Съвет на
Европейския съюз

Брюксел, 31 март 2016 г.
(OR. en)

Междуинституционално досие:
2012/0011 (COD)

5419/16
ADD 1 REV 1

DATAPROTECT 2
JAI 38
MI 25
DIGIT 21
DAPIX 9
FREMP 4
CODEC 52

ПРОЕКТ ЗА ИЗЛОЖЕНИЕ НА МОТИВИТЕ НА СЪВЕТА

Относно:	Позиция на Съвета на първо четене с оглед на приемането на РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА 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) — Проект за изложение на мотивите на Съвета

I. ВЪВЕДЕНИЕ

На 25 януари 2012 г. Комисията предложи всеобхватна реформа в областта на защитата на данните, състояща се от:

— посоченото по-горе предложение за общ регламент относно защитата на данните, което е предназначено да замени Директивата за защита на данните от 1995 г. (бивш първи стълб);

— предложение за директива 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 наказателни санкции и относно свободното движение на такива данни, което е предназначено да замени Рамковото решение за защита на данните от 2008 г. (бивш трети стълб).

На 12 март 2014 г. Европейският парламент прие позицията си на първо четене по предложението за общ регламент относно защитата на данните (док. 7427/14).

На 15 юни 2015 г. Съветът постигна съгласие по общ подход, като по този начин предостави на председателството мандат за водене на преговори, за да встъпи в тристранни разговори с Европейския парламент (док. 9565/15).

Европейският парламент и Съветът, на равнището на Комисията по граждански свободи, правосъдие и вътрешни работи и Комитета на постоянните представители, потвърдиха съответно на 17 и 18 декември 2015 г. съгласието си по компромисния текст, изготвен в резултат на тристранните преговори.

На заседанието си от 12 февруари 2016 г. Съветът постигна политическо споразумение по проекта за регламент (док. 5455/15). На заседанието си от 21 април 2016 г. Съветът прие позицията си на първо четене, която е изцяло в съответствие с компромисния текст на регламента, договорен по време на неформалните преговори между Съвета и Европейския парламент.

Европейският икономически и социален комитет даде становище по регламента през 2012 г. (ОВ C 229, 31.7.2012 г., стр. 90).

Комитетът на регионите даде становище по регламента (ОВ C 391, 18.12.2012 г., стр. 127).

Европейският надзорен орган по защита на данните беше консултиран и даде първо становище през 2012 г. (ОВ C 192, 30.6.2012 г., стр. 7) и второ становище през 2015 г. (ОВ C 301, 12.9.2015 г., стр. 1-8).

Агенцията за основните права даде становището си на 1 октомври 2012 г.

II. ЦЕЛ

В Общия регламент относно защитата на данните се хармонизират правилата за защита на данните в Европейския съюз. Целите на регламента са да се укрепят правата на физическите лица в областта на защитата на данните, да се улесни свободното движение на лични данни на единния пазар и да се намали административната тежест.

III. АНАЛИЗ НА ПОЗИЦИЯТА НА СЪВЕТА НА ПЪРВО ЧЕТЕНЕ

A. Общи бележки

В контекста на целта на Европейския съвет за постигане до края на 2015 г. на споразумение относно реформата в областта на защитата на данните, Европейският парламент и Съветът проведоха неформални преговори за сближаване на позициите си. Текстът на позицията на Съвета на първо четене по Общия регламент относно защитата на данните изцяло отразява компромиса, постигнат между двамата съзаконодатели със съдействието на Европейската комисия.

Позицията на Съвета на първо четене запазва целите на Директива 95/46/ЕО: защита на правата на защита на данните и свободното движение на лични данни. Същевременно тя се стреми да адаптира действащите правила за защита на данните в светлината на нарастващия обем на обработваните лични данни в резултат на технологичните промени и глобализацията. С оглед на това регламентът да бъде адекватен спрямо бъдещето, правилата за защита на данните в позицията на Съвета на първо четене са технологично неутрални.

За да се гарантира съгласувано ниво на защита на физическите лица в целия Съюз и за да се предотвратят различията, възпрепятстващи свободното движение на лични данни в рамките на вътрешния пазар, позицията на Съвета на първо четене до голяма степен предвижда единен набор от правила, които са пряко приложими на територията на целия Съюз. Това хармонизиране ще сложи край на фрагментарността, произтичаща от различните закони на държавите членки, прилагащи Директива 95/46. Все пак, за да се вземат под внимание изискванията, свързани с особени ситуации на обработване на данни, включително за публичния сектор, позицията на Съвета на първо четене дава възможност на държавите членки да уточнят допълнително как ще прилагат в националното си право предвидените в регламента правила за защита на данните.

Защитата на личните данни е основно право, заложено в член 8, параграф 1 от Хартата на основните права на Европейския съюз. Член 16 от Договора за функционирането на Европейския съюз постановява, че всеки има право на защита на личните си данни, независимо от националността или местопребиваването си, и че за тази цел и за целта на свободното движение на лични данни следва да се определят правила. Въз основа на това в позицията на Съвета на първо четене се определят принципите и правилата относно защитата на физическите лица по отношение на обработването на техните лични данни.

За да се постигнат целите на регламента, в позицията на Съвета на първо четене се предвиждат по-строги изисквания за отчетност на администраторите (отговарящи за определянето на целите и средствата за обработването на личните данни) и обработващите лични данни (отговарящи за обработването на личните данни от името на администраторите), което създава истинска култура на защита на данните. В този контекст в целия регламент се въвежда основан на риска подход, който дава възможност за адаптиране на задълженията на администратора и обработващия лични данни в зависимост от риска, свързан с извършваното от тях обработване на данни. Наред с това, за спазването на правилата за защита на данните допринасят кодекси за поведение и механизми за сертифициране. Този подход предотвратява въвеждането на прекалено ограничителни правила и намалява административната тежест, без това да засяга съответствието. Нещо повече, възпиращият характер на потенциалните санкции, които могат да бъдат наложени, създава стимули за администраторите да спазват регламента.

Наред с това новите правила за защита на данните, изложени в позицията на Съвета на първо четене, водят и до засилени и приложими права за гражданите. Това дава възможност на физическите лица да упражняват по-добър контрол върху личните си данни, което води до по-голямо доверие в онлайн услугите в трансграничен мащаб, което пък ще активизира цифровия единен пазар. За децата следва да се осигури специална защита, тъй като може те да са по-слабо осведомени за рисковете, свързани с обработването на лични данни, както и за правата си.

Освен това в позицията на Съвета на първо четене се укрепва независимостта на надзорните органи, като същевременно се хармонизират техните задачи и правомощия. Правилата за сътрудничество между надзорните органи и когато е подходящо, Комисията при трансгранични случаи (механизъм за съгласуваност) ще допринесат за последователното прилагане на регламента в целия Европейски съюз. Това ще предостави по-голяма правна сигурност и ще намали административната тежест. Наред с това механизмът „обслужване на едно гише“ ще доведе до наличието на един-единствен партньор за администраторите и обработващите лични данни във водените от тях трансгранични производства, включително обвързващи решения по спорове, постановени от новосъздадения Европейски комитет по защита на данните. Благодарение на този механизъм регламентът ще се прилага по-съгласувано. Наред с това той ще предостави по-голяма правна сигурност и ще намали административната тежест.

