I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА ДАННИТЕ

Становище на Европейския надзорен орган по защита на данните относно съобщението на Комисията до Европейския парламент, до Съвета, до Икономическия и социален комитет и до Комитета на регионите, озаглавено — „Всеобхватен подход за защита на личните данни в Европейския съюз“

(2011/C 181/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

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

като взе предвид Хартата на основните права на Европейския съюз, и по-специално членове 7 и 8 от нея,

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на лицата при обработването на лични данни и за свободното движение на тези данни ([1]),

като взе предвид Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. за защита на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни ([2]), и по-специално член 41 от него,

ПРИЕ НАСТОЯЩОТО СТАНОВИЩЕ:

A. **ОБЩА ЧАСТ**

1. **Въведение**

1.1. *Първа и обща оценка*

1. На 4 ноември 2010 г. Комисията прие съобщение, озаглавено „Всеобхватен подход за защита на личните данни в Европейския съюз“ (по-нататък наричано „съобщението“) ([3]). Съобщението бе изпратено на ЕНОЗД за консултация. ЕНОЗД изразява удовлетворение от факта, че Комисията се обърна към него за консултация в съответствие с член 41 от Регламент (ЕО) № 45/2001. Още преди приемането на съобщението на ЕНОЗД беше дадена възможност за неофициални коментари. Някои от тези коментари бяха взети предвид в окончателния текст на документа.

2. Целта на настоящото съобщение е да представи подхода на Комисията за преразглеждане на правната система на ЕС за защита на личните данни във всички области на дейност на Съюза, като се отчитат по-специално предизвикателствата, произтичащи от глобализацията и новите технологии ([4]).

3. ЕНОЗД изразява по принцип удовлетворение от съобщението, тъй като е убеден, че преразглеждане на настоящата правна рамка за защита на личните данни в ЕС е необходимо, за да се гарантира ефективна защита в едно постоянно развиващо се информационно общество. Още в своето становище от 25 юли 2007 г. относно прилагането на Директивата за защита на данните ([5]) той заключи, че в дългосрочен план промените в Директива 95/46/ЕО изглеждат неизбежни.

4. Съобщението представлява важна стъпка към такава законодателна промяна, която от своя страна ще бъде най-важното развитие в областта на защита на данните в ЕС след приемането на Директива 95/46/ЕО, считана всеобщо за основен крайъгълен камък на защита на данните в целия Европейски съюз (и по-широко в рамките на Европейското икономическо пространство).

5. Съобщението предоставя подходящата рамка за добре насочено преразглеждане, също и затова, че посочва, общо казано, основните проблеми и предизвикателства. ЕНОЗД споделя схващането на Комисията, че силна система за защита на данните ще бъде нужна и занапред, въз основа на това, че съществуващите общи принципи на защита на данните са все още валидни в общество, в което се извършват основни промени поради бързото развитие на технологиите и глобализацията. Това налага преразглеждане на съществуващата правна уредба.

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) ОВ L 8, 12.1.2001 г., стр. 1.
([3]) COM(2010) 609 окончателен.

([4]) Виж стр. 5 от съобщението, първо съображение.
([5]) Становище на ЕНОЗД относно Съобщението на Комисията до Европейския парламент и Съвета относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни (ОВ C 255, 27.10.2007 г., стр. 1).

6. В съобщението с право се подчертава, че предизвикателствата са огромни. ЕНОЗД споделя напълно тази констатация и подчертава, че вследствие на това предложените решения трябва да бъдат подобаващо амбициозни и да засилват ефективността на защитата.

1.2. *Цел на становището*

7. В становището се прави оценка на решенията, предложени в съобщението, въз основа на следните два критерия: амбициозност и ефективност. То е, общо взето, положително. ЕНОЗД подкрепя съобщението, но е същевременно критичен по някои аспекти, където според него повече амбициозност би довела до по-ефективна система.

8. ЕНОЗД си поставя за цел да допринесе с настоящото становище за по-нататъшното развитие на правната рамка за защита на данните. Той очаква предложението на Комисията, предвидено за средата на 2011 г., и се надява, че предложенията му ще бъдат взети предвид при изготвянето на това предложение. Той отбелязва също така, че съобщението, както изглежда, изключва някои области, като обработка на данните от институциите и органите на ЕС, от общия инструмент. Ако Комисията реши наистина да остави настрана някои области на този етап — за което ЕНОЗД би съжалявал, той настоява тя да поеме задължението да изгради напълно цялостна архитектура в краткосрочна и уточнена времева рамка.

1.3. *Компоненти на настоящото становище*

9. Настоящото становище не е изолирано. То се основава на предшестващи мнения, изразени от ЕНОЗД и европейските органи за защита на данните по различни поводи. Трябва по-специално да се подчертае, че във вече посоченото становище на ЕНОЗД от 25 юли 2007 г. бяха идентифицирани и разработени някои основни елементи за бъдещи промени ([6]). То се основава също на обсъждания с други заинтересовани страни в областите на неприкосновеността на личния живот и защитата на данните. Техният принос беше много полезен както за съобщението, така и за настоящото становище. В това отношение може да се заключи, че е налице известна степен на полезно взаимодействие относно начините за повишаване на ефективността на защитата на данните.

10. Друг важен компонент на настоящото становище е документът, озаглавен „Бъдещето на неприкосновеността на личния живот“, съвместен принос на работната група за защита на данните по член 29 и работната група по полицейско и съдебно сътрудничество към консултацията, започната от Европейската комисия през 2009 г. (по-нататък наричан „документът на РГ за бъдещето на неприкосновеността на личния живот“) ([7]).

11. Неотдавна, на пресконференция, състояла се на 15 ноември 2010 г., ЕНОЗД представи първите си реакции на настоящото съобщение. Настоящото становище излага подробно по-общите мнения, изказани на тази пресконференция ([8]).

12. Накрая, настоящото становище ползва някои предшестващи становища на ЕНОЗД, както и документи на работната група за защита на данните по член 29. Позоваванията на тези становища и документи могат да се намерят на различни места в настоящото становище, където това е уместно.

2. **Контекст**

13. Преразглеждането на правилата за защита на данните става в много важен исторически момент. Съобщението описва контекста обширно и по-убедителен начин. Въз основа на това описание ЕНОЗД идентифицира четирите основни фактора, определящи средата, в която се извършва преразглеждането.

14. Първият фактор е развитието на технологиите. Днешните технологии не са такива, каквито са били при приемането на Директива 95/46/ЕО. Технологични постижения като изчислителни облаци, поведенческо рекламиране, социални мрежи, събиране на пътна такса и устройства за геолокализиране промениха основно начина, по който се обработват данните и поставят защитата на данните пред огромни предизвикателства. Преразглеждането на европейските правила за защита на данните ще трябва да се справи ефективно с тези предизвикателства.

15. Вторият фактор е глобализацията. Постепенното премахване на търговските бариери придаде на предприятията все по-глобално измерение. Трансграничната обработка и международните предавания на данни се увеличиха неимоверно през последните години. Освен това обработката на данни се разпространи повсеместно поради информационните и комуникационните технологии: Интернет и изчислителните облаци дадоха възможност за необвързана с мястото обработка на големи количества данни в световен мащаб. Последното десетилетие стана също свидетел на разрастване на полицейските и съдебните действия за борба срещу тероризма и

([6]) По-специално (вж. съображение 77 от становището): не са необходими нови принципи, но съществува ясна необходимост от друга административна уредба; не следва да се променя широкият обхват на закона за защита на личните данни, приложим за всяко използване на лични данни; законът за защита на личните данни следва да позволява балансиран подход в конкретни случаи, а така също да позволява на органите за защита на данните да определят приоритети; системата следва да прилага изцяло използването на лични данни за целите на правоприлагането, въпреки че могат да бъдат необходими подходящи допълнителни мерки за справяне с конкретни проблеми в тази област.

([7]) Документ WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Основното му послание е, че законодателната промяна е добра възможност за изясняване на някои ключови правила и принципи (напр. съгласие, прозрачност), въвеждане на някои нови принципи (напр. неприкосновеност на личния живот още при разработването, отчетност), засилване на ефективността чрез модернизиране на уредбата (напр. чрез ограничаване на съществуващите изисквания за уведомление) и включване на всичко в една всеобхватна правна рамка (напр. полицейското и съдебното сътрудничество).

([8]) Темите на пресконференцията може да бъдат намерени на уебсайта на ЕНОЗД на адрес: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

други форми на международната организирана престъпност, подпомогнати от огромен обмен на информация за целите на правоприлагането. Всичко това изисква сериозно обсъждане на начините за ефективна защита на личните данни в днешния глобализиран свят, без да се създават съществени пречки за международните дейности по обработката.

16. Третият фактор е Лисабонският договор. Влизането в сила на Лисабонския договор отбелязва нова ера в областта на защита на данните. Член 16 от ДФЕС гарантира не само индивидуалните права на лицата, за които се събират данни, но и предоставя пряка правна основа за силно законодателство за защита на данните в целия ЕС. Освен това отмяната на структурата от стълбове задължава Европейския парламент и Съвета да предвидят защита на данните във всички области на правото на ЕС. С други думи, тя дава възможност за всеобхватна правна рамка за защита на данните, приложима в частния сектор, в публичния сектор в държавите-членки и в институциите и органите на ЕС. Стокхолмската програма ([9]) последователно заявява в тази връзка, че Съюзът трябва да осигури цялостна стратегия за защита на данните на територията на ЕС и в неговите отношения с трети страни.

17. Четвъртият фактор се състои в успоредни процеси на развитие, протичащи в международните организации. Продължават разни дискусии по модернизирането на настоящите правни инструменти за защита на данните. Важно е да се посочат в това отношение настоящите обсъждания за предстоящото преразглеждане на Конвенция 108 на Съвета на Европа ([10]) и Основните насоки на ОИСР за защитата на личния живот ([11]). Друго важно развитие се отнася до приемането на международни стандарти за защита на личните данни и неприкосновеността на личния живот, които може евентуално да доведат до приемането на обвързващ глобален инструмент за защита на данните. Всички тези инициативи заслужават пълна подкрепа. Тяхната обща цел трябва да бъде гарантиране на ефективна и последователна защита в задвижвана от технологиите и глобализирана околна среда.

3. **Основни перспективи**

3.1. *Защитата на данните укрепва доверието и трябва да бъде в подкрепа на други (публични) интереси*

18. Силната рамка за защита на данните е необходимо следствие от значението, което Лисабонският договор отдава на защитата на данните, по-специално в член 8 от Хартата на основните права на Съюза и член 16 от ДФЕС, както и силно изразената връзка с член 7 на хартата ([12]).

19. Силната рамка за защита на данните служи обаче и на по-широките публични и частни интереси в информационното общество с повсеместна обработка на данни. Защитата на данните укрепва доверието, а доверието е съществено важен елемент на доброто функциониране на нашето общество. От голямо значение е разпоредбите за защита на данните да бъдат съставени по такъв начин, че — в максимално възможна степен — да подкрепят активно, а не да пречат на други законни права и интереси.

20. Важни примери за други законни интереси са силната европейска икономика, сигурността на лицата, както и отчетността на правителствата.

21. Икономическото развитие в ЕС върви ръка за ръка с въвеждането и пускането на пазара на нови технологии и услуги. В информационното общество появата и успешното внедряване на информационни и комуникационни технологии и услуги зависи от доверието. Ако хората нямат доверие на ИКТ, тези технологии вероятно ще претърпят провал ([13]). А хората ще имат доверие в ИКТ само ако данните им за ефикасно защитени. Ето защо защитата на данните следва да бъде неразделна част от технологиите и услугите. Силната рамка за защита на данните укрепва европейската икономика, при условие че тази рамка е не само силна, но и правилно изградена. В тази перспектива по-нататъшната хармонизация в ЕС и минимизирането на административните тежести са от съществено значение (вж. глава 5 от настоящото становище).

22. Много беше казано през последните години за необходимостта от намиране на баланс между неприкосновеността на личния живот и сигурността, по-специално във връзка с инструментите за обработка и обмен на данни в областта на полицейското и съдебното сътрудничество ([14]). Твърде често защитата на данните беше погрешно окачествявана като пречка за пълната защита и физическата сигурност на лицата ([15]) или поне като неизбежно условие, което трябва да бъде изпълнявано от правоприлагащите органи. С това обаче нещата не се изчерпват. Силната рамка за защита на данните може да повиши и да засили сигурността. Въз основа на принципите на защита на данните, когато те бъдат приложени добре, администраторите са длъжни да гарантират, че информацията е точна и актуална и че излишните лични данни, които не са необходими за правоприлагането, ще бъдат елиминирани от системата. Може да се посочат също задълженията за прилагане на технологични и организационни мерки за гарантиране на

([9]) Стокхолмска програма — Отворена и сигурна Европа в услуга и за защита на гражданите (ОВ C 115, 4.5.2010 г., стр. 1), на стр. 10.

([10]) Конвенция 108 на Съвета на Европа за защита на физическите лица при автоматична обработка на лични данни, ETS № 108, 28.1.1981 г.

([11]) Основни насоки на ОИСР от 1980 г. за защитата на личния живот и трансграничните потоци лични данни, публикувана на адрес: http://www.oecd.org

([12]) Значението на защитата на данните и връзката със неприкосновеността на личния живот в хартата бяха подчертани от Съда на ЕС в 9 решението му от 9 ноември 2010 г., съединени дела C-92/09 и C-93/09, *Schecke*, още непубликувани в ECR.

([13]) Вж. Становище на ЕНОЗД относно повишаване на доверието в информационното общество чрез насърчаване на защитата на данните и на неприкосновеността на личния живот (ОВ C 280, 16.10.2010 г., стр. 1), съображение 113.

([14]) Вж. например Становище на ЕНОЗД от 10 юли 2009 г. относно съобщението на Комисията до Европейския парламент и Съвета „Пространство на свобода, сигурност и правосъдие за гражданите“ (ОВ C 276, 17.9.2009 г., стр. 8).

