на член 43 от Регламент (ЕО) № 45/2001 и на член 1 от Решение № 1247/2002/ЕО и предвижда статута и общите условия за изпълнение на задълженията на ЕНОЗД, както и неговите финансови и човешки ресурси.

Член 56 се основава на член 52 от Регламент (ЕС) 2016/679 и член 44 от Регламент (ЕО) № 45/2001 и пояснява условията за независимостта на ЕНОЗД при отчитане на съдебната практика на Съда на Европейския съюз.

В член 57 се определят — въз основа на член 45 от Регламент (ЕО) № 45/2001 — задълженията на ЕНОЗД за опазване на тайна , както по време на мандата му, така и

след края му, по отношение на поверителна информация, стигнала до знанието му в хода на изпълнение на служебните задължения.

Член 58 се основава на член 57 от Регламент (ЕС) 2016/679 и член 46 от Регламент (ЕО) № 45/2001 и определя задачите на ЕНОЗД, които включват разглеждане на жалби и извършване на разследване по тях, както и насърчаване на обществената информираност относно рисковете, правилата, гаранциите и правата.

Член 59 се основава на член 58 от Регламент (ЕС) 2016/679 и член 47 от Регламент (ЕО) № 45/2001 и определя правомощията на ЕНОЗД.

Член 60 се основава на член 59 от Регламент (ЕС) 2016/679 и член 48 от Регламент (ЕО) № 45/2001 и определя задължението на ЕНОЗД да изготвя годишен доклад за дейността.

ГЛАВА VII — СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ

Член 61 се основава на член 61 от Регламент (ЕС) 2016/679 и член 46 от Регламент (ЕО) № 45/2001 и въвежда изрични правила относно сътрудничеството на ЕНОЗД с националните надзорни органи.

В член 62 се предвиждат задълженията на ЕНОЗД, когато други актове на Съюза съдържат препращане към този член в рамките на координиран надзор с националните надзорни органи. С него се цели въвеждането на единен модел на координиран надзор. Посоченият модел би могъл да се използва за координиран надзор на мащабни информационни системи като Евродак, Шенгенската информационна система II, Визовата информационна система, Митническата информационна система или Информационната система за вътрешния пазар, а също така и за надзора над някои агенции на Съюза, като например Европол, когато е установен конкретен модел на сътрудничество между ЕНОЗД и националните органи. Европейският комитет по защита на данните следва да служи като единен форум за гарантиране на ефективния координиран надзор във всички области.

ГЛАВА VIII — СРЕДСТВА ЗА ПРАВНА ЗАЩИТА, ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ И САНКЦИИ

Член 63 се основава на член 77 от Регламент (ЕС) 2016/679 и член 32 от Регламент (ЕО) № 45/2001 и предвижда правото на всеки субект на данни да подаде жалба до ЕНОЗД. С него установява също така задължението на ЕНОЗД да разгледа жалбата и да информира субекта на данни за напредъка в разглеждането на жалбата и резултата от нея в срок от три месеца, след изтичането на който тя се счита за отхвърлена.

С член 64 се запазва член 32, параграф 1 от Регламент (ЕО) № 45/2001, като се установява компетентността на Съда на Европейския съюз да разглежда всички спорове във връзка с разпоредбите на настоящия регламент, включително искове за обезщетение за вреди.

В член 65 се установява правото на обезщетение за имуществени или неимуществени вреди, при условие че са изпълнени условията, включително тези относно отговорността, предвидени в Договорите.

Член 66 се основава на член 83 от Регламент (ЕС) 2016/679, като на ЕНОЗД се предоставя правомощието да налага административнонаказателни имуществени санкции на институции и органи на Съюза като санкция в краен случай и само когато институцията

или органът на Съюза не спази разпореждане на ЕНОЗД, посочено в член 59, параграф 2, букви а) — з) и буква й). В този член се посочват също така критериите за определяне на размера на административнонаказателната имуществена санкция във всеки отделен случай, като при определянето на максималните годишни размери за отправна точка са взети предвид размерите на санкциите, предвидени в някои държави членки.

С член 67 се разрешава — в съответствие с член 80, параграф 1 от Регламент (ЕС) 2016/679 — някои структури, организации или сдружения да подават жалба от името на субекта на данни.

В член 68 се предвиждат — в съответствие с член 33 от Регламент (ЕО) № 45/2001 — специални разпоредби, целящи защита на служителите на Съюза, подаващи жалби до ЕНОЗД във връзка с предполагаеми нарушения на разпоредбите на настоящия регламент, без да следват официалната процедура.

Член 69 се основава на член 49 от Регламент (ЕО) № 45/2001 и предвижда налагането на санкции за неспазването на задълженията по настоящия регламент от длъжностни лица или други служители на Европейския съюз.

ГЛАВА IX — АКТОВЕ ЗА ИЗПЪЛНЕНИЕ

Член 70 съдържа разпоредба за процедурата на комитет, необходима за предоставяне на изпълнителни правомощия на Комисията в случаите, при които в съответствие с член 291 от ДФЕС са необходими еднакви условия за изпълнение на правно обвързващи актове на Съюза. Прилага се процедурата по разглеждане.

ГЛАВА X — ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

С член 71 се отменят Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО и се предвижда, че позоваванията на двата отменени инструмента следва да се четат като позовавания на настоящия регламент.

В член 72 се пояснява, че настоящите мандати на Европейския надзорен орган по защита на данните и на неговия заместник няма да бъдат засегнати от настоящия регламент и че член 54, параграфи 4, 5 и 7 и членове 56 и 57 от регламента се прилагат към настоящия заместник до края на мандата му, а именно до 5 декември 2019 г.

В член 73 се определя 25 май 2018 г. като дата на влизане в сила на настоящия регламент с цел да се гарантира съгласуваност с датата на прилагане на Регламент (ЕС) 2016/679.

2017/0002 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 16, параграф 2 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[10],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Защитата на физическите лица във връзка с обработването на лични данни е основно право. Член 8, параграф 1 от Хартата на основните права на Европейския съюз („Хартата“) и член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС) предвиждат, че всеки има право на защита на неговите лични данни.

(2) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета[11] осигурява на физическите лица гарантирани от закона права, определя свързаните с обработването на данни задължения на администраторите в рамките на институциите и органите на Общността и създава независим надзорен орган, Европейския надзорен орган по защита на данните, който отговаря за наблюдението на обработването на лични данни от институциите и органите на Съюза. Той не се прилага обаче за обработването на лични данни при извършването на дейност на институциите и органите на Съюза, попадаща извън обхвата на правото на Съюза.

(3) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[12] и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета[13] бяха приети на 27 април 2016 г. Докато в регламента се установяват общи правила за защита на физическите лица във връзка с обработването на лични данни и за гарантиране на свободното движение на лични данни в рамките на Съюза, с директивата се установяват специални правила за защита на физическите лица във връзка с обработването на лични данни и за гарантиране на свободното движение на

---

10 ОВ С [...], [...] г., стр. [...].

11 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1).

12 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

13 Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

лични данни в рамките на Съюза в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество.

(4) В Регламент (ЕС) 2016/679 се подчертава нуждата от необходимите адаптации на Регламент (ЕО) № 45/2001, за да се осигури силна и съгласувана рамка за защита на данните в Съюза и да се даде възможност за прилагането му едновременно с Регламент (ЕС) 2016/679.

(5) Привеждането, доколкото е възможно, на правилата относно защитата на данните от страна на институциите и органите на Съюза в съответствие с правилата относно защита на данните, приети за публичния сектор в държавите членки, е в интерес както на постигането на съгласуван подход към защитата на личните данни навсякъде в Съюза, така и на свободното движение на лични данни навсякъде в Съюза. Когато разпоредбите на настоящия регламент се основават на една и съща концепция с разпоредбите на Регламент (ЕС) 2016/679, уместно е тълкуването на тези две разпоредби да бъде еднозначно, особено защото структурата на настоящия регламент следва да се схваща като еквивалентна на структурата на Регламент (ЕС) 2016/679.

(6) Лицата, чиито лични данни се обработват от институциите и органите на Съюза в някаква връзка, например поради това, че са служители на тези институции и органи, следва да бъдат защитени. Настоящият регламент не следва да се прилага за обработването на лични данни на починали лица. Настоящият регламент не обхваща обработването на лични данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка на юридическото лице.

(7) За да се избегне създаването на сериозен риск от заобикаляне на закона, защитата на физическите лица следва да бъде технологично неутрална и следва да не зависи от използваната техника. Защитата на физическите лица следва да се прилага за обработването на лични данни с автоматизирани средства, както и за ръчното им обработване, ако личните данни се съхраняват или са предназначени да се съхраняват в регистър с лични данни. Досиетата или групите от досиета, както и заглавните им страници, които не са структурирани съгласно специфични критерии, не следва да попадат в обхвата на настоящия регламент.

(8) В Декларация № 21 относно защитата на личните данни в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, приложена към заключителния акт на Междуправителствената конференция, която прие Договора от Лисабон, конференцията признава, че биха могли да са необходими специални правила относно защитата на личните данни и свободното движение на лични данни в областите на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество въз основа на член 16 от ДФЕС поради специфичното естество на тези области. Ето защо настоящият регламент следва да се прилага по отношение на агенциите на Съюза, извършващи дейности в областите на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество само доколкото в правото на Съюза, приложимо за тези агенции, не се съдържат специални правила относно обработването на лични данни.

(9) С Директива (ЕС) 2016/680 се предвиждат хармонизирани правила във връзка със защитата и свободното движение на личните данни, обработвани за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване. С цел да се осигури еднакво ниво на защита на физическите лица чрез гарантирани от закона права навсякъде в Съюза и да се предотвратят различията, възпрепятстващи обмена на лични данни между агенциите на Съюза, извършващи дейности в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, и компетентните органи в държавите членки, правилата за защитата и свободното движение на лични данни от оперативен характер, обработвани от тези агенции на Съюза, следва да се основават на принципите, които са в основата на настоящия регламент, и да бъдат съвместими с Директива (ЕС) 2016/680.

(10) Когато в учредителния акт на агенция на Съюза, извършваща дейности, попадащи в обхвата на глави 4 и 5 от дял V от Договора, се определя самостоятелен режим на защита на данните по отношение на обработването на лични данни от оперативен характер, този режим следва да не бъде засегнат от настоящия регламент. Все пак в съответствие с член 62 от Директива (ЕС) 2016/680 Комисията следва до 6 май 2019 г. да извърши преглед на актовете на Съюза, които регламентират обработването от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване, и ако е целесъобразно, да изготви необходимите предложения за изменение на тези актове, така че да се осигури съгласуван подход в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество.

(11) Принципите за защита на данните следва да се прилагат по отношение на всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано. Личните данни, които са били подложени на псевдонимизация, които могат да бъдат свързани с дадено физическо лице чрез използването на допълнителна информация, следва да се считат за информация, отнасяща се до физическо лице, което може да бъде идентифицирано. За да се определи дали дадено физическо лице може да бъде идентифицирано, следва да се вземат предвид всички средства, като например подбирането на лица за извършване на проверка, с които е най-вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице. За да се уточни дали има разумна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като например разходите и времето, необходими за идентифицирането, като се отчитат както наличните към момента на обработване на данните технологии, така и тяхното развитие. Поради това принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, а именно информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните вече не може да бъде идентифициран. Ето защо настоящият регламент не се отнася до обработването на такава анонимна информация, включително за статистически или изследователски цели.

(12) Прилагането на псевдонимизация на личните данни може да намали рисковете за съответните субекти на данни и да помогне на администраторите и на обработващите лични данни да изпълняват своите задължения за защита на данните. Изричното въвеждане на псевдонимизация в настоящия регламент не е предназначено да изключи други мерки за защита на данните.

(13) Физическите лица могат да бъдат свързани с онлайн идентификатори, предоставени от техните устройства, приложения, инструменти и протоколи, като адресите по интернет протокол (IP адреси) или идентификаторите, наричани „бисквитки“, или други идентификатори, например етикетите за радиочестотна идентификация. По този начин може да бъдат оставени следи, които в съчетание по-специално с уникални идентификатори и с друга информация, получена от сървърите, може да се използват за създаването на профили на физическите лица и за тяхното идентифициране.

(14) Съгласие следва да се дава чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път, или устна декларация. Това може да включва отбелязване с отметка в поле при посещението на уебсайт в интернет, избиране на технически настройки за услуги на информационното общество или друго заявление или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Поради това мълчанието, предварително отметнатите полета или липсата на действие не следва да представляват съгласие. Съгласието следва да обхваща всички дейности по обработване, извършени за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие. Ако съгласието на субекта на данни трябва да се даде след искане по електронен път, искането трябва да е ясно, сбито и да не нарушава излишно използването на услугата, за която се предвижда.

(15) Всяко обработване на лични данни следва да бъде законосъобразно и добросъвестно. За физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните. Принципът на прозрачност изисква всяка информация и комуникация във връзка с обработването на тези лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Този принцип се отнася в особена степен за информацията, която получават субектите на данни за самоличността на администратора и целите на обработването, и за допълнителната информация, гарантираща добросъвестно и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват. Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването. По-специално конкретните цели, за които се обработват лични данни, следва да бъдат ясни и законни и определени към момента на събирането на личните данни. Личните данни следва да са адекватни, релевантни и ограничени до

необходимото за целите, за които се обработват. Това налага по-специално да се гарантира, че срокът, за който личните данни се съхраняват, е ограничен до строг минимум. Личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства. С цел да се гарантира, че срокът на съхранение на личните данни не е по-дълъг от необходимия, администраторът следва да установи срокове за тяхното изтриване или периодичен преглед. Следва да бъдат предприети всички разумни мерки, за да се гарантира, че неточните лични данни се коригират или заличават. Личните данни следва да се обработват по начин, който гарантира подходяща степен на сигурност и поверителност на личните данни, включително за предотвратяване на непозволен достъп до лични данни и до оборудване за тяхното обработване или за предотвратяване на използването им.

(16) В съответствие с принципа на отчетност, когато институциите и органите на Съюза предават лични данни вътрешно или на други институции или органи на Съюза, те следва да проверяват дали тези лични данни са необходими за законното изпълнение на задачи от компетенциите на получателя, когато получателят не е част от администратора. По-специално след искане на получател за предаване на лични данни администраторът следва да удостовери наличието на съответно основание за законосъобразно обработване на лични данни от получателя, неговата компетентност, както и да извърши предварителна оценка на необходимостта от предаването на данните. В случай на възникнали съмнения относно тази необходимост администраторът следва да изисква допълнителна информация от получателя. Получателят следва да гарантира, че необходимостта от предаване на данните може да бъде впоследствие проверена.

(17) За да бъде обработването законосъобразно, личните данни следва да бъдат обработвани въз основа на необходимостта от изпълнение на задача от обществен интерес от страна на институции и органи на Съюза или при упражняването на техните официални правомощия, необходимостта от спазване на правното задължение, наложено на администратора на лични данни, или на друго законно основание, посочено в настоящия регламент, включително съгласието на субекта на данни, или необходимостта от изпълнение на договор, по който субектът на данни е страна, или с оглед предприемане на стъпки по искане на субекта на данни преди встъпване в договорни отношения. Обработването на лични данни за изпълнението на задачи от обществен интерес от страна на институции и органи на Съюза включва обработването на лични данни, които са необходими за управлението и функционирането на тези институции и органи. Обработването на лични данни следва да се счита за законосъобразно и когато е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице. Обработването на лични данни единствено въз основа на жизненоважен интерес на друго физическо лице следва да се състои по принцип, само когато обработването не може явно да се базира на друго правно основание. Някои видове обработване могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните, например когато обработването е необходимо за хуманитарни цели, включително за наблюдение на епидемии и тяхното разпространение, или при спешни хуманитарни ситуации, по-специално в случай на природни или причинени от човека бедствия.

(18) Правото на Съюза, включително посочените в настоящия регламент вътрешни правила, следва да бъде ясно и точно и прилагането му следва да бъде предвидимо за лицата, за които се прилага, в съответствие с практиката на Съда на Европейския съюз и на Европейския съд по правата на човека.

(19) Обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни, следва да бъде разрешено единствено когато обработването е съвместимо с целите, за които първоначално са събрани личните данни. В такъв случай не се изисква отделно правно основание, различно от това, с което е било разрешено събирането на личните данни. Ако обработването е необходимо за изпълнението на задача от обществен интерес или свързана с упражняването на официални правомощия, които са предоставени на администратора , в правото на Съюза могат да бъдат определени и уточнени задачите и целите, за които по-нататъшното обработване следва да се счита за съвместимо и законосъобразно. По-нататъшното обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели следва да се разглежда като съвместима законосъобразна операция по обработване. Правното основание, предвидено от правото на Съюза за обработване на лични данни, може да предостави и правно основание за по-нататъшно обработване. За да установи дали дадена цел на по-нататъшно обработване е съвместима с целта, за която първоначално са събрани личните данни, администраторът на лични данни, след като е спазил всички изисквания относно законосъобразността на първоначалното обработване, следва да отчете, *inter alia*: всички връзки между тези цели и целите на предвиденото по-нататъшно обработване; в какъв контекст са събрани личните данни, по-специално основателните очаквания на субектите на данните въз основа на техните взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни; естеството на личните данни; последствията от предвиденото по-нататъшно обработване на данни за субектите на данни; и наличието на подходящи гаранции при операциите по първоначалното и предвиденото по-нататъшно обработване.

(20) Когато обработването се извършва въз основа на съгласието на субекта на данните, администраторът следва да може да докаже, че субектът на данните е дал съгласието си за операцията по обработване. По-специално, в случай на писмена декларация по друг въпрос, с гаранциите следва да се обезпечи, че субектът на данни е информиран за това, че дава съгласието си, и в каква степен го дава. В съответствие с Директива 93/13/ЕИО на Съвета[14] следва да бъде осигурена предварително съставена от администратора декларация за съгласие в разбираема и лесно достъпна форма, на ясен и прост език, която следва да не съдържа неравноправни клаузи. За да бъде съгласието информирано, субектът на данни следва да знае поне самоличността на администратора и целите на обработването, за което са предназначени личните данни. Съгласието не следва да се разглежда като свободно дадено, ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

[14] Директива 93/13/ЕИО на Съвета от 5 април 1993 г. относно неравноправните клаузи в потребителските договори (ОВ J 95, 21.4.1993 г., стр. 29).

(21) На децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни. Тази специална защита следва да се прилага по-специално за създаването на личностни профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца на уебсайтове на институции и органи на Съюза, като например междуличностни съобщителни услуги или онлайн продажба на билети, и когато обработването на лични данни се основава на съгласие.

(22) Когато получатели, установени в Съюза и попадащи в обхвата на Регламент (ЕС) 2016/679 или Директива (ЕС) 2016/680, искат институции и органи на Съюза да им предадат лични данни, тези получатели следва да докажат, че предаването е необходимо за постигането на тяхната цел, пропорционално и не надхвърля необходимото за постигането на тази цел. Институциите и органите на Съюза следва да докажат такава необходимост, когато те самите предприемат предаването на данни, в съответствие с принципа на прозрачност.