И накрая, позицията на Съвета на първо четене установява всеобхватна рамка за предаване на лични данни от Европейския съюз на получатели в трети държави или в международни организации, с което предоставя нови инструменти в сравнение с Директива 95/46/ЕО.

Б. Ключови въпроси

Съветът и Европейският парламент, със съдействието на Европейската комисия, съгласуваха чрез неформални преговори позициите си, определени съответно в общия подход на Съвета и в позицията на Европейския парламент на първо четене. Позицията на Съвета на първо четене по Общия регламент относно защитата на данните изцяло отразява постигнатия компромис. Основните елементи на позицията на Съвета на първо четене са изложени по-долу.

1. Обхват

1.1. Материален обхват на регламента и разграничаване с Директивата в областта на правоприлагането

Позицията на Съвета на първо четене предвижда, че Общият регламент относно защитата на данните се прилага за обработването на лични данни, извършвано изцяло или частично с автоматизирани средства, както и за обработването с други средства на лични данни, които са част от структуриран набор от лични данни, достъпни съгласно определени критерии, или които са предназначени да съставляват част от такъв структуриран набор. Материалният обхват на Общия регламент относно защитата на данните и обхватът на Директивата за защита на данните в областта на правоприлагането са взаимно изключващи се. В регламента е посочено, че той не се прилага по отношение на обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, изпълнението на наказателни санкции, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване. Това ограничение дава възможност на правоприлагащите органи, и по-специално на полицията, принципно да прилагат предвидения в директивата режим на защита на данните, като същевременно гарантира съгласувана защита на високо равнище на личните данни на физическите лица — обект на операции по правоприлагане.

1.2. Институции и органи на ЕС

За да се осигури единна и съгласувана защита на субектите на данни по отношение на обработването на техните лични данни, в позицията на Съвета на първо четене се посочва, че необходимите изменения на Регламент (ЕО) № 45/2001, който се прилага за институциите, органите, службите и агенциите на ЕС, следва да се осъществят след приемането на Общия регламент относно защитата на данните, за да може той да е приложим едновременно с Общия регламент относно защитата на данните.

1.3. Изключение във връзка с домашни дейности

За да се избегне установяването на нормативна уредба, която ще създаде ненужна тежест за физическите лица, в позицията на Съвета на първо четене се предвижда, че регламентът не се прилага за обработването на лични данни от физическо лице в рамките на чисто лични или домашни дейности, които следователно нямат връзка с професионална или търговска дейност.

1.4. Териториален обхват

Позицията на Съвета на първо четене създава равни условия за администраторите и обработващите лични данни от гледна точка на териториалния обхват, като обхваща всички администратори и обработващи лични данни, независимо дали са установени в Съюза или не.

На първо място, в регламента се предвижда, че правилата за защита на данните се прилагат за обработването на лични данни в контекста на дейностите на администратор или обработващ лични данни на дадено място на установяване в Съюза, независимо дали обработването се извършва в Съюза или не. На второ място, за да се гарантира, че физическите лица не са лишени от защита на своите данни, регламентът се прилага за обработването на лични данни на субекти на данни, които са в рамките на Съюза, дори ако администраторът или обработващият лични данни не е установен в Съюза, но неговите дейности по обработване на данни са свързани с предлагането на стоки или услуги на такива субекти на данни в Съюза, както и с наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Европейския съюз. Освен това определянето на обхвата по такъв начин увеличава правната сигурност за администраторите и субектите на данни (физическите лица, чиито лични данни се обработват).

Също така в позицията на Съвета на първо четене се гарантира, че субектите на данни и надзорните органи разполагат с точка за контакт в ЕС, в случай че администраторите или обработващите лични данни не са установени в Съюза, но попадат под обхвата на действие на регламента: те трябва писмено да определят представител в Съюза. С цел да се избегне ненужната административна тежест, това задължение не се прилага за обработването на данни, което е малко вероятно да доведе до риск за правата и свободите на физическите лица, и за обработването от публичен орган или структура на третата държава.

2. Принципи, свързани с обработването на лични данни

Принципите за защита на данните се прилагат за всяка информация, отнасяща се до физически лица, които са идентифицирани или могат да бъдат идентифицирани, включително информация, която не може повече да бъде свързвана с конкретен субект на данни, без да се използва допълнителна информация, доколкото тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира невъзможността да се направи връзка с физическо лице, което е идентифицирано или което може да бъде идентифицирано (псевдонимизация). Спрямо Директива 95/46 регламентът до голяма степен осигурява приемственост по отношение на принципите, на които се основава обработването на лични данни. Същевременно принципът на „минимизиране на данните“ беше коригиран, за да се вземе под внимание цифровата реалност и с оглед на установяването на баланс между защитата на данните на физическите лица, от една страна, и възможностите за администраторите да обработват данни, от друга страна.

3. Законосъобразност на обработването

3.1. Условия за законосъобразност

С цел осигуряване на правна сигурност позицията на Съвета на първо четене се основава на Директива 95/46, като посочва, че обработването на лични данни е законосъобразно само ако е изпълнено най-малко едно от следните условия:

— съгласие на субекта на данни за една или повече конкретни цели;

— договор;

— правно задължение;

— защита на жизненоважни интереси на субекта на данни или на друго физическо лице;

— задача, изпълнявана в обществен интерес или при упражняването на официалните правомощия, които са предоставени на администратора;

— законни интереси, преследвани от администратор или от трета страна.

Две от условията е необходимо да бъдат допълнително уточнени: съгласие и законен интерес, преследван от администратор или от трета страна.

3.1.1. Съгласие

За да позволи обработването на личните си данни, субектът на данни може да даде съгласието си за това чрез ясно утвърдително действие, с което да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласието му свързаните с него лични данни да бъдат обработвани. Такова съгласие следва да обхваща всички дейности по обработване, извършвани за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях трябва да бъде дадено съгласие. Освен това администраторът трябва да може да докаже, че субектът на данни е дал съгласието си за операцията по обработване. Поради това мълчанието, предварително отметнатите полета или липсата на действие не представляват съгласие. Формулирането на понятието „съгласие“ осигурява приемственост спрямо достиженията на правото на ЕС по отношение на използването на това понятие въз основа на Директива 95/46/ЕО, като същевременно допринася за общото му разбиране и прилагане в целия Европейски съюз.

Наред с това, с оглед на защитата на правата за защита на данните на субекта на данни се уточнява, че ако той е дал съгласието си в контекста на писмена декларация, която се отнася и до други въпроси, никоя част от тази декларация, която представлява нарушение на регламента, не е обвързваща. Нещо повече, при преценката доколко съгласието е дадено свободно, трябва в най-голяма степен да се отчита дали, наред с другото, изпълнението на даден договор е обусловено от наличието на съгласие за обработване, което не е необходимо за изпълнението на договора.

Накрая, за да се даде възможност за дерогации от общата забрана за обработване на специални категории лични данни, в позицията на Съвета на първо четене се предвижда по-висок праг, отколкото за други видове обработване, тъй като субектът на данни трябва да даде изричното си съгласие за обработването на такива чувствителни лични данни.