([15]) Сигурността е по-широко понятие от физическата сигурност, но тук това понятие е използвано в по-ограниченото си значение като пример за изложените аргументи.

сигурността на системи, като системите за защита срещу неразрешено оповестяване или достъп, разработени в областта на защитата на данни.

23. Спазването на принципите на защита на данните може освен това да гарантира, че правоприлагащите органи ще работят на принципите на правовата държава, което създава доверие към тяхното поведение и следователно укрепва в по-широк смисъл доверието в нашите общества. Съдебната практика, установена в съответствие с член 8 от Европейската конвенция за защита на правата на човека, гарантира, че полицейските и съдебните власти могат да обработват всички данни, свързани с тяхната работа, но не неограничено. Защитата на данните изисква система за насрещни проверки (за полицията и съдебната власт вж. глава 9 от настоящото становище).

24. В демократичните общества правителствата носят отговорност за всички свои действия, включително за използването на лични данни за различните публични интереси, на които служат. То варира от публикуване на данни по интернет от съображения за прозрачност до използването на данни за осъществяване на политики в области като обществено здравеопазване, транспорт или данъчно облагане или наблюдението на лица за целите на правоприлагането. Силната рамка за защита на данните дава възможност на правителствата да спазват своите задължения и да носят отговорност като част от доброто управление.

3.2. *Последици за законовата рамка относно защита на данните*

3.2.1. Необходима е по-нататъшна хармонизация

25. В съобщението правилно се изтъква, че един от съществените недостатъци на настоящата рамка е, че тя предоставя на държавите-членки твърде голяма свобода на действие при прилагането на европейските разпоредби в националното законодателство. Липсата на хармонизация води до редица отрицателни последици в информационното общество, където физическите граници между държавите-членки имат все по-малко значение (вж. глава 5 от настоящото становище).

3.2.2. Общите принципи на защита на данните остават валидни

26. Първата и по-формална причина, поради която общите принципи на защитата на данни не трябва и не може да се променят, е от правно естество. Тези принципи са изложени в Конвенция 108 на Съвета на Европа, която е задължителна за всички държави-членки. Тази конвенция е основата на защитата на данни в ЕС. Освен това някои от основните принципи са изрично посочени в член 8 от Хартата на основните права на Съюза. Следователно изменението на тези принципи би наложило промени в Договорите.

27. С това обаче нещата не се изчерпват. Има и съществени причини да не се изменят общите принципи. ЕНОЗД е твърдо убеден, че информационното общество не може и не бива да функционира без достатъчна защита на неприкосновеността на личния живот и на личните данни на лицата. Когато се обработва повече информация, необходима е и по-добра защита. Информационното общество, в което се обработва изобилна информация за всеки човек, трябва да е изградено на принципа на контрол от страна на физическото лице, за да му се даде възможност да действа като индивид и да използва свободите си в едно демократично общество, като свобода на изразяването и на словото.

28. Трудно е освен това да си представим контрол от страна на лицето без задължения на администраторите да ограничават обработката в съответствие с принципите на необходимост, пропорционалност и ограничаване в рамките на целта. Също така трудно е да си представим контрол от страна на лицето при отсъствието на признати права на лицата, за които се събират данни, като право на достъп, поправяне, заличаване или блокиране на данни.

3.2.3. Защитата на данни като основно право

29. ЕНОЗД подчертава, че защитата на данни е призната като основно право. Това не означава, че защитата на данни трябва да има винаги *предимство* пред други важни права и интереси в едно демократично общество, но тя води до последици относно естеството и обхвата на защитата, която трябва да бъде осигурена с правна рамка на ЕС, за да се гарантира, че изискванията за защита на данни винаги се вземат *адекватно* предвид.

30. Тези основни последици могат да бъдат определени, както следва:

— Защитата трябва да бъде ефективна. Правната рамка трябва да предвиди инструменти, които дават възможност на физическите лица да упражняват на практика своите права.

— Правната рамка трябва да бъде стабилна в дългосрочен план.

— Защитата трябва да се предоставя при всички обстоятелства и да не зависи от политическите предпочитания през даден период от време.

— Може да се наложат ограничения на упражняването на това право, но те трябва да бъдат по изключение, надлежно обосновани и да не засягат съществените елементи на самото право ([16]).

ЕНОЗД препоръчва на Комисията да има предвид тези последици, когато предлага законодателни решения.

3.2.4. Необходима е нова правна уредба

31. Съобщението правилно поставя ударението върху необходимостта от укрепване на съществуващата правна уредба за защита на данните. В този контекст е уместно да се напомни, че в документа на РГ за бъдещето на неприкосновеността на личния живот ([17]) органите за защита на данните подчертаха необходимостта от засилване на

([16]) Вж. също Становище на ЕНОЗД относно Съобщението на Комисията до Европейския парламент и Съвета относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни, Съображение 17, което се основава на съдебната практика на Европейския съд по правата на човека и Съда на ЕС.

([17]) Виж бележка под линия на стр. 7.

ролите на различните фактори в областта на защита на данните, а именно на лицата, за които се събират данни, администраторите на лични данни и самите надзорни органи.

32. Очевидно е налице широко съгласие между заинтересованите страни, че по-силната правна уредба, отчитаща технологичните аспекти на развитието и глобализацията, има ключово значение за амбициозната и ефективна защита на данните и в бъдеще. Както бе вече отбелязано в съображение 7, това са критериите за оценката от страна на ЕНОЗД на всякакви предложени решения.

3.2.5. Всеобхватността като *conditio sine qua non*

33. Както се напомня в съобщението, Директива 95/46/ЕО се прилага към всички дейности по обработка на лични данни в държавите-членки в публичния и в частния сектор, с изключение на дейностите, попадащи извън обхвата на предишното право на Общността ([18]). Това изключение беше необходимо съгласно предишния Договор, но това не е вече така след влизането в сила на Лисабонския договор. Освен това изключението противоречи — на текста и във всеки случай на духа — на член 16 от ДФЕС.

34. Според ЕНОЗД един всеобхватен правен инструмент за защита на данните, включително за полицейското и съдебното сътрудничество по наказателноправни въпроси, трябва да се разглежда като основното усъвършенстване, което може да даде една нова правна рамка. Той е *conditio sine qua non* за ефективна защита на данните в бъдеще.

35. В подкрепа на това изявление ЕНОЗД изтъква следните доводи:

— Разликата между дейностите на частния сектор и на сектора на правоприлагане е неясна. Субектите от частния сектор може да обработват данни, които в крайна сметка се използват за целите на правоприлагането (пример: резервационните данни за пътниците ([19])), докато в други случаи от тях се изисква да съхраняват данни за целите на правоприлагането (пример: директивата за защита на данните ([20])).

— Няма съществена разлика между полицейските и съдебните органи и другите органи за прилагане на законодателството (данъчни, митнически, за борба с измамите, имиграционни) съгласно Директива 95/46/ЕО.

— Както точно е посочено в съобщението, правният инструмент за защита на данни, който се прилага понастоящем към полицейските и съдебните органи (Рамково решение 2008/977/ПВР ([21])), е недостатъчен.

— Повечето държави-членки са приложили Директива 95/46/ЕО и Конвенция 108 в своите национални законодателства, като са ги направили приложими и към полицейските и съдебните си органи.

36. Включването на полицията и съдебната система в общия правен инструмент не само ще даде повече гаранции на гражданите, но и ще улесни задачата на полицейските органи. Задължението да се прилагат различни набори от правила е обременително, ненужно времепоглъщащо и пречи на международното сътрудничество (вж. глава 9 от настоящото становище). Това също говори в полза на включване на дейностите по преработката от националните служби по сигурност, доколкото това е възможно, в съществуващото законодателство на ЕС.

3.2.6. Технологична неутралност

37. Периодът след приемането на Директива 95/46/ЕО през 1995 г. може да се окачествати като технологично бурен. Често се въвеждат нови технологични разработки и устройства. В много случаи това доведе до основни промени в начина, по който се обработват личните данни на физически лица. Информационното общество не може вече да бъде разглеждано като паралелна среда, в която отделният човек може да участва на доброволна основа, а е станало неразделна част от нашия всекидневен живот. Само един пример: идеята за „Интернет на нещата“ ([22]) установява връзки между физически обекти и свързаната с тях онлайн информация.

38. Технологията ще продължи да се развива. Това се отразява на новата правна рамка. Тя трябва да остане ефективна в течение на повече години, като същевременно не спъва понататъшните процеси на технологично развитие. Това налага правната уредба да бъде технологично неутрална. Рамката трябва обаче да даде също така повече правна сигурност на фирмите и на физическите лица. Те трябва да разберат какво се очаква от тях и да могат да упражняват своите права. Това налага правната уредба да бъде точна.

39. ЕНОЗД счита, че новият правен инструмент за защита на данните трябва, в рамките на възможното, да бъде формулиран по неутрален в технологично отношение начин. Това предполага правата и задълженията на различните субекти да бъдат формулирани по общ и неутрален начин, така че да останат по принцип валидни и приложими, независимо от технологията, избрана за обработка на личните данни. Няма друг изход, като се има предвид бързият темп на технологичния напредък

([18]) Настоящото становище поставя ударението главно върху предишния трети стълб (полицейско и съдебно сътрудничество по наказателноправни въпроси), тъй като предишният втори стълб е не само по-сложна област от правото на ЕС (както се признава и в член 16 от ДФЕС и член 39 от Договора за ЕС), но и се отнася в по-малка степен до обработката на данни.

([19]) Вж. напр. Съобщение на Комисията относно глобалния подход за предаване на резервационни данни на пътниците (PNR данни) на трети държави, COM(2010) 492 окончателен.

([20]) Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, (ОВ L 105, 13.4.2006 г., стр. 54).

([21]) Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, (ОВ L 350, 30.12.2008 г., стр. 60).

([22]) Както е определено в „Интернет на нещата — план за действие за Европа“, COM(2009) 278 окончателен.

днес. ЕНОЗД предлага да бъдат въведени нови „технологично неутрални“ права в допълнение към съществуващите принципи на защита на данните, които може да се окажат особено важни в бързо променящата се електронна среда (вж. главно глави 6 и 7).

3.2.7. В дългосрочен план: Правна сигурност за по-дълъг период от време

40. Директива 95/46/ЕО беше основният документ в областта на защита на данните в ЕС през последните 15 години. Тя бе въведена в законодателствата на държавите-членки и прилагана от различните субекти. С течение на годините прилагането ѝ се обогати от практически опит и от допълнителни насоки от страна на Комисията, на органите за защита на данните (на национално равнище и в рамките на работната група по член 29) и на националните и европейските съдилища.

41. Добре е да се подчертае, че тези развития се нуждаят от време и че (особено поради това, че имаме работа с обща рамка за осъществяване на основно право) това време е необходимо за създаването на правна сигурност и стабилност. Трябва да се изготви нов общ правен инструмент с амбицията той да бъде в състояние да създаде правна сигурност и стабилност за по-дълъг период от време, като не се забравя, че е много трудно да се предскаже по-нататъшното развитие на технологията и на глобализацията. Във всички случаи ЕНОЗД подкрепя напълно целта да се създаде правна сигурност за по-дълъг период от време в сравнение с обхвата на Директива 95/46/ЕО. Казано накратко, когато технологията се развива с бързо темпо, законодателството трябва да бъде стабилно.

3.2.8. В краткосрочен план: По-добро използване на съществуващите инструменти

42. В краткосрочен план е много важно да се гарантира ефективността на съществуващата правна уредба, на първо място, като ударението се постави върху правоприлагането на национално и европейско равнище (вж. глава 11 от настоящото становище).

Б. ЕЛЕМЕНТИ НА НОВАТА РАМКА

4. Всеобхватен подход

43. ЕНОЗД подкрепя напълно всеобхватния подход към защита на данните, който е не само надслов, но и отправна точка на съобщението и по необходимост включва разширяването на общите правила за защита на данните с полицейското и съдебното сътрудничество по наказателноправни въпроси ([23]).

44. Той обаче отбелязва също така, че Комисията не възнамерява да включи всички дейности по обработката на данни в този общ правен инструмент. По-специално, няма да бъде включена обработката на данни от институциите, органите, службите и агенциите на ЕС. Комисията заявява само, че „ще оцени необходимостта от адаптиране на други правни инструменти към новата обща рамка за защита на личните данни“.

45. ЕНОЗД изразява определеното си предпочитание за включване на обработката на равнището на ЕС в общата правна рамка. Той напомня, че това е било първоначалното намерение на предишния член 286 от ДЕО, където за първи път в Договора става дума за защита на данните. В член 286 от ДЕО просто се заявява, че правните инструменти за обработката на лични данни ще се прилагат и към институциите. Още по-важно е, че с един правен текст се избягва рискът от несъответствия между разпоредбите и той ще бъде най-подходящ за обмен на данни между равнището на ЕС и публичните и частните субекти в държавите-членки. С него ще се избегне също рискът след изменението на Директива 95/46/ЕО да отпадне интересът от изменение на Регламент (ЕО) № 45/2001 или на тези промени да не се даде нужният приоритет, за да се избегнат несъответствия по отношение на датите на влизане в сила.

46. ЕНОЗД настоява Комисията, ако тя стигне до заключение, че включването на обработката на равнището на ЕС в общия правен инструмент няма да бъде възможно, да поеме задължението да предложи адаптиране на Регламент (ЕО) № 45/2001 (не „да оцени необходимостта“) във възможно най-кратък срок, за предпочитане до края на 2011 г.

47. Също тъй важно е Комисията да гарантира, че няма да изостанат други области, и по-специално:

— защитата на данни в общата външна политика и политиката на сигурност въз основа на член 39 от ДЕС ([24]),

— секторно-специфичните режими на защита на данните за органи на ЕС, като Европол, Евроюст и за крупни информационни системи, доколкото се нуждаят от адаптиране към новия правен инструмент,

— Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации, доколкото се нуждае от адаптиране към новия правен инструмент.