(23) На личните данни, които по своето естество са особено чувствителни от гледна точка на основните права и свободи, се полага специална защита, тъй като контекстът на тяхното обработване би могъл да създаде значителни рискове за основните права и свободи. Посочените лични данни следва да включват личните данни, разкриващи расов или етнически произход, като използването на понятието „расов произход“ в настоящия регламент не означава, че Съюзът приема теориите, които се опитват да установят съществуването на отделни човешки раси. Обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице. В допълнение към специфичните изисквания за обработване на чувствителни данни следва да се прилагат общите принципи и другите правила, залегнали в настоящия регламент, по-специално по отношение на условията за законосъобразно обработване. Дерогации от общата забрана за обработване на такива специални категории лични данни следва изрично да бъдат предвидени, *inter alia*, когато субектът на данните даде изричното си съгласие или във връзка с конкретни нужди, по-специално когато обработването се извършва в хода на законната дейност на някои сдружения или фондации, чиято цел е да се позволи упражняването на основните свободи.

(24) Обработването на специални категории лични данни може да е необходимо по съображения от обществен интерес в областта на общественото здраве без съгласието на субекта на данните. Такова обработване следва да бъде предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на физическите лица. В този контекст понятието „обществено здраве“ следва да се тълкува по смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета[15] и означава всички елементи, свързани със здравето, а именно

[15] Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета от 16 декември 2008 г. относно статистиката на Общността в областта на общественото здраве и здравословните и безопасни условия на труд (текст от значение за ЕИП) (ОВ L 354, 31.12.2008 г., стр. 70).

здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху това здравословно състояние, потребности от здравно обслужване, средства, отделени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причини за смъртност. Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели от трети страни.

(25) Ако обработваните от администратора лични данни не му позволяват да идентифицира дадено физическо лице, администраторът на данни не следва да е задължен да се сдобие с допълнителна информация, за да идентифицира субекта на данните единствено с цел спазване на някоя от разпоредбите на настоящия регламент. Администраторът обаче не следва да отказва да приеме допълнителна информация, подадена от субекта на данни, за да подпомогне упражняването на неговите права. Идентификацията следва да включва цифровата идентификация на субекта на данни, например чрез механизъм за удостоверяване на автентичността като използването от субекта на данни на една и съща информация за удостоверяване на идентичността при регистрация за онлайн услуга, предлагана от администратора на лични данни.

(26) Обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели следва да се извършва при прилагане на подходящи гаранции за правата и свободите на субекта на данните в съответствие с настоящия регламент. Посочените гаранции следва да осигурят наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа за свеждане на данните до минимум. По-нататъшното обработване на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели се извършва, когато администраторът е преценил възможността за постигане на тези цели чрез обработването на лични данни, които не позволяват или повече не позволяват идентифицирането на субекта на данните, при условие че съществуват подходящи гаранции (като напр. псевдонимизацията на данните). Институциите и органите на Съюза следва да предвидят подходящи гаранции за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели в правото на Съюза, което може да включва вътрешни правила.

(27) Следва да бъдат предвидени ред и условия за улесняване на упражняването на правата на субектите на данни съгласно настоящия регламент, включително механизми за искане и ако е приложимо — получаване, без заплащане, по-специално на достъп до, коригиране или изтриване на лични данни и упражняване на правото на възражение. Администраторът следва да предостави и средства за подаване на искания по електронен път, особено когато личните данни се обработват електронно. Администраторът следва да бъде задължен да отговоря на исканията на субекта на данни без ненужно забавяне и най-късно в рамките на един месец, както и да посочи причините, ако не възнамерява да се съобрази с тези искания.

(28) Принципите на добросъвестно и прозрачно обработване изискват субектът на данни да бъде информиран за съществуването на операция по обработване и за

нейните цели. Администраторът следва да предостави на субекта на данните всяка допълнителна информация, която е необходима, за да се гарантира добросъвестно и прозрачно обработване на данните, като се вземат предвид конкретните обстоятелства и контекст, в които се обработват личните данни. Освен това субектът на данни следва да бъде информиран за извършването на профилиране и за последствията от това профилиране. Когато личните данни се събират от субекта на данни, той следва да бъде информиран и за това дали е задължен да предостави личните данни и за последствията, в случай че не ги предостави. Тази информация може да бъде предоставена в комбинация със стандартизирани икони, така че по лесно видим, разбираем и ясно четим начин да се представи съдържателен преглед на планираното обработване. Ако иконите се представят в електронен вид, те следва да бъдат машинночитаеми.

(29) Информацията за обработването на лични данни, свързани със субекта на данните, следва да му бъде предоставена в момента на събирането ѝ от субекта на данните или ако личните данни са получени от друг източник — в рамките на разумен срок, в зависимост от обстоятелствата на конкретния случай. В случаите, в които личните данни могат да бъдат законно разкрити на друг получател, субектът на данните следва да бъде информиран, когато личните данни се разкриват за първи път на получателя. Когато администраторът възнамерява да обработва личните данни за цел, различна от тази, за която те са събрани, той следва да предостави на субекта на данните преди това по-нататъшно обработване информация за въпросната друга цел и друга необходима информация. Когато на субекта на данните не може да се предостави информация за произхода на личните данни поради използването на различни източници, се представя обобщена информация.

(30) Всяко физическо лице следва да има право на достъп до събраните лични данни, които го засягат, и да упражнява това право лесно и на разумни интервали, за да бъде осведомено за обработването и да провери законосъобразността му. Това включва правото на субектите на данни на достъп до данните за здравословното им състояние, например данните в медицинските им досиета, които съдържат информация като диагнози, резултати от прегледи, становища на лекуващите лекари и проведени лечения или извършени операции. Поради това всеки субект на данни следва да има правото да е запознат и да получава информация, по-специално относно целите, за които се обработват личните данни, когато е възможно — срока, за който се обработват личните данни, получателите на личните данни, логиката на автоматизираното обработване на личните данни и последствията от такова обработване, най-малкото когато се извършва на основата на профилиране. Това право не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера. Тези съображения обаче не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни. Когато администраторът обработва голямо количество информация относно субекта на данни, администраторът следва да може да поиска от субекта на данните, преди да бъде предадена информацията, да посочи точно информацията или дейностите по обработването, за които се отнася искането.

(31) Субектът на данни следва да има право на коригиране на личните данни, свързани с него, както и правото „да бъде забравен“, когато запазването на тези

данни е в нарушение на настоящия регламент или на правото на Съюза, което се прилага спрямо администратора. Субектът на данни следва да има право личните му данни да се изтриват и да не бъдат обработвани повече, когато личните данни престанат да бъдат необходими с оглед на целите, за които те са били събрани или обработвани по друг начин, когато субектът на данните е оттеглил своето съгласие или е възразил срещу обработването на лични данни, свързани с него, или когато обработването на личните му данни по друг начин не е в съответствие с настоящия регламент. Това право е важно особено когато субектът на данни е дал съгласието си като дете и не е осъзнавал напълно рисковете, свързани с обработването, и впоследствие желае да премахне такива лични данни, особено когато са в интернет. Субектът на данни следва да може да упражни това право независимо от факта, че вече не е дете. По-нататъшното запазване на личните данни обаче следва да бъде законно, ако е необходимо за упражняване на правото на свобода на изразяване на мнение и правото на информация, за спазване на правно задължение, за изпълнение на задача от обществен интерес или при изпълнение на официални функции, възложени на администратора, по причини от обществен интерес в областта на общественото здравеопазване, за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели, или за установяване, упражняване или защита на правни претенции.

(32) С цел утвърждаване на „правото да бъдеш забравен“ в онлайн средата правото на изтриване следва да бъде разширено, като от администратора, който е направил личните данни обществено достъпни, следва да се изисква да информира администраторите, които обработват такива лични данни, да изтрият всякакви връзки към тези лични данни или техните копия или реплики. За тази цел администраторът следва да предприеме разумни мерки, като вземе предвид наличните технологии и средствата на разположение на администратора, в това число технически мерки, за да информира администраторите, които обработват личните данни, за искането на субекта на данните.

(33) Методите за ограничаване на обработването на лични данни биха могли да включват, *inter alia*, временно преместване на избраните лични данни в друга система за обработване, прекратяване на достъпа на ползвателите до тях или временно премахване на публикуваните данни от уебсайт. В автоматизираните регистри на лични данни ограничаването на обработването следва по принцип да бъде осигурено с технически средства, така че личните данни да не подлежат на операции по по-нататъшно обработване и да не могат да се променят. Фактът, че обработването на лични данни е ограничено, следва да бъде ясно посочен в системата.

(34) С цел допълнително засилване на контрола над собствените данни, когато обработването на лични данни става по автоматизиран начин, субектът на данните следва да има и правото да получава отнасящите се до него лични данни, които той е предоставил на администратора, в структуриран, широко използван, пригоден за машинно четене и оперативно съвместим формат и да ги предава на друг администратор. Администраторите следва да бъдат насърчавани да разработват оперативно съвместими формати, които позволяват преносимост на данните. Това право следва да се прилага, когато субектът на данни е предоставил личните данни въз основа на собственото си съгласие или обработването е необходимо поради договорно задължение. Ето защо това право

не следва да се прилага, когато обработването на личните данни е необходимо за спазване на правно задължение, на което е подчинен администраторът, или за изпълнение на задача от обществен интерес, или при упражняване на официално правомощие, предоставено на администратора. Правото на субекта на данни да предава или получава отнасящи се до него лични данни не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване. Когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни в съответствие с настоящия регламент. Освен това, това право не следва да засяга правото на субекта на данни на изтриване на лични данни и ограниченията на това право, както е посочено в настоящия регламент, и по-специално не следва да включва изтриването на лични данни относно субекта на данните, които той е предоставил в изпълнение на договор, в степента и за сроковете, за които личните данни са необходими за изпълнението на този договор. Когато това е технически осъществимо, субектът на данни следва да има право на пряко прехвърляне на личните данни от един администратор към друг.

(35) Когато личните данни биха могли да се обработват законно, тъй като обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официално правомощие, предоставено на администратора, всеки субект на данни следва все пак да има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. Администраторът следва да докаже, че неговите неоспорими законни интереси имат преимущество пред интересите или основните права и свободи на субекта на данни.

(36) Субектът на данни следва да има право да не бъде адресат на решение, което може да включва мярка за оценка на свързани с него лични аспекти единствено въз основа на автоматизирано обработване и което поражда правни последствия за него или го засяга също толкова значително, като например електронни практики за набиране на персонал без човешка намеса. Това обработване включва „профилиране“, което се състои от всякакви форми на автоматизирано обработване на лични данни за оценка на личните аспекти във връзка с дадено физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към изпълнението на професионалните задължения на субекта на данни, неговото икономическо състояние, здраве, лични предпочитания или интереси, надеждност или поведение, местонахождение или движения, когато то поражда правни последствия по отношение на лицето или го засяга също толкова значително. Въпреки това, вземането на решения въз основа на такова обработване, включително профилиране, следва да бъде позволено, когато е изрично разрешено от правото на Съюза. Във всеки случай такова обработване следва да подлежи на подходящи гаранции, които следва да включват конкретна информация за субекта на данните и правото на човешка намеса, на изразяване на мнение, на получаване на обяснение за решението, взето в резултат на такава оценка, и на обжалване на решението. Такава мярка не следва да се отнася до дете. С цел да се осигури добросъвестно и прозрачно обработване по отношение на субекта на данните, като се отчитат конкретните обстоятелства и контекстът, при които се обработват личните данни, администраторът следва да използва подходящи математически или статистически процедури за профилирането, да прилага съответните технически

и организационни мерки, по-специално за да гарантира, че факторите, които водят до неточности в личните данни, се коригират, а рискът от грешки се свежда до минимум, да защити личните данни по начин, който отчита потенциалните заплахи за интересите и правата на субекта на данните и който не поражда, *inter alia*, ефект на дискриминация за физическите лица въз основа на тяхната раса или етнически произход, политически възгледи, вероизповедание или убеждения, членство в синдикални организации, генетичен или здравен статус или сексуална ориентация или от който не произтичат мерки с такъв ефект. Автоматизираното вземане на решения и профилирането на базата на специални категории лични данни следва да бъде разрешено само при определени условия.

(37) Правни актове, приети въз основа на Договорите, или вътрешни правила на институции и органи на Съюза могат да налагат ограничения относно специални принципи и относно правото на информация, достъп до и коригиране или изтриване на лични данни, правото на преносимост на данните, поверителността на електронните съобщения, както и уведомяването на субекта на данни за нарушение на сигурността на личните данни и определени свързани с това задължения на администраторите, доколкото това е необходимо и пропорционално в едно демократично общество с оглед защитата на обществената сигурност, предотвратяването, разследването и наказателното преследване на престъпления или изпълнението на наказания, включително защитата срещу заплахи за обществената сигурност и тяхното предотвратяване, включително защитата на човешкия живот, особено при природни или предизвикани от човека бедствия, вътрешната сигурност на институциите и органите на Съюза, други важни цели от общ обществен интерес на Съюза или на държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, поддържането на публични регистри поради причини от широк обществен интерес или защитата на субекта на данни или на правата и свободите на други лица, включително социалната защита, общественото здраве и хуманитарните цели.

Когато дадено ограничение не е предвидено в правни актове, приети въз основа на Договорите, или в техни вътрешни правила, институциите и органите на Съюза могат да наложат в конкретен случай *ad hoc* ограничение относно специални принципи или правата на субекта на данните, при условие че то зачита същността на основните права и свободи и, във връзка с конкретна операция по обработване, представлява необходима и пропорционална мярка в едно демократично общество с оглед на защитата на една или повече от целите, споменати в параграф 1. Длъжностното лице по защита на данните следва да бъде уведомено за това ограничение. Всички ограничения следва да бъдат в съответствие с изискванията, определени в Хартата и в Европейската конвенция за защита на правата на човека и основните свободи.

(38) Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с настоящия регламент, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица. Рискът за правата и свободите на физическите лица, с

различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, имуществени или неимуществени вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация или други значителни икономически или социални неблагоприятни последствия; когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и престъпления или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения, икономическото състояние, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; когато обработването включва голям обем лични данни и засяга голям брой субекти на данни. Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск.

(39) Защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на настоящия регламент. За да може да докаже спазването на настоящия регламент, администраторът следва да приеме вътрешни политики и да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране. Такива мерки могат да се изразяват, *inter alia*, в свеждане до минимум на обработването на лични данни, псевдонимизиране на лични данни на възможно най-ранен етап, прозрачност по отношение на функциите и обработването на лични данни, създаване на възможност за субекта на данни да упражнява контрол върху обработването на данни, възможност за администратора да създава и подобрява елементите на сигурността. Принципите на защита на данните на етапа на проектирането и по подразбиране следва да се вземат предвид и в контекста на процедурите за възлагане на обществени поръчки.

(40) Защитата на правата и свободите на субектите на данни, както и отговорността и задълженията на администраторите и обработващите лични данни изискват ясно определяне на отговорностите съгласно настоящия регламент, включително когато администраторът определя целите и средствата на обработването съвместно с други администратори или когато дадена операция по обработване се извършва от името на даден администратор.

(41) За да се гарантира спазването на изискванията на настоящия регламент по отношение на обработването, извършвано от обработващия лични данни от

името на администратора, когато на обработващия се възлагат дейности по обработването, администраторът следва да използва само такива обработващи лични данни, които предоставят достатъчни гаранции, по-специално по отношение на експертни знания, надеждност и ресурси, че предприемат технически и организационни мерки, които отговарят на изискванията на настоящия регламент, включително на изискванията за сигурността на обработването. Придържането от страна на обработващите лични данни, различни от институциите и органите на Съюза, към одобрен кодекс на поведение или одобрен механизъм за сертифициране може да се използва като елемент за доказване, че са спазени задълженията на администратора. Извършването на обработването от обработващ лични данни следва да се урежда с договор или друг правен акт съгласно правото на Съюза или правото на държава членка, който обвързва обработващия лични данни с администратора, регламентира предмета и продължителността на обработването, естеството и целите на обработването, вида лични данни и категориите субекти на данни, като се вземат предвид конкретните задачи и отговорности на обработващия лични данни в контекста на обработването, което следва да се извърши, както и рискът за правата и свободите на субекта на данни. Администраторът и обработващият лични данни следва да могат да изберат да използват индивидуален договор или стандартни договорни клаузи, приети или пряко от Комисията, или от Европейския надзорен орган по защита на данните и впоследствие приети от Комисията. След приключване на обработването от името на администратора, обработващият личните данни следва, по избор на администратора, да ги върне или заличи, освен ако не е налице изискване за съхраняване на въпросните лични данни по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни.

(42) За да докажат спазването на настоящия регламент, както администраторите, така и обработващите лични данни следва да поддържат регистри на всички категории дейности по обработване, за които отговарят. Институциите и органите на Съюза следва да са длъжни да си сътрудничат с Европейския надзорен орган по защита на данните и да му предоставят своите регистри при поискване, за да могат да бъдат използвани за наблюдение на тези операции по обработване. Институциите и органите на Съюза следва да могат да създадат централен регистър на своите дейности по обработване на данни. От съображения за прозрачност те следва също така да могат да направят този регистър публичен.

(43) С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на настоящия регламент, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, имуществени или неимуществени вреди.

(44) Институциите и органите на Съюза следва да гарантират поверителността на електронните съобщения, предвидена в член 7 от Хартата. По-специално институциите и органите на Съюза следва да гарантират сигурността на своите електронни съобщителни мрежи, да защитават информацията, свързана с крайните устройства на крайните потребители, осъществяващи достъп до обществено достъпни уебсайтове и мобилни приложения в съответствие с Регламент (ЕС) XXXX/XX [нов Регламент за защитата на неприкосновеността на личния живот в сектора на електронните съобщения], и да защитават личните данни в указателите на потребителите.

(45) Нарушението на сигурността на личните данни може, ако по отношение на него не бъдат взети подходящи и своевременни мерки, да доведе до физически, имуществени или неимуществени вреди за физическите лица. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми Европейския надзорен орган по защита на данните за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа, след като е разбрал за него, освен ако администраторът е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и информацията може да се подаде поетапно без излишно допълнително забавяне. Когато такова забавяне е основателно, не толкова чувствителната или конкретна информация относно нарушението следва да бъде предоставена на възможно най-ранен етап, вместо преди уведомяването да се изчаква цялостно разрешаване на инцидента, който е в основата на нарушението.

(46) Администраторът следва да уведоми субекта на данни за нарушението на сигурността на личните данни без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице, за да му се даде възможност да предприеме необходимите предпазни мерки. В уведомлението следва да се посочва естеството на нарушението на сигурността на личните данни, както и да се дават препоръки на засегнатото физическо лице за това как да ограничи потенциалните неблагоприятни последици. Такива уведомления до субектите на данни следва да бъдат правени веднага щом това е разумно осъществимо и в тясно сътрудничество с Европейския надзорен орган по защита на данните, като се спазват насоките, предоставени от него или от други съответни органи, като например правоприлагащите органи.