Що се отнася до децата, позицията на Съвета на първо четене предвижда специален режим на защита за даването на съгласие от деца във връзка с предлагането на услуги на информационното общество. Обработването на личните данни на дете под максималната възраст от 16 години е законосъобразно, ако може да се провери, доколкото е възможно и като се вземат предвид наличните технологии, че такова съгласие е дадено или разрешено от носещия родителска отговорност за детето. Държавите членки, които считат, че е по-уместно да се предвиди по-ниска възрастова граница, имат право да определят по-малка максимална възраст, при условие че тя не е под 13 години.

3.1.2. Законен интерес на администратора

Обработването на лични данни може да бъде законосъобразно, ако е необходимо за целите на законните интереси, преследвани от администратор или от трета страна. Тези законни интереси обаче не са достатъчно основание за законосъобразно обработване, когато преимущество пред тях имат интересите или основните права и свободи на субекта на данни, които изискват защита на личните данни, по-специално когато субектът на данни е дете.

За установяването на законен интерес е необходима преценка, в т.ч. дали субектът на данни може по времето и в контекста на събирането на лични данни основателно да очаква, че може да се осъществи обработване за тази цел. Обработването на лични данни за целите на директния маркетинг може да се разглежда като осъществявано поради законен интерес. Като се има предвид, че е задължение на законодателя да уреди със закон правното основание за обработването на лични данни от публичните органи, това не се прилага спрямо обработването на лични данни от публичните органи при изпълнението на техните задачи.

3.2. Специфични правила на държавите членки, чрез които да се адаптира прилагането на регламента

Позицията на Съвета на първо четене дава възможност на държавите членки да запазят или да въведат по-конкретни разпоредби, които адаптират прилагането на заложените в регламента правила, ако личните данни се обработват с цел спазване на правно задължение или ако обработването е необходимо за задача, изпълнявана в обществен интерес или при упражняването на официалните правомощия, предоставени на администратора. Наред с това са предвидени дерогации, специфични изисквания и други мерки във връзка със специални операции по обработване, чрез които държавите членки съчетават правото на защита на личните данни с правото на свобода на изразяване и на информация, публичен достъп до официални документи, обработване на национални идентификационни номера, обработване в контекста на заетостта и обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели.

3.3. Допълнително обработване

Позицията на Съвета на първо четене предвижда, че обработването за друга цел, освен тази, за която личните данни са били събрани първоначално, е законосъобразно само ако това допълнително обработване е съвместимо с целите, за които личните данните са били първоначално обработени. Когато обаче субектът на данни е дал съгласието си или когато обработването се основава на правото на Съюза или на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество, за да се гарантират по-специално важни цели от широк обществен интерес, администраторът има право да обработва допълнително личните данни, независимо от съвместимостта на целите. Предвидени са повече права на субекта на данни в случай на допълнително обработване, по-специално по отношение на правото на информация и правото на възражение срещу по-нататъшното обработване, когато това не е необходимо за изпълнението на задача, осъществявана от съображения от обществен интерес.

За да установи дали дадена цел на допълнително обработване е съвместима с целта, за която първоначално са събрани данните, администраторът трябва да отчете, наред с другото, всички връзки между първоначалните цели и целите на предвиденото допълнително обработване, в какъв контекст са събрани личните данни, по-специално основателните очаквания на субекта на данни въз основа на неговите взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни, естеството им, последствията от предвиденото допълнително обработване на данни за субекта на данни и наличието на подходящи гаранции при операциите по първоначалното и предвиденото допълнително обработване.

3.4. Обработване на специални категории лични данни

На личните данни, които по своето естество са особено чувствителни, се полага специална защита, тъй като контекстът на тяхното обработване може да създаде значителни рискове за основните права и свободи на лицата. Поради тази причина позицията на Съвета на първо четене принципно запазва подхода на Директива 95/46 за забрана на обработването на специални категории лични данни.

Чрез дерогация от това правило в някои изчерпателно изброени случаи обработването на чувствителни данни е разрешено, например когато субектът на данни е дал изрично съгласие, когато обработването е необходимо по съображения, свързани със значим обществен интерес или когато обработването е необходимо за други цели, наред с другото, в областта на здравеопазването.

И накрая, в позицията на Съвета на първо четене се предвижда, че държавите членки могат да въведат допълнителни условия, включително ограничения, във връзка с обработването на генетични данни, биометрични данни или данни за здравословното състояние. Въпреки това тези допълнителни условия не трябва да възпрепятстват свободното движение на данни в Съюза.

4. Допълнителни права на субектите на данни

4.1. Въведение

Позицията на Съвета на първо четене оправомощава в още по-голяма степен субектите на данни, като им предоставя засилени права за защита на данните и въвежда задължения за администраторите. Сред правата на субектите на данни са правото на информация; на достъп до лични данни; на коригиране; на заличаване на личните данни, включително правото „да бъдеш забравен“; на ограничение на обработването; на преносимост на данните; на възражение, както и да не подлежат на решения, основани единствено на автоматизирано обработване, включително профилиране. Правата, които са претърпели важни промени в сравнение с Директива 95/46, са обяснени по-подробно по-долу.

Администраторите са задължени да улесняват упражняването на правата на субектите на данни и да обработват лични данни в съответствие с принципа на прозрачност, по-специално като предоставят информация за обработването на лични данни, което извършват.

Ако обработваните от администратора лични данни не му позволяват да идентифицира даден субект на данни, администраторът на данни не е задължен да се сдобие с допълнителна информация, за да идентифицира субекта на данни единствено с цел спазване на някоя от разпоредбите на регламента.

Независимо от тези права на субектите на данни и задължения на администраторите, позицията на Съвета на първо четене запазва подхода на Директива 95/46, като дава възможност за ограничения на общите принципи и на правата на лицето, ако въпросните ограничения се основават на правото на Съюза или на държава членка. Тези ограничения трябва да зачитат същността на основните права и свободи и да са необходими и пропорционални в едно демократично общество с оглед на защитата на определени обществени интереси.

4.2. Прозрачност

В съответствие с принципа на прозрачност администраторите трябва да предоставят информация и съобщения, свързани с обработването на лични данни, в сбита, прозрачна, разбираема и лесно достъпна форма, като използват ясни и недвусмислени формулировки, особено при всяка информация, адресирана до дете. Информацията се предоставя писмено или по друг начин, а когато е целесъобразно в електронна форма.

В позицията на Съвета на първо четене се определят още срокове за искания за информация, съобщения или други действия на администратора, които по принцип трябва да се извършват безплатно. Когато исканията от даден субект на данни обаче са очевидно неоснователни или прекомерни, по-специално поради своята повтаряемост, администраторът може да начисли такса в разумен размер, като взема предвид административните разходи за предоставяне на информацията или съобщението или предприемане на исканото действие, или може да откаже да предприеме действия по искането. В тези случаи администраторът носи тежестта на доказване на очевидно неоснователния или прекомерен характер на искането.