48. Накрая, към общия правен инструмент за защита на данните може и вероятно трябва да бъдат добавени допълнителни секторни и специфични разпоредби, например за полицейското и съдебното сътрудничество, но и за други области ([25]). При необходимост и в съответствие с принципа на субсидиарност тези допълнителни разпоредби следва да бъдат приети на равнището на ЕС. Държавите-членки могат да изготвят допълнителни разпоредби в специфични области, където има основание за това (вж. 5.2).

([23]) Вж. стр. 14 от съобщението и раздел 3.2.5 от настоящото становище.

([24]) Вж. също Становище на ЕНОЗД от 24 ноември 2010 г. относно съобщението на Комисията до Европейския парламент и до Съвета, озаглавено „Политиката на ЕС за борба с тероризма: главни постижения и бъдещи предизвикателства“, съображение 31,

([25]) Вж. също документа на РГ за бъдещето на неприкосновеността на личния живот (бележка под линия 7), съображения 18—21.

5. **По-нататъшна хармонизация и опростяване**

5.1. *Необходимостта от хармонизация*

49. Хармонизацията е от първостепенно значение за законодателството на ЕС за защита на данните. В съобщението правилно се изтъква, че защитата на данните има ясно изразено измерение, свързано с вътрешния пазар, тъй като тя трябва да гарантира свободното движение на лични данни между държавите-членки в рамките на вътрешния пазар. Степента на хармонизация съгласно настоящата директива е оценена обаче като незадоволителна. Съобщението признава, че това е една от основните и често възникващи причини за безпокойство на заинтересованите страни. По-специално заинтересованите страни подчертават необходимостта от увеличаване на правната сигурност, намаляване на административната тежест и гарантиране на равнопоставени условия на конкуренция за икономическите оператори. Както правилно отбелязва Комисията, това важи в особена степен за администраторите на лични данни, установени в няколко държави-членки и задължени да се съобразяват с изискванията (които може да са различни) на националните законодателства за защита на данните ([26]).

50. Хармонизацията е важна не само за вътрешния пазар, но и с оглед на осигуряването на достатъчна защита на данните. В съответствие с член 16 от ДФЕС „всеки“ има право на защита на личните данни, които се отнасят до него. За да бъде ефективно спазено това право, трябва да се гарантира еднаква степен на защита в целия ЕС. В документа на РГ за бъдещето на неприкосновеността на личния живот се подчертава, че няколко разпоредби, свързани с положението на лицата, за които се събират данни, не са били приложени или изтълкувани еднакво във всички държави-членки ([27]). В глобализирания и взаимно свързан свят тези различия може да попречат или да ограничат защитата на физическите лица.

51. ЕНОЗД счита, че по-нататъшната и по-добрата хармонизация е една от главните цели на процедурата за преразглеждане. ЕНОЗД приветства поетото от Комисията задължение да разгледа начините за постигане на по-нататъшна хармонизация на правилата за защита на данните на равнището на ЕС. Той обаче отбелязва с известна изненада, че на този етап Комисията не е предложила конкретни варианти. Ето защо ЕНОЗД посочва сам няколко области, където е най-спешно да се постигне поголямо унифициране (вж. 5.3). По-нататъшната хармонизация в тези области следва да се постигне не само чрез намаляване на свободата на действие на националното законодателство, но и чрез предотвратяване на неправилното прилагане от държавите-членки (вж. също глава 11) и осигуряване на по-последователно и съгласувано правоприлагане (вж. също глава 10).

([26]) Съобщението, стр. 10.

([27]) Вж. документа на РГ за бъдещето на неприкосновеността на личния живот (бележка под линия 7), съображение 70. Документът се отнася по-специално до разпоредбите за отговорност и възможността за искове за нематериални щети.

5.2. *Напаляване на свободата на действие при прилагането на директивата*

52. Директивата съдържа някои разпоредби, които са широко формулирани и поради това оставят значително място за различно прилагане. В съображение 9 на директивата изрично е потвърдено, че на държавите-членки се дава известна свобода на действие и че в рамките на тази свобода на действие биха могли да възникнат несъответствия при прилагането на директивата. Няколко разпоредби са приложени различно от държавите-членки, в това число някои съществено важни разпоредби ([28]). Това положение е незадоволително и трябва да се търси поголямо унифициране.

53. Това не значи, че различията следва да бъдат изключени напълно. В някои области може да е необходима гъвкавост, с цел да бъдат запазени обосновани особености, важни публични интереси или институционалната автономия на държавата-членка. Според ЕНОЗД мястото за различия между държавите-членки следва да се ограничи по-специално до следните специфични ситуации:

— Свобода на изразяване: съгласно настоящата рамка (член 9) държавите-членки могат да предвиждат изключения или дерогации относно обработването на лични данни, когато то се извършва единствено за целите на журналистическа дейност или на литературно или художествено изразяване. Тази гъвкавост изглежда уместна при спазване, разбира се, на ограниченията в хартата и в Европейската конвенция за защита на правата на човека, като се имат предвид различните традиции и културните различия, които може да съществуват в тази област в държавите-членки. Това обаче няма да попречи на евентуално актуализиране на настоящия член 9, с оглед на развитията в интернет.

— Специфични публични интереси: съгласно настоящата рамка (член 13) държавите-членки могат да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, ако подобно ограничаване представлява необходима мярка за гарантиране на важни публични интереси, като националната сигурност, отбраната, обществената сигурност и пр. Тази компетенция на държавите-членки остава обоснована. Все пак тълкуването на изключенията следва, когато е възможно, да бъде допълнително хармонизирано (вж. раздел 9.1). Освен това настоящият обхват за изключения от член 6, параграф 1 изглежда прекалено широк.

— Правни средства за защита, санкции и административни процедури: европейската правна рамка следва да определи основните условия, но съгласно настоящото състояние на правото на ЕС определянето на санкциите, правните средства за защита, процедурните правила и условията за проверка, приложими на национално равнище, трябва да бъде предоставено на държавите-членки.

([28]) Съществуват също някои несъответствия в подходите по отношение на ръчното въвеждане на данни.

5.3. *Области за по-нататъшна хармонизация*

54. *Определения* (член 2 от Директива 95/46/ЕО). Определенията са крайъгълният камък на правната система и следва да бъдат еднакво тълкувани в държавите-членки, без свобода на действие при прилагането. При настоящата рамка възникнаха несъответствия, например във връзка с понятието „администратор“ ([29]). ЕНОЗД предлага към настоящия списък в член 2 да се добавят нови определения, с оглед да се създаде по-голяма правна сигурност, като например анонимни данни, псевдоанонимни данни, съдебни данни, предаване на данни и длъжностно лице за защита на данните.

55. *Законност на обработването* (член 5). Новият правен инструмент следва да бъде максимално точен по отношение на основните елементи, определящи законността на обработването на данни. Член 5 от директивата (както и съображение 9), даващ право на държавите-членки да определят по-точно условията, при които обработването на данни е законно, може поради това да не е вече необходим в бъдещата рамка.

56. *Основания за обработването на данни* (членове 7 и 8). Определянето на условията за обработването на данни е съществен елемент на всеки законодателен акт за защита на данните. На държавите-членки не трябва се дава възможност да въвеждат допълнителни или изменени основания за обработване или да изключват някое от тях. Възможността за дерогации следва да бъде изключена или ограничена (по-специално по отношение на чувствителните данни ([30])). В новия правен инструмент основанията за обработването на данни следва да бъдат ясно формулирани, което ще намали свободата на преценка при изпълнението или правоприлагането. По-специално понятието „съгласие“ може да се нуждае от допълнително уточняване (вж. раздел 6.5). Освен това основанието, почиващо на законните интереси на администратора на лични данни (член 7, буква е)), дава възможност за много различни тълкувания поради гъвкавостта си. Необходимо е допълнително уточнение. Друга разпоредба, която се налага да бъде евентуално уточнена, е член 8, параграф 2, буква б), който разрешава обработването на чувствителни данни, необходимо за целите на изпълнението на задълженията и специфичните права на администратора в областта на трудовото право ([31]).

57. *Права на лицата, за които се събират данни* (членове 10—15). Това е една от областите, в които не всички елементи на директивата се прилагат и тълкуват последователно от държавите-членки. Правата на лицата, за които се събират данни, са централен елемент за ефективна защита на данните. Следователно свободата на действие следва да бъде значително намалена. ЕНОЗД препоръчва информацията, предоставяна от администратора на лицата, за които се събират данни, да бъде една и съща в целия ЕС.

58. *Международни предавания на данни* (членове 25—26). Това е област, която предизвика множество критики поради липсата на единна практика на територията на ЕС. Заинтересованите страни критикуваха, че решенията на Комисията за достатъчност се тълкуват и прилагат много различно от държавите-членки. Задължителните фирмени правила (ЗФП) са друг елемент, по отношение на който ЕНОЗД препоръчва по-нататъшна хармонизация (вж. глава 9).

59. *Национални органи за защита на данните* (член 28). Към националните ОЗД се прилагат силно различаващи се правила в 27-те държави-членки, по-специално във връзка със статута, ресурсите и правомощията им. Член 28 допринесе отчасти за тези различия поради недостатъчната си точност ([32]) и следва да бъде уточнен допълнително в съответствие с решението на Съда на Европейския съюз по дело C-518/07 ([33]) (вж. по-нататък глава 10).

5.4. *Опростяване на системата за уведомяване*

60. Изискванията за уведомяване (членове 18—21 от Директива 95/46/ЕО) са друга област, в която на държавите-членки е била предоставена досега значителна свобода. В съобщението правилно се признава, че хармонизираната система би намалила разходите, както и административната тежест за администраторите на лични данни ([34]).

61. Това е област, в която опростяването следва да бъде основна цел. Преразглеждането на рамката за защита на данните е единствена по рода си възможност за по-нататъшно опростяване и/или намаляване на обхвата на настоящите изисквания за уведомяване. Съобщението признава, че по общо съгласие на заинтересованите страни настоящата система за уведомяване е доста обременителна и не дава, сама по себе си, допълнителна стойност за защитата на личните данни на физическите лица ([35]). Ето защо ЕНОЗД приветства поетото от Комисията задължение да проучи различни възможности за опростяване на настоящата система за уведомяване.

62. Според него изходната точка за това опростяване ще бъде преминаване от система, в която уведомяването е правило, ако не е предвидено друго (т.е. „система за освобождаване“) към една по-целенасочена система. Системата за освобождаване се оказа неефикасна, тъй като бе приложена непоследователно в различните държави-членки ([36]). ЕНОЗД предлага да бъдат разгледани следните алтернативи:

([29]) Вж. Становище 1/2010 на РГ по член 29 относно понятията „администратор на лични данни“ и „лице, което обработва данните“ (WP 169).

([30]) Член 8, параграфи 4 и 5 разрешават понастоящем при определени условия на държавите-членки да определят допълнителни дерогации по отношение на чувствителните данни.

([31]) Вж. по този въпрос първия доклад на Комисията за прилагането на Директивата за защита на личните данни, цитиран по-горе, стр. 14.

([32]) Документ на РГ за бъдещето на неприкосновеността на личния живот, съображение 87.

([33]) Дело C-518/07, *Комисията с/у Германия*, все още непубликувано в ECR.

([34]) Виж бележка под линия на стр. 26.

([35]) Виж бележка под линия на стр. 26.

([36]) Доклад на работната група по член 29 относно задължението за уведомяване на работната група по член 29 на националните контролни органи, оптималното използване на изключенията и опростяванията и ролята на длъжностните лица за защита на данните в Европейския съюз, WP 106, 2005 г., стр. 7.

— ограничаване на задължението за уведомяване до специфични видове операции на обработка, свързани със специфични рискове (тези уведомления могат да предизвикат по-нататъшни стъпки, като предварителна проверка на обработването),

— задължение за проста регистрация, изискващо от администраторите на лични данни да се регистрират (за разлика от разширената регистрация на всички операции по обработката на данни).

Освен това може да се въведе стандартен общоевропейски формуляр за уведомяване, с оглед да се осигури хармонизиран подход по отношение на исканата информация.

63. Преразглеждането на настоящата система за уведомяване следва да се направи, без да се засяга подобряването на задълженията за предварителна проверка за определени задължения за обработване, за които може да се очаква, че ще представляват специфични рискове (като например крупни информационни системи). ЕНОЗД е за включване в новия правен инструмент на неизчерпателен списък на случаите, при които се изисква такава предварителна проверка. Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на ЕС предоставя полезен образец за тази цел ([37]).

5.5. *Регламент, не директива*

64. Накрая ЕНОЗД счита, че процедурата на преразглеждане е също възможност да се преразгледа видът на правния инструмент за защита на данните. Регламентът като единен инструмент, който е пряко приложим в държавите-членки, е най-ефективният начин да се защити основното право на защита на данните и да се създаде реален вътрешен пазар, в който личните данни могат да се движат свободно и в който степента на защита е еднаква, независимо от държавата или от сектора, където данните се обработват.

65. Един регламент би намалил мястото за противоречиви тълкувания и необосновани различия при изпълнението и прилагането на законодателството. Той би намалил също значението на определяне на законодателството, приложимо към операциите на обработване на територията на ЕС, което е един от най-спорните аспекти на настоящата система (вж. глава 9).

66. В сферата на защитата на данни изборът на регламент е още по-обоснован, тъй като:

— член 16 от ДФЕС издигна правото на защита на личните данни до равнището на Договора и предвижда — или дори налага — единна степен на защита на физическите лица в целия ЕС,

— обработката на данните се извършва в електронна среда, в която вътрешните граници между държавите-членки не са толкова важни.

67. Изборът на регламент като общ инструмент дава при необходимост възможност за разпоредби, насочени пряко към държавите-членки, където е нужна гъвкавост. Той освен това не засяга компетенцията на държавите-членки да приемат допълнителни правила за защита на данните, когато това е необходимо, в съответствие с правото на ЕС.