(47) Регламент (ЕО) № 45/2001 предвижда общо задължение на администратора да уведоми за обработването на лични данни длъжностното лице по защита на данните, което, на свой ред, води регистър на операциите по обработване, за които е направено уведомление. Това задължение създава административна и финансова тежест и невинаги е допринасяло за подобряването на защитата на личните данни. Ето защо такива неправещи разграничения общи задължения за уведомяване следва да бъдат премахнати и заменени с ефективни процедури и механизми, които да са насочени към онези видове операции по обработване, които има вероятност да доведат до висок риск за правата и свободите на физическите лица поради своето естество, обхват, контекст и цели. Такива могат

да бъдат операциите по обработване, които по-конкретно включват използването на нови технологии или представляват нов вид технологии и при които преди това от администратора не е извършвана оценка на въздействието върху защитата на данните или които стават необходими предвид времето, изминало от първоначалното обработване. В такива случаи преди обработването администраторът следва да извърши оценка на въздействието върху защитата на данните, за да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Посочената оценка на въздействието следва да включва по-специално предвидените мерки, гаранции и механизми за ограничаване на този риск, с които се осигурява защитата на личните данни и се доказва спазването на настоящия регламент.

(48) Когато в оценката на въздействието върху защитата на данните е указано, че при липса на гаранции, мерки за сигурност и механизми за ограничаване на риска обработването би довело до висок риск за правата и свободите на физическите лица, и администраторът счита, че рискът не може да бъде ограничен с разумни средства от гледна точка на наличните технологии и разходи за прилагане, преди началото на дейностите по обработването следва да се осъществи консултация с Европейския надзорен орган по защита на данните. Има вероятност такъв висок риск да бъде породен от определени видове обработване и от степента и честотата на обработване, които могат да доведат и до нанасяне на вреди или до възпрепятстване на упражняването на правата и свободите на физическото лице. Европейският надзорен орган по защита на данните следва да отговори на искането за консултация в рамките на определен срок. Въпреки това, отсъствието на отговор от Европейския надзорен орган по защита на данните в рамките на този срок не следва да препятства евентуалната намеса на Европейския надзорен орган по защита на данните в съответствие със задълженията и правомощията му, установени в настоящия регламент, включително правомощието да забранява операции по обработване. Като част от този процес на консултации, следва да бъде възможно да се представи на Европейския надзорен орган по защита на данните резултатът от оценка на въздействието върху защитата на данните, извършена във връзка с въпросното обработване, и по-конкретно мерките, предвидени за ограничаване на възможните рискове за правата и свободите на физическите лица.

(49) Европейският надзорен орган по защита на данните следва да бъде информиран за административните мерки и вътрешните правила на институциите и органите на Съюза, които предвиждат обработването на лични данни, определят условия за ограничения на правата на субекта на данни или предоставят подходящи гаранции за правата на субекта на данни, за да се гарантира, че планираното обработване отговаря на изискванията на настоящия регламент, и по-специално за да се ограничат рисковете, свързани със субекта на данни.

(50) С Регламент (ЕС) 2016/679 бе създаден Европейският комитет по защита на данните като независим орган на Съюза, притежаващ правосубектност. Комитетът следва да допринася за съгласуваното прилагане на Регламент (ЕС) 2016/679 и Директива 2016/680 навсякъде в Съюза, включително като съветва Комисията. В същото време Европейският надзорен орган по защита на данните следва да продължи да упражнява своите надзорни и консултативни функции по отношение на всички институции и органи на Съюза, включително по своя

собствена инициатива или при поискване. С цел да се гарантира съгласуваност на правилата за защита на данните навсякъде в Съюза Комисията следва да извършва задължително консултация след приемането на законодателни актове или при подготовката на делегирани актове и актове за изпълнение, определени в членове 289, 290 и 291 от ДФЕС, и след приемането на препоръки и предложения, свързани със споразумения с трети държави и международни организации, предвидени в член 218 от Договора за функционирането на Европейския съюз, които имат въздействие върху правото на защита на личните данни. В тези случаи Комисията следва да бъде задължена да се консултира с Европейския надзорен орган по защита на данните, с изключение на случаите, когато Регламент (ЕС) 2016/679 предвижда задължителна консултация с Европейския комитет по защита на данните, например във връзка с решения относно адекватното ниво на защита или делегирани актовете относно стандартизирани икони и изисквания за механизмите за сертифициране. Когато въпросният акт има особено значение за защитата на правата и свободите на физическите лица по отношение на обработването на лични данни, Комисията следва да може също така да се консултира с Европейския комитет по защита на данните. В тези случаи Европейският надзорен орган по защита на данните следва, като член на Европейския комитет по защита на данните, да координира работата си с него с оглед на изготвянето на съвместно становище. Европейският надзорен орган по защита на данните и когато е приложимо, Европейският комитет по защита на данните следва да представят писменото си становище в срок от осем седмици. Този срок следва да бъде намален за спешни случаи и когато това е уместно, например когато Комисията подготвя делегирани актове и актове за изпълнение.

(51) Във всяка институция или орган на Съюза трябва да има длъжностно лице по защита на данните, което да гарантира прилагането на разпоредбите на настоящия регламент и да съветва администраторите и обработващите лични данни по изпълнението на техните задължения. Длъжностното лице по защита на данните следва да бъде лице с експертни познания в областта на правото и практиките за защита на данните, което следва да се определя по-специално в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за личните данни, обработвани от администратора или обработващия лични данни. Тези длъжностни лица по защита на данните следва да са в състояние да изпълняват своите задължения и задачи по независим начин.

(52) Когато лични данни се предават от институциите или органите на Съюза на администратори, обработващи лични данни или други получатели в трети държави или на международни организации, нивото на защита на физическите лица, гарантирано в Съюза с настоящия регламент, не следва да бъде излагано на риск, включително в случаите на последващо предаване на лични данни от третата държава или международната организация на администратори или обработващи лични данни в същата или друга трета държава или международна организация. Във всеки случай предаването на данни на трети държави и международни организации може да се извършва единствено в пълно съответствие с настоящия регламент. Предаването може да се извършва само ако администраторът или обработващият лични данни изпълняват условията, установени в разпоредбите на настоящия регламент, относно предаването на

лични данни на трети държави или международни организации, при спазване на другите разпоредби на настоящия регламент.

(53) Комисията може също така да реши в съответствие с член 45 от Регламент (ЕС) 2016/679, че дадена трета държава, територия или конкретен сектор в трета държава, или дадена международна организация предоставя адекватно ниво на защита на данните. В тези случаи предаването на лични данни на такава трета държава или международна организация от институция или орган на Съюза може да се извършва, без да е необходимо допълнително разрешение.

(54) При липсата на решение относно адекватното ниво на защита администраторът или обработващият лични данни следва да предприеме мерки, за да компенсира липсата на защита на данни в дадена трета държава чрез подходящи гаранции за субекта на данните. Тези подходящи гаранции може да се състоят от стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от Европейския надзорен орган по защита на данните, или договорни клаузи, разрешени от Европейския надзорен орган по защита на данните. Когато обработващият лични данни не е институция или орган на Съюза, тези подходящи гаранции може също така да се състоят от задължителни фирмени правила, кодекси за поведение и механизми за сертифициране, използвани за международното предаване на данни по силата на Регламент (ЕС) 2016/679. Тези гаранции следва да осигуряват спазването на изискванията относно защитата на данните и на правата на субектите на данни, подходящи при обработване в рамките на Съюза, включително наличието на приложими права на субектите на данни и на ефективни средства за правна защита, включително с цел получаване на ефективна административна или съдебна защита и предявяване на искове за обезщетение в Съюза или в трета държава. Те следва да се отнасят по-специално до спазването на общите принципи, свързани с обработването на лични данни, и до принципите за защита на данните на етапа на проектирането и по подразбиране. Данни може да се предават и от институциите или органите на Съюза на публични органи или организации в трети държави или на международни организации със съответните задължения или функции, включително въз основа на разпоредбите, които ще бъдат включени в административните договорености, като например меморандум за разбирателство, с които да се предоставят приложими и ефективни права за субектите на данни. Когато гаранциите са предвидени в административни договорености, които нямат задължителен характер, следва да се получи разрешение от Европейския надзорен орган по защита на данните.

(55) Възможността администраторът или обработващият лични данни да използва стандартни клаузи за защита на данните, приети от Комисията или от Европейския надзорен орган по защита на данните, не следва да възпрепятства администраторите или обработващите лични данни да включат стандартни клаузи за защита на данните в договор с по-голям обхват, като договор между обработващия лични данни и друг обработващ лични данни, нито да добавят други клаузи или допълнителни гаранции, при условие че същите не противоречат пряко или косвено на стандартните договорни клаузи, приети от Комисията или от Европейския надзорен орган по защита на данните, нито засягат основните права или свободи на субектите на данни. Администраторите и обработващите лични данни следва да бъдат насърчавани да предоставят

допълнителни гаранции чрез договорни ангажименти, които допълват стандартните клаузи за защита на данните.

(56) Някои трети държави приемат закони, подзаконови и други правни актове, които имат за цел пряко да регулират дейностите по обработване на данни от страна на институциите или органите на Съюза. Това може да включва решения на съдилища или трибунали или решения на административни органи в трети държави, с които от администратора или обработващия лични данни се изисква да предаде или да разкрие лични данни и които не се основават на международно споразумение, което е в сила между третата държава, отправила искането, и Съюза. Извънтериториалното прилагане на тези закони, подзаконови и други правни актове може да бъде в нарушение на международното право и да възпрепятства осигуряването на защитата на физическите лица, гарантирана в Съюза с настоящия регламент. Предаването на данни следва е разрешено само когато са изпълнени условията на настоящия регламент относно предаването на данни на трети държави. Такъв може да бъде случаят, *inter alia*, когато разкриването е необходимо поради важно съображение от обществен интерес, признато в правото на Съюза.

(57) Следва да се предвиди възможността в особени случаи да се предават данни при определени обстоятелства, когато субектът на данните е дал изричното си съгласие, когато предаването засяга отделни случаи и е необходимо във връзка с договор или правна претенция, независимо от това дали е в рамките на съдебна, административна или друга извънсъдебна процедура, включително процедура пред регулаторни органи. Следва да се предвиди и възможността да се предават данни, когато това се налага поради важни съображения от обществен интерес, предвидени в правото на Съюза, или когато предаването се извършва от регистър, създаден със закон и предназначен за справки от обществеността или от лица, които имат законен интерес. В този случай, освен ако това е разрешено от правото на Съюза, предаването не следва да включва всички лични данни или цели категории данни, съдържащи се в регистъра, а когато регистърът е предназначен за справка от лица, които имат законен интерес, предаването следва да се извършва единствено по искане на тези лица или ако те са получателите, като се вземат изцяло под внимание интересите и основните права на субекта на данните.

(58) Тези дерогации следва да се прилагат по-специално за предаването на данни, което се изисква и е необходимо по важни причини от обществен интерес, например при международен обмен на данни между институциите и органите на Съюза и органи по защита на конкуренцията, данъчни или митнически власти, органи за финансов надзор и служби, компетентни по въпросите на социалната сигурност или общественото здраве, например в случай на проследяване на контакти при заразни болести или с цел намаляване и/или премахване на употребата на допинг в спорта. Предаването на лични данни следва също да се разглежда като законосъобразно, когато е необходимо за защитата на интерес от съществено значение за жизненоважни интереси на субекта на данни или на друго лице, включително физическата неприкосновеност или живота, ако субектът на данните не е в състояние да даде съгласие. При липсата на решение относно адекватното ниво на защита правото на Съюза може по важни причини от обществен интерес изрично да определи ограничения за предаването на специални категории от данни на трета държава или международна организация.

Всяко предаване на международна хуманитарна организация на лични данни на субект на данни, който е физически или юридически неспособен да даде своето съгласие, с оглед на изпълнението на задължение по силата на Женевските конвенции или прилагането на международното хуманитарно право, приложимо в условията на военни конфликти, може да се счита за необходимо поради важна причина от обществен интерес или защото е от жизненоважен интерес за субекта на данни.

(59) Във всеки случай, когато Комисията не е взела решение относно адекватното ниво на защита на данните в трета държава, администраторът или обработващият данни следва да използва решения, които предоставят приложими и ефективни права на субектите на данни по отношение на обработването на техните данни в Съюза след предаването на тези данни, така че те да продължат да се ползват от основните права и гаранциите.

(60) Трансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, по-специално да се защитят срещу неправомерна употреба или разкриване на тези данни. В същото време надзорните органи в Съюза, включително Европейският надзорен орган по защита на данните, могат да бъдат изправени пред невъзможността да разглеждат жалби или да провеждат разследвания, свързани с дейности, извършвани извън тяхната юрисдикция. Техните усилия за сътрудничество в трансграничния контекст могат да бъдат възпрепятствани и от недостатъчни правомощия за предотвратяване или защита, различаващи се правни режими, както и от практически пречки като ограничения на ресурсите. Поради това по-тясното сътрудничество между Европейския надзорен орган по защита на данните и други надзорни органи по защита на данните следва да бъде насърчавано, за им се помогне да обменят информация със своите международни партньори.

(61) Създаването с Регламент (ЕО) № 45/2001 на Европейския надзорен орган по защита на данните, оправомощен да изпълнява своите задачи и упражнява своите правомощия при пълна независимост, е първостепенен елемент от защитата на физическите лица във връзка с обработването на личните им данни. Настоящият регламент следва допълнително да укрепи и да изясни неговите роля и независимост.

(62) За да се гарантира съгласувано наблюдение и прилагане на правилата за защита на данните навсякъде в Съюза, Европейският надзорен орган по защита на данните следва да има еднакви задачи и ефективни правомощия с надзорните органи в държавите членки, включително правомощия за разследване, корективни правомощия и правомощия за налагане на санкции, правомощия за даване на разрешения и становища, особено в случаи на жалби от физически лица, и правомощието да довежда нарушенията на настоящия регламент до знанието на Съда на Европейския съюз и да участва в съдебни производства в съответствие с първичното право. Тези правомощия следва да включват и правомощието за налагане на временно или окончателно ограничаване, включително забрана, на обработването на данни. С цел избягване на излишни разходи и прекалени неудобства за лицата, които могат да бъдат засегнати по неблагоприятен начин, всяка мярка на Европейския надзорен орган по защита на данните следва да бъде подходяща, необходима и пропорционална с оглед на

осигуряването на съответствие с настоящия регламент, като се отчитат обстоятелствата при всеки конкретен случай и се зачита правото на всяко лице да бъде изслушано, преди да бъде взета каквато и да е конкретна мярка. Всяка мярка със задължителен характер на Европейския надзорен орган по защита на данните следва да бъде в писмен вид, да бъде ясна и недвусмислена, да посочва датата на издаване на мярката, да е подписана от Европейския надзорен орган по защита на данните, да посочва основанията за мярката и да се позовава на правото на ефективни правни средства за защита.

(63) Решенията на Европейския надзорен орган по защита на данните относно изключенията, гаранциите, разрешенията и условията във връзка с операциите по обработване на данни, както са определени в настоящия регламент, следва да се публикуват в доклад за дейността. Независимо от публикуването на годишен доклад за дейността, Европейският надзорен орган по защита на данните може да публикува доклади по конкретни теми.

(64) Националните надзорни органи наблюдават прилагането на Регламент (ЕС) 2016/679 и допринасят за неговото съгласувано прилагане навсякъде в Съюза с цел защита на физическите лица по отношение на обработването на личните им данни и улесняване на свободното движение на личните данни в рамките на вътрешния пазар. С цел да се повиши съгласуваността при прилагане на правилата за защита на данните, приложими в държавите членки, и на правилата за защита на данните, приложими за институциите и органите на Съюза, Европейският надзорен орган по защита на данните следва да си сътрудничи ефективно с националните надзорни органи.

(65) В някои случаи правото на Съюза предвижда модел на споделен между Европейския надзорен орган по защита на данните и националните надзорни органи координиран надзор. Освен това Европейският надзорен орган по защита на данните е надзорният орган на Европол, а посредством съвет за сътрудничеството, който има консултативни функции, е създаден конкретен модел на сътрудничество с националните надзорни органи. С цел подобряване на ефективния надзор и прилагане на материалните правила за защита на данните, в Съюза следва да бъде въведен единен, съгласуван модел на координиран надзор. Поради това Комисията следва, когато е уместно, да представи законодателни предложения за изменение на правните актове на Съюза, които предвиждат модел на координиран надзор, за да се приведат в съответствие с модела за координиран надзор от настоящия регламент. Европейският комитет по защита на данните следва да служи като единен форум за гарантиране на ефективния координиран надзор във всички области.

(66) Всеки субект на данни следва да има право да подаде жалба до Европейския надзорен орган по защита на данните, както и право на ефективни правни средства за защита пред Съда на Европейския съюз в съответствие с Договорите, ако счита, че правата му по настоящия регламент са нарушени или ако Европейският надзорен орган по защита на данните не предприема действия по подадена жалба, изцяло или частично отхвърля или оставя без разглеждане жалба или не предприема действия, когато такива са необходими, за да се защитят правата на субекта на данни. Разследването въз основа на жалби следва да подлежи на съдебен контрол и да се извършва в целесъобразна за конкретния случай степен. Европейският надзорен орган по защита на данните следва да

информира субекта на данните за напредъка и резултата от жалбата в разумен срок. Ако случаят изисква допълнително координиране с национален надзорен орган, на субекта на данните следва да бъде предоставена междинна информация. За да се улесни подаването на жалбите, Европейският надзорен орган по защита на данните следва да вземе мерки, като например осигуряване на формуляр за подаване на жалби, който да може да бъде попълнен и по електронен път, без да се изключват други средства за комуникация.

(67) Всяко лице, което е претърпяло имуществени или неимуществени вреди в резултат на нарушение на настоящия регламент, следва да има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди при спазване на условията, предвидени в Договорите.

(68) С цел да се укрепи надзорната роля на Европейския надзорен орган по защита на данните и ефективното прилагане на настоящия регламент Европейският надзорен орган по защита на данните следва да има правомощието да налага като санкция в краен случай административнонаказателни имуществени санкции. Те следва да имат за цел санкционирането на институцията или органа, а не на физически лица, за неспазване на настоящия регламент, възпирането на бъдещи нарушения на настоящия регламент, както и насърчаването на култура на защита на личните данни в рамките на институциите и органите на Съюза. В настоящия регламент следва да се посочат нарушенията, както и горните граници и критериите за определяне на съответните административнонаказателни имуществени санкции. Европейският надзорен орган по защита на данните следва да определи размера на съответните административнонаказателни имуществени санкции във всеки отделен случай, като взема предвид всички обстоятелства, свързани с конкретната ситуация, по-специално при надлежно отчитане на естеството, тежестта и продължителността на нарушението и на последиците от него, както и на мерките, предприети, за да се гарантира спазване на задълженията по настоящия регламент и за да се предотвратят или смекчат последиците от нарушението. При налагането на административнонаказателна имуществена санкция на орган на Съюза Европейския надзорен орган по защита на данните следва да прецени пропорционалността на размера на имуществената санкция. Административното производство за налагането на имуществени санкции на институции и органи на Съюза следва да зачита общите принципи на правото на Съюза, както се тълкуват от Съда на Европейския съюз.