4.3. Информация и съобщения, които трябва да бъдат предоставени от администратора

С цел постигане на баланс между предоставянето на достатъчно информация на субектите на данни относно обработването на личните им данни, от една страна, и избягването на обременителните задължения за предоставяне на информация от администраторите, от друга страна, позицията на Съвета на първо четене предвижда двуетапен подход, за да се гарантира, че субектите на данни са подходящо информирани както в случаите, когато личните данни са получени от субекта на данни, така и в случаите, когато те не са получени от него. Като първа стъпка, администраторът е длъжен в момента на получаване на личните данни да предостави на субекта на данни посочената в регламента информация. Като втора стъпка, администраторът трябва да предостави допълнителната информация, която е посочена в регламента и е необходима за осигуряване на добросъвестно и ефикасно обработване. Също така администраторите информират субектите на данни, когато възнамеряват да извършат допълнително обработване за цел, различна от целта, за която личните данни са събрани първоначално.

Администраторът не е длъжен да предоставя информацията, посочена в първата или втората стъпка, когато субектът на данни вече разполага с тази информация. Когато личните данни не са получени от субекта на данни, администраторът не дава никаква информация на субекта на данни, в случай че записването или разкриването на лични данни на други страни е изрично предвидено със закон или ако предоставянето на информация на субекта на данни се окаже невъзможно или изисква непропорционално големи усилия.

И накрая, администраторите са длъжни да съобщават за всяка корекция, заличаване или ограничаване на обработването на данни на всеки получател, на когото са били разкрити личните данни, освен ако това е невъзможно или изисква непропорционално големи усилия. Освен това администраторът трябва да информира субекта на данни относно тези получатели, ако субектът на данни поиска това.

4.4. Икони

Принципът на прозрачно обработване изисква субектът на данни да бъде информиран за осъществяването на обработването и за неговите цели. В този контекст позицията на Съвета на първо четене предвижда, че предоставянето на информация на субекта на данни може да бъде придружено със стандартизирани икони. Администраторите могат да решават на доброволна основа дали използването на тези стандартизирани икони би било полезно за извършваното от тях обработване на лични данни. Иконите следва да представят по лесно видим, разбираем и ясно четим начин смислен обзор на планираното обработване. Иконите трябва да се предоставят едновременно с информацията. Ако иконите се представят в електронен вид, те трябва да бъдат машинночетими. За да се допринесе за стандартизираното използване на икони в ЕС, регламентът дава правомощия на Комисията да приема делегирани актове за определяне на информацията, която следва да представят иконите, както и на процедурите за предоставянето на стандартизирани икони. Европейският комитет по защита на данните трябва да даде становище относно предложените от Комисията икони. Възможността за приемане на делегирани актове не възпрепятства Европейския комитет по защита на данните да издава насоки, становища и добри практики относно иконите.

4.5. Право на достъп

Субектът на данни има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако такива лични данни се обработват, да получи достъп до посочената в регламента информация. Във връзка с това в регламента се посочва, че администраторът трябва безплатно да предостави копие от личните данни, които се обработват. За допълнителни копия, поискани от субекта на данни, администраторът може да наложи разумна такса въз основа на административните разходи. Правото на получаване на копие не влияе неблагоприятно върху правата и свободите на други лица.

4.6. Право на заличаване (право „да бъдеш забравен“)

Позицията на Съвета на първо четене дава право на субектите на данни свързаните с тях лични данни да бъдат заличени, когато обработването на тези данни не е в съответствие с регламента или с правото на Съюза или на държава членка, което се прилага спрямо администратора.

„Правото да бъдеш забравен“ се споменава с оглед на необходимостта от адаптиране на правото на заличаване, по-специално в контекста на цифровизацията. Администратори, които са оповестили публично лични данни, които субектът на данни желае да бъдат забравени, е длъжен да предприеме разумни мерки, включително от технически характер, за да информира администраторите, които обработват личните данни за искането на субекта на данни за заличаване на връзките към такива данни или на копията или репликите на тези данни, като се вземат предвид наличните технологии и разходите за прилагане. Европейският комитет по защита на данните може да издава насоки, препоръки и добри практики относно процедурите за заличаването на връзки, копия или реплики на личните данни от обществено достъпни съобщителни услуги.

Правото на заличаване и задължението на администратора да информира другите администратори за искането за заличаване не се прилага, доколкото обработването на лични данни е необходимо за целите, които са изчерпателно изброени в регламента, като правото на свобода на изразяване и на информация.

4.7. Право на преносимост на данните

В позицията на Съвета на първо четене се посочва, че когато обработването на личните данни се извършва с автоматизирани средства, субектите на данни имат право да получат отнасящите се до тях лични данни, които са предоставили на администратора, в структуриран, широко използван, оперативно съвместим и машинночетим формат, и да ги предадат на друг администратор. Освен това следва да се уточни, че когато това е технически осъществимо, субектите на данни имат право личните им данни да бъдат предавани пряко от един администратор на друг. Това допълнително засилва контрола на субектите на данни върху техните данни. Освен това по този начин се насърчава конкуренцията между администраторите.

Правото на преносимост на данните обаче не се отнася до обработването, необходимо за задача, изпълнявана в обществен интерес, или при упражняването на официалните правомощия, които са предоставени на администратора. Освен това когато в определен набор от лични данни участва повече от един субект на данни, правото на субекта на данни да получи личните данни не засяга правата и свободите на останалите.

4.8. Право на възражение

В случаите, когато личните данни биха могли да се обработват законно, тъй като обработването е необходимо за задача, изпълнявана в обществен интерес или при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или на трета страна, субектът на данни има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. В този случай администраторът вече няма право да обработва 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.

В този контекст следва да се уточни, че когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време на възражение срещу обработването на отнасящите се до него лични данни. Това включва профилирането, доколкото то е свързано с такъв директен маркетинг. „Профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използване на тези данни за оценяване на някои лични аспекти, свързани с дадено физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения, икономическото състояние, здравето, личните предпочитания, интересите, надеждността, поведението, местоположението или движението на това физическо лице. Когато субектът на данни възрази срещу обработването на данните за целите на директния маркетинг, обработването на личните данни за тези цели вече не е позволено. Нещо повече, това право трябва да бъде изрично и ясно представено на вниманието на субекта на данни най-късно при осъществяване на първия контакт на администратора на лични данни със субекта на данни.

Освен това в позицията на Съвета на първо четене се споменава онлайн функцията „не ме проследявай“, като се уточнява, че в контекста на използването на услугите на информационното общество субектът на данни може да упражнява правото си на възражение чрез автоматизирани средства посредством използване на тези технически спецификации.

4.9. Автоматизирано вземане на индивидуални решения, включително профилиране

Субектът на данни има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, което оценява свързани с него лични аспекти и поражда правни последици за него или по подобен начин го засяга в значителна степен. Примери за това са автоматичен отказ на онлайн искания за кредит или практики за електронно набиране на персонал без човешка намеса. Това автоматизирано обработване на данни може да включва профилиране. Правото да не бъде обект на такова автоматизирано обработване обаче не се прилага:

— когато е необходимо за сключването или изпълнението на договор между субекта на данни и администратора;

— когато е разрешено от правото на Съюза или на държава членка, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на правата и свободите и законните интереси на субекта на данни, като наблюдението на измамите и на укриването на данъци; или

— когато се основава на изричното съгласие на субекта на данни.