6. **Засилване на правата на физическите лица**

6.1. *Необходимост от засилване на правата*

68. ЕНОЗД подкрепя напълно съобщението, когато то предлага засилване на правата на физическите лица, тъй като съществуващите правни инструменти не осигуряват напълно ефективната защита, необходима в един все по-сложен дигитализиран свят.

69. От друга страна, развитието на дигитализиран свят води до рязко нарастване на събирането, използването и по-нататъшното предаване на лични данни по изключително сложен и непрозрачен начин. Физическите лица често не знаят или не разбират как става това, кой събира техните данни, нито как да упражняват контрол. Пример за това явление е мониторинга от страна на доставчици на рекламни мрежи на търсенията на физическите лица в мрежата с помощта на „бисквитки“ или други подобни похвати за целите на целевото рекламиране. Когато потребителите посещават интернет страници, те не очакват невидима трета страна да се включва в тези посещения и да създава регистри на потребителите въз основа на информация за техния начин на живот или на това какво харесват и какво не харесват.

70. От друга страна, развитието насърчава физическите лица да споделят проактивно своята лична информация, например в социалните мрежи. Все повече млади хора участват в социални мрежи и взаимодействат със свои връстници. Съмнително е дали тези (млади) хора съзнават мащаба на разкриваните от тях данни и дългосрочните последици от действията си.

6.2. *Увеличаване на прозрачността*

71. Прозрачността е от първостепенна важност при всеки режим за защита на данните, не само поради присъщата си стойност, но и защото дава възможност да бъдат приложени други принципи на защита на данните. Само ако физическите лица познават обработването на данни, те ще могат да упражняват правата си.

72. Няколко разпоредби в Директива 95/46/ЕО са посветени на прозрачността. Членове 10 и 11 включват задължение за предоставяне на информация на физическите лица за събирането на техни лични данни. Освен това в член 12 се признава правото на лицето да получи копие от личните си данни в разбираема форма (право на достъп). В член 15 се признава правото на лицето да има достъп до логиката, по която се вземат автоматизирани решения, водещи до правни последици. Накрая, но не на последно място по значение, член 6, параграф 1, буква а), изискващ обработването да бъде справедливо, също включва изискване за прозрачност. Личните данни не могат да се обработват по скрити или тайни причини.

([37]) Вж. член 27 от Регламента (ОВ L 8, 12.1.2001 г., стр. 1).

73. Съобщението предлага да се добави общ принцип на прозрачност. В отговор на това предложение ЕНОЗД подчертава, че идеята за прозрачност е вече неразделна част от настоящата правна рамка за защита на данните, макар да не е изрично формулирана. Такъв извод може да се направи въз основа на различните разпоредби, уреждащи прозрачността, както е посочено в предходното съображение. Според ЕНОЗД добавена стойност може да се получи чрез включване на *изричен* принцип на прозрачността, било със или без връзка със съществуващата разпоредба за справедливо обработване. Това ще увеличи правната сигурност и ще потвърди, че администраторът трябва при всички обстоятелства да обработва личните данни по прозрачен начин — не само при поискване или когато конкретна правна разпоредба го задължава да прави това.

74. Все пак по-важно може би е да се засилят съществуващите разпоредби, свързани с прозрачността, като настоящите членове 10 и 11 от Директива 95/46/ЕО. В тези разпоредби е указано каква информация се предоставя, но те не уточняват начините. По-конкретно ЕНОЗД предлага засилване на съществуващите разпоредби с добавянето на:

— Изискване администраторът да предоставя информация за обработването на данни по начин, който е лесно достъпен и лесен за разбиране, и при използване на ясни и недвусмислени формулировки ([38]). Информацията следва да бъде ясна, разбираема и добре видима. Разпоредбата може да включва също задължението да се осигури лесно разбиране на информацията. Това задължение ще направи неправомерни политиките за неприкосновеността на личния живот, които са неясни или трудно разбираеми.

— Изискване за предоставяне на информацията лесно и пряко на лицата, за които се събират данни. Информацията следва също така да бъде постоянно достъпна, а не да изчезва след много кратко време от електронната медия. Това ще помогне на потребителите да съхраняват и възпроизвеждат информацията в бъдеще, давайки възможност за допълнителен достъп.

6.3. *Подкрепа на задължение за докладване на нарушения на сигурността*

75. ЕНОЗД подкрепя въвеждането в общия инструмент на разпоредба за уведомяване при нарушения на сигурността на личните данни, която разширява задължението, включено в преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации за някои доставчици, като го отнася до всички администратори на лични данни, както се предлага в съобщението. Съгласно преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации задължението се прилага само за доставчици на електронни съобщителни услуги (доставчици на телефонни (включително VoIP) услуги и достъп до интернет. Други администратори на лични данни не попадат в обхвата на това задължение Причините, които обосновават задължението, се отнасят напълно и до администраторите на лични данни, които не са доставчици на електронни съобщителни услуги.

76. Уведомяването при нарушения на сигурността служи на различни цели. Най-очевидната от тях, подчертана от Комисията, е да служи като информационен инструмент за уведомяване на физическите лица относно рисковете, на които се излагат, когато се злоупотребява с личните им данни. Това може да им помогне да вземат необходимите мерки за намаляване на тези рискове. Например когато бъдат предупредени за нарушения, засягащи финансовите им данни, физическите лица ще могат, наред с други неща, да сменят паролите си или да закрият своите сметки. Освен това уведомяването при нарушения на сигурността допринася за ефективното прилагане на други принципи и задължения съгласно директивата. Така например изискванията за уведомяване при нарушения на сигурността са стимул за администраторите на лични данни да прилагат по-строги мерки за сигурност, за да се избягват нарушения. Това уведомяване е също така инструмент за засилване на отговорността на администраторите на лични данни и по-специално за повишаване на отчетността (вж. глава 7). Накрая, то служи като инструмент за правоприлагане от страна на органите за защита на данните (ОЗД). Уведомяването на ОЗД за нарушения може да доведе до проверка на общите практики на администратора на лични данни.

77. Специфичните правила относно нарушенията на сигурността в преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации бяха широко обсъдени по време на парламентарния етап на законодателната рамка, предшествал приемането на директивата. При тези обсъждания становищата на работната група по член 29 и ЕНОЗД бяха взети предвид заедно с мненията на други заинтересовани страни. Правилата отразяват схващанията на различни заинтересовани страни. Те представляват баланс на интереси: докато критериите, пораждащи задължението за уведомяване, са по принцип достатъчни за защита на физическите лица, те правят това, без да налагат прекалено обременителни и безполезни изисквания.

6.4. *Засилване на съгласието*

78. В член 7 от Директивата за защита на данните са изброени шест правни основания за обработването на лични данни. Съгласието на физическото лице е едно от тях. Администраторът на лични данни може да обработва лични данни само ако физическите лица са дали информирано съгласие данните им да бъдат събрани и след това обработени.

79. На практика потребителите често имат ограничен контрол върху своите данни, преди всичко в технологична среда. Един от използваните понякога начини е този на мълчаливото съгласие, т.е. на направен извод за съгласие. Той може да бъде направен от действие на лицето (напр. действието, състоящо се в използване на даден уебсайт,

([38]) Вж. съобщението, стр. 6.

се тълкува като съгласие за записване на данните на потребителя за търговски цели). Той може да се направи и от мълчание или бездействие (неизтриване на маркировката на отбелязано поле се счита за съгласие).

80. В съответствие с директивата, за да бъде съгласието валидно, то трябва да е информирано, дадено свободно и конкретно. То трябва да се състои в информирано посочване на желанията на физическото лице, с което то дава израз на съгласието си да бъдат обработени личните данни, отнасящи се до него. Начинът, по който се дава съгласието, трябва да бъде недвусмислен.

81. Съгласието, за което е направен извод от дадено действие и, още повече, от мълчание или бездействие, често пъти не е недвусмислено съгласие. Невинаги е ясно обаче какво точно е истинско, недвусмислено съгласие. Някои администратори на лични данни използват тази несигурност, като разчитат на начини, които не са подходящи за даване на истинско, недвусмислено съгласие.

82. Имайки предвид гореизложеното, ЕНОЗД подкрепя Комисията относно необходимостта да бъдат изяснени границите на съгласието и да се гарантира, че само съгласие, изразено по твърд начин, се приема като такова. В този контекст ЕНОЗД предлага следното ([39]):

— може да се помисли за разширяване на случаите, в които се изисква изрично съгласие и които към настоящия момент са ограничени до чувствителните данни,

— приемане на допълнителни правила за съгласие в интернет среда,

— приемане на допълнителни правила за съгласие да се обработват данни за вторични цели (напр. когато обработването е вторично по отношение на основното или не е очевидно),

— в допълнителен законодателен инструмент — било приет, било неприет от Комисията съгласно член 290 от ДФЕС, да се определи видът на изискваното съгласие, например като се уточни степента на съгласие за обработването на данни от приемо-предавателите за RFID на потребителските продукти или за други специфични технически способи.

6.5. *Преносимост на данните и правото да бъдеш забравен*

83. Преносимостта на данните и правото да бъдеш забравен са два взаимно свързани принципа, предложени в съобщението за засилване на правата на лицата, за които се събират данни. Те са допълващи към принципите, посочени вече в директивата, като предоставят право на лицето, за което се събират данни, да възрази против по-нататъшното обработване на данните му и задължение за администратора на лични данни да заличи информацията, когато тя не е вече необходима за целите на обработването.

84. Тези две нови понятия имат добавена стойност най-вече в контекста на информационното общество, в което все повече данни се съхраняват автоматично и се пазят за неопределени периоди от време. Практиката показва, че дори ако данните са въведени от самото лице, за което се събират данни, степента на контрол, който то ефективно има върху своите лични данни, е на практика много ограничена. Казаното е още по-вярно, като се има предвид гигантската памет, която представлява днес интернет. Освен това от икономическа гледна точка за администратора на лични данни е по-скъпоструващо да заличава данните, отколкото да ги съхранява. Ето защо упражняването на правата на физическите лица е противопоставено на естествената икономическа тенденция.

85. Както преносимостта на данните, така и правото да бъдеш забравен могат да допринесат за промяна на баланса в полза на лицата, за които се събират данни. Целта на преносимостта на данните ще бъде да се предостави повече контрол на лицето върху неговата информация, докато правото да бъдеш забравен ще осигури автоматичното заличаване на информацията след определен период от време, дори ако лицето, за което се събират данни, не предприеме нищо или дори не знае, че данните са били изобщо съхранени.

86. По-конкретно преносимостта на данните се разбира като възможност на потребителите да променят предпочитанията си относно обработването на техните данни във връзка, по-специално, с новите технологични услуги. Това все повече се отнася до услуги, които предполагат съхранение на информация, включително на лични данни, като мобилната телефония, и услуги, които съхраняват снимки, електронни писма и друга информация, използвайки понякога изчислителни облаци.

87. Физическите лица трябва да могат лесно и свободно да сменят доставчика и да предават личните си данни на друг доставчик на услуги. ЕНОЗД счита, че съществуващите права, установени в Директива 95/46/ЕО, могат да бъдат засилени чрез включване на право на преносимост, по-специално в контекста на услугите на информационното общество, за да се помогне на физическите лица да са сигурни, че доставчиците и другите администратори ще им предоставят достъп до личната им информация, като същевременно се гарантира, че предишните доставчици или други администратори ще заличат тази информация, дори ако биха желали да я запазят за свои собствени правомерни цели.

88. Едно новоформулирано „право да бъдеш забравен“ ще гарантира заличаването на личните данни или забраната за по-нататъшното им използване, без да са необходими действия от страна на лицето, за което се събират данни,

([39]) РГ по член 29 работи понастоящем върху становище относно понятието „съгласие“. Това становище може да доведе до допълнителни предложения.

но при условие че тези данни са били вече съхранявани през известен период от време. Данните, с други думи, ще получат нещо като срок на валидност. Този принцип е вече потвърден в националната съдебна практика или е приложен в специфични сектори, например за полицейски, криминални досиета или дисциплинарни досиета: съгласно някои национални законодателства информацията за физически лица се заличава автоматично или престава да бъде използвана или разпространявана по-нататък, по-специално след определен период от време, без да е необходим предварителен анализ на всеки случай поотделно.

89. В този смисъл новото „право да бъдеш забравен“ следва да бъде свързано с преносимостта на данните. Добавената от него стойност ще се състои в това, че то няма да изисква усилия, нито настойчивост от страна на лицето, за което се събират данни, да бъдат данните му заличени, тъй като това ще става по обективен и автоматичен начин. Само при много специални обстоятелства, когато може да бъде установена специална нужда за по-дълго задържане на данните, администраторът на лични данни може да получи право да запази данните. Това „право да бъдеш забравен“ ще прехвърли по този начин тежестта на доказване от физическото лице върху администратора на лични данни и ще представлява настройка „неприкосновеност на личния живот по подразбиране“ за обработването на личните данни.

90. ЕНОЗД счита, че правото да бъдеш забравен може да се окаже особено полезно в контекста на услугите на информационното общество. Задължението за заличаване или спиране на по-нататъшното разпространяване на информацията след определен период от време е особено уместно в медиите или в интернет и по-конкретно в социалните мрежи. То ще бъде полезно и по отношение на терминалните устройства: данните, записани в мобилни апарати или компютри, ще бъдат автоматично заличени или блокирани след определен период от време, когато те не са вече във владение на физическото лице. В този смисъл правото да бъдеш забравен може да бъде превърнато в задължение за „неприкосновеност на личния живот още при разработването“.

91. В обобщение, ЕНОЗД счита, че преносимостта на данните и правото да бъдеш забравен са полезни принципи. Може би си струва те да бъдат включени в правния инструмент, но вероятно ограничени в рамките на електронната среда.