(69) Когато субектът на данни смята, че правата му по настоящия регламент са нарушени, той следва да има право да възложи на структура, организация или сдружение с нестопанска цел, което е учредено съгласно правото на Съюза или правото на държава членка, има уставни цели, които са в обществен интерес, и работи в областта на защитата на личните данни, да подаде жалба от негово име до Европейския надзорен орган по защита на данните. Тази структура, организация или сдружение следва също така да може да упражнява правото на съдебна защита от името на субектите на данни или да упражнява правото да получи обезщетение от името на субектите на данни.

(70) Длъжностно лице или друг служител на Съюза, който не спазва задълженията, предвидени в настоящия регламент, подлежи на дисциплинарна или друга мярка в съответствие с правилата и процедурите, установени в Правилника за

длъжностните лица на Европейския съюз или Условията за работа на другите служители на Европейския съюз.

(71) За да се гарантират еднакви условия за прилагането на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия, когато това е предвидено в регламента. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) №182/2011 на Европейския парламент и на Съвета[16]. За приемането на стандартните договорни клаузи между администратори и обработващи лични данни и между обработващи лични данни, за приемането на списък на операциите по обработване, за които е необходима предварителна консултация с Европейския надзорен орган по защита на данните за обработване, извършвано от администраторите на данни при изпълнението на задача от обществен интерес и за приемането на стандартни договорни клаузи, предвиждащи подходящи гаранции за международно предаване на данни, следва да бъде използвана процедурата по разглеждане.

(72) Поверителната информация, която статистическите органи на национално равнище и на равнището на Съюза събират за изготвянето на официална европейска и официална национална статистика, следва да бъде защитена. Европейската статистика следва да се разработва, изготвя и разпространява в съответствие със статистическите принципи, установени в член 338, параграф 2 от ДФЕС. Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета[17] конкретизира допълнително изискванията относно поверителността на данните на европейската статистика.

(73) Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО следва да бъдат отменени. Позоваванията на отменения регламент и на отменените решение следва да се считат за позовавания на настоящия регламент.

(74) За да се гарантира пълната независимост на членовете на независимия надзорен орган, мандатите на настоящия Европейски надзорен орган по защита на данните и неговия заместник следва да не бъдат засегнати от настоящия регламент. Настоящият заместник следва да продължи да изпълнява мандата си до неговото изтичане освен ако е изпълнено някое от условията за преждевременно прекратяване на мандата на Европейския надзорен орган по защита на данните, определени в настоящия регламент. До края на мандата на заместника спрямо него следва да се прилагат съответните разпоредби на настоящия регламент.

---

16 Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите-членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

17 Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета от 11 март 2009 г. относно европейската статистика и за отмяна на Регламент (ЕО, Евратом) № 1101/2008 за предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности, на Регламент (ЕО) № 322/97 на Съвета относно статистиката на Общността и на Решение 89/382/ЕИО, Евратом на Съвета за създаване на Статистически програмен комитет на Европейските общности (ОВ L 87, 31.3.2009 г., стр. 164).

(75) В съответствие с принципа на пропорционалност е необходимо и подходящо за постигането на основната цел за осигуряване на еквивалентно ниво на защита на физическите лица и свободното движение на лични данни навсякъде в Съюза да бъдат установени правила относно обработването на лични данни в институциите и органите на Съюза. С настоящия регламент не се надхвърля необходимото за постигането на поставените цели в съответствие с член 5, параграф 4 от Договора за Европейския съюз.

(76) В съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001 беше проведена консултация с Европейския надзорен орган по защита на данните, който представи становище на XX/XX/XXXX.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1
Предмет и цели

1. С настоящия регламент се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза, както и правилата по отношение на свободното движение на лични данни между самите тях или до получатели, установени в Съюза и попадащи в обхвата на разпоредбите на Регламент (ЕС) 2016/679[18] или на разпоредбите на националното право, приети съгласно Директива (ЕС) 2016/680[19].

2. С настоящия регламент се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

3. Европейският надзорен орган по защита на данните („ЕНОЗД“) следи за прилагането на разпоредбите на настоящия регламент по отношение на всички операции по обработване на лични данни, извършвани от институция или орган на Съюза.

---

[18] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

[19] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

Член 2
Обхват

1. Настоящият регламент се прилага за обработването на лични данни от всички институции и органи на Съюза дотолкова, доколкото това обработване се извършва при упражняване на дейности, които попадат изцяло или частично в обхвата на правото на Съюза.

2. Настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматизирани средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.

Член 3
Определения

1. За целите на настоящия регламент се прилагат следните определения:

   а) определенията, съдържащи се в Регламент (ЕС) 2016/679, с изключение на определението на „администратор“ в член 4, параграф 7 от посочения регламент;

   б) определението на „електронно съобщение“ в член 4, параграф 2, буква а) от Регламент (ЕС) № XX/XXXX [Регламент за защитата на неприкосновеността на личния живот в сектора на електронните съобщения];

   в) определенията на „електронна съобщителна мрежа“ и „краен потребител“ в член 2, параграфи 1 и14 от Директива № 00/0000/ЕС [Директива за създаване на Европейски кодекс за електронните съобщения];

   г) определението на „крайно устройство“ в член 1, параграф 1 от Директива 2008/63/ЕО[20] на Комисията.

2. За целите на настоящия регламент се прилагат и следните определения:

   а) „институции и органи на Съюза“ означава институциите, органите, службите и агенциите на Съюза, създадени с Договора за Европейския съюз, Договора за функционирането на Европейския съюз или Договора за Евратом или въз основа на тези договори;

   б) „администратор“ означава институцията, органа, службата или агенцията на Съюза или генералната дирекция, или всяка друга организационна структура, която самостоятелно или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за обработването са определени със специален акт на Съюза,

[20] Директива 2008/63/ЕО на Комисията от 20 юни 2008 г. относно конкуренцията на пазарите на крайни далекосъобщителни устройства (ОВ L 162, 21.6.2008 г., стр. 20).

администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза;

в) „потребител“ означава всяко физическо лице, използващо мрежа или крайно устройство, експлоатирани под контрола на институция или орган на Съюза;

г) „указател“ означава обществено достъпен указател на потребителите или вътрешен указател на потребителите, който е наличен в институция или орган на Съюза или е споделен между институциите и органите на Съюза, независимо дали е на хартиен носител, или в електронна форма.

ГЛАВА II

ПРИНЦИПИ

Член 4
Принципи, свързани с обработването на лични данни

1. Личните данни трябва да бъдат:

а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

б) събирани за конкретни, изрично указани и законни цели и да не се обработват по-нататък по начин, който е несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 13, за несъвместимо с първоначалните цели („ограничение на целите“);

в) адекватни, релевантни и не надхвърлят необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни или непълни лични данни, като се имат предвид целите, за които те се обработват („точност“);

д) съхранявани във вид, който позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 13, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

2. Администраторът носи отговорност за спазването на параграф 1 и трябва да е в състояние да го докаже („отчетност“).

Член 5
Законосъобразност на обработването

1. Обработването е законосъобразно само ако и доколкото е приложимо поне едно от следните условия:

а) обработването е необходимо за изпълнението на задача от обществен интерес въз основа или при упражняването на официални правомощия, които са предоставени на институцията или органа на Съюза;

б) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

в) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

г) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

д) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице.

2. Задачите, посочени в параграф 1, буква а) се определят в правото на Съюза.

Член 6
Обработване за друга съвместима цел

Когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на съгласието на субекта на данните или на правото на Съюза, което представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по член 25, параграф 1, администраторът, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, *inter alia*, взема под внимание:

а) всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;

б) контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и администратора;

в) естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно член 10, или се обработват лични данни, отнасящи се до присъди и престъпления, съгласно член 11;

г) възможните последствия от предвиденото по-нататъшно обработване за субектите на данните;

д) наличието на подходящи гаранции, които могат да включват криптиране или псевдонимизация.

Член 7
Условия за даване на съгласие

1. Когато обработването се извършва въз основа на съгласие, администраторът трябва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни.

2. Ако съгласието на субекта на данните е дадено в рамките на писмена декларация, която се отнася и до други въпроси, искането за съгласие се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като използва ясен и прост език. Никоя част от такава декларация, която представлява нарушение на настоящия регламент не е обвързваща.

3. Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това. Оттеглянето на съгласие е също толкова лесно, колкото и даването му.

4. Когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали, *inter alia*, изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор.

Член 8
Условия, приложими за съгласието на деца във връзка с услугите на информационното общество

1. Когато се прилага член 5, параграф 1, буква г) във връзка с прякото предлагане на услуги на информационното общество на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 13 години. Ако детето е под 13 години, това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

2. В такива случаи администраторът полага разумни усилия за удостоверяване, че съгласието е дадено или разрешено от носещия родителска отговорност за детето, като взема предвид наличната технология.

3. Параграф 1 не засяга общото договорно право на държавите членки като разпоредбите относно действителността, сключването или последиците от даден договор по отношение на дете.

Член 9

Предаване на лични данни на получатели, които са различни от институции и органи на Съюза, установени са в Съюза и попадат в обхвата на Регламент (ЕС) 2016/679 или Директива (ЕС) 2016/680

1. Без да се засягат разпоредбите на членове 4, 5, 6 и 10, лични данни се предават на получатели, установени в Съюза и попадащи в обхвата на Регламент (ЕС) 2016/679 или на националното законодателство, прието съгласно Директива (ЕС) 2016/680, ако получателят докаже, че:

   а) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия; или

   б) е необходимо данните да бъдат предадени, предаването е пропорционално на целите си и няма основания да се предполага, че правата и свободите, както и законните интереси на субекта на данните могат да бъдат накърнени.

2. Когато предаването по силата на настоящия член се осъществява по инициатива на администратора, администраторът доказва, че предаването на лични данни е необходимо и пропорционално за целите на предаването, като прилага критериите, определени в параграф 1, буква а) или буква б).

Член 10

Обработване на специални категории лични данни

1. Забранява се обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в професионални съюзи, както и обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравето или сексуалния живот и сексуалната ориентация на лицето.

2. Параграф 1 не се прилага, ако е налице едно от следните условия:

   а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на Съюза се предвижда, че посочената в параграф 1 забрана не може да бъде отменена от субекта на данни;

   б) обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила дотолкова, доколкото това е разрешено от правото на Съюза, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните; или

в) обработването е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данните или на друго лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването се извършва в хода на законно упражняваните дейности и при подходящи мерки за защита от орган с нестопанска цел, който представлява интегрирана в дадена институция или орган на Съюза структура, както и се извършва с политическа, философска, религиозна или професъюзна цел и при условие че обработването касае единствено членове или бивши членове на този орган или лица, които редовно контактуват с него във връзка с неговите цели, и че данните не се разкриват пред трета страна без съгласието на субектите на данните;

д) обработването е свързано с данни, които явно са направени обществено достояние от субекта на данните;

е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато Съдът на Европейския съюз действа в качеството си на правораздаващ орган; или

ж) обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

з) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинска диагноза, осигуряването на здравни или социални грижи или лечение или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза или съгласно договор с медицинско лице и при условията и гаранциите, посочени в параграф 3;

и) обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, въз основа на правото на Съюза, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна;

й) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели на основание правото на Съюза, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

3. Личните данни, посочени в параграф 1, могат да бъдат обработвани за целите, посочени в параграф 2, буква з), когато въпросните данни се обработват от или

под ръководството на професионален работник, обвързан от задължението за професионална тайна по силата на правото на Съюза.

Член 11
Обработване на лични данни, свързани с присъди и престъпления

Обработването на лични данни, свързани с присъди и престъпления или със свързаните с тях мерки за сигурност, въз основа на член 5, параграф 1 може да се извършва само когато е разрешено от правото на Съюза, в което може да са включени вътрешни правила, предвиждащо подходящи гаранции за правата и свободите на субектите на данни.

Член 12
Обработване, за което не се изисква идентифициране

1. Ако целите, за които администратор обработва лични данни, не изискват или вече не изискват идентифициране на субекта на данните от администратора, администраторът не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данни с единствената цел да бъде спазен настоящият регламент.

2. Когато в случаи, посочени в параграф 1 от настоящия член, администраторът може да докаже, че не е в състояние да идентифицира субекта на данни, администраторът уведомява съответно субекта на данни, ако това е възможно. В такива случаи членове 17—22 не се прилагат, освен когато субектът на данни, с цел да упражни правата си по тези членове, предостави допълнителна информация, позволяваща неговото идентифициране.

Член 13
Гаранции, свързани с обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели

Обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели подлежи в съответствие с настоящия регламент на подходящи гаранции за правата и свободите на субекта на данни. Тези гаранции осигуряват наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа на свеждане на данните до минимум. Мерките могат да включват псевдонимизация, при условие че посочените цели могат да бъдат постигнати по този начин. Когато посочените цели могат да бъдат постигнати чрез по-нататъшно обработване, което не позволява или повече не позволява идентифицирането на субектите на данни, целите се постигат по този начин.

ГЛАВА III

ПРАВА НА СУБЕКТА НА ДАННИ

РАЗДЕЛ 1

ПРОЗРАЧНОСТ И УСЛОВИЯ

Член 14
Прозрачна информация, комуникация и условия за упражняването на правата на субекта на данни

1. Администраторът предприема необходимите мерки за предоставяне на всякаква информация по членове 15 и 16 и на всякаква комуникация по членове 17—24 и член 38, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства.

2. Администраторът съдейства за упражняването на правата на субекта на данните по членове 17—24. В случаите, посочени в член 12, параграф 2, администраторът не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му по членове 17—24, освен ако докаже, че не е в състояние да идентифицира субекта на данните.

3. Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с искане по членове 17—24, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се вземат предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

4. Ако администраторът не предприеме действия по искането на субекта на данни, администраторът уведомява субекта на данни без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до Европейския надзорен орган по защита на данните и търсене на защита по съдебен ред.

5. Информацията по членове 15 и 16 и всяка комуникация и действия по членове 17—24 и член 38 се предоставят безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да откаже да предприеме действия по искането.

Администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

6. Без да се засягат разпоредбите на член 12, когато администраторът има основателни съмнения във връзка със самоличността на физическото лице, което подава искане по членове 17—23, той може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

7. Информацията, която трябва да се предостави на субектите на данни съгласно членове 15 и 16, може да бъде предоставена в комбинация със стандартизирани икони, чрез което по лесно видим, разбираем и ясно четим начин да се представи смислен преглед на планираното обработване. Ако иконите се представят в електронен вид, те трябва да бъдат машинночитаеми.

8. Ако Комисията приеме съгласно член 12, параграф 8 от Регламент (ЕС) 2016/679 делегирани актове за определяне на информацията, която трябва да бъде представена под формата на икони, и на процедурите за предоставяне на стандартизирани икони, институциите и органите на Съюза предоставят, когато е уместно, в комбинация с тези стандартизирани икони информацията по членове 15 и 16.

РАЗДЕЛ 2

ИНФОРМАЦИЯ И ДОСТЪП ДО ЛИЧНИ ДАННИ

Член 15

Информация, предоставяна при събиране на лични данни от субекта на данните

1. Когато лични данни, свързани с даден субект на данни, се събират от субекта на данните, в момента на получаване на личните данни администраторът предоставя на субекта на данните цялата посочена по-долу информация:

   а) самоличността и координатите за връзка на администратора;

   б) координатите за връзка на длъжностното лице по защита на данните;

   в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

   г) получателите или категориите получатели на личните данни, ако има такива;

д) когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 49 позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

2. Освен информацията, посочена в параграф 1, в момента на получаване на личните данни администраторът предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

б) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или когато е приложимо, право да се направи възражение срещу обработването или правото на преносимост на данните;

в) когато обработването се основава на член 5, параграф 1, буква г) или член 10, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

г) правото на подаване на жалба пред Европейския надзорен орган по защита на данните;

д) дали предоставянето на лични данни е законоустановено или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и какви са евентуалните последствия, ако тези данни не бъдат предоставени;

е) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

3. Когато администраторът възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в параграф 2.

4. Параграфи 1, 2 и 3 не се прилагат, когато и доколкото субектът на данните вече разполага с информацията.

Член 16

Информация, предоставяна, когато личните данни не са получени от субекта на данните

1. Когато личните данни не са получени от субекта на данните, администраторът предоставя на субекта на данните следната информация:

   а) самоличността и координатите за връзка на администратора;

   б) координатите за връзка на длъжностното лице по защита на данните;

   в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

   г) съответните категории лични данни;

   д) получателите или категориите получатели на личните данни, ако има такива;

   е) когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 49 позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

2. Освен информацията, посочена в параграф 1, администраторът предоставя на субекта на данните следната допълнителна информация, необходима за осигуряване на добросъвестно и прозрачно обработване на данните по отношение на субекта на данните:

   а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

   б) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или когато е приложимо, право да се направи възражение срещу обработването или правото на преносимост на данните;

   в) когато обработването се основава на член 5, параграф 1, буква г) или член 10, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

   г) правото на подаване на жалба пред Европейския надзорен орган по защита на данните;

   д) източника на личните данни и ако е приложимо, дали данните са от обществено достъпен източник;

е) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

3. Администраторът предоставя информацията, посочена в параграфи 1 и 2:

а) в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;

б) ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или

в) ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

4. Когато администраторът възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са придобити, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в параграф 2.

5. Параграфи 1—4 не се прилагат, когато и доколкото:

а) субектът на данните вече разполага с информацията;

б) предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия; по-специално за обработване на данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели или доколкото съществува вероятност задължението, посочено в параграф 1 от настоящия член, да направи невъзможно или сериозно да затрудни постигането на целите на това обработване;

в) получаването или разкриването е изрично установено от правото на Съюза; или

г) личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, което се урежда от правото на Съюза.

Член 17
Право на достъп на субекта на данните

1. Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

а) целите на обработването;

б) съответните категории лични данни;

в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

е) правото на подаване на жалба до Европейския надзорен орган по защита на данните;

ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

з) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

2. Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции по член 49 във връзка с предаването.

3. Администраторът предоставя копие от личните данни, които са в процес на обработване. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго.

4. Правото на получаване на копие, посочено в параграф 3, не влияе неблагоприятно върху правата и свободите на други лица.

РАЗДЕЛ 3

КОРИГИРАНЕ И ИЗТРИВАНЕ

Член 18
Право на коригиране

Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването, субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация.