Освен във втория случай, отнасящ се до обработване, разрешено съгласно правото на Съюза или на държава членка, администраторът, който извършва обработването с автоматизирани средства, трябва да осигури подходящи гаранции по отношение на правата и свободите на субектите на данни, както и на законните им интереси. Тези гаранции трябва да включват най-малко правото на получаване на човешка намеса от страна на администратора и възможността субектът на данни да изрази гледната си точка и да оспори решението. Освен това, за да се гарантира добросъвестно и прозрачно обработване, администраторите следва да използват подходящи математически и статистически процедури за профилирането и мерки, които да сведат до минимум потенциалните рискове за интересите на субектите на данни.

Субектът на данни разполага с допълнителни права, тъй като администраторът е длъжен да му предостави, когато е необходимо, за да се гарантира добросъвестно и прозрачно обработване, информация за наличието на автоматизирано вземане на решения, включително профилиране, и поне в тези случаи съдържателна информация относно приложената логика, както и значението и очакваните последствия от това обработване за субекта на данни.

И накрая, автоматизираното вземане на решения и профилирането на базата на специални категории лични данни се разрешава само при специфични условия, включително правото на субекта на данни на възражение срещу такова обработване, когато тези лични данни се обработват за научни или исторически изследвания или за статистически цели, освен ако обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес.

Европейският комитет по защита на данните може да издава насоки, препоръки и добри практики с цел по-подробно уточняване на критериите и условията за решенията, основани на профилиране.

5. Администратор и обработващ лични данни

5.1. Въведение

Позицията на Съвета на първо четене определя правната рамка за отговорностите и задълженията във връзка с всяко обработване на лични данни, извършено от администратор или от негово име от обработващ лични данни. В съответствие с принципа за отчетност администраторът е длъжен да прилага подходящи технически и организационни мерки и да бъде в състояние да докаже, че извършваните от него операции по обработване са в съответствие с регламента. В този контекст регламентът определя правила относно отговорностите на администратора във връзка с оценките на въздействието, воденето на документация за обработването, нарушенията на сигурността на данните, определянето на длъжностно лице по защита на данните и кодексите за поведение и механизмите за сертифициране.

5.2. Оценки на въздействието

Администраторът отговаря за извършването на оценка на въздействието върху защитата на данните, за да прецени дали има вероятност обработването да доведе до висок риск за правата и свободите на лицата. В позицията на Съвета на първо четене се определят случаите, когато се изисква по-конкретно оценка на въздействието върху защитата на данните, например за някои специфични мащабни операции по обработване. Когато в такава оценка на въздействието е указано, че операциите по обработването водят до висок риск, който администраторът не може да ограничи с подходящи мерки от гледна точка на наличните технологии и разходите за прилагане, преди обработването трябва да се осъществи консултация с надзорния орган. След това надзорният орган може да даде съвети на администратора и използва правомощията си.

Европейският комитет по защита на данните може да издава насоки относно операции по обработване, които е вероятно да доведат до висок риск за правата и свободите на физическите лица, и да дава указания какви мерки могат да бъдат достатъчни в такива случаи за преодоляването на потенциален риск.

5.3. Регистри на дейности по обработване на данни

С цел да се даде възможност за последващ контрол от страна на надзорния орган, администраторът или, ако има такъв, представителят на администратора, или обработващият лични данни трябва да водят документация за дейностите по обработване, за които отговарят, включително относно нарушенията на сигурността на личните данни. С оглед намаляване на административната тежест, задължението за регистриране не се прилага за предприятия или организации с по-малко от 250 служители, освен ако съществува вероятност извършваното от тях обработване да доведе до риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва чувствителни данни или данни, свързани с наказателни присъди и престъпления.

5.4. Нарушения на сигурността на данните

Нарушаването на сигурността на личните данни може да доведе до физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на данни, защитени от професионална тайна, или някакви други икономически или социални неблагоприятни последствия за засегнатите лица. Позицията на Съвета на първо четене предвижда, че администраторите трябва да уведомяват надзорните органи за нарушения на сигурността на данните, освен ако няма вероятност нарушението на сигурността на данните да доведе до риск за правата и свободите на лицата. Освен това те са длъжни да информират съответните субекти на данни относно нарушения, които могат да представляват висок риск. Уведомяването на надзорните органи ще им даде възможност за намеса, ако такава е необходима. Нещо повече, информирането на съответните субекти на данни ще им даде възможност да вземат предпазни мерки.

С цел да се намали административната тежест, в позицията на Съвета на първо четене се прилагат различни прагове за уведомяване на надзорния орган и за информиране на съответните субекти на данните, като праговете за информиране са по-високи от тези за уведомяване. Администраторите са задължени, веднага след като установят нарушение на сигурността на лични данни, да уведомят компетентния надзорен орган без ненужно забавяне и, когато е осъществимо, не по-късно от 72 часа след установяване на нарушението. Независимо от това администраторите могат да не пристъпят към уведомяване, ако са в състояние да докажат, че не съществува вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на лицата. Освен в някои изключения, администраторите са задължени без ненужно забавяне да съобщят на съответните субекти на данни за нарушението на сигурността на личните данни, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на тези субекти на данни.

Европейският комитет по защита на данните може да дава насоки, препоръки и добри практики за установяване на нарушения на сигурността на данните и определянето на понятието за ненужно забавяне, след като администраторът е узнал за нарушението, за конкретните обстоятелства, при които се изисква администраторът да уведомява за нарушение на сигурността на личните данни, както и за обстоятелствата, при които дадено нарушение на сигурността на личните данни има вероятност да породи висок риск за правата и свободите на съответните лица.

5.5. Длъжностно лице по защита на данните

Целта на определянето на длъжностно лице по защита на данните е да се подобри спазването на регламента. Следователно длъжностното лице по защита на данните трябва да бъде лице с експертни познания в правото и практиките в областта на защитата на данните и трябва да подпомага администратора или обработващия лични данни да наблюдават вътрешното съответствие с регламента. Длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги. Предвидена е възможност за определяне на едно длъжностно лице по защита на данните за група от предприятия или когато администраторът или обработващият лични данни е публичен орган. В позицията на Съвета на първо четене се предвижда задължение за определяне на длъжностно лице по защита на данните, когато:

— обработването се извършва от публичен орган, освен когато става въпрос за съдилища или независими съдебни органи, изпълняващи съдебните си функции;

— основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

— основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на чувствителни данни и на данни, свързани с наказателни присъди и престъпления.

5.6. Кодекси за поведение и механизми за сертифициране

Позицията на Съвета на първо четене съдържа стимули за прилагането на кодекси за поведение и насърчава по-широкото използване на механизми за сертифициране за защита на данните и печати и маркировки за защита на данните. Тези инициативи допринасят за спазването на правилата за защита на данните и същевременно избягват задаването на прекалено ограничителни правила и водят до намаляване на разходите за публичните органи, отговарящи за прилагането. Освен това кодексите за поведение могат да бъдат съобразени със специфичните характеристики на обработването, което се извършва в определени сектори, както и с потребностите на микропредприятията и на малките и средните предприятия. Механизмите за сертифициране, както и печатите и маркировките за защита на данните, от своя страна допринасят за спазването на регламента, тъй като субектите на данни могат лесно да оценяват нивото на защита на данните на съответните продукти и услуги.

Позицията на Съвета на първо четене включва сложен набор от правила по отношение на кодексите за поведение и механизмите за сертифициране, печатите и маркировките за защита на данните, които дават възможност за частна инициатива, като същевременно се защитават стандартите за защита на данните чрез участието на надзорните органи.

5.6.1. Кодекси за поведение

Надзорният орган може да одобрява кодекси за поведение, техни изменения или допълнения. Когато проектът на кодекс за поведение е свързан с дейности по обработване в няколко държави членки, компетентният надзорен орган е длъжен преди одобряването да представи на Европейския комитет по защита на данните за становище проект на кодекс, изменение или допълнение.

Комисията може да приема актове за изпълнение, за да реши дали новите кодекси за поведение и измененията или допълненията към съществуващи кодекси за поведение, одобрени от компетентния надзорен орган, са общовалидни в рамките на Съюза.

Европейският комитет по защита на данните следва да насърчава изготвянето на кодекси за поведение. Освен това той трябва да събира всички одобрени кодекси за поведение и измененията към тях в регистър и да ги прави обществено достъпни чрез всички подходящи средства.

5.6.2. Механизми за сертифициране и печати и маркировки за защита на данните

В позицията на Съвета на първо четене се посочва, че всяка държава членка трябва да предвиди дали сертифициращите органи се акредитират от надзорния орган или от националния орган по акредитация. Акредитираните сертифициращи органи могат да сертифицират администраторите и обработващите лични данни въз основа на критериите, одобрени от компетентния надзорен орган или — в съответствие с механизма за съгласуваност — от Европейския комитет по защита на данните. В последния случай, одобряването на критериите от Европейския комитет по защита на данните може да доведе до единно сертифициране — „Европейски печат за защита на данните“. Сертификатите се издават на администраторите и обработващите лични данни за максимален срок от 3 години, с възможност за удължаване. Сертифициращият орган трябва да предостави на надзорния орган мотивите за издаване или отнемане на искания сертификат. Впоследствие надзорният орган може да отхвърли въпросния сертификат или да го обяви за невалиден.

Комисията е компетентна да приема делегирани актове за прецизиране на изискванията, които трябва да се отчитат по отношение на механизмите за сертифициране за защита на данните. Европейският комитет по защита на данните трябва да даде становище относно тези изисквания. Комисията може да приема и актове за изпълнение относно техническите стандарти за механизмите за сертифициране и за печатите и маркировките за защита на данните, както и за механизми за насърчаване и признаване на механизмите за сертифициране и на печатите и маркировките за защита на данните.

Европейският комитет по защита на данните следва още да насърчава създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните.

6. Предаване на лични данни на трети държави или международни организации

6.1. Въведение

Трансграничните потоци от лични данни към и от държави извън Съюза и международни организации са от решаващо значение в контекста на глобалната търговия и трансграничната цифрова икономика. Нивото на защита, гарантирано от Съюза, не трябва да бъде засегнато, ако личните данни на гражданите на ЕС се предават извън Съюза.

Като общо правило всяко предаване на лични данни на трета държава или международна организация може да се осъществява само ако администраторите и обработващите лични данни спазват разпоредбите на регламента. Позицията на Съвета на първо четене е съобразена изцяло със съдебната практика на Съда на Европейския съюз, в т.ч. неговото решение от 6 октомври 2015 г. по дело C-362/14. В позицията на Съвета са запазени различни начини за разрешаване на трансграничното предаване на лични данни, като същевременно се засилват гаранциите, че правата на защита на данните се спазват. Тези различни начини за предаване на данни са решенията относно адекватността, подходящите гаранции и дерогациите.

В позицията на Съвета на първо четене се пояснява също, че всяко решение на съд или трибунал и решение на административен орган на трета държава, което изисква администратор или обработващ лични данни да предаде или разкрие лични данни, може да бъде признато или изпълнено по какъвто и да е начин само ако се основава на международно споразумение, което е в сила между отправилата искането трета държава и Съюза или негова държава членка. Нещо повече, в позицията на Съвета на първо четене изрично се посочва, че такива международни споразумения не засягат други предвидени в регламента основания за трансгранично предаване.

6.2. Решения относно адекватността

Предаването на данни в международен мащаб може да се осъществява въз основа на решение на Комисията относно адекватността, съгласно което въпросната трета държава, територия или един или повече конкретни сектори в рамките на тази трета държава, или въпросната международна организация гарантират ниво на защита, което по своята същност е равностойно на гарантираното в рамките на Съюза. По този начин се осигуряват правна сигурност и еднообразно прилагане навсякъде в Съюза.

Комисията може да реши да отмени решение относно адекватността, след като е отправила предизвестие и е предоставила пълна обосновка на третата държава или международната организация. Комисията приема решения относно адекватността и решения за оттегляне на такива решения под формата на актове за изпълнение. Актовете за изпълнение трябва да предвиждат механизъм за периодичен преглед най-малко на всеки четири години. Комисията трябва да следи събитията в трети държави и международни организации, които могат да имат отражение върху функционирането на решенията относно адекватността. За целите на наблюдението и извършването на периодичните прегледи Комисията следва да вземе предвид становищата и констатациите на Европейския парламент и Съвета, както и на други релевантни органи и източници. В рамките на оценката и прегледа на регламента Комисията трябва също периодично да докладва на Съвета и на Европейския парламент. Накрая, Европейският комитет по защита на данните трябва да предоставя на Комисията становище за оценка на адекватността на нивото на защита в трета държава или международна организация, включително за оценка на това дали повече не може да бъде гарантирано адекватно ниво на защита.

Решенията, приети от Комисията въз основа на член 25, параграф 6 от Директива 95/46/ЕО, остават в сила, докато не бъдат изменени, заменени или отменени от решение на Комисията. В същия дух, разрешенията, издадени от държава членка или надзорен орган въз основа на член 26, параграф 2 от Директива 95/46/ЕО, и решенията, приети от Комисията въз основа на член 26, параграф 4 от Директива 95/46/ЕО, остават валидни, докато не бъдат изменени, заменени или отменени, ако е необходимо, съответно от този надзорен орган или посредством решение на Комисията. Като гарантира приемственост, позицията на Съвета на първо четене създава правна сигурност.

6.3. Подходящи гаранции

В допълнение към решенията относно адекватността, трансграничното предаване на данни може също да се извършва, ако администраторът или обработващият лични данни са осигурили подходящи гаранции за компенсиране на липсата на защита на данните в третата държава или международната организация. Такива подходящи гаранции могат да се изразяват в приемането на правно обвързващи и подлежащи на изпълнение инструменти между публичните органи, задължителни фирмени правила, използването на стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от надзорен орган, или договорни клаузи, разрешени от надзорен орган. Администраторите или обработващите лични данни в дадена трета държава също могат да осигурят подходящи гаранции за предаването на лични данни на трети държави или международни организации. Те могат да направят това чрез одобрен кодекс за поведение заедно с обвързващи и подлежащи на изпълнение ангажименти за прилагане на подходящи гаранции чрез договорен или друг правно обвързващ инструмент, включително що се отнася до правата на субектите на данни. Това може да се направи и посредством механизъм за сертифициране, одобрен от компетентния надзорен орган, заедно със задължителни и подлежащи на изпълнение ангажименти на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни.