6.6. Обработване на лични данни на деца

92. Директива 95/46/ЕО не предвижда специални правила във връзка с обработването на лични данни на деца. Това не отчита необходимостта за специфична защита на децата при специфични обстоятелства поради тяхната уязвимост и защото така се създава правна несигурност, по-специално в следните области:

— събирането на данни на деца и начинът, по който те трябва да бъдат уведомявани за събирането,

— начинът, по който се получава съгласието на децата. Тъй като няма специални правила за това как да бъде взето съгласието на децата и за възрастта, под която децата следва да се считат за такива, тези въпроси се третират съгласно националното право, което е различно в отделните държави-членки ([40]),

— начинът и условията, при които децата или техните законни представители могат да упражняват правата им съгласно директивата.

93. ЕНОЗД счита, че специфичните интереси на децата ще бъдат най-добре защитени, ако новият правен инструмент съдържа допълнителни разпоредби, отнасящи се конкретно до събирането и по-нататъшното обработване на данни на деца. Такива специфични разпоредби ще създадат освен това правна сигурност в тази специфична област и ще бъдат от полза за администраторите на лични данни, които понастоящем са изложени на различни законови изисквания.

94. ЕНОЗД предлага включването на следните разпоредби в правния инструмент:

— изискване информацията да бъде съобразена с децата, за да бъде по-лесно за тях да разберат какво означава събирането на данни от тях,

— други изисквания за информация, съобразена с децата, относно начина, по който трябва да се предоставя информацията и евентуално относно съдържанието,

— специална разпоредба, защитаваща децата срещу поведенческо рекламиране,

— принципът на ограничаване в рамките на целта следва да се засили по отношение на данните за деца,

— някои категории данни не бива изобщо да се събират от деца,

— възрастова граница. Под тази граница информацията от деца следва по принцип да се събира само с изрично и подлежащо на проверка родителско съгласие,

— ако е необходимо родителско съгласие, ще се наложи да бъдат установени правила за това как да се удостовери възрастта на детето, с други думи, как да се

([40]) Съгласието е свързано обикновено с възрастта, на която децата могат да поемат договорни задължения. Това е възрастта, на която се предполага, че децата са стигнали до определена степен на зрелост. Испанското право например изисква родителско съгласие за събирането на данни за деца, които не са навършили 14-годишна възраст. Над тази възраст се приема, че децата са в състояние да дадат съгласие. В Обединеното кралство Законът за защита на данните не посочва конкретна възраст или праг. Органите за защита на данните в Обединеното кралство обаче е дал тълкуване, че децата на възраст над 12 години могат да дават съгласие. И напротив, децата на възраст под 12 години не могат да дават съгласие и за да бъдат получени техните лични данни, първо трябва да се вземе разрешението на родител или попечител.

разбере, че детето е малолетно или непълнолетно и как да се провери родителското съгласие. Това е област, в която ЕС може да почерпи идеи от други държави, например от САЩ ([41]).

6.7. *Механизми за колективна защита*

95. Засилването на правата на физическите лица по същество ще бъде безпредметно, ако липсват ефективни процедурни механизми за прилагането на тези права. В този контекст ЕНОЗД препоръчва в законодателството на ЕС да бъдат въведени механизми за колективна защита при нарушаване на правилата за защита на данните. По-специално, механизмите за колективна защита, оправомощаващи групи граждани да обединят жалбите си в един иск, може да се окажат много мощен инструмент за улесняване на прилагането на правилата за защита на данните ([42]). Това нововъведение се подкрепя и от органите за защита на данните в документа на работната група за бъдещето на неприкосновеността на личния живот.

96. В по-маловажни случаи едва ли жертвите на нарушаване на правилата за защита на данните биха предприели индивидуални искове срещу администраторите, като се имат предвид разходите, забавянията, несигурностите, рисковете тежестите, на които биха се изложили. Тези трудности могат да бъдат преодолени или значително облекчени, ако съществува система за колективна защита, оправомощаваща жертвите на нарушения да обединят отделните си жалби в един иск. ЕНОЗД е също така за оправомощаването на квалифицирани структури, като потребителски асоциации или публични органи, да подават искове за щети от името на жертви на нарушения при защита на данните. Тези искове следва да не засягат правото на лицето, за което се събират данни, да подава индивидуални искове.

97. Колективните искове са важни не само за гарантиране на пълна компенсация или за други коригиращи действия; те освен това упражняват косвено засилваща възпирането функция. Рискът от понасяне на големи колективни щети по такива искове ще увеличи стимулите за администраторите да спазват ефективно правилата. В това отношение засиленото правоприлагане от страна на частни лица посредством механизми за колективна защита ще допълни правоприлагането от публични органи.

98. В съобщението липсва становище по тази тема. ЕНОЗД е в течение на продължаващата дискусия на европейско равнище относно въвеждането на колективна защита на потребителите. Той освен това разбира риска от ексцеси, до който тези механизми може да доведат, като се има предвид опитът в други правни системи. Тези фактори обаче не дават според него достатъчно доводи за отхвърляне или отлагане на тяхното въвеждане в законодателството за защита на данните, като се имат предвид ползите, до които ще доведат ([43]).

7. **Засилване на ролята на организациите/администраторите**

7.1. *Общи положения*

99. ЕНОЗД счита, че освен засилването на правата на физическите лица, съвременният правен инструмент за защита на данните трябва да включва необходимите инструменти за засилване на отговорността на администраторите на лични данни. По-специално рамката трябва да съдържа стимули за администраторите на лични данни в частния или в публичния сектор да включват проактивно мерки за защита на данните в своите работни процеси. Тези инструменти ще бъдат преди всичко полезни, тъй като, както бе казано вече, технологичните развития доведоха до рязко нарастване на събирането, използването и понататъшното предаване на лични данни, а това увеличава рисковете за неприкосновеността на личния живот и защитата на личните данни на физическите лица, които следва да бъдат компенсирани по ефективен начин. На второ място, в настоящата рамка липсват — с изключение на няколко добре формулирани разпоредби — такива инструменти и администраторите на лични данни могат да подходят *изчаквателно* към защитата на данни и неприкосновеността на личния живот и да действат едва след като е възникнал проблем. Този подход е отразен в статистически данни, показващи лоши практики на съответствие и загуби на данни като често възникващи проблеми.

100. Според ЕНОЗД съществуващата рамка не е достатъчна за ефективна защита на личните данни при настоящите и бъдещите условия. Колкото по-големи са рисковете, толкова по-голяма е необходимостта от прилагане на конкретни мерки, които защитават информацията на практическо равнище и дават ефективна защита. Ако тези проактивни мерки не бъдат де факто изпълнени, грешките, пропуските и небрежността вероятно ще продължат, застрашавайки неприкосновеността на личния живот на физическите лица в това все по-дигитализиращо се общество. За постигането на тази цел ЕНОЗД предлага следните мерки.

7.2. *Засилване на отчетността на администраторите на лични данни*

101. ЕНОЗД предлага да се добави нова разпоредба в правния инструмент, изискваща от администраторите на лични данни да осъществяват достатъчни и ефикасни мерки за изпълнение на принципите и задълженията съгласно правния инструмент и при поискване да представят доказателства за това.

([41]) В САЩ регламентът COPPA изисква от операторите на интернет страниците, които се занимават с търговия и са насочени към деца на възраст до 13 години, да получат родителско съгласие, преди да събират лична информация, а от операторите на интернет страниците, които се занимават с търговия и са насочени към широката публика, да си дават реално сметка, че някои от посетителите са деца.

([42]) Вж. също Становище на ЕНОЗД от 25 юли 2007 г. относно Съобщението на Комисията до Европейския парламент и Съвета относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни, (ОВ C 255, 27.10.2007 г., стр. 10).

([43]) Някои национални законодателства предвиждат вече подобни механизми.

102. Подобна разпоредба не е изцяло нова. Член 6, параграф 2 от Директива 95/46/ЕО посочва принципите, отнасящи се до качеството на данните, и изтъква, че „администраторът осигурява спазването на параграф 1“. Член 17, параграф 1 също изисква от администраторите на лични данни да прилагат мерки както от технически, така и от организационен характер. Приложното поле на тези разпоредби е обаче ограничено. Добавянето на обща разпоредба за отчетността ще стимулира администраторите да въведат проактивни мерки, за да могат да спазват във всяко отношение законодателството за защита на данните.

103. Една разпоредба за отчетността ще задължи администраторите на лични данни да въведат вътрешни механизми и контролни системи, осигуряващи съответствие с принципите и задълженията съгласно рамката. Това ще наложи например участие на висшето ръководство в политиките за защита на данните, картиране на процедурите за осигуряване на правилна идентификация на всички операции по обработването на данни, наличие на обвързващи политики за защита на данните, които трябва освен това да бъдат постоянно преразглеждани и актуализирани, за да включат в приложното си поле новите операции за обработване на данни, спазване на принципите за качество на данните, уведомяване, сигурност, достъп и т.н. То ще наложи също администраторите да съхраняват документи за доказване на съответствие пред органите при поискване от тяхна страна. Представянето на доказателства за съответствие пред широката общественост следва в някои случаи също да стане задължително. Това може да се направи например като администраторите бъдат задължени да включват защитата на данните в публичните (годишните) доклади, когато такива доклади се изготвят задължително на други основания.

104. Очевидно видът на вътрешните и външните мерки, които се прилагат, трябва да бъде подходящ и зависи от фактите и обстоятелствата във всеки конкретен случай. Не е все едно дали администраторът обработва няколко стотици записи на потребители, състоящи се само от имена или адреси, или обработва данни на милиони пациенти, включително техните медицински истории. Същото е в сила и за специфичните начини, по които трябва да се оценява ефективността на мерките. Необходимо е степенуване.

105. Общият всеобхватен правен инструмент за защита на данните не следва да определя специфичните изисквания за отчетността, а само основните елементи. Съобщението предвижда някои елементи за засилване на отговорността на администраторите на лични данни, които заслужават категорично одобрение. По-специално ЕНОЗД подкрепя напълно идеята длъжностните лица за защита на данните и оценките на въздействието върху неприкосновеността на личния живот да станат задължителни при определени прагови условия.

106. Освен това ЕНОЗД препоръчва да се делегират правомощия на Комисията в съответствие с член 290 от ДФЕС за допълване на основните изисквания, необходими, за да се отговори на стандартите за отчетност. Използването на тези правомощия ще увеличи правната сигурност на администраторите на лични данни и ще хармонизира съответствието в целия ЕС. При разработването на тези специфични инструменти следва да се направят консултации с работната група по член 29 и ЕНОЗД.

107. Накрая, конкретните мерки за отчетност, прилагани от администраторите на лични данни, могат да бъдат наложени и от органите за защита на данните в контекста на техните правомощия по прилагане на законодателството. За тази цел на органите за защита на данните следва да се дадат нови правомощия, позволяващи им да налагат коригиращи мерки или санкции. Примерите трябва да включват изготвяне на вътрешни програми за съответствие, прилагане на принципа за неприкосновеност на личния живот още при разработването на специфични продукти и услуги и т.н. Коригиращи мерки следва да се налагат само ако са адекватни, пропорционални и ефективни за осигуряване на съответствие с приложимите стандарти с правно действие.

7.3. Неприкосновеност на личния живот още при разработването

108. Принципът за неприкосновеност на личния живот още при разработването се отнася до включването на защитата на данни и неприкосновеността на личния живот от самото начало на създаване на нови продукти, услуги и процедури, които предполагат обработване на лични данни. Според ЕНОЗД принципът за неприкосновеност на личния живот още при разработването е елемент на отчетността. Следователно администраторите на лични данни ще бъдат също длъжни да доказват, че са приложили принципа за неприкосновеност на личния живот още при разработването, когато това е уместно. Неотдавна 32-та Международна конференция на комисарите по защита на личните данни и неприкосновеността на личния живот издаде резолюция, признаваща принципа за неприкосновеност на личния живот още при разработването като съществен елемент от основната неприкосновеност на личния живот ([44]).

109. Директива 95/46/ЕО съдържа някои разпоредби, насърчаващи защитата на личния живот още при разработването ([45]), но не определя изрично такова задължение. ЕНОЗД отбелязва със задоволство одобрението от страна на Комисията на принципа за неприкосновеност на личния живот още при разработването като инструмент, осигуряващ спазване на правилата за защита на данни. Той предлага да се включи задължителна разпоредба, въвеждаща задължение за „неприкосновеност на личния живот още при разработването“, което може да се основава на доразвиване на съображение 476 от Директива 95/46/ЕО. По-конкретно разпоредбата следва да изисква изрично от администраторите на лични данни

([44]) Резолюция относно защитата на личния живот още при разработването, приета от 32-та Международна конференция на комисарите по защита на личните данни и неприкосновеността на личния живот, Ерусалим, 27—29 октомври 2010 г.

([45]) Директивата съдържа разпоредби, които непряко и в различни ситуации изискват прилагане на принципа за неприкосновеност на личния живот още при разработването. По-специално, член 17 изисква администраторите на данните да прилагат подходящи технически и организационни мерки за защита срещу незаконна обработка на данни. Директивата за правото на неприкосновеност на личния живот и електронни комуникации е по-ясна. Член 14, параграф 3 предвижда, че „когато се изисква, могат да се приемат мерки, за да се осигури терминалното оборудване да бъде конструирано по начин, който е съвместим с правото на потребителите да защитават и контролират използването на техните лични данни, в съответствие с Директива 1999/5/ЕО и Решение 87/95/ЕИО на Съвета от 22 декември 1986 г. относно стандартизация в областта на информационните технологии и съобщения“.

да изпълняват технически и организационни мерки, както по време на проектиране на системите за обработка, така и по време на самата обработка, по-специално с цел да се гарантира защитата на личните данни и да се предотврати всякаква неразрешена обработка ([46]).

110. Въз основа на подобна разпоредба администраторите на лични данни ще бъдат длъжни — наред с други неща — да осигурят проектиране на системите за обработка на данните по такъв начин, че да обработват колкото се може по-малко лични данни, да прилагат настройки по подразбиране за неприкосновеността на личния живот, например в социалните мрежи, да не дават по подразбиране достъп на други до профилите на физическите лица и да използват инструменти, даващи възможност на потребителите да защитават по-добре личните си данни (напр. контрол на достъпа, криптиране).