Член 19
Право на изтриване (право „да бъдеш забравен“)

1. Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

   а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

   б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните съгласно член 5, параграф 1, буква г) или член 10, параграф 2, буква а), и няма друго правно основание за обработването;

   в) субектът на данните възразява срещу обработването съгласно член 23, параграф 1 и няма законни основания за обработването, които да имат преимущество;

   г) личните данни са били обработвани незаконосъобразно;

   д) личните данни трябва да бъдат изтрити с цел спазването на правно задължение, което се прилага спрямо администратора;

   е) личните данни са били събрани във връзка с предлагането на услуги на информационното общество по член 8, параграф 1.

2. Когато администраторът е направил личните данни обществено достояние и е задължен съгласно параграф 1 да изтрие личните данни, той, като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

3. Параграфи 1 и 2 не се прилагат, доколкото обработването е необходимо:

   а) за упражняване на правото на свобода на изразяването и правото на информация;

   б) за спазване на правно задължение, което се прилага спрямо администратора, или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора;

   в) по причини от обществен интерес в областта на общественото здраве в съответствие с член 10, параграф 2, букви з) и и), както и член 10, параграф 3;

   г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото

съществува вероятност правото, посочено в параграф 1, да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или

д) за установяването, упражняването или защитата на правни претенции.

Член 20
Право на ограничаване на обработването

1. Субектът на данните има право да изиска от администратора ограничаване на обработването, когато е налице едно от следните условия:

а) точността на личните данни се оспорва от субекта на данните за срок, който позволява на администратора да провери точността, включително пълнотата, на личните данни;

б) обработването им е неправомерно, но субектът на данните не желае те да бъдат заличени, а изисква вместо това ограничаване на използването им;

в) администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

г) субектът на данните е възразил срещу обработването съгласно член 23, параграф 1 в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

2. Когато обработването е ограничено съгласно параграф 1, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции, или за защита на правата на друго физическо или юридическо лице или поради важни причини от обществен интерес за Съюза или държава членка.

3. Когато субект на данните е изискал ограничаване на обработването съгласно параграф 1, администраторът го информира преди отмяната на ограничаването на обработването.

4. В автоматизираните регистри с лични данни ограничаването на обработването по принцип се осигурява с технически средства. Фактът, че обработването на личните данни е ограничено, се указва в регистъра по начин, който ясно показва, че личните данни не могат да се ползват.

Член 21
Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването

Администраторът съобщава за всяко извършено в съответствие с член 18, член 19, параграф 1 и член 20 коригиране, изтриване или ограничаване на обработване на всеки

получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Член 22
Право на преносимост на данните

1. Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато:

   а) обработването е основано на съгласие в съответствие с член 5, параграф 1, буква г) или член 10, параграф 2, буква а) или на договор съгласно член 5, параграф 1, буква в); и

   б) обработването се извършва по автоматизиран начин.

2. Когато упражнява правото си на преносимост на данните по параграф 1, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

3. Упражняването на правото, посочено в параграф 1 от настоящия член, не засяга член 19. Посоченото право не се отнася до обработването, необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

4. Правото, посочено в параграф 1, не влияе неблагоприятно върху правата и свободите на други лица.

РАЗДЕЛ 4

ПРАВО НА ВЪЗРАЖЕНИЕ И АВТОМАТИЗИРАНО ВЗЕМАНЕ НА ИНДИВИДУАЛНИ РЕШЕНИЯ

Член 23
Право на възражение

1. Субектът на данните има право по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на член 5, параграф 1, буква а), включително профилиране, основаващо се на посочената разпоредба. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

2. Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото по параграф 1, което му се представя по ясен начин и отделно от всяка друга информация.

3. Без да се засягат разпоредбите на членове 34 и 35, в контекста на използването на услугите на информационното общество субектът на данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

4. Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от обществен интерес.

Член 24

Автоматизирано вземане на индивидуални решения, включително профилиране

1. Субектът на данните има право да не бъде адресат на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за него или по подобен начин го засяга в значителна степен.

2. Параграф 1 не се прилага, ако решението:

   а) е необходимо за сключването или изпълнението на договор между субекта на данни и администратора;

   б) е разрешено от правото на Съюза, в което също се предвиждат подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните; или

   в) се основава на изричното съгласие на субекта на данни.

3. В случаите, посочени в параграф 2, букви а) и в), администраторът прилага подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните, най-малко правото на човешка намеса от страна на администратора, правото да изрази гледната си точка и да оспори решението.

4. Решенията по параграф 2 не се основават на специалните категории лични данни, посочени в член 10, параграф 1, освен ако се прилага член 10, параграф 2, буква а) или буква ж) и са въведени подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните.

РАЗДЕЛ 5

ОГРАНИЧЕНИЯ

Член 25
Ограничения

1. Правни актове, приети въз основа на Договорите, или, по въпроси, свързани с функционирането на институциите и органите на Съюза, вътрешни правила, установени от тези органи и институции, могат да ограничават прилагането на членове 14—22, член 34 и член 38, както и на член 4, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—22, когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантират:

   а) националната сигурност, обществената сигурност или отбраната на държавите членки;

   б) предотвратяването, разследването, разкриването и наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;

   в) други важни цели от широк обществен интерес за Съюза или за държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;

   г) вътрешната сигурност на институциите и органите на Съюза, включително сигурността на техните електронни съобщителни мрежи;

   д) защитата на независимостта на съдебната власт и съдебните производства;

   е) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

   ж) функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите, посочени в букви а)—в);

   з) защитата на субекта на данните или на правата и свободите на други лица;

   и) изпълнението по гражданскоправни претенции.

2. Когато дадено ограничение не е предвидено в правен акт, приет въз основа на Договорите, или във вътрешно правило в съответствие с параграф 1, институциите и органите на Съюза могат да ограничават прилагането на членове 14—22, член 34 и член 38, както и на член 4, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—22, ако подобно ограничение е съобразено със същността на основните права и свободи, що се отнася до конкретна операция по обработване, и представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на една или повече от целите, посочени в параграф 1. Компетентното длъжностно лице по защита на данните се уведомява за това ограничение.

3. Когато личните данни се обработват за научни или исторически изследвания или за статистически цели, в правото на Съюза, което може да включва вътрешни правила, могат да бъдат предвидени дерогации от правата, посочени в членове 17, 18, 20 и 23, при спазване на условията и гаранциите, посочени в член 13, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели и посочените дерогации са необходими за постигането на тези цели.

4. Когато личните данни се обработват за целите на архивирането в обществен интерес, в правото на Съюза, което може да включва вътрешни правила, могат да бъдат предвидени дерогации от правата, посочени в членове 17, 18, 20, 21, 22 и 23, при спазване на условията и гаранциите, посочени в член 13, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели и посочените дерогации са необходими за постигането на тези цели.

5. Вътрешните правила, посочени в параграфи 1, 3 и 4, трябва да са достатъчно ясни и точни и трябва да бъдат публикувани по подходящ начин.

6. Ако бъде наложено ограничение съгласно параграф 1 или 2, субектът на данните се информира в съответствие с правото на Съюза за основните причини, обосноваващи прилагането на ограничението, и за правото му да подаде жалба до Европейския надзорен орган по защита на данните.

7. Ако ограничение, наложено съгласно параграф 1 или 2, се използва за отказване на достъп на субекта на данните, при разглеждане на жалбата Европейският надзорен орган по защита на данните го информира единствено за това дали данните са били правилно обработени и ако не са, дали са извършени необходимите корекции.

8. Предоставянето на информацията, посочена в параграфи 6 и 7 и в член 46, параграф 2, може да бъде отложено, пропуснато или отказано, ако предоставянето би премахнало ефекта от ограничението, наложено съгласно параграф 1 или 2.

ГЛАВА IV

АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

РАЗДЕЛ 1

ОБЩИ ЗАДЪЛЖЕНИЯ

Член 26
Отговорност на администратора

1. Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.

2. Когато това е пропорционално на дейностите по обработване, посочените в параграф 1 мерки включват прилагане от страна на администратора на подходящи политики за защита на данните.

Член 27
Защита на данните на етапа на проектирането и по подразбиране

1. Като взема предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, например псевдонимизация, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и да се осигури защита на правата на субектите на данни.

2. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

Член 28
Съвместни администратори

1. Когато дадена институция или орган на Съюза заедно с един или повече администратори, които може да са или да не са институции или органи на Съюза, съвместно определят целите и средствата на обработването, те са съвместни администратори. Те определят по прозрачен начин съответните си отговорности за изпълнение на съответните си задължения за защита на данните, по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информацията, посочена в членове 15 и 16, посредством договореност помежду си, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо администраторите. В договореността може да се посочи точка за контакт за субектите на данни.

2. Договореността, посочена в параграф 1, надлежно отразява съответните роли и връзки на съвместните администратори спрямо субектите на данни. Съществените характеристики на договореността са достъпни за субекта на данните.

3. Субектът на данни може да упражнява своите права по настоящия регламент спрямо и срещу един или повече от съвместните администратори, като взима предвид ролите им, определени в условията на договореността, посочена в параграф 1.

Член 29
Обработващ личните данни

1. Когато обработването се извършва от името на даден администратор, администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на настоящия регламент и да гарантира защитата на правата на субектите на данни.

2. Обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение обработващият данни винаги информира администратора за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като по този начин даде възможност на администратора да оспори тези промени.

3. Обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора и който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора. В този договор или друг правен акт се предвижда по-специално, че обработващият лични данни:

а) обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;

б) гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

в) взема всички необходими мерки съгласно член 33;

г) спазва условията по параграфи 2 и 4 за включване на друг обработващ лични данни;

д) като взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените в глава III права на субектите на данни;

е) подпомага администратора да гарантира изпълнението на задълженията съгласно членове 33—40, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

ж) по избор на администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка изисква тяхното съхранение;

з) осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора.

Предвид буква з) от първа алинея обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава настоящия регламент или други разпоредби на Съюза или на държавите членки относно защитата на данни.

4. Когато обработващ лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на администратора, чрез договор или друг правен акт съгласно правото на Съюза или правото на държава членка на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни, както е посочено в параграф 3, по-специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така

че обработването да отговаря на изискванията на настоящия регламент. Когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този друг обработващ лични данни.

5. Когато обработващ лични данни не е институция или орган на Съюза, придържането на този обработващ към одобрен кодекс за поведение, посочен в член 40, параграф 5 от Регламент (ЕС) 2016/679, или към одобрен механизъм за сертифициране, посочен в член 42 от Регламент (ЕС) 2016/679, може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграфи 1 и 4 от настоящия член.

6. Без да се засягат разпоредбите на индивидуален договор между администратора и обработващия лични данни, договорът или другият правен акт, посочени в параграфи 3 и 4 от настоящия член, може да се основават изцяло или отчасти на стандартни договорни клаузи, посочени в параграфи 7 и 8 от настоящия член, включително когато са част от сертифициране, предоставено на обработващия лични данни, различен от институция или орган на Съюза, съгласно член 42 от Регламент (ЕС) 2016/679.

7. Комисията може да установява стандартни договорни клаузи по въпроси, посочени в параграфи 3 и 4 от настоящия член, и в съответствие с процедурата по разглеждане, посочена в член 70, параграф 2.

8. Европейският надзорен орган по защита на данните може да приема стандартни договорни клаузи по въпросите, посочени в параграфи 3 и 4.

9. Договорът или другият правен акт, посочени в параграфи 3 и 4, се изготвят в писмена форма, включително в електронна форма.

10. Без да се засягат членове 65 и 66, ако обработващ лични данни наруши настоящия регламент, определяйки целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

Член 30

Обработване под ръководството на администратора и обработващия лични данни

Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването се изисква от правото на Съюза или правото на държава членка.

Член 31

Регистри на дейностите по обработване

1. Всеки администратор поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа цялата по-долу посочена информация:

а) името и координатите за връзка на администратора, на длъжностното лице по защита на данните и, когато е приложимо, на обработващия лични данни и на съвместните администратори;

б) целите на обработването;

в) описание на категориите субекти на данни и на категориите лични данни;

г) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в държави членки, трети държави или международни организации;

д) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация и документация за подходящите гаранции;

е) когато е възможно, предвидените срокове за изтриване на различните категории данни;

ж) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 33.

2. Всеки обработващ лични данни поддържа регистър на всички категории дейности по обработването, извършени от името на администратор, в който се съдържат:

а) името и координатите за връзка на обработващия или обработващите лични данни, на всеки администратор, от чието име действа обработващият лични данни, и на длъжностното лице за защита на данните;

б) категориите обработване, извършвано от името на всеки администратор;

в) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация и документация за подходящите гаранции;

г) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 33.

3. Регистрите, посочени в параграфи 1 и 2, се поддържат в писмена форма, включително в електронен формат.

4. Институциите и органите на Съюза предоставят на Европейския надзорен орган по защита на данните достъп до регистрите при поискване от негова страна.

5. Институциите и органите на Съюза могат да решат да съхраняват своите регистри на дейностите по обработване в централен регистър. В този случай те могат също да решат да предоставят публичен достъп до този регистър.

Член 32
Сътрудничество с Европейския надзорен орган по защита на данните

При поискване от Европейския надзорен орган по защита на данните институциите и органите на Съюза му сътрудничат при изпълнението на неговите задачи.

РАЗДЕЛ 2

СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ И ПОВЕРИТЕЛНОСТ НА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ

Член 33
Сигурност на обработването

1. Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно:

   а) псевдонимизация и криптиране на личните данни;

   б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

   в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

   г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

2. При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

3. Администраторът и обработващият лични данни предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора, освен ако от въпросното лице се изисква да прави това по силата на правото на Съюза.

Член 34
Поверителност на електронните съобщения

Институциите и органите на Съюза следва да гарантират поверителността на електронните съобщения, по-специално като осигуряват сигурността на своите електронни съобщителни мрежи.

Член 35
Защита на информацията, свързана с крайните устройства на крайните потребители

Институциите и органите на Съюза защитават информацията, свързана с крайните устройства на крайните потребители, осъществяващи достъп до техни обществено достъпни уебсайтове и мобилни приложения, в съответствие с Регламент (ЕС) XX/XXXX [нов Регламент за защитата на неприкосновеността на личния живот в сектора на електронните съобщения], и по-специално член 8 от него.

Член 36
Указатели на потребителите

1. Личните данни, които се съдържат в указатели на потребителите, както и достъпът до такива указатели се ограничават до степента, която е строго необходима за специфичните цели на указателите.

2. Институциите и органите на Съюза предприемат всички необходими мерки за предотвратяване на използването за преки маркетингови цели на съдържащите се в тези указатели лични данни, независимо дали те са или не са обществено достъпни.

Член 37
Уведомяване на Европейския надзорен орган по защита на данните за нарушение на сигурността на личните данни

1. В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни Европейския надзорен орган по защита на данните, освен ако съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до Европейския надзорен орган по защита на данните съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

2. Обработващият лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

3. В уведомлението, посочено в параграф 1, се съдържа най-малко следното:

   а) описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителният

брой на засегнатите субекти на данни и категориите и приблизителният брой на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

4. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

5. Администраторът уведомява длъжностното лице по защита на данните за нарушението на сигурността на личните данни.

6. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на Европейския надзорен орган по защита на данните да провери дали е спазен настоящият член.

Член 38

Съобщаване на субекта на данните за нарушение на сигурността на личните данни

1. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът без ненужно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.

2. В съобщението до субекта на данните, посочено в параграф 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в член 37, параграф 3, букви б), в) и г).

3. Посоченото в параграф 1 съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

а) администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни, посочен в параграф 1;

в) то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

4. Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, Европейският надзорен орган по защита на данните може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията по параграф 3.

РАЗДЕЛ 3

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ И ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ

Член 39
Оценка на въздействието върху защитата на данните

1. Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

2. При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на данните.

3. Оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално в случай на:

а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматизирано обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

б) мащабно обработване на специални категории данни, посочени в член 10, или на свързани с присъди и престъпления лични данни, посочени в член 11; или

в) систематично мащабно наблюдение на публично достъпна зона.

4. Европейският надзорен орган по защита на данните съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1.

5. Европейският надзорен орган по защита на данните може също да състави и оповести списък на видовете операции по обработване, за които не се изисква оценка на въздействието върху защитата на данните.

6. Оценката съдържа най-малко:

а) системен опис на предвидените операции по обработване и целите на обработването;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за гарантиране на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други засегнати лица.

7. При оценката на въздействието на операциите по обработване, извършвани от съответните обработващи лични данни, различни от институции и органи на Съюза, надлежно се отчита и спазването от тяхна страна на одобрените кодекси за поведение, посочени в член 40 от Регламент (ЕС) 2016/679, по-специално за целите на оценката на въздействието върху защитата на данните.

8. Когато е целесъобразно, администраторът се обръща към субектите на данните или техните представители за становище относно планираното обработване, без да се засяга защитата на обществените интереси или сигурността на операциите по обработване.

9. Когато обработването съгласно член 5, параграф 1, буква а) или б) има правно основание в правен акт, приет въз основа на Договорите, който регулира конкретната операция по обработване или набор от такива операции, и вече е извършена оценка на въздействието върху защитата на личните данни като част от общата оценка на въздействието, предшестваща приемането на този правен акт, параграфи 1—6 не се прилагат, освен ако в правото на Съюза е предвидено друго.

10. При необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

Член 40
Предварителна консултация

1. Администраторът се консултира с Европейския надзорен орган по защита на данните преди обработването, когато оценката на въздействието върху защитата на данните съгласно член 39 покаже, че при липса на гаранции, мерки за сигурност и механизми за ограничаване на риска обработването би довело до висок риск за правата и свободите на физическите лица, и администраторът счита, че рискът не може да бъде ограничен с разумни средства от гледна точка на наличните технологии и разходи за прилагане. Администраторът иска становището на длъжностното лице по защита на данните относно необходимостта от предварителна консултация.

2. Когато Европейският надзорен орган по защита на данните е на мнение, че планираното обработване, посочено в параграф 1, нарушава настоящия регламент, особено когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, Европейският надзорен орган по защита на данните в срок до осем седмици от получаване на искането за консултация дава писмено становище на администратора и, когато е приложимо, на обработващия лични данни, като може да използва всяко от правомощията си, посочени в член 59. Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване. Европейският надзорен орган по защита на данните информира администратора и, когато е приложимо, обработващия лични данни за такова удължаване в срок от един месец от получаване на искането за консултация, включително за причините за забавянето. Тези срокове могат да бъдат спрени, докато Европейският надзорен орган по защита на данните получи поисканата от него информация за целите на консултацията.

3. Когато се консултира с Европейския надзорен орган по защита на данните в съответствие с параграф 1, администраторът предоставя на Европейския надзорен орган по защита на данните следната информация:

   а) когато е приложимо — информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, участващи в обработването;

   б) целите на планираното обработване и средствата за него;

   в) предвидените мерки и гаранции за защита на правата и свободите на субектите на данни съгласно настоящия регламент;

   г) координатите за връзка на длъжностното лице по защита на данните;

   д) оценката на въздействието върху защитата на данните по член 39; и

   е) всякаква друга информация, поискана от Европейския надзорен орган по защита на данните.