6.4. Дерогации

При липсата на решение относно адекватността или на подходящи гаранции предаването или съвкупността от предавания на лични данни на трета държава или международна организация могат да се извършат въз основа на дерогациите, които са упоменати в изчерпателния списък в регламента. Една от тези дерогации се отнася за законните интереси, преследвани от администратора, при положение че интересите или правата и свободите на субекта на данните нямат предимство пред тези интереси. С оглед на предоставянето на достатъчно гаранции при трансграничното предаване на лични данни, законните интереси на администратора са строго ограничени и позоваване на тях може да се прави само в краен случай (като „*ultimum remedium*“). С цел да се гарантира последователното прилагане на регламента, Европейският комитет по защита на данните трябва, по своя инициатива или по искане на Комисията, да изготвя и преразглежда насоки, препоръки и добри практики с цел допълнително уточняване на критериите и изискванията за предаването на данни при отсъствие на решение относно адекватността или на подходящи гаранции.

7. Надзорни органи

7.1. Независимост

Всяка държава членка трябва да предвиди един или повече независими публични органи да отговарят за наблюдението на прилагането на регламента на нейна територия, с цел да се защитят основните права и свободи на лицата във връзка с обработването на личните им данни и да се улесни свободното движение на личните данни в рамките на Съюза. Всеки надзорен орган и неговите членове трябва да действат при пълна независимост, включително с интегритет, при изпълнението на задачите и упражняването на правомощията, които са им възложени.

Всеки надзорен орган трябва да допринася за последователното прилагане на регламента в рамките на Съюза. За тази цел надзорните органи трябва да си сътрудничат помежду си, с Европейския комитет по защита на данните и с Комисията. Последователното прилагане на регламента се осигурява също чрез установяване на правомощията на надзорните органи и чрез определяне на задачите и на минималните правомощия, които надзорните органи трябва да притежават за разследване, даване на разрешение и извършване на корективни и консултативни действия.

7.2. Професионална тайна

Позицията на Съвета на първо четене определя правилата за професионална тайна на надзорните органи и на техните членове. На първо място, както по време на мандата си, така и след неговото приключване, членът или членовете и персоналът на всеки надзорен орган, в съответствие с правото на Съюза или на държава членка, трябва да бъдат обвързани от задължението за опазване на професионалната тайна по отношение на всяка поверителна информация, която е стигнала до тяхното знание при изпълнението на техните задачи или упражняването на техните правомощия. Уточнява се още, че по време на техния мандат това задължение за опазване на професионалната тайна се прилага по-специално по отношение на подаването на сигнали от физически лица за нарушения на регламента. Освен това Европейският комитет по защита на данните има за задача да издава насоки, препоръки и добри практики за установяване на общи процедури за докладване от страна на физическите лица за нарушения на регламента.

8. Сътрудничество и съгласуваност

8.1. Европейски комитет по защита на данните

С позицията на Съвета на първо четене се създава Европейски комитет по защита на данните, който е орган на Съюза, притежаващ юридическа правосубектност, с цел да се гарантира правилното и съгласувано прилагане на регламента. Намесата на Комитета се изразява по-конкретно в предоставяне на становища, приемане на обвързващи решения в контекста на уреждане на спорове между надзорни органи или изготвяне на насоки по въпроси, отнасящи се до прилагането на регламента, за да се гарантира последователното му изпълнение.

Европейският комитет по защита на данните е съставен от ръководителите на по един надзорен орган от всяка държава членка и Европейския надзорен орган по защита на данните, или от съответните им представители. Комисията има право да участва в дейностите и заседанията на Европейския комитет по защита на данните без право на глас. Обсъжданията на Европейския комитет по защита на данните са поверителни, когато Комитетът счита това за необходимо, както е посочено в процедурния му правилник.

В случай че Европейският комитет по защита на данните приема решение със задължителен характер във връзка с разрешаване на спорове, Европейският надзорен орган по защита на данните има право на глас само за решения, които засягат принципи и правила, приложими за институциите, органите, службите и агенциите на Съюза, които по същество съответстват на тези на регламента.

8.2. Механизъм за съгласуваност

В случаи на трансгранично обработване на лични данни с участието на повече от един надзорен орган, механизмът за съгласуваност гарантира, че се взема едно-единствено решение, което ще бъде приложимо на цялата територия на Европейския съюз, като се взема под внимание становището на различните засегнати надзорни органи. Следователно механизмът за съгласуваност увеличава близостта между субектите на данни и надзорния орган, който взема решение, чрез привличане на „местните“ надзорни органи в процеса на вземане на решение. Нещо повече, при възникването на спорове между надзорните органи от различни държави членки, новосъздаденият Европейски комитет по защита на данните е компетентен да взема обвързващи решения.

Правилата на механизма за съгласуване не се прилагат, когато обработването се извършва от публични органи или от частни структури в обществен интерес. В такива случаи единственият надзорен орган, който е компетентен, е надзорният орган на държавата членка, в която е установен публичният орган или частната структура.

В позицията на Съвета на първо четене се предвижда, че в контекста на оценката на регламента, която Комисията извършва, ще бъде разгледано прилагането на механизма за сътрудничество и съгласуваност.

9. Средства за правна защита, отговорност за причинени вреди и санкции

В позицията на Съвета на първо четене се предвижда подробен набор от правила, който дава на субектите на данни няколко възможности за правна защита, включително предявяването на иск за обезщетение при причинени вреди в резултат на нарушение на регламента.

9.1. Право на подаване на жалба и право на съдебна защита

В позицията на Съвета на първо четене се предвижда, че всеки субект на данни има правото да подаде жалба пред надзорния орган, ако счита, че отнасящото се до него обработване на лични данни не е в съответствие с регламента. Нещо повече, всеки субект на данни има право на ефективна съдебна защита срещу правно обвързващо решение на надзорен орган, което се отнася до него. Субектът на данни има също правото на ефективна съдебна защита, в случаите когато надзорният орган не предприема действия във връзка с жалбата или не предоставя информация относно развитието по жалбата или резултата от нея.

Всеки субект на данни има също правото на ефективна съдебна защита, ако счита, че неговите права по този регламент са били нарушени в резултат на обработването на негови лични данни в нарушение на регламента.

Гарантирана е близостта между субекта на данни и националния съд, тъй като субектът на данни има право да поиска от националния съд преразглеждане на решението на неговия орган по защита на данните, независимо от това в коя държава членка е установен администраторът или обработващият лични данни. Производствата срещу даден администратор или обработващ лични данни трябва да се образуват пред съдилищата на държавата членка, в която администраторът или обработващият лични данни има място на установяване. Като алтернативен вариант такива производства могат да се образуват пред съдилищата на държавата членка, в която субектът на данните има обичайно местопребиваване, освен ако администраторът или обработващият лични данни е публичен орган на държава членка, действащ в изпълнение на публичните си правомощия.

Наред с това, всяко физическо или юридическо лице има правото да внася иск за отмяна на решения на Европейския комитет по защита на данните пред Съда на Европейския съюз при условията, предвидени в член 263 от ДФЕС.

9.2. Представителство на субектите на данни

Субектът на данни има право да възложи на органи, организации или сдружения, които отговарят на специфични критерии, като работещи с нестопанска цел или развиващи дейност в областта на защитата на личните данни, да подадат жалба от негово име, да упражнят правото на съдебна защита от негово име и да упражнят правото на обезщетение от негово име, ако това е предвидено в правото на държавата членка. Въпросните специфични критерии имат за цел да се избегне утвърждаването на култура на търговски искове в сферата на защитата на данните. В допълнение държавите членки могат да предвидят, че всеки такъв орган, организация или сдружение, независимо от възложения от субекта на данни мандат, има право да подаде в съответната държава членка жалба до компетентния надзорен орган и да упражни правото на съдебна защита, ако счита, че правата на субект на данни са били нарушени в резултат на обработване на лични данни, което не съответства на регламента.

9.3. Спиране на производство

С оглед да се избегне разглеждането от различни съдилища на един и същи въпрос във връзка с обработване от един и същ администратор или обработващ лични данни, всеки компетентен съд, освен първия сезиран съд, може да спре производството или, по молба на една от страните, да се откаже от компетентност.

9.4. Право на обезщетение и отговорност за причинени вреди

В позицията на Съвета на първо четене се предвижда, че всеки субект на данни, който е претърпял материални или нематериални вреди в резултат на нарушение на регламента, има право да получи обезщетение от администратора или обработващия лични данни. С цел на субектите на данни да се предостави възможност да предявяват иск за обезщетение в случай на вреди, а на администраторите и обработващите лични данни да се предостави правна сигурност, в регламента се определят техните отговорности за причинени вреди. Всеки администратор, който участва в обработването, носи отговорност за причинените от него вреди. Обработващият лични данни носи отговорност само когато не е спазил задълженията по регламента, които са изрично насочени към обработващите лични данни, или е действал извън законосъобразните указания на администратора или в противоречие с тях. Независимо от това администраторът или обработващият лични данни се освобождава от отговорност, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

Когато в една и съща операция по обработване участват повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, и когато те са отговорни за някаква вреда във връзка с обработването, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни. Независимо от това, когато администратор или обработващ лични данни е изплатил пълното обезщетение за причинената вреда, той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция по обработване, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда.

9.5. Санкции

С цел да се гарантира спазването на регламента, в позицията на Съвета на първо четене се предвижда, че надзорните органи могат да налагат административни глоби. Тези глоби трябва да бъдат ефективни, пропорционални и възпиращи. Държавите членка могат да предвидят правила относно това дали и до каква степен могат да бъдат налагани административни глоби на публични органи и структури, установени в тази държава членка. Освен налагането на административни глоби надзорните органи могат да използват и други корективни правомощия, например предупреждения или порицания. С оглед повишаване на хармонизацията Европейският комитет по защита на данните трябва да изготви насоки за надзорните органи относно прилагането на корективните правомощия на надзорните органи и определянето на административни глоби.

Позицията на Съвета на първо четене съдържа списък с критерии за надзорния орган при вземането на решение дали да наложи административна санкция и, ако да, какъв следва да бъде размерът на глобата. Тези критерии са свързани наред с другото с естеството, тежестта и продължителността на нарушението на регламента, както и с това дали то е било извършено умишлено или по небрежност. В регламента се изброяват както нарушенията, така и съответстващите им максимални административни глоби. В рамките на тези максимални административни глоби надзорният орган трябва да определи целесъобразен размер в зависимост от обстоятелствата по всяко отделно нарушение. С оглед на осигуряването на правна сигурност за администраторите и обработващите лични данни, както и по-голямо хармонизиране на административните глоби в рамките на Съюза, като същевременно се запази известна свобода на преценка за надзорните органи, тези нарушения са разделени в три категории. Нарушенията в първата категория, които се отнасят до задълженията на администраторите и обработващите лични данни, подлежат на глоби в размер до 10 000 000 EUR или, ако става дума за предприятие — до 2% от общия му годишен оборот в целия свят за предходната финансова година, като се взема по-високата от двете суми. За втората категория нарушения, свързани с правата на субектите на данни и общите принципи, максималният размер е 20 000 000 EUR или 4 % от оборота. Третата категория нарушения се отнася до неспазването на разпореждане на надзорен орган и също се санкционира с максимален размер на глобата от 20 000 000 EUR или 4 % от оборота.

10. Специфични ситуации във връзка с обработването на данни

10.1. Обработване на лични данни и свобода на изразяване и информация

Държавите членки са длъжни да предвидят със закон съчетаването на правото на защита на личните данни с правото на свобода на изразяване и информация, включително обработването на лични данни за журналистически цели и за целите на академичното, художественото или литературното изразяване. С цел да се осигури прозрачност във връзка със съчетаването на тези права, всяка държава членка е длъжна да уведоми Комисията за съответните разпоредби в своето право и за измененията на тези разпоредби, както и за съответни нови разпоредби.

10.2. Обработване в контекста на трудово правоотношение

Държавите членки могат със закон или с колективни споразумения да предвидят по-конкретни правила, за да гарантират защитата на правата и свободите по отношение на обработването на личните данни на наетите лица в контекста на трудово правоотношение.

Тези правила трябва да включват подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на субекта на данните. Всяка държава членка трябва да уведоми Комисията за съответните разпоредби в своето право и за измененията на тези разпоредби, както и за съответни нови разпоредби.

10.3. Гаранции и дерогации за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели

Позицията на Съвета на първо четене определя специфични правила за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели. Целта на тези правила е да бъдат съчетани от една страна интересът от наличието на лични данни за поддържане на архиви, предоставяне на статистически данни или провеждане на изследвания и от друга страна, правата за защита на данните.

Обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели трябва да се извършва при прилагане на подходящи гаранции за правата и свободите на субекта на данните в съответствие с регламента. При специфични условия и при наличието на подходящи гаранции за субектите на данни, държавите членки имат право да предоставят спецификации и дерогации по отношение на изискванията за информацията и правата за поправяне, заличаване, ограничаване на обработването, преносимост на данните, правото да бъдеш забравен и правото на възражение при обработване на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели.

В позицията на Съвета на първо четене се предвижда и дерогация от забраната за обработване на чувствителни лични данни при обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели. Такава дерогация се позволява, когато въпросното обработване се основава на правото на Съюза или на държава членка, което трябва да е пропорционално на преследваната цел, да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данни.

11. По-рано сключени споразумения

В позицията на Съвета на първо четене се уточнява, че международните споразумения, включващи предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди влизането в сила на този регламент и са в съответствие с правото на Съюза, приложимо преди влизането в сила на регламента, остават в сила, докато не бъдат изменени, заменени или отменени. По този начин се гарантира правна сигурност за администраторите и се избягва ненужна административна тежест за държавите членки. В позицията се отчита също, че за изменянето на съществуващи споразумения, държавите членки са зависими от сътрудничеството на третата държава или международната организация.

IV. ЗАКЛЮЧЕНИЕ

Позицията на Съвета на първо четене отразява компромиса, постигнат при неформалните преговори между Съвета и Европейския парламент със съдействието на Комисията. Съветът приканва Европейския парламент официално да одобри позицията на Съвета на първо четене без изменения, така че да може да бъде създадена новата законодателна рамка на ЕС за защита на данните, която ще укрепи правата за защита на данните, като същевременно ще улесни движението на лични данни на цифровия пазар.