111. Предимствата на по-изричното формулиране на принципа за неприкосновеност на личния живот още при разработването може да бъдат обобщени, както следва:

— то ще подчертае значението на самия принцип като инструмент за гарантиране, че процедурите, продуктите и услугите се проектират от самото начало, като се изхожда от неприкосновеността на личния живот,

— ще намали нарушенията на неприкосновеността на личния живот, ще сведе до минимум ненужното събиране на данни и ще оправомощи физическите лица да имат свободен избор по отношение на личните си данни,

— ще избегне необходимостта от използване на палиативни средства за решаване на проблеми, които може да е трудно, ако не и невъзможно да бъдат отстранени,

— ще улесни също така ефективното прилагане и налагане на този принцип от страна на органите за защита на данните.

112. Комбинираният ефект от това задължение ще доведе до по-голямо търсене на продукти и услуги, съобразени с принципа за неприкосновеност на личния живот още при разработването, което ще увеличи стимулите за индустрията да отговори на това търсене. Следва да се помисли, в допълнение на всичко това да се създаде отделно задължение за проектантите и производителите на нови продукти и услуги, за които е вероятно да окажат въздействие върху защитата на данните и неприкосновеността на личния живот. ЕНОЗД предлага да се включи такова отделно задължение, което може да помогне допълнително на администраторите на лични данни да изпълняват своите собствени задължения.

113. Кодификацията на принципа за неприкосновеност на личния живот още при разработването може да бъде допълнена с разпоредба, определяща общи изисквания за неприкосновеност на личния живот още при разработването, приложими в различните отрасли, продукти и услуги, като например осигуряване на мерки за оправомощаване на потребителите, които да се приемат в съответствие с принципа.

114. Освен това ЕНОЗД препоръчва да се делегират правомощия на Комисията в съответствие с член 290 от ДФЕС за допълване — където е уместно — на основните изисквания за неприкосновеност на личния живот още при разработването при избрани продукти и услуги. Използването на тези правомощия ще увеличи правната сигурност на администраторите на лични данни и ще хармонизира съответствието в целия ЕС. При разработването на тези специфични инструменти следва да се направят консултации с работната група по член 29 и ЕНОЗД (вж. също съображение 106 относно отчетността).

115. Накрая, на органите за защита на данните следва да се дадат правомощия да налагат коригиращи мерки или санкции при подобни ограничителни условия като вече посочените в съображение 107, когато администраторите не са вече изпълнили задължението си да вземат конкретни мерки в случаи, при които това се налага.

7.4. Услуги, свързани със сертифициране

116. Съобщението признава необходимостта да се проучи създаването на схеми на ЕС за сертифициране на продукти и услуги, спазващи неприкосновеността на личния живот. ЕНОЗД подкрепя напълно тази цел и предлага включване на разпоредба за тяхното създаване и евентуалните им последици за целия ЕС, която може по-късно да бъде разработена допълнително в нов законодателен акт. Тази разпоредба следва да допълва разпоредбите за отчетност и неприкосновеност на личния живот още при разработването.

117. Схемите за доброволно сертифициране ще дадат възможност да се провери, че даден администратор на лични данни е въвел мерки за съответствие с правния инструмент. Освен това администраторите на лични данни — или дори продуктите и услугите, получили знак за сертифициране — ще имат вероятно конкурентно предимство пред останалите. Тези схеми ще помогнат също на органите за защита на данните в тяхната надзорна и правоприлагаща функция.

8. **Глобализация и приложимо законодателство**

8.1. Ясна необходимост от по-последователна защита

118. Както бе посочено по-горе в глава 2, предаването на лични данни отвъд границите на ЕС нарасна експоненциално в резултат на развитието на нови технологии, ролята на мултинационалните компании и нарастващото влияние на правителствата в обработването и обмена на лични данни в международен мащаб. Това е една от основните причини, обосноваващи преразглеждането на настоящата правна рамка. Следователно това е една от областите, в които ЕНОЗД настоява за амбициозност и ефективност, тъй като има ясна необходимост от по-последователна защита, когато данните се обработват извън ЕС.

([46]) Съгласно настоящата рамка съображение 46 поощрява администраторите да прилагат такива мерки, но съображенията нямат естествено обвързваща сила.

8.2. *Инвестиране в международни правила*

119. Според ЕНОЗД са нужни повече инвестиции в разработването на международни правила. Повече хармонизация по отношение на степента на защита на личните данни в целия свят ще внесе значителна яснота по същността на принципите, които трябва да бъдат спазвани, и по условията за предаване на данни. Тези глобални правила ще трябва да намерят компромисно решение между изискването за висок стандарт на защита на данните, включващ основните елементи на ЕС за защита на данните, и регионалната специфика.

120. ЕНОЗД подкрепя амбициозната работа, извършена досега в рамките на Международна конференция на комисарите по защита на личните данни за разработването и разпространението на така наречените „стандарти от Мадрид“, с цел те да бъдат включени в задължителен инструмент и да доведат евентуално до свикване на междуправителствена конференция ([47]). Той призовава Комисията да предприеме необходимите инициативи в помощ на осъществяването на тази цел.

121. Според ЕНОЗД важно е също така да се осигури последователност между тази инициатива за международни стандарти, настоящото преразглеждане на рамката на ЕС за защита на данните и други развития, като настоящото преразглеждане на Основните насоки на ОИСР за защитата на личния живот и на Конвенция 108 на Съвета на Европа, която е открита за подписване от трети държави (вж.също съображение 17). ЕНОЗД счита, че Комисията трябва да изиграе тук особена роля, като уточни как ще се постигне такава последователност в преговорите с ОИСР и Съвета на Европа.

8.3. *Изясняване на критериите за приложимо законодателство*

122. Тъй като пълна последователност не може да се постигне лесно, ще останат — поне в близкото бъдеще — известни различия между законодателствата в ЕС и още повече извън границите на ЕС. ЕНОЗД счита, че новият правен инструмент ще трябва да изясни критериите, определящи приложимото законодателство, и да осигури опростени механизми за потоците данни, както и отчетност на факторите, участващи в тези потоци.

123. На първо място, правният инструмент следва да гарантира, че законодателството на ЕС се прилага, когато лични данни се обработват извън границите на ЕС, но при наличие на обосновано искане за прилагане на законодателството на ЕС. Примерът с неевропейските услуги „изчислителни облаци“, насочени към лица, постоянно пребиваващи в ЕС, говори ясно, че това е необходимо. В среда, където данните не се съхраняват и обработват физически на определено място, където доставчици на услуги и потребители, разположени в различни държави, оказват променящо въздействие върху данните, е много трудно да се определи кой е отговорен за съответствието с кои принципи за защита на данните. Дават се указания, по-специално от органите за защита на данните, относно тълкуването и прилагането на Директива 95/46/ЕО в такива случаи, но само указания не стигат, за да се гарантира сигурност в тази нова среда.

124. На територията на ЕС необходимостта от повече прецизност на правната рамка и от опростен критерий за определяне на приложимото законодателство е подчертана от работната група по член 29 в едно неотдавна публикувано становище ([48]).

125. Според ЕНОЗД за предпочитане е вариантът, при който правният инструмент да бъде изложен в регламент, който ще доведе до едни и същи правила, приложими във всички държави-членки. Един регламент ще направи не толкова важно определянето на приложимото законодателство. Това е една от причините, поради които ЕНОЗД е категорично за приемането на регламент. Регламентът би дал обаче и известна свобода на действие на държавите-членки. Ако в новия инструмент се запази възможност за значителна свобода на действие, ЕНОЗД ще подкрепи предложението на работната група за преминаване от разделно прилагане на различните национални законодателства към централизирано прилагане на единно законодателство във всички държави-членки, в които е установен администратор. Той пледира също за повече сътрудничество и съгласуваност между органите за защита на данните при транснационалните дела и жалби (вж. глава 10).

8.4. *Опростяване на механизмите за потоците данни*

126. Необходимостта от последователност и високи критерии трябва да се има предвид не само във връзка с глобалните принципи за защита на данните, но и по отношение на международните предавания на данни. ЕНОЗД подкрепя напълно целта на Комисията да опрости настоящите процедури за международни предавания на данни и да осигури по-единен и последователен подход по отношение на трети държави и международни организации.

127. Механизмът на потоците данни включа както предавания в частния сектор, по-специално по договорните клаузи на задължителните фирмени правила (ЗФП), така и предавания между публични органи. ЗФП са един от елементите, при които е желателен по-последователен и по-опростен подход. ЕНОЗД препоръчва условията за ЗФП да бъдат уредени в новия правен инструмент ([49]) чрез:

— изрично признаване на ЗФП като инструменти, предоставящи достатъчни гаранции,

— излагане на основните елементи/условия за приемането на ЗФП,

([47]) Както се предлага в резолюцията за международните стандарти, приета от 32-та Международна конференция на комисарите по защита на личните данни и неприкосновеността на личния живот, Ерусалим, 27—29 октомври 2010 г.

([48]) Становище 8/2010 на работната група по член 29 относно приложимото законодателство, WP 179.

([49]) За международните предавания на данни вж. също глава 8 от настоящото становище.

— създаване на процедури за сътрудничество при приемането на ЗФП, включително на критерии за избор на водещ надзорен орган („обслужване на едно гише“).

9. **Областта на полицията и правосъдието**

9.1. *Общият инструмент*

128. Комисията нееднократно е изтъквала значението на засилване на защитата на данни в контекста на правоприлагането и предотвратяването на престъпления, където обменът и използването на лична информация се увеличиха значително. В Стокхолмската програма, одобрена от Европейския съвет, също се посочва силният режим на защита на данните като основна предпоставка за стратегията на ЕС за управление на информацията в тази област ([50]).

129. Преразглеждането на общата рамка за защита на данните е идеална възможност за постигане на напредък в това отношение, особено след като Комисията с право описва Рамково решение 2008/977/ПВР като недостатъчно ([51]).

130. В раздел 3.2.5 на настоящото становище ЕНОЗД изложи своите аргументи защо областта на полицейското и съдебното сътрудничество следва да бъде включена в общия инструмент. Включването на полицията и правосъдието има редица допълнителни предимства. То означава, че правилата няма да се прилагат вече само към трансграничния обмен на данни ([52]), но и към вътрешната обработка. Достатъчната защита при обмена на лични данни с трети държави ще бъде по-добре осигурена, в това число и във връзка с международните споразумения. Освен това ОЗД ще имат същите широки и хармонизирани правомощия по отношение на полицейските и съдебните органи, каквито имат по отношение на администраторите на лични данни. Накрая, настоящият член 13, предоставящ на държавите-членки правомощия да приемат специфични законодателни актове за ограничаване на задълженията и правата съгласно общия инструмент за специфичните публични интереси, ще трябва да се прилага по същия рестриктивен начин, по какъвто се прилага в други области. По-специално, специфичните предпазни мерки, предоставени по силата на общия инструмент в тази област, ще трябва да се спазват и в националното законодателство, прието в областта на полицейското и съдебното сътрудничество.

9.2. *Допълнителни специфични правила за полицията и правосъдието*

131. Включването им не изключва обаче специалните правила и дерогации, които вземат надлежно предвид особеностите в този сектор в съответствие с Декларация 21, приложена към Лисабонския договор. Може да се предвидят ограничения на правата на лицата, за които се събират данни, но тези ограничения трябва да бъдат необходими, пропорционални и да не променят основните елементи на самото право. Следва да се подчертае в този контекст, че Директива 95/46/ЕО, включително нейният член 13, се прилага понастоящем към правоприлагането в различни области (като данъчно облагане, митници, борба с измамите), които не се отличават принципно от много дейности в областта на полицията и правосъдието.

132. Освен това специфични предпазни мерки трябва да се въведат за компенсации на лицето, за което се събират данни, като му се предостави допълнителна защита в област, в която обработката на лични данни може да бъде по-натрапчива.

133. С оглед на гореизложеното ЕНОЗД счита, че новата рамка следва да включва най-малко следните елементи, в съответствие с Конвенция 108 и Препоръка № R (87) 15:

— разграничение между различните категории данни и досиета в съответствие с тяхната точност и надеждност в потвърждение на принципа, че данните, основаващи се на факти, следва да се разграничават от данните, основаващи се на мнения или лични оценки,

— разграничение между различните категории лица, за които се събират данни (заподозрени в престъпления, жертви, свидетели), и досиета (временни, постоянни и разузнавателни досиета). Специфични условия и предпазни мерки трябва да се предвидят при обработката на данни на незаподозрени лица,

— механизми за осигуряване на периодична проверка и корекция, за да се гарантира качеството на обработваните данни,

— специфични разпоредби и/или предпазни мерки може да бъдат разработени във връзка с (все по-актуалната) обработка на биометрични и генетични данни в областта на правоприлагането. Тяхното използване следва да се ограничи само в случаите, при които няма на разположение по-щадящи средства за осигуряване на същия резултат ([53]),

— условия за предаване на лични данни на некомпетентни органи и частноправни субекти, както и за достъп и по-нататъшно използване от правоприлагащите органи на лични данни, събрани от частноправни субекти.

([50]) Вж. по този въпрос Становище на ЕНОЗД от 30 септември 2010 г. относно съобщението на Комисията до Европейския парламент и до Съвета „Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието“, съображения 9—19.

([51]) Вж. раздел 3.2.5 по-горе.

([52]) Такова е към настоящия момент приложното поле на Рамково решение 2008/977/ПВР.

([53]) В тази насока вж. Документ на РГ за бъдещето на неприкосновеността на личния живот, съображение 112.

9.3. *Секторно-специфични режими на защита на данните*

134. В съобщението се посочва, че „рамковото решение не заменя различните секторно-специфични законодателни актове за полицейско и съдебно сътрудничество по наказателноправни въпроси, приети на равнище ЕС, и по-специално, които уреждат функционирането на Европол, Евроюст, Шенгенската информационна система (ШИС) и Митническата информационна система (МИС), които или съдържат специални режими за защита на данните и/или обикновено се позовават на инструментите за защита на данните на Съвета на Европа“.