4. Комисията може посредством акт за изпълнение да определи списък от случаи, в които администраторите трябва да се консултират с Европейския надзорен орган по защита на данните или да получат неговото предварително

разрешение във връзка с обработването за целите на изпълнението на задача, осъществявана от администратора в обществен интерес, включително обработването на такива данни във връзка със социалната закрила и общественото здраве.

РАЗДЕЛ 4

ИНФОРМАЦИЯ И ЗАКОНОДАТЕЛНИ КОНСУЛТАЦИИ

Член 41
Информация

Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните при изготвяне на административни мерки и вътрешни правила във връзка с обработването на лични данни, в което самостоятелно или съвместно с други участва институция или орган на Съюза.

Член 42
Законодателни консултации

1. След приемането на предложения за законодателен акт и на препоръки или предложения до Съвета съгласно член 218 от ДФЕС и при подготовката на делегирани актове или актове за изпълнение, които имат въздействие върху защитата на правата и свободите на физическите лица по отношение на обработването на лични данни, Комисията се консултира с Европейския надзорен орган по защита на данните.

2. Когато акт, посочен в параграф 1, има особено значение за защита на правата и свободите на физическите лица по отношение на обработката на лични данни, Комисията може също така да се консултира с Европейския комитет по защита на данните. В тези случаи Европейският надзорен орган по защита на данните и Европейския комитет по защита на данните координират работата си с оглед на издаването на съвместно становище.

3. Консултациите, посочени в параграфи 1 и 2, се предоставят в писмена форма в срок до осем седмици от получаване на искането за провеждане на консултация, посочена в параграфи 1 и 2. В спешни случаи или при друга необходимост Комисията може да съкрати крайния срок.

4. Настоящият член не се прилага, когато Комисията е длъжна в съответствие с Регламент (ЕС) 2016/679 да се консултира с Европейския комитет по защита на данните.

РАЗДЕЛ 5

ЗАДЪЛЖЕНИЕ ЗА РЕАГИРАНЕ НА ТВЪРДЕНИЯ

Член 43
Задължение за реагиране на твърдения

Когато Европейският надзорен орган по защита на данните упражнява правомощията, предвидени в член 59, параграф 2, букви а), б) и в), администраторът или обработващият лични данни информира Европейския надзорен орган по защита на данните относно становището си в разумен срок, който се определя от Европейския надзорен орган по защита на данните при отчитане на обстоятелствата по всеки отделен случай. Отговорът включва и описание на предприетите мерки, ако има такива, в отговор на отправените от Европейския надзорен орган по защита на данните забележки.

РАЗДЕЛ 6

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Член 44
Определяне на длъжностното лице по защита на данните

1. Всяка институция или орган на ЕС определя длъжностно лице по защита на данните.

2. Няколко институции и органи на Съюза могат да определят едно-единствено длъжностно лице за себе си, като вземат предвид своите организационна структура и размер.

3. Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 46.

4. Длъжностното лице по защита на данните може да бъде член на персонала на институцията или органа на Съюза или да изпълнява задачите въз основа на договор за услуги.

5. Институциите и органите на Съюза публикуват координатите за връзка на длъжностното лице по защита на данните и ги съобщават на Европейския надзорен орган по защита на данните.

Член 45

Длъжност на длъжностното лице по защита на данните

1. Институциите и органите на Съюза гарантират, че длъжностното лице по защита на данните участва по подходящ начин и своевременно по всички въпроси, свързани със защитата на личните данни.

2. Институциите и органите на Съюза подпомагат длъжностното лице по защита на данните при изпълнението на посочените в член 46 задачи, като осигуряват ресурсите, необходими за изпълнението на тези задачи, и достъп до личните данни и операциите по обработване, а така също поддържат неговите експертни знания.

3. Институциите и органите на Съюза правят необходимото длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на своите задачи. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни.

4. Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия регламент.

5. Длъжностното лице по защита на данните и неговият персонал са длъжни да спазват секретността или поверителността на изпълняваните от тях задачи в съответствие с правото на Съюза.

6. Длъжностното лице по защита на данните може да изпълнява и други задачи и задължения. Администраторът или обработващият лични данни прави необходимото тези задачи и задължения да не водят до конфликт на интереси.

7. Администраторът и обработващият личните данни, съответният комитет по персонала и всяко физическо лице могат, без да е необходимо да следват официална процедура, да се консултират с длъжностното лице по защита на данните по всеки въпрос, отнасящ се до тълкуването или прилагането на настоящия регламент. Никой не може да претърпи вреди, поради това че е отнесъл до вниманието на компетентното длъжностно лице по защита на данните въпрос, твърдейки за наличие на извършено нарушение на разпоредбите на настоящия регламент.

8. Длъжностното лице по защита на данните се назначава за срок от три до пет години и може да бъде преназначавано. Длъжностното лице по защита на данните може да бъде освободено от длъжността от институцията или органа на Съюза, който го е назначил, само със съгласието на Европейския надзорен орган по защита на данните, ако престане да отговаря на необходимите условия за изпълнение на своите задължения.

9. След назначаване на длъжностното лице по защита на данните институцията или органът, който го е назначил, го регистрира при Европейския надзорен орган по защита на данните.

Член 46

Задачи на длъжностното лице по защита на данните

1. Длъжностното лице по защита на данните изпълнява следните задачи:

а) информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби на Съюза за защитата на данните;

б) осигурява по независим начин вътрешното прилагане на настоящия регламент и наблюдава спазването на настоящия регламент, на други разпоредби за защитата на данните, съдържащи се в правото на Съюза, и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

в) гарантира, че субектите на данните са информирани за своите права и задължения съгласно настоящия регламент;

г) предоставя при поискване съвети във връзка с необходимостта от уведомяване или съобщаване за нарушение на сигурността на личните данни съгласно членове 37 и 38;

д) предоставя при поискване съвети във връзка с оценката на въздействието върху защитата на данните и наблюдава извършването на оценката съгласно член 39, както и се консултира с Европейския надзорен орган по защита на данните в случай на съмнение относно необходимостта от оценка на въздействието върху защитата на данните;

е) предоставя при поискване съвети във връзка с необходимостта от предварителна консултация с Европейския надзорен орган по защита на данните съгласно член 40, както и се консултира с Европейския надзорен орган по защита на данните в случай на съмнение относно необходимостта от предварителна консултация;

ж) отговаря на запитвания от страна на Европейския надзорен орган по защита на данните и в рамките на своите компетенции си сътрудничи с Европейския надзорен орган по защита на данните по негово искане или по своя собствена инициатива.

2. Длъжностното лице по защита на данните може да отправя на администратора и на обработващия лични данни препоръки за практическото подобряване на защитата на данните и да ги съветва по въпроси, свързани с прилагането на разпоредби относно защитата на данните. Освен това длъжностното лице по защита на данните може по своя инициатива или по искане на администратора или на обработващия лични данни, на съответния комитет по персонала или на всяко физическо лице да разследва пряко свързани с неговите задачи въпроси и факти, за които е уведомено, и да докладва обратно на лицето, което е възложило разследването, или на администратора или обработващия лични данни.

3. Всяка институция или орган на Съюза приема допълнителни правила за прилагане, отнасящи се до длъжностното лице по защита на данните. Правилата за прилагане се отнасят в частност до задачите, задълженията и правомощията на длъжностното лице по защита на данните.

ГЛАВА V

Предаване на лични данни на трети държави или международни организации

Член 47
Общ принцип на предаването на данни

Предаване на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация, се осъществява само ако, при спазване на другите разпоредби на настоящия регламент, администраторът и обработващият лични данни спазват условията по настоящата глава, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация. Всички разпоредби на настоящата глава се прилагат, за да се гарантира, че нивото на защита на физическите лица, гарантирано от настоящия регламент, не се излага на риск.

Член 48
Предаване на данни въз основа на решение относно адекватното ниво на защита

1. Предаване на лични данни на трета държава или на международна организация може да се осъществи, ако Комисията е решила в съответствие с член 45, параграф 3 от Регламент (ЕС) 2016/679, че въпросната трета държава, територия, или един или повече конкретни сектори в тази трета държава, или въпросната международна организация осигуряват адекватно ниво на защита и че личните данни се предават единствено за да стане възможно изпълнението на задачи от компетенциите на администратора.

2. Институциите и органите на Съюза информират Комисията и Европейския надзорен орган по защита на данните за случаи, в които те считат, че съответната трета държава или международна организация не осигурява адекватно ниво на защита по смисъла на параграф 1.

3. Институциите и органите на Съюза предприемат необходимите мерки, за да се съобразят с взетите от Комисията решения, когато съгласно член 45, параграфи 3 и 5 от Регламент (ЕС) 2016/679 тя установява, че дадена трета държава или международна организация осигурява или вече не осигурява адекватно ниво на защита.

Член 49
Предаване на данни с подходящи гаранции

1. При липса на решение съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни може да предава лични данни на трета държава или международна организация само ако е предвидил подходящи гаранции и при условие че са налице приложими права на субектите на данни и ефективни правни средства за защита.

2. Подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени, без да се изисква специално разрешение от Европейския надзорен орган по защита на данните, посредством:

   а) правно обвързващ инструмент с изпълнителна сила между публичните органи или структури;

   б) стандартни клаузи за защита на данните, приети от Комисията в съответствие с процедурата по разглеждане, посочена в член 70, параграф 2;

   в) стандартни клаузи за защита на данните, приети от Европейския надзорен орган по защита на данните и одобрени от Комисията съгласно процедурата по разглеждане, посочена в член 70, параграф 2;

   г) задължителни фирмени правила, кодекси за поведение и механизъм за сертифициране съгласно член 46, параграф 2, букви б), д) и е) от Регламент (ЕС) 2016/679, когато обработващият лични данни не е институция или орган на Съюза.

3. При условие че Европейският надзорен орган по защита на данните е дал разрешение, подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени по-специално и посредством:

   а) договорни клаузи между администратора или обработващия лични данни и администратора, обработващия лични данни или получателя на личните данни в третата държава или международната организация; или

   б) разпоредби, които да се включват в административните договорености между публичните органи или структури, съдържащи приложими и ефективни права на субектите на данни.

4. Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните за категориите случаи, в които настоящият член е бил приложен.

5. Разрешенията, издадени от Европейския надзорен орган по защита на данните въз основа на член 9, параграф 7 от Регламент (ЕС) 2016/679, остават валидни, докато не бъдат изменени, заменени или отменени, ако е необходимо, от Европейския надзорен орган по защита на данните.

Член 50

Предаване или разкриване на данни, което не е разрешено от правото на Съюза

Всяко решение на съд или трибунал и всяко решение на административен орган на трета държава, с което от администратор или обработващ лични данни се изисква да предаде или разкрие лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само ако се основават на международно споразумение, като договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза, без да се засягат другите основания за предаване на данни съгласно настоящата глава.

Член 51

Дерогации в особени случаи

1. При липсата на решение съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 или на подходящи гаранции съгласно член 49, предаване или съвкупност от предавания на лични данни на трета държава или международна организация се извършва само при едно от следните условия:

   а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за него поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции;

   б) предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

   в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;

   г) предаването е необходимо поради важни причини от обществен интерес;

   д) предаването е необходимо за установяването, упражняването или защитата на правни претенции; или

   е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие; или

   ж) предаването се извършва от регистър, който съгласно правото на Съюза е предназначен за предоставяне на информация на обществеността и е открит за извършване на справки от широката общественост или от всяко лице, което може да докаже законен интерес, но само при условие че в конкретния случай са изпълнени предвидените в правото на Съюза условия за извършване на справки.

2. Предаването съгласно параграф 1, буква ж) не трябва да включва всички лични данни или всички категории лични данни, съдържащи се в регистъра, освен ако

това е разрешено от правото на Съюза. Когато регистърът е предназначен за справка от лица, които имат законен интерес, предаването се извършва единствено по искане на тези лица или ако те са получателите.

3. Общественият интерес, посочен в параграф 1, буква г), трябва да е признат в правото на Съюза.

4. При липсата на решение относно адекватното ниво на защита правото на Съюза може по важни причини от обществен интерес изрично да определи ограничения за предаването на специални категории от лични данни на трета държава или международна организация.

5. Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните за категориите случаи, в които настоящият член е бил приложен.

Член 52
Международно сътрудничество за защита на личните данни

По отношение на трети държави и международни организации Европейският надзорен орган по защита на данните, в сътрудничество с Комисията и Европейския комитет по защита на данните, предприема подходящи мерки за:

а) разработване на механизми за международно сътрудничество с цел подпомагане ефективното прилагане на законодателството за защита на личните данни;

б) осигуряване на международна взаимопомощ при прилагането на законодателството за защита на личните данни, включително чрез уведомяване, препращане на жалби, помощ при разследвания и обмен на информация, при условие че има подходящи гаранции за защитата на личните данни и другите основни права и свободи;

в) включване на съответните заинтересовани страни в обсъждания и дейности, насочени към насърчаване на международното сътрудничество за прилагането на законодателството за защита на личните данни;

г) насърчаване на обмена и документирането на законодателството и практиките в областта на защитата на личните данни, включително относно спорове за компетентност с трети държави.

ГЛАВА VI

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ

Член 53
Европейски надзорен орган по защита на данните

1. Създава се Европейският надзорен орган по защита на данните.

2. По отношение на обработването на лични данни задачата на Европейския надзорен орган по защита на данните е да гарантира спазването от страна на институциите и органите на Съюза на основните права и свободи на физическите лица, и по-специално правото им на защита на данните.

3. Европейският надзорен орган по защита на данните отговаря за наблюдението и гарантирането на прилагането на разпоредбите на настоящия регламент и всеки друг акт на Съюза, който се отнася до защитата на основните права и свободи на физическите лица по отношение на обработването на лични данни от институция или орган на Съюза, както и за предоставянето на консултации на институциите и органите на Съюза и субектите на данни по всички въпроси, свързани с обработването на лични данни. За тази цел Европейският надзорен орган по защита на данните изпълнява задачите, предвидени в член 58, и упражнява правомощията, предоставени съгласно член 59.

Член 54
Назначаване на Европейския надзорен орган по защита на данните

1. Европейският надзорен орган по защита на данните се назначава с общо съгласие от Европейския парламент и Съвета за срок от пет години въз основа на съставен от Комисията списък след публично отправена покана за представяне на кандидатури. Поканата за представяне на кандидатури предоставя възможност на всички заинтересовани страни в Съюза да представят своите кандидатури. Списъкът на кандидатите, съставен от Комисията, е публичен. Въз основа на списъка, съставен от Комисията, компетентната комисия на Европейския парламент може да реши да проведе изслушване, за да получи възможност да изрази предпочитанията си.

2. Съставеният от Комисията списък, от който се избира Европейският надзорен орган по защита на данните, се състои от лица, чиято независимост не подлежи на съмнение и за които е признато, че притежават необходимите опит и умения, за да изпълняват задълженията на Европейски надзорен орган по защита на данните, например поради това, че работят или са работили в надзорните органи, създадени по силата на член 41 от Регламент (ЕС) 2016/679.

3. Мандатът на Европейския надзорен орган по защита на данните може да бъде подновен еднократно.

4. Задълженията на Европейския надзорен орган по защита на данните се прекратяват при следните обстоятелства:

а) ако Европейският надзорен орган по защита на данните бъде сменен;

б) ако Европейският надзорен орган по защита на данните подаде оставка:

в) ако Европейският надзорен орган по защита на данните бъде освободен от длъжност или ако подлежи на задължително пенсиониране.

5. Европейският надзорен орган по защита на данните може да бъде освободен от длъжност или лишен от правото на пенсия или други заместващи пенсията облаги от Съда на Европейския съюз по искане на Европейския парламент, Съвета или Комисията, ако престане да отговаря на необходимите условия за изпълнение на своите задължения или в случай на тежко провинение.

6. В случай на нормална смяна или доброволна оставка Европейският надзорен орган по защита на данните въпреки всичко продължава да заема длъжността си, докато бъде сменен.

7. Разпоредбите на членове 11 — 14 и член 17 от Протокола за привилегиите и имунитетите на Европейския съюз се прилагат за Европейския надзорен орган защита на данните.

Член 55

Правилник и общи условия за изпълнение на задълженията на Европейския надзорен орган по защита на данните, персонал и финансови средства

1. Счита се, че Европейският надзорен орган по защита на данните има статут, равностоен на този на съдия от Съда на Европейския съюз, що се отнася до определяне на размера на възнаграждението, надбавките, пенсията за осигурителен стаж и възраст и всякакви други обезщетения, които заместват възнаграждението.

2. Бюджетният орган гарантира осигуряването на Европейския надзорен орган по защита на данните на необходимите за изпълнение на неговите задачи човешки и финансови ресурси.

3. Бюджетът на Европейския надзорен орган по защита на данните фигурира в отделна бюджетна позиция в раздел IX на общия бюджет на Европейския съюз.

4. Европейският надзорен орган по защита на данните се подпомага от секретариат. Длъжностните лица и другите служители в секретариата се назначават от Европейския надзорен орган по защита на данните, който е и техен висшестоящ ръководител. Те подлежат изцяло на неговото ръководство. Числеността на персонала се определя всяка година като част от бюджетната процедура.

5. За длъжностните лица и другите служители в секретариата на Европейския надзорен орган по защита на данните важат правилата и разпоредбите, приложими за длъжностните лица и другите служители на Европейския съюз.

6. Седалището на Европейския надзорен орган по защита на данните е в Брюксел.

Член 56
Независимост

1. Европейският надзорен орган по защита на данните действа напълно независимо при изпълнението на задачите си и упражняването на правомощията си съгласно настоящия регламент.

2. При изпълнението на задачите си и упражняването на правомощията си в съответствие с настоящия регламент Европейският надзорен орган по защита на данните остава независими от външно влияние, било то пряко или непряко, и нито търси, нито приема инструкции от когото и да било.

3. Европейският надзорен орган по защита на данните се въздържа от всякакви несъвместими със задълженията му действия и по време на своя мандат не упражнява никакви други дейности, независимо дали срещу възнаграждение, или безвъзмездно.

4. След приключване на мандата си Европейският надзорен орган по защита на данните проявява почтеност и въздържаност относно приемането на постове и облаги.

Член 57
Професионална тайна

По време и след приключване на мандата Европейският надзорен орган по защита на данните и неговият персонал подлежат на задължение за опазване на професионалната тайна по отношение на всякаква поверителна информация, която е стигнала до тяхното знание в хода на изпълнение на служебните им задължения.