135. Според ЕНОЗД новата правна рамка следва да бъде колкото е възможно по-ясна, по-проста и по-последователна. Когато нараства броят на различните режими, прилагани например към Европол, Евроюст, ШИС и Прюм, спазването на правилата остава сложно или дори все повече се усложнява. Това е една от причините, поради които ЕНОЗД е за всеобхватен правен инструмент за всички сектори.

136. ЕНОЗД разбира обаче, че съгласуването на правилата от различните системи ще изисква много работа, която трябва да се извърши внимателно. ЕНОЗД счита, че постепенният подход, посочен в съобщението, е разумен, стига да остане ясен и отчетлив ангажиментът за гарантиране на висока степен на защита на данните по последователен и ефективен начин. Казано по-конкретно:

— като първи етап общият правен инструмент за защита на данните следва да се направи приложим към всяка обработка в областта на полицейското и съдебното сътрудничество, включително уточненията за полицията и правосъдието (както е изложено в 9.2),

— на втория етап секторно-специфичните режими за защита на данните следва да бъдат съгласувани с този общ инструмент. Комисията следва да поеме задължение да приеме предложения за този втори етап в краткосрочна и уточнена времева рамка.

10. **Органите за защита на данните (ОЗД) и сътрудничеството между тях**

10.1. *Засилване на ролята на ОЗД*

137. ЕНОЗД подкрепя напълно целта на Комисията да реши въпроса за статута на органите за защита на данните (ОЗД) и да постави по-ясно ударение върху засилването на независимостта, ресурсите и правомощията им по прилагане на законодателството.

138. ЕНОЗД настоява също върху необходимостта от изясняване в новия правен инструмент на съществуването понятие за независимостта на ОЗД. Съдът на Европейския съюз издаде неотдавна решение по този въпрос по дело C-518/07 ([54]), в което той подчертава, че независимост означава липсата на всякакво външно влияние. ОЗД не може да иска, нито да получава указания от когото и да било. ЕНОЗД предлага тези елементи на независимостта да бъдат изрично кодифицирани в законодателния акт.

139. За да могат да изпълняват своите задачи, на ОЗД трябва да бъдат дадени достатъчно човешки и финансови ресурси. ЕНОЗД предлага включването на това изискване в законодателния акт ([55]). Накрая, той изтъква необходимостта да се гарантира, че властите са хармонизирали напълно правомощията за разследване и налагане на достатъчно възпиращи и коригиращи мерки и санкции. Това ще засили правната сигурност на лицата, за които се събират данни, и на администраторите на лични данни.

140. Засилването на независимостта, ресурсите и правомощията на ОЗД следва да се съпътстват със засилено сътрудничество на многостранно равнище, по-специално с оглед на нарастващия брой проблеми във връзка със защита на данните в европейски мащаб. Основната инфраструктура, която следва да се използва за това сътрудничество, е очевидно работната група по член 29.

10.2. *Засилване на ролята на работната група*

141. Историческата справка показва, че от своето създаване през 1997 г. досега функциите на групата са еволюирали. Тя се е развила в посока на по-голяма независимост и не може вече да бъде квалифицирана на практика като обикновена консултантска работна група към Комисията. ЕНОЗД предлага допълнително усъвършенстване на функциите на работната група, включително на нейната инфраструктура и независимост.

142. ЕНОЗД е убеден, че силата на групата е неразривно свързана с независимостта и правомощията на нейните членове. Автономията на работната група следва да бъде гарантирана в новата правна рамка в съответствие с критериите, изложени за пълна независимост на ОЗД от Съда на Европейския съюз по дело C-518/07. ЕНОЗД счита, че на работната група следва освен това да се предоставят достатъчно ресурси и бюджет и подсилен секретариат в помощ на нейната продукция.

143. Относно секретариата на работната група ЕНОЗД оценява факта, че той е включен в отдел „Защита на данните“ към ГД „Правосъдие“ с предимството, че самата работна група може да използва ефикасни и гъвкави контакти и актуална информация по аспектите на развитието на защитата на данни. От друга страна, той поставя под въпрос факта, че Комисията (и по-специално този отдел) е едновременно член, секретариат и адресат на становищата на работната група. Това дава основания за повече независимост на секретариата. ЕНОЗД приканва Комисията да прецени — в тесни консултации със заинтересованите страни — как най-добре да се осигури тази независимост.

([54]) Дело C-518/07, *Комисията с/у Германия*, все още непубликувано в ECR.

([55]) Вж. например член 43, параграф 2 от Регламент (ЕО) № 45/2001, в който се съдържат такива изисквания за ЕНОЗД.

144. Накрая, засилването на правомощията на ОЗД изисква също повече правомощия за работната група, със структура, включваща по-добри правила и предпазни мерки, както и повече прозрачност. Това ще допринесе за консултантската, както и за правоприлагащата функция на работната група.

10.3. *Консултантската роля на работната група*

145. Позициите на работната група трябва да бъдат ефективно прилагани, що се отнася до нейната консултантска роля при Комисията, по-специално във връзка с тълкуването и прилагането на принципите на директивата и на други инструменти за защита на данните — с други думи, за утвърждаване на авторитета на позициите на работната група. Допълнителни обсъждания са необходими между ОЗД, за да се реши как да бъде включено това в правния инструмент.

146. ЕНОЗД препоръчва решения, които да направят становищата на работната група по-авторитетни, без да внасят съществени промени в нейния начин на функциониране. ЕНОЗД предлага включване на задължение на ОЗД и на Комисията да отчитат в максимална степен становищата и общите позиции, приети от работната група, въз основа на модела, приет за позициите на Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС) ([56]). Освен това новият правен инструмент може да възложи на работната група изричната задача да приема „тълкувателни препоръки“. Тези решения ще засилят ролята на позициите на работната група, също и пред съдилищата.

10.4. *Съгласувано прилагане на законодателството от страна на работната група*

147. Съгласно настоящата рамка прилагането на законодателството за защита на данните в държавите-членки е предоставено на 27 органи за защита на данните при малко съгласуване във връзка с подхода към специфични случаи. Когато става въпрос за случаи, засягащи повече от една държава-членка или притежаващи безспорно глобално измерение, това увеличава разходите за предприятията, които са принудени да се обръщат към различни публични органи за една и съща дейност, и засилва риска от непоследователно прилагане: в някои изключителни случаи един и същи начин на обработване може да се счита за законосъобразен от един ОЗД и да бъде забранен от друг.

148. Някои случаи имат стратегическо измерение и те следва да се уреждат централизирано. Работната група по член 29 подпомага съгласуването и правоприлагащите дейности между ОЗД ([57]) при особено важни въпроси на защита на данните с такива международни последици. Такъв беше случаят със социалните мрежи и браузърите ([58]), както и във връзка със съгласуваните проверки, извършени в различни държави-членки по въпроси на далекосъобщенията и здравното осигуряване.

149. Има обаче граници на мерките по прилагане на законодателството, които работната група може да предприеме по силата на настоящата рамка. Работната група може да приеме общи позиции, но няма инструмент, който да гарантира, че тези позиции ще бъдат ефективно приложени на практика.

150. ЕНОЗД предлага включване в правния инструмент на допълнителни разпоредби, които да бъдат в подкрепа на съгласуваното правоприлагане, а именно:

— Задължение да се гарантира, че органите за защита на данните и Комисията ще отчитат в максимална степен становищата и общите позиции, приети от работната група по член 29 ([59]).

— Задължение на органите за защита на данните да сътрудничат в дух на доверие помежду си и с Комисията и работната група по член 29 ([60]). Като практически пример за сътрудничество в дух на доверие може да бъде създадена процедура, според която ОЗД информират Комисията или работната група в случай на национални мерки за правоприлагане с трангсраничен елемент, по аналогия с процедурата, прилагана в настоящата рамка във връзка с националните решения за достатъчност.

— Уточняване на правилата за гласуване, с оглед да се увеличат поетите от ОЗД задължения да прилагат решенията на работната група. Може да се предвиди работната група да взема решения с единодушие, а когато единодушие не може да бъде постигнато, да

([56]) Регламент (ЕО) № 1211/2009 на Европейския парламент и на Съвета от 25 ноември 2009 г. за създаване на Орган на европейските регулатори в областта на електронните съобщения (ОЕРЕС) и на Служба, (ОВ L 337, 18.12.2009 г., стр. 1).

([57]) Освен работната група по член 29, Европейската конференция на комисарите по защита на личните данни създаде преди около десет години постоянен семинар, имащ за цел съгласувано уреждане на трансгранични жалби. Въпреки че този семинар представлява безспорна добавена стойност поради обмена между служителите на органите за защита на данните и предлага надеждна мрежа от звена за връзка, той не може да бъде разглеждан като механизъм за съгласуване при вземането на решения.

([58]) Вж. писмата на работната група по член 29 (РГ 29) от 12 май 2010 г. и 26 май 2010 г., публикувани на интернет страницата на РГ 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Както бе посочено по-горе, подобно задължение е установено в Регламент (ЕО) № 1211/2009, който определя ролята н Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС).

([60]) Вж. в тази връзка член 3 от Регламент (ЕО) № 1211/2009, цитиран по-горе.

предприема мерки за прилагане на законодателството само с квалифицирано мнозинство. В допълнение на това в едно съображение може да се предвиди органите за защита на данните, които са гласували положително по даден документ, да имат задължение или политически ангажимент да го прилагат на национално равнище.

151. ЕНОЗД е склонен да повдигне възражения срещу въвеждането на по-силни мерки, като например позициите на работната група по член 29 да станат обвързващи. Това ще наруши независимия статут на отделните ОЗД, който трябва да бъде гарантиран от държавите-членки по силата на националното законодателство. Ако решенията на работната група оказват пряко въздействие върху трети страни, като администраторите на лични данни, следва да се предвидят нови процедури, включително предпазни мерки, като прозрачност и искове, включително евентуално обжалване пред Съда на Европейския съюз.

10.5. *Сътрудничество между ЕНОЗД и работната група*

152. Начинът, по който ЕНОЗД и работната група си сътрудничат, също може да бъде прецизиран. ЕНОЗД е член на работната група и той дава принос в рамките на групата за позициите по основните стратегически насоки на развитие в ЕС, осигурявайки същевременно съгласуваност със своите собствени позиции. ЕНОЗД отбелязва нарастващия брой проблеми с неприкосновеността на личния живот както в частния, така и в публичния сектор, които могат да имат последици на национално равнище в много държави-членки и при които на работната група се пада особена роля.

153. ЕНОЗД има допълнителна задача да предоставя становища относно аспектите на развитието в контекста на ЕС, която следва да бъде запазена. В качеството си на европейски орган той упражнява тази консултантска функция спрямо институциите на ЕС по същия начин, както националните ОЗД съветват своите правителства.

154. ЕНОЗД и работната група действат в различна, но допълваща се перспектива. Нужно е поради тези причини да се запази и може би да се подобри сътрудничеството между работната група и ЕНОЗД, за да се гарантира, че те работят съвместно по основните въпроси на защита на данните, например като съгласуват редовно дневния си ред ([61]) и осигуряват прозрачност по въпроси, които имат по-скоро национален или по-скоро специфичен европейски аспект.

155. Съгласуването не е споменато в настоящата директива поради простата причина, че ЕНОЗД не е съществувал по времето, когато директивата е била приета, но след шест години съществуване допълващите се функции на ЕНОЗД и на работната група са очевидни и може да бъдат формално признати. ЕНОЗД напомня, че съгласно Регламент (ЕО) № 45/2001 той е длъжен да си сътрудничи с националните ОЗД и да участва в дейността на работната група. ЕНОЗД препоръчва да се назове изрично сътрудничеството в новия правен инструмент, като то бъде включено в структурата, където е необходимо, например като се определи процедура за сътрудничество.

10.6. *Сътрудничество между ЕНОЗД и ОЗД при надзора на системи на ЕС*

156. Тези съображения са в сила и за области, където надзорът трябва да бъде съгласуван между европейското и националното равнище. Такъв е случаят с органите на ЕС, които обработват значително количество данни, предоставени от националните власти, или с крупните информационни системи с европейски и национален компонент.

157. Съществуващата система за някои органи на ЕС и крупни информационни системи — например Европол, Евроюст и първото поколение на Шенгенската информационна система (ШИС) имат съвместни надзорни органи с представители на националните ОЗД — е остатък от междуправителственото сътрудничество от периода преди Лисабон и не съответства на институционалната структура на ЕС, от която Европол и Евроюст са сега неразделна част и в която достиженията на правото от Шенген са вече също включени ([62]).

158. В съобщението се обявява, че през 2011 г. Комисията ще започне консултация със заинтересованите страни относно преразглеждането на тези системи за надзор. ЕНОЗД настоява Комисията да изясни възможно най-бързо (в краткосрочна и уточнена времева рамка, вж. по-горе) своята позиция в продължаващата дискусия по надзора. В тази дискусия той ще заеме следното становище.

159. Като начало трябва да се гарантира, че надзорните органи отговарят на необходимите критерии за независимост, ресурси и правомощия по прилагане на законодателството. Освен това е необходима гаранция, че перспективите и компетентността, които съществуват на равнището на ЕС, ще бъдат взети предвид. Това значи, че сътрудничеството следва да се осъществява не само между националните органи, но и с европейския ОЗД (към настоящия момент с ЕНОЗД). ЕНОЗД счита за необходимо да се следва модел, който отговаря на тези изисквания ([63]).

160. През последните години бе изграден моделът на „съгласуван надзор“. Този модел на надзор, който действа сега в „Евродак“ и в части от Митническата информационна система, скоро ще бъде разширен и ще включи Визовата информационна система (ВИС) и второто поколение на Шенгенската информационна система (ШИС II). Моделът има три пласта: 1 надзорът на национално равнище се осигурява от ОЗД; 2 надзорът

([61]) Напр. въз основа на описа на законодателни дейности, публикуван ежегодно и актуализиран редовно, който може да се намери на уебсайта на ЕНОЗД.