Член 58
Задачи

1. Без да се засягат останалите задачи, определени в настоящия регламент, Европейският надзорен орган по защита на данните:

   а) наблюдава и осигурява прилагането на настоящия регламент и на други актове на Съюза, отнасящи се до защитата на физически лица по отношение на обработването на лични данни от институция или орган на Съюза, с изключение на обработването на лични данни от Съда на Европейския съюз при изпълнение на съдебните му функции;

   б) насърчава обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработването. Обръща се специално внимание на дейностите, специално насочени към децата;

   в) насърчава информираността на администраторите и обработващите лични данни за задълженията им по силата на настоящия регламент;

г) при поискване предоставя информация на всеки субект на данни във връзка с упражняването на правата му по силата на настоящия регламент и ако е необходимо, си сътрудничи за тази цел с надзорните органи в държави членки;

д) разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение в съответствие с член 67, и разследва предмета на жалбата, доколкото това е целесъобразно, и информира жалбоподателя за напредъка и резултатите от разследването в разумен срок, особено ако е необходимо по-нататъшно разследване или координиране с друг надзорен орган;

е) извършва проучвания относно прилагането на настоящия регламент, включително въз основа на информация, получена от друг надзорен или публичен орган;

ж) съветва всички институции и органи на Съюза относно законодателни и административни мерки, отнасящи се до защитата на правата и свободите на физическите лица по отношение на обработването на лични данни;

з) наблюдава развитието по-специално в областта на информационните и комуникационни технологии дотолкова, доколкото те имат въздействие върху защитата на личните данни;

и) приема стандартните договорни клаузи, посочени в член 29, параграф 8 и член 49, параграф 2, буква в);

й) съставя и поддържа списък във връзка с изискването за оценка на въздействието върху защитата на данните съгласно член 39, параграф 4;

к) участва в дейностите на Европейския комитет по защита на данните, създаден по силата на член 68 от Регламент (ЕС) № 2016/679;

л) осигурява секретариата на Европейския комитет по защита на данните в съответствие с член 75 от Регламент (ЕС) 2016/679;

м) дава становища по обработването, посочено в член 40, параграф 2;

н) дава разрешение за договорните клаузи и разпоредбите, посочени в член 49, параграф 3;

о) поддържа вътрешен регистър на нарушенията на настоящия регламент, както и на предприетите мерки в съответствие с член 59, параграф 2;

п) изпълнява други задачи, свързани със защитата на лични данни; и

р) приема свой процедурен правилник.

2. Европейският надзорен орган по защита на данните улеснява подаването на жалбите, посочени в параграф 1, буква д), посредством формуляр за подаване на жалби, който може да бъде попълнен и по електронен път, без да се изключват други средства за комуникация.

3. Изпълнението на задълженията на Европейския надзорен орган по защита на данните е безплатно за субекта на данни.

4. Когато исканията са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Европейският надзорен орган по защита на данните може да откаже да предприеме действия по искането. Европейският надзорен орган по защита на данните носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

Член 59
Правомощия

1. Европейският надзорен орган по защита на данните има следните правомощия за разследване:

   а) да разпорежда на администратора и на обработващия лични данни да предоставят всяка информация, която той поиска за изпълнението на своите задачи;

   б) да провежда разследвания под формата на одити във връзка със защитата на данните;

   в) да уведомява администратора или обработващия лични данни за предполагаемо нарушение на настоящия регламент;

   г) да получава от администратора и обработващия лични данни достъп до всички лични данни и до цялата информация, от която се нуждае за изпълнението на своите задачи;

   д) да получава достъп до всички помещения на администратора и обработващия лични данни, включително до всяко оборудване и средство за обработване на данни, в съответствие с процесуалното право на Съюза или на държавата членка.

2. Европейският надзорен орган по защита на данните има следните корективни правомощия:

   а) да отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операциите по обработване на данни, които те възнамеряват да извършат, да нарушат разпоредбите на настоящия регламент;

   б) да отправя официално предупреждение до администратора или обработващия лични данни, когато операции по обработване на данни са нарушили разпоредбите на настоящия регламент;

   в) да отнесе въпроса до администратора или обработващия лични данни, а при необходимост и до Европейския парламент, Съвета и Комисията;

г) да разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;

д) да разпорежда на администратора или обработващия лични данни да съобразят операциите по обработване на данни с разпоредбите на настоящия регламент и, ако е целесъобразно, това да стане по указан начин и в определен срок;

е) да разпорежда на администратора да съобщава на субекта на данните за нарушение на сигурността на личните данни;

ж) да налага временно или окончателно ограничаване, включително забрана, на обработването на данни;

з) да разпорежда коригирането или изтриването на лични данни, или ограничаването на обработването им съгласно членове 18, 19 и 20, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно член 19, параграф 2 и член 21;

и) да налага административнонаказателна имуществена санкция съгласно член 66 при неизпълнение от страна на институция или орган на Съюза на една от мерките, посочени в настоящия параграф, и в зависимост от обстоятелствата по всеки отделен случай;

й) да разпорежда преустановяване на предаването на данни към получател в държава членка или към международна организация.

3. Европейският надзорен орган по защита на данните има следните разрешителни и консултативни правомощия:

а) да съветва субектите на данни при упражняване на техните права;

б) да съветва администратора в съответствие с процедурата по предварителна консултация, посочена в член 40;

в) да издава по собствена инициатива или при поискване становища до институциите и органите на Съюза и до обществеността по всякакви въпроси, свързани със защитата на лични данни;

г) да приема стандартните клаузи за защита на данните, посочени в член 29, параграф 8 и в член 49, параграф 2, буква в);

д) да дава разрешение за договорните клаузи, посочени в член 49, параграф 3, буква а);

е) да дава разрешение за административните договорености, посочени в член 49, параграф 3, буква б).

4. Упражняването на правомощията, предоставени на Европейския надзорен орган по защита на данните по силата на настоящия член, подлежи на

подходящи гаранции, включително ефективни средства за съдебна защита и справедлив съдебен процес, определени в правото на Съюза.

5. Европейският надзорен орган по защита на данните има правомощието сезира Съда на Европейския съюз при условията, предвидени в Договора, и да встъпва по дела, заведени пред Съда на Европейския съюз.

Член 60
Доклад за дейността

1. Европейският надзорен орган по защита на данните представя на Европейския парламент, Съвета и Комисията годишен доклад за дейността си и същевременно го публикува.

2. Европейският надзорен орган по защита на данните изпраща доклада за дейността си на другите институции и органи на Съюза, които могат да представят коментари с оглед на евентуално разглеждане на доклада в Европейския парламент.

ГЛАВА VII

СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ

Член 61
Сътрудничество с националните надзорни органи

Европейският надзорен орган по защита на данните си сътрудничи с надзорните органи, създадени съгласно член 41 от Регламент (ЕС) 2016/679 и член 51 от Директива (ЕС) 2016/680 (наричани по-нататък „национални надзорни органи“), и със съвместния надзорен орган, създаден съгласно член 25 от Решение 2009/917/ПВР[21] на Съвета, доколкото това е необходимо за изпълнението на съответните негови и техни задължения, по-специално като обменя с тях съответна информация, като отправя искания до национални надзорни органи да упражняват своите правомощия или като отговаря на искания от тези органи.

Член 62
Координиран надзор, осъществяван от Европейския надзорен орган по защита на данните и националните надзорни органи

1. В случаите, когато даден акт на Съюза препраща към настоящия член, Европейският надзорен орган по защита на данните си сътрудничи активно с националните надзорни органи, за да се осигури ефективен надзор на мащабни информационни системи или агенции на Съюза.

[21] Решение 2009/917/ПВР на Съвета от 30 ноември 2009 г. относно използването на информационни технологии за митнически цели, (ОВ L 323, 10.12.2009 г., стр. 20—30).

2. Европейският надзорен орган по защита на данните, действайки в обхвата на съответните си компетенции и в рамките на отговорностите си, осъществява обмен на съответна информация, оказва съдействие при извършването на одити и проверки, разглежда трудности при тълкуването или прилагането на настоящия регламент и други приложими правни актове на Съюза, проучва проблеми, свързани с упражняването на независим надзор или с упражняването на правата на субектите на данни, изготвя хармонизирани предложения за разрешаване на проблеми и насърчава информираността относно правата на защита на данните, когато е необходимо, съвместно с националните надзорни органи.

3. За целите, посочени в параграф 2, Европейският надзорен орган по защита на данните провежда заседания с националните надзорни органи най-малко два пъти в годината в рамките на Европейския комитет по защита на данните. Разходите за тези заседания и обслужването им са за сметка на Европейския комитет по защита на данните. На първото заседание се приема процедурен правилник. При необходимост съвместно се разработват допълнителни методи на работа.

4. Веднъж на всеки две години Европейският комитет по защита на данните изпраща на Европейския парламент, Съвета и Комисията съвместен доклад за дейностите по координиран надзор.

ГЛАВА VIII

СРЕДСТВА ЗА ПРАВНА ЗАЩИТА, ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ И САНКЦИИ

Член 63

Право на подаване на жалба до Европейския надзорен орган по защита на данните

1. Без да се засягат които и да било средства за съдебна, административна или извънсъдебна защита, всеки субект на данни има право да подаде жалба до Европейския надзорен орган по защита на данните, ако счита, че обработването на лични данни, отнасящи се до него, нарушава настоящия регламент.

2. Европейският надзорен орган по защита на данните информира субекта на данните за напредъка в разглеждането на жалбата и за резултата от нея, включително за възможността за съдебна защита съгласно член 64.

3. Ако Европейският надзорен орган по защита на данните не разгледа жалбата или не информира субекта на данните в срок от три месеца за напредъка в разглеждането на жалбата или за резултата от нея, жалбата се счита за отхвърлена.

Член 64
Право на ефективна съдебна защита

Съдът на Европейския Съюз е компетентен да разглежда всички спорове във връзка с разпоредбите на настоящия регламент, включително искове за вреди.

Член 65
Право на обезщетение

Всяко лице, което е претърпяло имуществени или неимуществени вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди, при спазване на условията, предвидени в Договорите.

Член 66
Административнонаказателни имуществени санкции

1. Европейският надзорен орган по защита на данните може да налага административнонаказателни имуществени санкции на институции и органи на Съюза, в зависимост от обстоятелствата по всеки отделен случай, когато институция или орган на Съюза не изпълни разпореждане на Европейския надзорен орган по защита на данните, издадено съгласно член 59, параграф 2, букви а) — з) и буква й). Когато се взема решение дали да бъде наложена административнонаказателна имуществена санкция и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи:

   а) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда;

   б) действията, предприети от институцията или органа на Съюза за смекчаване на последиците от вредите, претърпени от субектите на данни;

   в) степента на отговорност на институцията или органа на Съюза, като се вземат предвид техническите и организационни мерки, въведени от тях в съответствие с членове 27 и 33;

   г) всички подобни предишни нарушения от страна на институцията или органа на Съюза;

   д) степента на сътрудничество с Европейския надзорен орган по защита на данните с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;

   е) категориите лични данни, засегнати от нарушението;

ж) начинът, по който нарушението е станало известно на Европейския надзорен орган по защита на данните, по-специално дали и до каква степен институцията или органът на Съюза са съобщили за нарушението;

з) когато срещу въпросната институция или въпросния орган на Съюза преди са били разпоредени мерки, посочени в член 59, във връзка със същия предмет, дали тези мерки са спазени.

Производството, водещо до налагане на тези имуществени санкции, следва да се проведе в разумен срок в зависимост от обстоятелствата по случая и при отчитане на съответните мерки и производства, посочени в член 69.

2. В съответствие с параграф 1 на институция или орган на Съюза, които нарушат задълженията си съгласно членове 8, 12, 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 и 46, се налагат административнонаказателни имуществени санкции в размер до 25 000 EUR за всяко отделно нарушение и в общ размер до 250 000 EUR годишно.

3. В съответствие с параграф 1 на институция или орган на Съюза, които нарушат следните разпоредби, се налагат административнонаказателни имуществени санкции в размер до 50 000 EUR за всяко отделно нарушение и в общ размер до 500 000 EUR годишно:

а) основните принципи за обработване на лични данни, включително условията, свързани с даването на съгласие, в съответствие с членове 4, 5, 7 и 10;

б) правата на субектите на данни съгласно членове 14—24;

в) предаването на лични данни на получател в трета държава или международна организация съгласно членове 47—51.

4. Ако институция или орган на Съюза при една и съща операция или при свързани или непрекъснати операции по обработване наруши няколко разпоредби на настоящия регламент или една и съща разпоредба няколко пъти, общият размер на административнонаказателната имуществената санкция не може да надвишава сумата, определена за най-тежкото нарушение.

5. Преди да вземе решения по силата на настоящия член, Европейският надзорен орган по защита на данните дава на институцията или органа на Съюза, по отношение на които се провеждат производствата, възможността да бъдат изслушани във връзка с въпросите, по които надзорният орган е изразил възражения. Европейският надзорен орган по защита на данните основава своите решения единствено на възражения, по които засегнатите страни са имали възможност да изразят становище. Жалбоподателите се привличат за тясно сътрудничество по производството.

6. Правото на защита на засегнатите страни се съблюдава в хода на цялото производство. Те имат правото на достъп до преписката на Европейския надзорен орган по защита на данните, при условие че се зачита законният интерес на физическите лица или на предприятията за защита на техните лични данни или търговски тайни.

7. Средствата, събрани чрез налагането на имуществени санкции съгласно настоящия член, представляват приход в общия бюджет на Европейския съюз.

Член 67
Представителство на субектите на данни

Субектът на данни има право да възложи на структура, организация или сдружение с нестопанска цел, което е надлежно учредено в съответствие с правото на Съюза или с правото на държава членка, има уставни цели, които са в обществен интерес, и действа в областта на защитата на правата и свободите на субектите на данни по отношение на защитата на техните лични данни, да подаде жалба от негово име до Европейския надзорен орган по защита на данните и да упражни от негово име правата по член 63, както и правото на обезщетение по член 65.

Член 68
Жалби от длъжностни лица и други служители на Съюза

Всяко лице, нает на работа от институция или орган на Съюза, може да подаде жалба до Европейския надзорен орган по защита на данните във връзка с предполагаемо нарушение на разпоредбите на настоящия регламент, без да следва официална процедура. Никой не може да претърпи вреди заради подадена жалба до Европейския надзорен орган по защита на данните, в която се твърди, че е извършено такова нарушение.

Член 69
Санкции

За всяко неспазване, независимо дали умишлено или по непредпазливост, на задълженията, предвидени в настоящия регламент, длъжностно лице или друг служител на Европейския съюз подлежи на дисциплинарни или други мерки в съответствие с правилата и процедурите, установени в Правилника за длъжностните лица на Европейския съюз или в Условията за работа на другите служители на Европейския съюз.

ГЛАВА IX

АКТОВЕ ЗА ИЗПЪЛНЕНИЕ

Член 70
Процедура на комитет

1. Комисията се подпомага от комитета, създаден съгласно член 93 от Регламент (ЕС) 2016/679. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

ГЛАВА X

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 71
Отмяна на Регламент (ЕО) № 45/2001 и на Решение № 1247/2002/ЕО

Регламент (ЕО) № 45/2001[22] и Решение № 1247/2002/ЕО[23] се отменят, считано от 25 май 2018 ´г. Позоваванията на отменения регламент и на отменението решение се считат за позовавания на настоящия регламент.

Член 72
Преходни мерки

1. Решение № 2014/886/ЕС на Европейския парламент и на Съвета[24] и текущият мандат на Европейския надзорен орган по защита на данните и на заместника на надзорния орган не се засягат от настоящия регламент.

2. Счита се, че заместникът на надзорния орган има статут, равностоен на този на секретаря на Съда на Европейския съюз, що се отнася до определяне на размера на възнаграждението, надбавките, пенсията за осигурителен стаж и възраст и всякакви други обезщетения, които заместват възнаграждението.

3. Член 54, параграфи 4, 5 и 7, както и членове 56 и 57 от настоящия регламент се прилагат по отношение на настоящия заместник на надзорния орган до изтичането на мандата му на 5 декември 2019 г.

4. Заместникът на надзорния орган подпомага Европейския надзорен орган по защита на данните при изпълнението на неговите задължения и го замества, когато Европейският надзорен орган по защита на данните отсъства или е възпрепятстван да изпълнява задълженията си, до изтичането на мандата на заместника на надзорния орган на 5 декември 2019 г.

---

22 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Съюза и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г.).

23 Решение № 1247/2002/ЕО от 1 юли 2002 г. относно статута и общите условия, регулиращи изпълнението на задълженията на Европейския надзорен орган по защита на данните (ОВ L 183, 12.7.2002 г., стр. 1).

24 Решение 2014/886/ЕС на Европейския парламент и на Съвета от 4 декември 2014 г. относно назначаването на ръководител на Европейския надзорен орган по защита на данните и на негов заместник (ОВ L 351, 9.12.2014 г., стр. 9).

Член 73
Влизане в сила и прилагане

1. Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

2. Прилага се от 25 май 2018 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

1.2. Съответни области на политиката в структурата на УД/БД

1.3. Естество на предложението/инициативата

1.4. Цел(и)

1.5. Основания за предложението/инициативата

1.6. Срок на действие и финансово отражение

1.7. Планирани методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Система за управление и контрол

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

3.2.2. Очаквано отражение върху бюджетните кредити за оперативни разходи

3.2.3. Очаквано отражение върху бюджетните кредити за административни разходи

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Участие на трети страни във финансирането

3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО

1.2. Съответни области на политиката в структурата на УД/БД[25]

Правосъдие — Защита на лични данни

1.3. Естество на предложението/инициативата

☐ Предложението/инициативата е във връзка с **нова дейност**

☐ Предложението/инициативата е във връзка с **нова дейност след пилотен проект/подготвителна дейност**[26]

– Предложението/инициативата е във връзка с продължаване на съществуваща дейност

☐ Предложението/инициативата е във връзка с **дейност, пренасочена към нова дейност**

1.4. Цел(и)

1.4.1. Многогодишни стратегически цели на Комисията, за чието изпълнение е предназначено предложението/инициативата

Влизането в сила на Договора от Лисабон — и по-специално, въвеждането на ново правно основание (член 16 от ДФЕС) — дава възможност да бъде установена всеобхватна рамка за защита на данните, която включва всички области.

На 27 април 2016 г. Съюзът прие Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

[25] УД: управление по дейности; БД: бюджетиране по дейности.

[26] Съгласно член 54, параграф 2, буква а) или б) от Финансовия регламент.

В същия ден Съюзът прие Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

Настоящото предложение има за цел да завърши създаването на всеобхватна рамка за защита на данните в Съюза чрез привеждане на правилата за защита на данните, приложими за институциите и органите на Съюза, в съответствие със сдържащите се в Регламент (ЕС) 2016/679 правилата за защита на личните данни . От съображения за последователност и съгласуваност институциите и органите на Съюза следва да прилагат набор от правила за защита на данните, подобни на прилаганите от публичния сектор в държавите членки.

1.4.2. Конкретни цели и съответни дейности във връзка с УД/БД

Конкретна цел № 1:

Гарантиране на съгласуваното прилагане на правилата за защита на данните навсякъде в Съюза.

Конкретна цел № 2:

Рационализиране на сегашния модел на управление на защитата на данните в институциите и органите на Съюза.

Конкретна цел № 3:

Гарантиране на по-добро спазване и прилагане на правилата за защита на данните в институциите и органите на Съюза.

1.4.3. Очаквани резултати и отражение

Да се посочи въздействието, което предложението/инициативата следва да окаже по отношение на бенефициерите/целевите групи.

Що се отнася до институциите и органите на Съюза, те следва, в качеството си на администратори на данни, да извлекат полза от преминаването от сегашните (ex ante подход) административни процеси, свързани със защитата на данните, към ефективно спазване и по-строго прилагане на материалните правила за защита на данните и на новите принципи и понятия за защита на данните, въведени с Регламент (ЕС) 2016/679 (ex post подход), които ще бъдат приложими навсякъде в Съюза.

Лицата, чиито данни се обработват от институциите и органите на Съюза, ще упражняват по-добър контрол върху своите лични данни и ще имат по-голямо доверие в цифровата среда. Освен това ще съществува по-голяма отчетност от страна на институциите и органите на Съюза.

Европейският надзорен орган по защита на данните ще бъде в състояние да се съсредоточи в по-голяма степен върху своята надзорна роля. Разпределението на задачата за предоставяне на консултации на Комисията между Европейския комитет по защита на данните, създаден с Регламент (ЕС) 2016/679, и Европейския надзорен орган по защита на данните ще бъде изяснена и ще се избегне дублирането.

1.4.4. Показатели за резултатите и за отражението

Да се посочат показателите, които позволяват да се проследи изпълнението на предложението/инициативата.

Показателите включват следните елементи:

брой на становищата, издадени от Европейския комитет по защита на данните и Европейския надзорен орган по защита на данните,

разбивка на дейностите на длъжностните лица по защита на данните,

използването на оценките на въздействието върху защитата на данните,

брой жалби, подадени от субекти на данни,

санкции, наложени на администратори на данни, отговорни за нарушения във връзка със защитата на данни.

1.5. Основания за предложението/инициативата

1.5.1. Нужди, които трябва да бъдат задоволени в краткосрочен или дългосрочен план

В Регламент (ЕС) 2016/679 (член 2, параграф 3, член 98, съображение 17) съзаконодателите на Съюза призовават за адаптиране на Регламент (ЕО) № 45/2001 към принципите и правилата, установени в Регламент (ЕС)

2016/679, с цел да се осигури силна и съгласувана рамка за защита на данните в Съюза и да се позволи започване на прилагането на двата инструмента по същото време, т.е. на 25 май 2018 г.

1.5.2. Добавена стойност от намесата на ЕС

Правилата за защита на данните, приложими за институциите и органите на Съюза, могат да бъдат въведени само чрез акт на ЕС.

1.5.3. Изводи от подобен опит в миналото

Настоящото предложение се основава на опита с Регламент (ЕО) № 45/2001 и оценката на неговото прилагане, направена в проучване за оценка (извършена от външен изпълнител между септември 2014 г. и юни 2015 г.)[27].

1.5.4. Съвместимост и евентуална синергия с други подходящи инструменти

Настоящото предложение се основава на Регламент (ЕС) 2016/679 и завършва изграждането на стабилна, съгласувана и съвременна рамка за защита на данните в Съюза, която е технологично неутрална и съобразена с бъдещото развитие.

[27] JUST/2013/FRAC/FW/0157/A4 в контекста на рамков договор за многократно предоставяне на услуги; JUST/2011/EVAL/01 (RS 2013/05) — Evaluation Study on Regulation (EC) 45/2001 (Проучване за оценка относно Регламент (ЕО) № 45/2001), Ernst and Young

1.6. Срок на действие и финансово отражение

☐ Предложение/инициатива с **ограничен срок на действие**

– ☐ Предложение/инициатива в сила от [ДД/ММ]ГГГГ до [ДД/ММ]ГГГГ

– ☐ Финансово отражение от ГГГГ до ГГГГ

- Предложение/инициатива с **неограничен срок на действие**
- Осъществяване с период на започване на дейност от [2017] г. до 25 май 2016 г., последван от функциониране с пълен капацитет.

1.7. Планирани методи на управление[28]

- Пряко управление от Комисията

– ☐ от нейните служби, включително от нейния персонал в делегациите на Съюза;

– ☐ от изпълнителните агенции

☐ **Споделено управление** с държавите членки

☐ **Непряко управление** чрез възлагане на задачи по изпълнението на бюджета на:

– ☐ трети държави или органите, определени от тях;

– ☐ международни организации и техните агенции (да се уточни);

– ☐ ЕИБ и Европейския инвестиционен фонд;

– ☐ органите, посочени в членове 208 и 209 от Финансовия регламент;

– ☐ публичноправни органи;

– ☐ частноправни органи със задължение за обществена услуга, доколкото предоставят подходящи финансови гаранции;

– ☐ органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и които предоставят подходящи финансови гаранции;

– ☐ лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.

[28] Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

– *Ако е посочен повече от един метод на управление, пояснете в частта „Забележки“.*

Бележки

Настоящото предложение се ограничава до и засяга всички институции и органи на Съюза.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Настоящото предложение се ограничава до прилагането на правила за защита на данните от институциите и органите на Съюза. Надзорът и прилагането на тези правила е задача, която се осъществява от Европейския надзорен орган по защита на данните. Поради това наблюдението и докладването се извършват от Европейския надзорен орган по защита на данните. По-специално по силата на член 60 от настоящото предложение Европейският надзорен орган по защита на данните е задължен да представя годишен доклад за дейността си пред Европейския парламент, Съвета и Комисията, като същевременно го огласява публично.

2.2. Система за управление и контрол

2.2.1. Установени рискове

В периода между септември 2014 г. и юни 2015 г. от външен изпълнител бе направено проучване за оценка на прилагането на Регламент (ЕО) № 45/2001. В него също така се разглежда въздействието от въвеждането на ключовите понятия и принципи на Регламент (ЕС) 2016/679 в рамките на институциите и органите на Съюза.

Новият модел за защита на данните ще се съсредоточи върху ефективното спазване на правилата за защита на данните и ефективния надзор и прилагане на тези правила. Това ще изисква промяна на културата на защита на данните в институциите и органите на Съюза, като се премине от административен *ex ante* подход към осигуряване на ефективен *ex post* подход.

2.2.2. Информация за изградената система за вътрешен контрол

Съществуващите методи на контрол, прилагани от институциите и органите на Съюза.

2.2.3. Оценка на разходите и ползите от проверките и на очаквания риск от грешка

Съществуващите методи на контрол, прилагани от институциите и органите на Съюза.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита.

Съществуващите мерки за предотвратяване на измами, прилагани от институциите и органите на Съюза.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

- Съществуващи бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
	Номер [Функция.....]	Многогод./едногод.[29].	от държави от ЕАСТ[30]	от държави кандидатки [31]	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
	[XX.YY.YY.YY]	Многогод./едногод.	ДА/НЕ	ДА/НЕ	ДА/НЕ	ДА/НЕ

- Поискани нови бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
	Номер [Функция.....]	Многогод./едногод.	от държави от ЕАСТ	от държави кандидатки	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
	[XX.YY.YY.YY]		ДА/НЕ	ДА/НЕ	ДА/НЕ	ДА/НЕ

[29] Многогод. = многогодишни бюджетни кредити / Едногод. = едногодишни бюджетни кредити

[30] ЕАСТ: Европейска асоциация за свободна търговия.

[31] Държави кандидатки и ако е приложимо, държави потенциални кандидатки от Западните Балкани.

3.2. Очаквано отражение върху разходите

Въздействието върху разходите на настоящото предложение се ограничава до разходите на институциите и органите на Съюза. При все това оценката на разходите, свързани с настоящото предложение, показва, че то не създава значителни допълнителни разходи за институциите и органите на Съюза.

Що се отнася до администраторите на данни в институциите и органите на Съюза, проучването за оценка на Регламент (ЕО) № 45/2001 показва, че техните дейности по защита на данните отговарят на около 70 еквивалента на пълно работно време (ЕПРВ), т.е. около 9,3 милиона евро годишно. Понастоящем около 20 % от техните дейности по защита на данните са посветени на уведомления за обработване на данни. Тази дейност е премахната в настоящия регламент, което съответства на годишни икономии от 1,922 милиона евро за администраторите на данни в институциите и органите на Съюза. Тези икономии се очаква да бъдат балансирани от увеличените инвестиции на администраторите на данни при прилагането на новите принципи и понятия, въведени с настоящия регламент.

По-точно резултатите от анкетата, проведена в рамките на проучването за оценка посочиха, че въвеждането на:

а) принципа за свеждане до минимум на данните би довело до минимално или никакво въздействие върху институциите и органите на Съюза;

б) принципа за прозрачност не би имало значимо въздействие върху институциите и органите на Съюза;

в) нарасналите задължения за предоставяне на информация ще увеличат работното натоварване на администраторите на лични данни и на длъжностните лица по защита на данните;

г) правото „да бъдеш забравен“ не би имало значимо въздействие върху институциите и органите на Съюза;

д) правото на преносимост на данните би довело до минимално или никакво въздействие върху институциите и органите на Съюза;

е) оценки на въздействието върху защитата на данните би било умерено значимо за работното натоварване на администраторите на данни и на длъжностните лица по защита на данните, тъй като някои институции и органи на Съюза вече се извършват оценки на въздействието и случаите, в които такава оценка на въздействието върху защитата на данните ще трябва да бъдат извършвани, са ограничени;

ж) уведомления за нарушения на сигурността на личните данни ще доведе до увеличаване на работното натоварване на администраторите на данни, но подобни нарушения не са чести;

з) защита на данните на етапа на проектирането и по подразбиране вече се използва в няколко институции и органи на Съюза.

Освен това в оценката на въздействието, извършена преди приемането на предложението за пакет за реформа в областта на защитата на данните, съдържа заключението, че „никаква административна тежест няма да бъде поета от публичните органи или администраторите на данни в резултат на въвеждането на принципа за защита на данните на етапа на проектирането“.[32]

По отношение на длъжностните лица по защита на данните в проучването за оценка разходите на настоящата мрежа от длъжностни лица по защита на данните (ДЛЗД) и координатори за защита на данните (КЗД) в институциите и органите на Съюза се оценяват на 82,9 ЕПРВ или 10,9 милиона евро годишно. Те прекарват 26 % от времето си, посветено на защита на данните, за дейностите, отменени с настоящия регламент, т.е. изготвяне на уведомления (вместо администраторите на данни), извършване на оценка на получените уведомления и поддържане на записите в регистъра и изпълнение на предварителни проверки. Това води до допълнителни икономии в размер на 2,834 милиона евро годишно за институциите и органите на Съюза. Освен това настоящият регламент създава възможност за потенциални допълнителни икономии, като позволява на институциите и органите на Съюза да възлагат на външни изпълнители дейности на ДЛЗД, вместо да използват собствени служители за тази цел.

Спестяванията по отношение на дейностите на ДЛЗД ще бъдат балансирани чрез участието на ДЛЗД в увеличените задължения за предоставяне на информация, оценките на въздействието върху защитата на данните (при ограничените обстоятелства, при които те ще се изискват) и предварителното консултиране с Европейския надзорен орган по защита на данните (чийто обхват ще бъде далеч по-ограничен, отколкото сегашното задължение за предварителна проверка).

Що се отнася до Европейския надзорен орган по защита на данните, годишният му бюджет е сравнително стабилен от 2011 г. насам и възлиза на приблизително 8 милиона евро. Понастоящем неговият отдел за надзор и прилагане и отделът за политики и консултации имат приблизително еднакъв брой служители, който е сравнително постоянен от 2008 г. насам. Повишеното внимание, което се отделя в настоящия регламент на надзорната роля на Европейския надзорен орган по защита на данните, ще бъде балансирано с по-целенасочена консултативна роля и премахването на дублирането на задачи с Европейския комитет по защита на данните. Поради това преразпределението на персонал на Европейския надзорен орган по защита на данните може да бъде извършено вътрешно.

[32] Работен документ на службите на Комисията, „Оценка на въздействието“, SEC (2012) 72 final, страница 110.

В настоящото предложение се предвижда възможността за Европейския надзорен орган по защита на данните да налагат административнонаказателни имуществени санкции на институции и органи на Съюза. На всяка институция или орган на Съюза, може да бъде наложена имуществена санкция в размер до 250 000 EUR годишно (25 000 EUR за всяко отделно нарушение), или 500 000 EUR годишно (50 000 EUR за всяко отделно нарушение) за най-тежките нарушения на настоящия регламент. Очаква се тези санкции да се прилагат само в най-тежките случаи и след неспазване на регламента от институция или орган на Съюза в отговор на упражнени други корективни правомощия от страна на Европейския надзорен орган по защита на данните. Поради това се очаква финансовото въздействие на тези санкции да бъде ограничено.

3.2.1. Обобщение на очакваното отражение върху разходите

млн. EUR (до третия знак след десетичната запетая)

Функция от многогодишната финансова рамка	Номер	[Функция.....]

ГД: <…….>			Година **N**[33]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
• Бюджетни кредити за оперативни разходи										
Номер на бюджетния ред	Поети задължения	(1)								
	Плащания	(2)								
Номер на бюджетния ред	Поети задължения	(1a)								
	Плащания	(2a)								
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми[34]										

33 Година N е годината, през която започва да се осъществява предложението/инициативата.

34 Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

Номер на бюджетния ред		(3)								
ОБЩО бюджетни кредити за ГД<…….>	Поети задължения	=1+1a +3								
	Плащания	=2+2a +3								

•ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)								
	Плащания	(5)								
• ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)								
ОБЩО бюджетни кредити Междинен сбор за ФУНКЦИЯ <….> от многогодишната финансова рамка	Поети задължения	=4+ 6								
	Плащания	=5+ 6								

<u>Ако предложението/инициативата има отражение върху повече от една функция:</u>

•ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)								
	Плащания	(5)								
• ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)								
ОБЩО бюджетни кредити за ФУНКЦИИ 1—4 от многогодишната финансова рамка (Референтна стойност)	Поети задължения	=4+ 6								
	Плащания	=5+ 6								

Функция от многогодишната финансова рамка	**5**	„Административни разходи“

млн. EUR (до третия знак след десетичната запетая)

		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ГД: <…….>									
• Човешки ресурси									
Други административни разходи									
ОБЩО ГД <…….>	Бюджетни кредити								

ОБЩО бюджетни кредити за ФУНКЦИЯ 5 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)								

млн. EUR (до третия знак след десетичната запетая)

		Година **N**[35]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ОБЩО бюджетни кредити за ФУНКЦИИ 1—5 от многогодишната финансова рамка	Поети задължения								
	Плащания								

[35] Година N е годината, през която започва да се осъществява предложението/инициативата.

3.2.2. Очаквано отражение върху бюджетните кредити за оперативни разходи

- Предложението/инициативата не налага използване на бюджетни кредити за оперативни разходи

☐ Предложението/инициативата налага използване на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

Бюджетни кредити за поети задължения в млн. EUR (до третия знак след десетичната запетая)

Да се посочат целите и резултатите			Година **N**		Година **N+1**		Година **N+2**		Година **N+3**		Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)						**ОБЩО**	
	РЕЗУЛТАТИ																	
⇩	Вид[36]	Среден разход	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Общ брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[37]…																		
— Резултат																		
— Резултат																		
— Резултат																		
Междинен сбор за конкретна цел № 1																		
КОНКРЕТНА ЦЕЛ № 2…																		
— Резултат																		
Междинен сбор за конкретна цел № 2																		

[36] Резултатите са продуктите и услугите, които ще бъдат доставени (напр. брой финансирани обмени на студенти, брой км построени пътища и т.н.).

[37] Съгласно описанието в точка 1.4.2. „Конкретни цели…“.

ОБЩО РАЗХОДИ																

3.2.3. Очаквано отражение върху бюджетните кредити за административни разходи

3.2.3.1. Обобщение

- Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

☐ Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. EUR (до третия знак след десетичната запетая)

	Година **N** [38]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ФУНКЦИЯ 5 от многогодишната финансова рамка								
Човешки ресурси								
Други административни разходи								
Междинна сума за ФУНКЦИЯ 5 от многогодишната финансова рамка								

извън ФУНКЦИЯ 5[39] **от многогодишната финансова рамка**								
Човешки ресурси								
Други разходи с административен характер								
Междинна сума извън ФУНКЦИЯ 5 от многогодишната финансова рамка								

ОБЩО								

Нуждите от бюджетни кредити за човешки ресурси и за другите разходи с административен характер ще бъдат покрити с бюджетните кредити на ГД, които вече са отпуснати за управлението на дейността и/или които са преразпределени в

38 Година N е годината, през която започва да се осъществява предложението/инициативата.

39 Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

рамките на ГД, при необходимост заедно с всички допълнителни ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

3.2.3.2. Очаквани нужди от човешки ресурси

- Предложението/инициативата не налага използване на човешки ресурси.

☐ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в еквиваленти на пълно работно време

	Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
• Длъжности в щатното разписание (длъжностни лица и временно наети лица)							
XX 01 01 01 (Централа и представителства на Комисията)							
XX 01 01 02 (Делегации)							
XX 01 05 01 (Непреки научни изследвания)							
10 01 05 01 (Преки научни изследвания)							
• Външен персонал (в еквивалент на пълно работно време: ЕПРВ)[40]							
XX 01 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)							
XX 01 02 02 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)							
XX 01 04 **yy** [41] — в централата							
XX 01 04 **yy** [41] — делегациите							
XX01 05 02 (ДНП, КНЕ, ПНА — Непреки научни изследвания)							
10 01 05 02 (ДНП, ПНА, КНЕ — Преки научни изследвания)							

40 ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

41 Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

Други бюджетни редове (да се посочат)							
ОБЩО							

XXе съответната област на политиката или бюджетен дял.

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и временно наети служители	
Външен персонал	

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

- Предложението/инициативата е съвместимо(а) с настоящата многогодишна финансова рамка.

☐ Предложението/инициативата налага препрограмиране на съответната функция от многогодишната финансова рамка.

Обяснете какво препрограмиране е необходимо, като посочите съответните бюджетни редове и суми.

☐ Предложението/инициативата налага да се използва Инструментът за гъвкавост или да се преразгледа многогодишната финансова рамка.

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми.

3.2.5. Участие на трети страни във финансирането

- Предложението/инициативата не предвижда съфинансиране от трети страни.

Предложението/инициативата предвижда съфинансиране съгласно следните прогнози:

Бюджетни кредити в млн. EUR (до третия знак след десетичната запетая)

	Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

3.3. Очаквано отражение върху приходите

- Предложението/инициативата няма финансово отражение върху приходите.

☐ Предложението/инициативата има следното финансово отражение:

– ☐ върху собствените ресурси

– ☐ върху разните приходи

млн. EUR (до третия знак след десетичната запетая)

Приходен бюджетен ред:	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата[42]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
член …….								

За разните „целеви“ приходи да се посочат съответните разходни бюджетни редове.

Да се посочи методът за изчисляване на отражението върху приходите.

[42] Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднати 25 % за разходи по събирането.