([62]) По силата на Регламент (ЕО) № 45/2001 ЕНОЗД е длъжен да си сътрудничи с тези органи.

([63]) За Евроюст моделът трябва също факта, че надзорът върху защитата на данни зачита независимостта на съдебната система, доколкото Евроюст обработва данни в контекста на наказателни дела.

на равнището на ЕС се осигурява от ЕНОЗД; 3 съгласуването се осигурява чрез редовни срещи, свиквани от ЕНОЗД в качеството му на секретариат на този механизъм за съгласуване. Този модел е доказал своята успешност и ефективност и следва да се има предвид в бъдеще за други информационни системи.

В. **КАК ДА СЕ ПОДОБРИ ПРИЛАГАНЕТО НА НАСТОЯЩАТА РАМКА?**

11. **В краткосрочен план**

161. Докато процедурата на преразглеждане продължава, усилията следва да бъдат насочени към осигуряване на пълното и ефективно прилагане на настоящите правила. Тези правила ще останат в сила до приемането на бъдещата рамка, след което ще бъдат приложени в националните законодателства на държавите-членки. В тази посока могат да се посочат няколко линии на действие.

162. Първо, Комисията следва да продължи да следи дали държавите-членки спазват Директива 95/46/ЕО и, ако е необходимо, да използва правомощията си с съответствие с член 258 от ДФЕС. Напоследък бяха открити процедури за нарушение поради неизпълнение на задължението да бъде приложен правилно член 28 от директивата във връзка с условието за независимост на органите за защита на данните ([64]). И в други области е необходим мониторинг и налагане на пълно съответствие ([65]). Ето защо ЕНОЗД приветства и подкрепя напълно задълженията, поети от Комисията в съобщението, да продължава активно политиката си на установяване на нарушения. Комисията следва освен това да продължи структурния диалог с държавите-членки относно прилагането ([66]).

163. Второ, правоприлагането на национално равнище трябва да бъде поощрено, за да се осигури практическото прилагане на правилата за защита на данните, в това число във връзка с новите технологични явления и глобалните участници. Органите за защита на данните следва да използват изцяло своите правомощия за разследване и налагане на санкции. Важно е също така съществуващите права на лицата, за които се събират данни, и по-специално правото на достъп, да бъдат изцяло прилагани в практиката.

164. Трето, повече съгласуваност при правоприлагането изглежда необходима в краткосрочен план. Ролята на работната група по член 29 и нейните тълкувателни документи в тази връзка са много важни, но ОЗД трябва също да положат максимални усилия за практическото им прилагане. Трябва да се избягват разнопосочните резултати при случаите от европейски или глобален мащаб, като общ подход може и трябва да се постигне в рамките на работната група. Съгласуваните разследвания на територията на ЕС под егидата на работната група може също да внесат значителна добавена стойност.

165. Четвърто, принципите за защита на данните следва да бъдат „вградени“ проактивно в нови разпоредби, които може да окажат пряко или косвено въздействие върху защитата на данни. На равнището на ЕС ЕНОЗД полага значителни усилия да съдейства за по-добро европейско законодателство, като такива усилия трябва да се предприемат и на национално равнище. Органите за защита на данните трябва следователно да използват изцяло консултантските си правомощия за осигуряването на такъв проактивен подход. Органите за защита на данните, включително ЕНОЗД, могат да изпълняват проактивна функция и при мониторинг на технологичните развития. Мониторингът е важен с оглед установяване на рано очертаващите се тенденции, определяне на възможните последици за защитата на данни, съдействие за доброволно уреждане на спорове във връзка със защитата на данни и повишаване на осведомеността на заинтересованите страни.

166. Накрая, трябва да се работи активно за по-нататъшното сътрудничество между различните участници на международно равнище. Важно е поради това да се засилят международните инструменти на сътрудничество. Инициативи като стандартите от Мадрид и продължаващата работа в Съвета на Европа и ОИСР заслужават пълна подкрепа. В този контекст много положителен факт е, че и Федералната търговска комисия на САЩ се присъедини вече към семейството на комисарите по неприкосновеността на личния живот и защита на личните данни в рамките на тяхната Международна конференция.

Г. **ЗАКЛЮЧЕНИЯ**

ОБЩИ БЕЛЕЖКИ

167. ЕНОЗД изразява по принцип удовлетворение от съобщението на Комисията, тъй като е убеден, че преразглеждане на настоящата правна рамка за защита на личните данни е необходимо, за да се гарантира ефективна защита в едно постоянно развиващо се и глобализирано информационно общество.

168. Съобщението определя основните проблеми и предизвикателства. ЕНОЗД споделя схващането на Комисията, че силна система за защита на данните ще бъде нужна и занапред, въз основа на това, че съществуващите общи принципи на защита на данните са все още валидни в общество, в което се извършват основни промени. ЕНОЗД споделя констатацията на съобщението, че предизвикателствата са огромни и подчертава, че вследствие на това предложените решения трябва да бъдат подобаващо амбициозни и да засилват ефективността на защитата. Ето защо той настоява за по-амбициозен подход по някои въпроси.

169. ЕНОЗД подкрепя напълно всеобхватния подход към защитата на данни. Той съжалява обаче, че съобщението изключва някои области, като обработка на данните от институциите и органите на ЕС, от общия правен инструмент. Ако Комисията реши да остави настрана

([64]) Вж. дело C-518/07, цитирано по-горе, и прессъобщение на Комисията от 28 октомври 2010 г. (IP/10/1430).

([65]) Комисията откри процедура за нарушение срещу Обединеното кралство поради твърдение за нарушение на различни разпоредби за защита на данните, включително на изискването за поверителност на електронните съобщения във връзка с поведенческо рекламиране. Виж прессъобщение на Комисията от 9 април 2009 г. (IP/09/570).

([66]) Вж. първия доклад на Комисията за прилагането на Директивата за защита на личните данни, цитиран по-горе, стр. 22 и следв.

тези области, ЕНОЗД настоява тя да приеме предложение за равнището на ЕС във възможно най-кратък срок, но за предпочитане до края на 2011 г.

ОСНОВНИ ПЕРСПЕКТИВИ

170. Според ЕНОЗД отправните точки за процедурата на преразглеждане са, както следва:

— правната уредба за защита на данните трябва максимално активно да подкрепя, а не да накърнява други законни интереси (като европейската икономика, сигурността на физическите лица, както и отчетността на правителствата),

— общите принципи на защита на данните не трябва и не може да бъдат променяни,

— по-нататъшната хармонизация следва да бъде една от ключовите цели на преразглеждането,

— защитата на данни като основно право следва да бъде поставена в центъра на процедурата на преразглеждане; основното право има за цел да защити гражданите при всички обстоятелства,

— новият правен инструмент трябва да включва полицейския и съдебния секторv,

— новият правен инструмент трябва да бъде формулиран по възможно най-неутрален в технологично отношение начин и трябва да има за цел създаване на правна сигурност в дългосрочен план.

ЕЛЕМЕНТИ НА НОВАТА РАМКА

Хармонизация и опростяване

171. ЕНОЗД приветства поетото от Комисията задължение да разгледа начините за постигане на по-нататъшна хармонизация на защитата на данни на равнището на ЕС. ЕНОЗД определя областите, в които има спешна необходимост от по-нататъшна и по-добра хармонизация: определения, основания за обработване на данни, права на лицата, за които се събират данни, международни предавания и органи за защита на данните.

172. ЕНОЗД предлага да бъдат разгледани следните алтернативи за опростяване и/или намаляване на обхвата на изискванията за уведомяване:

— ограничаване на задължението за уведомяване до специфични видове обработване, свързани със специфични рискове,

— задължение за проста регистрация, изискващо от администраторите на лични данни да се регистрират (за разлика от разширената регистрация на всички операции по обработката на данни),

— въвеждане на стандартен общоевропейски формуляр за уведомяване.

173. Според ЕНОЗД регламентът като единен инструмент, който е пряко приложим в държавите-членки, е най-ефикасният начин да се защити основното право за защита на данните и да се постигне повече сближаване във вътрешния пазар.

Засилване на правата на физическите лица

174. ЕНОЗД подкрепя изложеното в съобщението предложение за засилване на правата на физическите лица. Той прави следните предложения:

— В законодателния акт може да се включи принцип на прозрачността. По-важно е обаче да се засилят съществуващите разпоредби, свързани с прозрачността (като настоящите членове 10 и 11 от Директива 95/46/ЕО).

— Разпоредба за уведомяване при нарушения на сигурността на личните данни, която разширява задължението, включено в преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации за някои доставчици, като го отнася до всички администратори на лични данни, следва да бъде включена в общия инструмент.

— Трябва да бъдат изяснени границите на съгласието. Следва да се помисли за разширяване на случаите, в които се изисква изрично съгласие, както и за приемане на допълнителни правила за интернет средата.

— Следва да се въведат допълнителни права, като преносимост на данните и правото да бъдеш забравен, по-специално за интернет услугите за информационното общество.

— Интересите на децата следва да бъдат по-добре защитени с няколко допълнителни разпоредби, отнасящи се конкретно до събирането и по-нататъшното обработване на данни на деца.

— В законодателството на ЕС следва да бъдат въведени механизми за колективна защита при нарушаване на правилата за защита на данните, които да оправомощават квалифицирани структури да подават искове от името на групи физически лица.

Засилване на задълженията на организациите/администраторите

175. Новата рамка трябва да съдържа стимули за администраторите на лични данни да включват проактивно мерки за защита на данните в своите работни процеси. ЕНОЗД предлага да се въведат общи разпоредби за отчетност и „неприкосновеност на личния живот още при разработването“. Следва да бъде въведена и разпоредба относно схеми за сертифициране при спазване на неприкосновеността на личния живот.

Глобализация и приложимо законодателство

176. ЕНОЗД подкрепя амбициозната работа в рамките на Международната конференция на комисарите по защита на личните данни за разработване на така наречените „стандарти от Мадрид“, с цел те да бъдат включени в задължителен инструмент и да доведат евентуално до свикване на междуправителствена конференция. ЕНОЗД призовава Комисията да предприеме конкретни стъпки в тази насока в тясно сътрудничество с ОИСР и Съвета на Европа.

177. Новият правен инструмент трябва да изясни критериите, определящи приложимото законодателство. Трябва да се гарантира, че данни, които се обработват извън границите на ЕС, остават под юрисдикцията на ЕС, когато е налице обосновано искане за прилагане на законодателството на ЕС. Ако правната рамка приеме формата на регламент, ще има едни и същи правила във всички държави-членки и няма да е толкова важно да се определя приложимото законодателство (в рамките на ЕС).

178. ЕНОЗД подкрепя напълно целта да се осигури по-единен и последователен подход по отношение на трети държави и международни организации. Задължителните фирмени правила (ЗФП) следва да бъдат включени в правния инструмент.

Областта на полицията и правосъдието

179. В един всеобхватен инструмент, включващ полицията и правосъдието, може да има специални правила, които вземат надлежно предвид особеностите в този сектор в съответствие с Декларация 21, приложена към Лисабонския договор. Специфични предпазни мерки трябва да се въведат за компенсации на лицата, за които се събират данни, като им се предостави допълнителна защита в област, в която обработката на лични данни поради самото си естество е по-натрапчива.

180. Новата правна рамка следва да бъде колкото е възможно по-ясна, по-проста и по-последователна. Следва да се избягва нарастване на броя на различните режими, прилагани например към Европол, Евроюст, ШИС и Прюм. ЕНОЗД разбира, че съгласуването на правилата от различните системи ще да се извърши внимателно и постепенно.

Органите за защита на данните (ОЗД) и сътрудничеството между тях

181. ЕНОЗД подкрепя напълно целта на Комисията да реши въпроса за статута на органите за защита на данните (ОЗД) и да засили независимостта, ресурсите и правомощията им по прилагане на законодателството. Той препоръчва:

— кодифициране в новия правен инструмент на съществения понятие за независимостта на ОЗД, както то е определено от СЕО,

— изискване в законодателството за предоставяне на достатъчно ресурси на ОЗД,

— даване на органите на хармонизирани правомощия за разследване и санкциониране.

182. ЕНОЗД предлага допълнително усъвършенстване на функциите на работната група по член 29, включително на нейната независимост и инфраструктура. На работната група следва също така да се предоставят достатъчно ресурси и подсилен секретариат.

183. ЕНОЗД предлага засилване на консултантската роля на работната група чрез включване на задължение на ОЗД и на Комисията *да отчитат в максимална степен становищата и общите позиции*, приети от работната група. ЕНОЗД не е за това позициите на работната група да станат обвързващи, по-специално заради независимия статут на отделните ОЗД. ЕНОЗД препоръчва Комисията да включи в новия правен инструмент специфични разпоредби за засилване на сътрудничеството с ЕНОЗД.

184. ЕНОЗД настоява Комисията да приеме във възможно най-кратък срок становище относно въпроса за надзора на органите на ЕС и крупните информационни системи, като вземе предвид, че всички надзорни органи следва да отговарят на необходимите критерии за независимост, ресурси и правомощия по прилагане на законодателството и че следва да се гарантира представителност на европейската перспектива. ЕНОЗД подкрепя модела на „съгласуван надзор“.

Подобрения в рамките на настоящата система:

185. ЕНОЗД призовава Комисията:

— да продължи да следи дали държавите-членки спазват Директива 95/46/ЕО и, ако е необходимо, да използва правомощията си с съответствие с член 258 от ДФЕС,

— да насърчава правоприлагането на национално равнище и съгласуваност на правоприлагането,

— да вгради проактивно принципите за защита на данните в нови разпоредби, които може да окажат пряко или косвено въздействие върху защитата на данни,

— да работи активно за по-нататъшното сътрудничество между различните участници на международно равнище.

Съставено в Брюксел на 14 януари 2011 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните