РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

01248/07/EN
WP 136

Становище 4/2007 относно понятието „лични данни”

Прието на 20 юни

Работната група е създадена в съответствие с член 29 от Директива 95/46/ЕО. Тя е независим европейски съвещателен орган за защита на личните данни и личния живот. Задачите ѝ са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретарската служба се осигурява от Дирекция С (Гражданско правосъдие, права и гражданство) на Европейската комисия (Генерална дирекция „Правосъдие, свобода и сигурност“), B-1049 Брюксел, Белгия, Бюро № LX-46 01/43

Уебстраница: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

РАБОТНАТА ГРУПА ЗА ЗАЩИТА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ,

създадена по силата на Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995[1] г.,

като взе предвид член 29 и член 30, параграф 1, буква а) и параграф 3 от горепосочената директива и член 15, параграф 3 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г.,

като взе предвид член 255 от Договора за създаване на Европейската общност и Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията,

като взе предвид правилника за дейността си,

ПРИЕ НАСТОЯЩОТО СТАНОВИЩЕ:

[1] ОВ L 281, 23.11.1995 г., стр. 31, текстът може да се намери на адрес: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. ВЪВЕДЕНИЕ.....3

II. ОБЩИ СЪОБРАЖЕНИЯ И ВЪПРОСИ, СВЪРЗАНИ С ПОЛИТИКАТА.....4

III. АНАЛИЗ НА ОПРЕДЕЛЕНИЕТО ЗА „ЛИЧНИ ДАННИ“ СПОРЕД ДИРЕКТИВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.....6

1. ПЪРВИ ЕЛЕМЕНТ: „ВСЯКА ИНФОРМАЦИЯ” 7

2. ВТОРИ ЕЛЕМЕНТ: „СВЪРЗАНА С“.....10

3. ТРЕТИ ЕЛЕМЕНТ: „ИДЕНТИФИЦИРАНО ИЛИ ПОДЛЕЖАЩО НА ИДЕНТИФИКАЦИЯ“ [ФИЗИЧЕСКО ЛИЦЕ] 14

4. ЧЕТВЪРТИ ЕЛЕМЕНТ: „ФИЗИЧЕСКО ЛИЦЕ“.....26

IV. КАКВО СЕ СЛУЧВА, АКО ДАННИТЕ ПОПАДАТ ИЗВЪН ОПРЕДЕЛЕНИЕТО?.....29

V. ЗАКЛЮЧЕНИЯ.....29

I. ВЪВЕДЕНИЕ

Работната група е наясно с необходимостта да бъде проведен задълбочен анализ на понятието лични данни. Информацията за текущата практика в държавите-членки на ЕС показва, че съществува известна несигурност и различия в практиките сред държавите-членки по отношение на важни аспекти на това понятие, които могат да окажат влияние върху правилното функциониране на съществуващата рамка за защита на данните в различни ситуации. Резултатът от този анализ на един основен елемент за приложението и тълкуването на правилата за защита на данните със сигурност окаже силно влияние върху редица важни въпроси и ще бъде от особено значение за теми като управление на самоличността в контекста на електронното управление и електронното здравеопазване, както и в контекста на радиочестотната идентификация (RFID).

Целта на настоящото становище на работната група е да доведе до общо разбиране на понятието „лични данни“, ситуациите, в които трябва да се прилага националното законодателство за защита на данните, и начина, по който следва да бъде прилагано. Разработването на общо определение на понятието „лични данни” е равнозначно на определянето на това, което попада в обхвата на правилата за защита на данните и на това, което остава извън този обхват. Резултатът от тази работа трябва да осигури насоки за начина, по който националните разпоредби за защита на данните следва да бъдат прилагани в определени категории ситуации,

възникващи навсякъде в Европа, като по този начин допринесе за уеднаквеното прилагане на тази норми, което е основна функция на работната група по член 29.

Този документ използва примери, взети от националната практика на европейските органи за защита на данните, за да подкрепят и илюстрират анализа. Повечето примери са изменени само с цел да бъдат пригодени за употреба в този контекст.

II. ОБЩИ СЪОБРАЖЕНИЯ И ВЪПРОСИ, СВЪРЗАНИ С ПОЛИТИКАТА

Директивата съдържа широко понятие за лични данни

Определението „лични данни“, съдържащо се в Директива 95/46/ЕО (наричана по-долу „Директива за защита на личните данни“ или „директивата“) гласи както следва:

„лични данни“ означава всяка информация, свързана с идентифицирано или подлежащо на идентификация лице („съответно физическо лице“); за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност.

Необходимо е да се отбележи, че това определение отразява намерението на европейския законодател за създаване на широко понятие „лични данни”, което бе поддържано през целия законодателен процес. В първоначалното предложение на Комисията се обясняваше, че *както и в Конвенция 108, се приема широко определение с цел да обхване цялата информация, която би могла да се свърже с едно физическо лице*[2]. В измененото предложение на Комисията се отбелязва, че *измененото предложение отговаря на желанието на Парламента определението за лични данни да бъде колкото е възможно по-общо, така че да включва цялата информация, отнасяща се до едно подлежащо на идентификация лице*[3], желание, което Съветът също взе предвид и в общата си позиция[4].

Целта на правилата, съдържащи се в директивата, е да се предпазят физическите лица.

В член 1 на Директива 95/46/ЕО и в член 1 на Директива 2002/58/ЕО недвусмислено се заявява, че крайната цел на правилата, съдържащи се в тях, е да защищават основните права и свободи на физическите лица и в частност правото им на личен живот при обработването на лични данни. Това е много важен елемент, който трябва да се вземе под внимание при тълкуването и прилагането на правилата и в двата инструмента. Той може да има съществена роля при определяне на това, как да се прилагат разпоредбите на директивата в редица ситуации, в които правата на физическите лица не са изложени на риск, и

---

2 COM (90) 314 окончателен, 13.9.1990 г., стр. 19 (коментар върху член 2)

3 COM (92) 422 окончателен, 28.10.1992 г., стр. 10 (коментар върху член 2)

4 Обща позиция (ЕО) № 1/95, приета от Съвета на 20 февруари 1995 г., ОВ С 93, 13.4.1995 г., стр.20

може да предотврати тълкуване на същите правила, което би лишило физическите лица от защита на техните права.

Приложното поле на директивата изключва редица дейности, а в текста се въвежда гъвкавост, която да осигури подходящ правен отговор на спорните обстоятелства.

Въпреки широките понятия „лични данни“ и „обработване“, съдържащи се в директивата, единствено фактът, че дадена ситуация може да бъде разглеждана като включваща „обработване на лични данни” по смисъла на определението, не е достатъчен, за да определи, че тази ситуация следва да бъде предмет на правилата на директивата, по-специално съгласно член 3 от нея. Освен изключенията, които се дължат на приложното поле на правото на Общността, изключенията по член 3 вземат под внимание техническия начин на обработване (чрез ръчна, неструктурирана форма) и намерението за употреба (за предимно лични или домашни занимания на физическото лице). Дори когато става въпрос за обработване на лични данни в приложното поле на директивата, не всички правила, които се съдържат в нея могат да бъдат приложими по отношение на конкретния случай. Голям брой от разпоредбите на директивата се характеризират със значителна степен на гъвкавост, така че да се поддържа подходящото равновесие между защитата на правата на съответното физическо лице, от една страна, а от друга страна, на законните интереси на администраторите на лични данни, на трети страни и обществения интерес, който може да съществува. Някои примери за подобни разпоредби се съдържат в член 6 (период на съхранение в зависимост от данните, които са необходими), в член 7, буква е) (баланс на интересите за оправдаване на обработката), в последния параграф на член 10, буква в) и в 11.1, буква в) (информация за съответното физическо лице, когато е необходимо да се гарантира справедливо обработване), или член 18 (освобождаване от изискване за уведомление) и това са само няколко случая.

Обхватът на правилата за защита на данните не бива да бъде прекалено разширен

Би се получил нежелан ефект да се стигне дотам да се прилагат правилата за защита на данните по отношение на ситуации, за които не е съществувало намерение да бъдат обхванати от тези правила и за които тези правила не са били предназначени от законодателя. Съществените изключения по член 3, посочени по-горе, и разясненията в съображения 26 и 27 на директивата показват по какъв начин законодателят е замислил приложението на защитата на данните.

Едно от ограниченията се отнася до начина на обработване на данните. От полза е да припомним, че причините за приемането на първите закони за защита на данните през седемдесетте години се породиха факта, че нова технология под формата на електронно обработване на данни позволява по-лесен и по-разпространен достъп до лични данни, отколкото традиционните форми за обработка на данните. Съответно защитата на данните съгласно директивата цели защитатата на такива форми на обработване, които са типични за висок

риск от „лесен достъп до личните данни“ (съображение 27). Обработването на лични данни чрез неавтоматизирани средства се включа в приложното поле на директивата, само когато данните съставляват част от файлова система или са предназначени да бъдат част такава система (член 3).

Друго общо ограничение за прилагането на защитата на данните съгласно директивата би било обработването на данни при обстоятелства, при които средствата за идентифициране на съответното физическо лице не „биха могли да бъдат използвани разумно“ (съображение 26), въпрос, който ще бъде обсъждан по-късно.

Неоправданото ограничаване на тълкуването на понятието „лични данни” също трябва да бъде избегнато

В случаите, когато едно механично прилагане на всяка отделна разпоредба на директивата на пръв поглед би довело до прекалено тежки или може би дори абсурдни обстоятелства, трябва да се провери: 1) дали ситуацията попада в приложното поле на директивата, по-конкретно съгласно член 3 от нея; и 2) когато ситуацията попада в нейното приложно поле, дали самата директива или националното законодателство, прието в съответствие с нея, не позволяват освобождаване или опростяване по отношение на конкретни ситуации с цел да бъде постигнат съответен правен отговор, като в същото време се гарантира защитата на правата на физическото лице и на съответните интереси. По-добър вариант е да не се ограничава неоправдано тълкуването на определението „лични данни”, а по-скоро да се отбележи, че има съществена гъвкавост в прилагането на правилата към данните.

Националните надзорни органи за защита на данните играят съществена роля в това отношение в рамките на тяхната мисия за наблюдаване на приложението на закона за защита на данните, което включва осигуряване на тълкуване на законовите разпоредби и конкретни насоки за администраторите и съответните физически лица. Те следва да приемат определение, което е достатъчно широко, че да позволява включването на промени и да обхване всички „сенчести зони” , като използва пълноправно гъвкавостта, съдържаща се в директивата. Всъщност текстът на директивата приканва към разработване на политика, която комбинира едно широко тълкуване на понятието „лични данни“ и подходящо равновесие в приложението на правилата на директивата.

III. АНАЛИЗ НА ОПРЕДЕЛЕНИЕТО ЗА „ЛИЧНИ ДАННИ“ СПОРЕД ДИРЕКТИВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Определението в директивата съдържа четири основни градивни елемента, които ще бъдат анализирани отделно за целите на настоящия документ. Те са следните:

- „всяка информация“
- „свързана с“

- „идентифицирано или подлежащо на идентификация“

- „физическо лице“

Тези четири градивни елемента са тясно преплетени и взаимозависими. Въпреки това, заради методологията, която трябва да се следва в този документ, всяка от тези единици ще бъде разгледана поотделно.

1. ПЪРВИ ЕЛЕМЕНТ: „ВСЯКА ИНФОРМАЦИЯ“

Терминът „всяка информация“, който се съдържа в директивата, ясно сигнализира желанието и готовността на законодателя да създаде широко понятие за личните данни. Този израз изисква широко тълкуване.

От гледна точка на естеството на информацията понятието „лични данни“ включва всеки вид твърдение за едно лице. То включва „обективна” информация като наличието на определено вещество в кръвта на даден човек. Също включва и „субективна“ информация, мнения или оценки. Последният вид твърдения съставляват значителен дял от обработката на лични данни в такива сектори като банковото дело за оценяване надеждността на кредитополучателите („Х е надежден кредитополучател"), застраховането („Не се очаква Х да почине скоро“) или при наемане на работа („Х е добър служител и заслужава повишение“).

За да бъде една информация “лични данни”, не е необходимо тя да бъде вярна или доказана. Всъщност правилата за защита на личните данни вече предвиждат възможността тази информация да бъде невярна и осигуряват правото на съответното физическо лице да я оспори с помощта на съответни средства за правна защита[5].

От гледна точка на съдържанието на информацията понятието „лични данни“ включва данни, предоставящи всякакъв вид информация. Това разбира се обхваща лична информация, която се разглежда като „чувствителни данни“ в член 8 от директивата поради особено рисковият ѝ характер, но също така и по-обща информация. Терминът „лични данни“ включва информация, засягаща *stricto sensu* личния и семеен живот на физическото лице, но също и информация относно всякакъв вид дейност, предприета от физическото лице, като например такава, която засяга работни отношения или икономическо и социално поведение на лицето. Следователно той включва информация за физическите лица, независимо от положението им (в качеството на потребители, пациенти, служители, клиенти и др).

Пример №. 1: Професионално поведение и практики

Информация при предписване на лекарства (например идентификационен номер на лекарството, наименование на лекарството, сила на лекарството, производител, продажна цена, ново или повторно изпълнение на рецептата, причини да не се заменя лекарството, име и фамилия на предписващото лице, телефонен номер и т.н.), независимо дали под формата на индивидуална рецепта или под формата на тенденции от определен брой рецепти, може да се разглежда

[5] Поправка може да бъде направена, като се прибави опровергващ коментар или като се използват съответни средства за правна защита като механизми за обжалване

като лични данни за лекаря, който предписва това лекарство, дори ако пациентът е анонимен. По този начин предоставянето на информация за рецепти, написани от идентифицирани или подлежащи на идентификация лекари, на производители на лекарства, изписвани по рецепта, представлява съобщаване на лични данни на трети лица получатели по смисъла на директивата.

Това тълкуване е подкрепено от формулировката на самата директива. От друга страна, трябва да се вземе предвид факта, че понятието личен и семеен живот е широко понятие, както Европейският съд за правата на човека недвусмислено показва[6]. От друга страна, правилата за защита на личните данни отиват отвъд защитата на широкото понятие за правото да бъде спазвана неприкосновеността на личния и семейния живот. Следва да се отбележи, че в член 8 на Хартата на основните права на Европейския съюз защитата на лични данни е вписана като автономно право, отделно и различно от правото на личен живот, посочено в член 7 от нея, като същият е случаят на национално ниво в някои държави-членки. Това е в съответствие с условията на член 1.1, които целят защита на „основните права и свободи на физическите лица, и *по-специално* [но не изключително] тяхното право на личен живот“. Съответно директивата прави специална препратка към обработването на лични данни в контекст извън дома и семейството, като този, предвиден в трудовото законодателство (член 8.2, буква б)), криминални присъди, административни санкции или решения по граждански дела (член 8.5) или директен маркетинг (член 14, буква б)). Съдът на Европейските общности[7] одобри този широк подход.

По отношение на <u>формата</u> или носителя, на който се съдържа тази информация, понятието „лични данни“ включва информация под каквато и да е форма, било то азбучна, цифрова, графична, фотографска или акустична. Например то включва информация, съхранявана на хартия, както и информация, съхранявана в компютърна памет посредством двоичен код или на видеолента. Това е логично последствие от включването на автоматичното обработване на лични данни в приложното поле на понятието. По-специално, звуковите данни и изображенията се определят като лични данни от тази гледна точка, доколкото могат да представляват информация относно физическо лице. В това отношение специалната препратка към обработването на звук и картина в член 33 на директивата трябва да се разбира като потвърждение и разяснение, че този вид данни наистина е включен в приложното ѝ поле (при условие че всички други условия са изпълнени) и че директивата се прилага по отношение на тях. Всъщност, това е логично предположение относно разпоредбата, която се

---

6 Решение на Европейския съд за правата на човека по делото Amann срещу Швейцария от 16.2.2000 г., §65 : *[...]терминът „личен живот“ не бива да се тълкува ограничително. По-конкретно, спазването на неприкосновеността на личния живот включва правото да се установяват и развиват взаимоотношения с други човешки същества; освен това няма принципно основание да се оправдае изключването на дейности от професионално или бизнес естество от понятието „личен живот“ (виж решението по дело Niemetz срещу Германия от 16 декември 1992 г., серия А, №. 251-В, стр. 33-34, § 29 и решението по дело Halford, цитирано по-горе, стр. 1015-16, § 42). Това широко тълкуване съответства на тълкуването на Конвенцията на Съвета на Европа от 28 януари 1981г. [...]*

7 Решение на Съда на Европейските общности C-101/2001от 6.11.2003 г. (Lindqvist), §24: *Терминът „лични данни“, използван в член 3, параграф 1от Директива 95/46, обхваща, съгласно определението в член 2, буква а) от нея, всяка информация, свързана с идентифицирано или подлежащо на идентификация физическо лице. Терминът несъмнено обхваща името на лицето във връзка с неговите телефонни номера или информация за неговите работни условия или любими занимания.*

съдържа в този член, чиято цел е да оцени дали правилата на директивата осигуряват подходящ правен отговор в тези области. Това е допълнително разяснено в съображение 14, в което се посочва, че *поради значимостта на извършващото се понастоящем развитие в рамките на Информационното общество, на техниките, използвани за улавяне, предаване, манипулиране, запис, съхранение и предаване на звук и картина, отнасящи се до физическите лица, настоящата директива следва да се прилага за обработването на такива данни*. От друга страна, не е необходимо, за да се разглежда информацията като лични данни, тя да се съдържа в структурирана база данни или файл. Също и информация, съдържаща се в свободен текст в електронен документ, може да се се определи като лични данни, при условие че са изпълнени другите критерии от определението за лични данни. Електронният адрес например съдържа лични данни.

Пример № 2: телефонно банкиране:

При телефонното банкиране, когато гласът на клиента, който дава указания на банката се записва на лента, тези записани указания следва да бъдат считани за лични данни.

Пример № 3: видеонаблюдение

Изображенията на физически лица, записани от система за видеонаблюдение, могат да бъдат лични данни дотолкова, доколкото лицата са разпознаваеми.

Пример № 4: детски рисунки

В резултат на невропсихиатричен тест, проведен върху момиче в контекста на съдебна процедура за нейното попечителство, е предоставена нейна рисунка, която представя семейството ѝ. Рисунката осигурява информация за настроението на момичето и за това какво изпитва то към различните членове на семейство си. В това отношение тя би могла да се разглежда като представляваща лични данни. Рисунката действително ще разкрие информация, отнасяща се до детето (нейното здравно състояние от психиатрична гледна точка), а също и например за поведението на бащата или майката. В резултат на това, родителите в този случай може да имат възможност да упражнят правото си на достъп до тази специфична информация.

Тук следва специално да се отбележат биометричните данни. Тези данни могат да бъдат определени като биологични свойства, психологични характеристики, специфични черти или повторяеми действия, когато тези особености и/или действия са единствени по рода си за това лице и измерими, дори ако моделите, използвани в практиката за тяхното измерване, включват определена степен на вероятност. Типичен пример за такива биометрични данни се осигуряват от отпечатъците на пръстите, структурата на ретината, лицевата конструкция, гласа, но също и формата на ръцете, структурата на вените или дори някои дълбоко вкоренени умения или други поведенчески характеристики (като собственоръчен подпис, динамика на натискане на клавиши, особена походка или начин на говорене и т.н...)

Особеността на биометричните данни е в това, че те могат да бъдат разглеждани както като *съдържание* на информацията за конкретното физическо лице (това са

пръстовите отпечатъци на X), така и като елемент, който да установи *връзка* между една част от информацията и лицето (този предмет е бил докоснат от някой, който притежава тези пръстови отпечатъци, а тези пръстови отпечатъци отговарят на X; следователно този предмет е бил докоснат от X). Така те могат да служат за „идентификатори“. Действително, заради уникалната си връзка с конкретното физическо лице, биометричните данни могат да бъдат използвани за идентификация на физическите лица. Този двойствен характер се проявява и в случая с ДНК данните, които предоставят информация относно човешкото тяло и позволяват недвусмислено и уникално идентифициране на дадено лице.

Пробите от човешки тъкани (като например кръвната проба) са източници, от които се извличат биометрични данни, но самите те не са биометрични данни (както например пръстовият отпечатък представлява биометрични данни, но самият пръст не е). Следователно извличането на информация от пробите е събиране на лични данни, към които се прилагат правилата на директивата. Събирането, съхранението и използването на самите тъкани може да подлежи на отделен набор от правила[8].

2. ВТОРИ ЕЛЕМЕНТ: „СВЪРЗАНА С“

Този градивен елемент от определението е от голямо значение, тъй като е особено важно да се установи кои са взаимоотношенията/връзките, които имат значение и как да ги да бъдат разпознати.

В общ план информацията може да се счита, че „има връзка“ с дадено физическо лице, когато тя е *се отнася до* това лице.

В много ситуации тази връзка може лесно да бъде установена. Например данните, регистрирани в личното досие на дадено лице в отдел „Персонал“ съвсем ясно „са свързани“ с положението на лицето като служител. Това важи и за резултатите от медицинските изследвания на пациента, съдържащи се в медицинските регистри, или изображението на човека, заснето в негово видео интервю.

Могат да бъдат споменати редица други ситуации, въпреки че не винаги е толкова очевидно както в предишните случаи, че информацията „е свързана“ с дадено физическо лице.

В някои ситуации информацията от данните се отнася най-вече до предмети, а не до физически лица. Тези предмети обикновено принадлежат на някого или може да бъдат обект на особено влияние от страна на физически лица или върху тях, или могат да поддържат някакъв вид физическа или географска близост с лица или с други предмети. Тогава само косвено може да се счита, че информацията има връзка с тези физически лица или предмети.

Пример № 5: стойността на къща

Стойността на дадена къща е информация за предмет. Правилата за защита на личните данни със сигурност няма да се прилагат, когато тази информация бъде използвана единствено, за да илюстрира нивото на цените на недвижимите

[8] Виж Препоръка на Съвета на Европа № Rec (2006) 4 на Комитета на Министрите към държавите-членки относно изследванията на биологичен материал от човешки произход от 15.3.2006 г.

имоти в определен район. Обаче при определени обстоятелства подобна информация също следва да се счита за лични данни. Всъщност къщата е актив на собственика, което следователно ще бъде използвано да се определи например степента на задължение на това лице да плаща някакви данъци. В този контекст ще бъде безспорно, че такава информация следва да се разглежда като лични данни.

Подобен анализ е приложим, когато данните са предимно за процеси и събития, например информация за функционирането на машина, където се изисква човешка намеса. При някои обстоятелства информацията може също да се разглежда като „свързана“ с дадено физическо лице.

Пример № 6: данни за сервизно обслужване на автомобил

Сервизният регистър на една кола, поддържан от механик или сервиз, съдържа информация за колата, пробег, дати на сервизните проверки, технически проблеми и материално състояние. Тази информация се свързва в регистъра с регистрационен номер и номер на двигателя, които от своя страна могат да бъдат свързани със собственика. Когато гаражът установи връзка между превозното средство и собственика с цел фактуриране, информацията ще се бъде свързана със собственика или водача. Ако връзката бъде направена с механика, който работи по автомобила с цел да се установи неговата продуктивност, тази информация също ще бъде „свързана“ с механика.

Работната група вече обърна внимание на въпроса кога информацията може да бъде разглеждана като „свързана“ с дадено лице. В контекста на обсъжданията на въпросите за защита на личните данни във връзка с RFID (радиочестотна идентификация) етикетите работната група отбеляза, че *данните са „свързани“ с дадено лице, ако се отнасят до самоличността, характеристиките или поведението на лицето или ако тази информация се използва, за да се определи или да се въздейства върху начина, по който това лице е третирано или оценено*[9].

С оглед на случаите, споменати по-горе, може да се уточни в същата насока, че за да се разглеждат данните като свързани с дадено физическо лице, трябва да е налице елемент на **съдържание** ИЛИ елемент на **цел** или елемент на **резултат**.

Елементът **съдържание** е налице в онези случаи, когато – в съответствие с най-очевидното и общоприето разбиране в обществото за думата „свързан съм“ – се дава информация за конкретно физическо лице, независимо от каквато и да било цел от страна на администратора на данни или на трета страна, или за въздействието на тази информация върху съответното физическо лице. Информацията „е свързана“ с дадено лице, когато е „за“ това лице, като това трябва да бъде преценено в светлината на всички обстоятелства, свързани със случая. Например резултатите от медицински анализ ясно са свързвани с пациента или информацията, която се съдържа в папка на компания с името на определен клиент, ясно е свързана с него. Информацията, която се съдържа в RFID таг или в баркод, вграден в документ за самоличност на определено лице, е

[9] Документ на работната група № WP 105: „Работен документ по проблемите на защитата на данните, свързани с технологията за радиочестотна идентификация“, приет на 19.1.2005 г., стр. 8.

свързана с това лице както при бъдещите паспорти с чип за радиочестотна идентификация.

Също и елементът на **цел** може да да води до това, че информацията е свързана с определено лице. Този елемент на цел може да се приеме, че съществува, когато данните се използват или има вероятност да бъдат използвани, като се вземат предвид всички обстоятелства, обособяващи конкретния случай, с цел да се оцени, третира по някакъв начин или да се окаже въздействие върху положението или поведението на дадено лице.

Пример № 7: извадка на входящите и изходящи повиквания

Регистрираните входящи и изходящи повиквания от даден телефон в офиса на компания осигуряват информация за повикванията, които са направени от този телефон, свързан към определена линия. Тази информация може да бъде свързана с различни субекти. От друга страна, линията е предоставена за ползване на компанията, като тя е задължена по договор да плаща за тези телефонни повиквания. Телефонният апарат е под контрола на определен служител през работното време, като се предполага, че обажданията са направени от него. Извадката може да осигури информация за получаващото обажданията лице. Телефонът освен това може да бъде използван от което и да е лице, допуснато в помещението, при отсъствие на служителя (например от персонал по почистването). С различна цел информацията относно използването на телефонния апарат може да бъде свързана с компанията, служителя или чистачите (например, за да се провери по кое време почистващият персонал напуска работното място, тъй като се очаква те да потвърждават по телефона кога си тръгват, преди да заключат помещенията). Следва да се отбележи, че понятието „лични данни“ тук включва както изходящите, така и входящите повиквания, тъй като всички те съдържат информация, засягаща личния живот на социалните взаимоотношения и комуникацията на хората. .

Третият вид „свързване“ с конкретни лица възниква, когато е налице елемент на **резултат**. Въпреки липсата на елемент на съдържание или елемент на цел може да се приеме, че данните „са свързани“ с дадено лице, защото е вероятно употребата им да окаже въздействие върху правата и интересите на определено лице, като се вземат предвид всички обстоятелства в конкретния случай. Следва да се отбележи, че не е задължително възможният резултат да е със значително въздействие. Достатъчно е, ако към лицето може да има по-различно отношение, отколкото към други лица, в резултат на обработването на тези данни.

Пример № 8: наблюдение на местоположението на таксиметровите автомобили с цел оптимизиране на услугата, което има въздействие върху шофьорите.

Система за сателитно локализиране е въведена от таксиметрова компания, която прави възможно определянето на положението на свободните таксиметрови коли в реално време. Целта на обработването е да се осигури по-добра услуга и да се пести гориво, като за всеки клиент, който поръчва такси, се определя автомобил, който е най-близо до адреса на клиента. Строго погледнато, данните, необходими за тази система, се отнасят до автомобила, а не до шофьорите. Целта на обработването не е да се оценява резултата от работата на таксиметровите шофьори, например чрез оптимизация на маршрутите им. Все пак системата позволява наблюдение на работата на таксиметровите шофьори и проверка дали спазват ограниченията за скоростта, дали търсят подходящи маршрути, дали са зад волана или си почиват отвън и т.н. Това следователно може да има значително въздействие върху тези лица, като тези данни може да се считат за свързани с физическите лица. Обработването трябва да е предмет на правилата за защита на личните данни.

Тези три елемента (съдържание, цел, резултат) трябва да се разглеждат като независими едно от друго условия, а не като сбор от тях. По-специално, когато е

налице елемент на съдържание, не е необходимо другите елементи да бъдат налице, за да се счита, че информацията се отнася за лицето. Естествена последица от това е, че една и съща информация може да се отнася едновременно за различни лица, в зависимост от това кой елемент е налице по отношение на всяко едно от тях. Една и съща информация може да е свързана с лицето X заради елемента на съдържание (данните очевидно са за X) И с Y заради елемента на цел (тя ще се използва с цел да се подходи към Y по определен начин) И със Z заради елемента на резултат (има вероятност информацията да окаже въздействие върху правата и интересите на Z). Това означава също, че не е необходимо данните да са насочени върху някого, за да се смята, че те са свързвани с него. В резултат от този анализ въпросът дали данните са свързвани с конкретно лице е нещо, на което трябва да се даде отговор за всяка специфична единица от тези данни по същество. По същия начин, фактът, че информацията може да бъде свързана с различни лица, трябва да се има предвид при прилагането на разпоредбите по същество (например относно обхвата на правото на достъп).

Пример № 9: информация, която се съдържа в протокол от събрание.

Един пример за необходимостта да се проведе предходният анализ по отношение на всяка информация поотделно, е информацията, съдържаща се в протокол от събрание, в който обикновено се регистрира присъствието на участниците X, Y и Z; изказванията, направени от X и Y и доклад за разискванията по определени теми, обобщени от автора на протокола – Z. За лични данни, свързани с X, можем да считаме само информацията, че той е присъствал на събранието по определено време и на определено място, както и че е направил конкретни изказвания. Присъствието на Y на събранието, неговите изказвания и разискванията по даден въпрос, обобщени от Z, НЕ са лични данни, свързани с X. Това е така, дори ако тази информация се съдържа в същия документ и дори ако X е предизвикал обсъждането на този въпрос на събранието. Следователно тя е изключена от правото на достъп на X до своите лични данни. Дали и до каква степен тази информация може да се счита за лични данни на Y и Z ще трябва да се определи отделно, като се използва анализа, описан по-горе.

3. ТРЕТИ ЕЛЕМЕНТ: „ИДЕНТИФИЦИРАНО ИЛИ ПОДЛЕЖАЩО НА ИДЕНТИФИКАЦИЯ“ [ФИЗИЧЕСКО ЛИЦЕ]

Директивата изисква информацията да е свързана с физическо лице, което е „идентифицирано или подлежащо на идентификация“. Това поражда следващите бележки.

В общи линии едно физическо лице може да бъде считано за „идентифицирано“, когато в рамките на една група от лица, то „се отличава“ от другите членове на групата. Съответно, физическото лице е „подлежащо на идентификация“ когато, въпреки че лицето все още не е било идентифицирано, е възможно това да бъде направено (както подсказва думата „подлежащо“). Ето защо тази втора възможност е на практика необходимо условие, което определя дали информацията влиза в обхвата на третия елемент.

Идентификация обикновено се постига чрез определена информация, която може да бъде наречена „идентификатори“ и която има определено специално и тясно взаимоотношение с конкретното лице. Примери за това са характеристиките на външността като височина, цвят на косата, облекло и т.н.... или някакво качество на това лице, което не може да бъде възприето веднага като професия, длъжност, име и т.н. Директивата споменава тези „идентификатори“ в определението за лични данни в член 2, където се пояснява, че физическо лице *може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност.*

Идентифицирано пряко или непряко

Допълнителни разяснения се съдържат в обяснителните бележки към членовете на измененото предложение на Комисията, а именно че *едно лице може да бъде идентифицирано пряко по име или непряко по телефонен номер, регистрационен номер на автомобил, номер на социално осигуряване, номер на паспорт или чрез комбинация от значими критерии, които позволяват лицето да се разпознае в малка група, към която принадлежи (възраст, професия, местожителство, др.).* Това твърдение ясно посочва, че степента, до която определени идентификатори са достатъчни, за да се постигне идентификация, е нещо което зависи от контекста на конкретната ситуация. Едно доста често срещано фамилно име няма да бъде достатъчно да идентифицира някого, т.е. да го разграничи от цялото население на страната, докато е вероятно да спомогне да бъде идентифиран ученик в класна стая. Дори спомагателна информация като например „мъжът, който носи черен костюм“ може да идентифицира някого измежду пешеходците, чакащи светофар. Така че въпросът дали едно лице, с което се свързва информацията, е идентифицирано или не, зависи от обстоятелствата в случая.

По отношение на пряко идентифицирани или подлежащи на идентификация лица **името** на лицето е действително най-разпространеният идентификатор и на практика понятието „идентифицирано лице“ предполага най-често препратка към името на лицето.

За да се потвърди тази самоличност, понякога името на лицето трябва да бъде комбинирано с друга информация (дата на раждане, имена на родителите, адрес или снимка в лице), за да се избегне объркване на това лице с евентуални съименници. Например информацията, че X притежава определена парична сума може да се счита за свързана с идентифицирано лице, защото се отнася за името на лицето. Името е информация, която разкрива, че лицето използва комбинация от букви и звукове, за да се разграничи и да бъде отличавано от други лица, с които то установява отношения. Името може също да бъде отправна точка, която води към информация за това къде живее лицето или къде може да бъде открито, може също така да дава информация за хората в неговото семейство (чрез фамилното име) и за ред други различни юридически и социални отношения, свързани с това име (образователни данни, медицински данни, банкови сметки). Дори е възможно да се научи външността на лицето, ако с това име се свързва и негова снимка. Цялата тази информация, свързана с името, може да позволи на някого да разкрие подробности за конкретно лице и ето защо първоначалната

информация е свързана посредством идентификаторите с физическо лице, което може да бъде отличено от други лица.

Що се отнася до непряко идентифицираните или подлежащи на идентификация лица, тази категория по принцип се свързва с явлението „единствени по рода си комбинации“, независимо дали малки или големи по размер. В случаи, когато *prima facie* размерът на наличните идентификатори не позволява разграничаване на конкретно лице, това лице все пак може да „подлежи на идентификация“, тъй като тази информация, комбинирана с друга такава (независимо дали последната е запазена от администратора на данни или не) ще позволи лицето да бъде отличено от другите. Ето защо директивата пояснява „един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност“. Някои характеристики са до такава степен уникални, че някой може да бъде идентифициран без никакво усилие („настоящият министър-председател на Испания“), но комбинацията от подробности на ниво категория (възрастова категория, произход от дадена област и т.н.) също може да бъде достатъчно решаваща при някои обстоятелства, особено ако се разполага с достъп до някакъв вид допълнителна информация. Това явление е изследвано доста обширно от статистици, които винаги са имали силен стремеж към избягване на нарушаването на поверителността.

Пример № 10: откъслечна информация в пресата

Публикувана е информация за бивше криминално дело, което си е спечелило много голямо обществено внимание в миналото. В настоящата публикация не присъства нито един от традиционните идентификатори, а именно име или дата на раждане на което и да е от засегнатите лица.

Не изглежда доста трудно да се получи допълнителна информация, позволяваща на човек да открие кои са главните лица, свързани със случая, например като се прегледат вестниците от съответния период. Наистина може да се предположи, че съществува известна вероятност някой да предприеме такива мерки (като преглед на стари вестници), които най-вероятно биха спомогнали за откриване на имената и другите идентификатори за лицата, посочени в примера. Затова изглежда оправдано да се разглежда информацията в дадения пример като „информация за подлежащи на идентификация лица“ и като техни лични данни.

Тук трябва да се отбележи, че докато идентификацията по име е най-често срещано явление в практиката, името може само по себе си да не е необходимо във всички случаи, за да се идентифицира едно лице. Това може да се случи, когато за отличаване на някого се използват други идентификатори. Например компютърните файлове, регистриращи лични данни, обикновено определят на регистрираното лице единствен по рода си идентификатор, за са избегне объркване между две лица във файла. Също и в мрежата средствата за наблюдение на мрежовия трафик правят поведението на една машина лесно за определяне, а съответно и поведението на нейния потребител. По този начин индивидуалността на лицето се сглобява от парченца, за да се отнесат определени решения към него. Без дори да се търсят името и адреса на лицето, е възможно то да се категоризира въз основа на социално-икономически, психологически, философски или други критерии и да се отнесат определени решения към него, тъй като мястото за контакт с лицето (компютър) вече не изисква задължително разкриването на неговата самоличност в тесния смисъл на думата. С други думи, възможността да се идентифицира едно лице вече не означава задължително да се открие неговото име. Определението на личните данни отразява този факт[10].

Съдът на Европейските общности се произнесе в този смисъл, когато заяви *препращането в интернет страниците към различни лица и тяхното идентифициране по име или чрез други средства, например чрез предоставяне на телефонните им номера или на информация* относно *работните им условия или любими занимания, представлява обработване на лични данни [...]по смисъла на [...] Директива 95/46/ЕО*[11].

Пример №. 11: кандидати за убежище

Кандидатите за убежище, криещи истинските си имена, получават кодов номер за административни цели в институциите, предоставящи убежище. Този номер

[10] Доклад за приложението на принципите за защита на личните данни към световните телекомуникационни мрежи, от г-н Ив Пуйе и неговия екип, за Комитета T-PD на Съвета на Европа, точка 2.3.1, T-PD (2004) 04 окончателен

[11] Решение на Съда на Европейските общности C-101/2001от 06.11.2003 г. (Lindqvist), §27

служи като идентификатор, така че различната информация относно престоя на кандидата за убежище в институцията ще бъде прикачена към него, а с помощта на снимка или други биометрични показатели, кодовият номер ще има тясна и непосредствена връзка със физическото лице, като по този начин се позволи неговото отличаване от други кандидати за убежище и отнасяне на различна информация към него, която след това ще препраща към „идентифицирано“ физическо лице.

В член 8, параграф 7 се предвижда също, че *държавите-членки определят условията, при които може да се обработва национален идентификационен номер или какъвто и да е друг идентификатор с общо приложение*. Струва си да се отбележи смисъла на тази разпоредба, която не съдържа никакво специално указание за това какъв вид условия би трябвало да приемат държавите-членки, но която все пак е заложена в този член, който засяга чувствителни данни. В съображение 33 този вид данни са наречени *данни, които по своя характер могат да нарушат основните свободи или личния живот*. Логично е да се предположи, че законодателят е имал подобни съображения относно националните идентификационни номера поради силния потенциал за лесно и недвусмислено свързване на различна информация за дадено лице.

Средства за идентифициране

В съображение 26 от директивата се отделя специално внимание на термина „подлежащ на идентификация: *като имат предвид, че за да се определи дали едно лице подлежи на идентификация, следва да се разглежда <u>съвкупността от всички средства, които биха могли да бъдат използвани разумно</u> от администратора или от друго лице с цел идентифицирането на даденото лице.* Това означава, че само предполагаемата възможност за разграничаване на лицето не е достатъчна, за да се смята, че човекът „подлежи на идентификация“. Ако такава възможност не съществува или е незначителна, като се вземат предвид *всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице,* лицето не следва да се разглежда като подлежащо на идентификация, а информацията – като лични данни. Критерият *всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице* следва по-специално да вземе предвид всички въпросни фактори. Цената за провеждане на идентификация е един такъв фактор, но не е единствен. Желаната цел, начинът, по който е стурктурирана обработката, очакваната от администратора полза, оспорваните интереси на лицата, както и риска от организационни проблеми с функционирането (например нарушаване на задълженията за спазване на поверителност) и техническите проблеми също трябва да бъдат отчетени. От друга страна този тест е динамичен и трябва да отчете съвременното ниво в технологиите по време на обработването и възможностите за развитие през периода, за който ще се обработват данните. Идентификацията може да не е възможна днес с всички средства, които биха могли да бъдат използвани разумно днес. Ако е планирано данните да се съхраняват един месец, не може да се очаква идентификацията да е възможна по време на продължителността на действие на информацията и не може те да се разглеждат като лични данни. Ако обаче е планирано те да се съхраняват 10 години, администраторът трябва да отчете възможността за идентифициране, която може да възникне през деветата година от продължителността на тяхното действие и която може да ги превърне лични данни в този момент. Системата трябва да бъде в състояние да се приспособява към тези промени в момента на

настъпването им и да включва съответните технически и организационни мерки своевременно.

Пример № 12: публикуване на рентгенови снимки заедно със собственото име на лицето

Рентгеновата снимка на дама е била публикувана в научно списание заедно със собственото име на дамата, което е било много необичайно. Собственото име на лицето заедно с факта, че роднини или познати знаят, че то страда от определено заболяване, го прави подлежащо на идентификация от определен брой хора, като рентгеновата снимка тогава би могла да се счита за лични данни.

Пример № 13: данни за фармацевтични изследвания

Болници или отделни лекари прехвърлят на компания данни за пациентите си от медицинските регистри за целите на медицински изследвания. Не са използвани имена на пациенти, а само серийни номера, отнесени произволно към всеки клиничен случай, за да се гарантира съгласуваност и да се избегне объркване на информация за различни пациенти. Имената на пациентите остават изключително на разположение на съответните лекари, обвързани с медицинска тайна. Данните не съдържат никаква допълнителна информация, която прави идентифицирането на пациентите възможно чрез комбинирането ѝ. Освен това са били предприети всякакви други юридически, технически или организационни мерки, за да се предотврати възможността съответното физическо лице да бъде идентифицирано или да стане възможно неговото идентифициране. При тези обстоятелства органите за защита на данните може да преценят, че не съществуват средства при обработването, извършено от фармацевтичната компания, които биха могли да бъдат разумно използвани за идентифициране на физическите лица.

Както бе споменато по-горе, един свързан с въпроса фактор, за оценка на *всички средства, които биха могли да бъдат използвани разумно* за идентифициране на лицата, ще бъдат всъщност целта, преследвана от администратора на данни при обработването им. Националните органи за защита на данните са били изправени пред случаи, в които администраторът твърди, от една страна, че е обработвана само разпокъсана информация без препращане към име или други преки идентификатори и застъпва тезата, че данните не следва да се разглеждат като лични данни и не следва да бъдат предмет на правилата за защита на личните данни. От друга страна, обработването на тази информация има смисъл само, ако то позволи идинтифициране на определени лица и третирането им по определен начин. В тези случаи, когато целта на обработването предполага идентифициране на лица, може да се допусне, че администраторът или всяко друго ангажирано лице има или ще има средствата, които „биха могли да бъдат използвани разумно“ за идентифициране на съответното физическо лице. Всъщност да се твърди, че лицата не подлежат на идентификация, когато целта на обработването е именно те да бъдат идентифицирани, би било явно противоречие. Затова информацията следва да се разглежда като свързана с подлежащи на идентификация лица, а обработването следва да бъде предмет на правилата за защита на личните данни.

Пример № 14: видеонаблюдение

Това важи особено в контекста на видеонаблюдението, за което администраторите често твърдят, че идентификация би се получила само в малка част от събрания материал и затова, преди да се осъществи идентификация в тези редки случаи, не се обработват лични данни. Обаче, тъй като целта на видеонаблюдението е да се идентифицират лицата, които се виждат на видеоизображението във всички случаи, в които такова идентифициране се счита за необходимо от администратора, цялостното приложение като такова трябва да бъде разглеждано като обработване на данни за подлежащи на идентификация лица, дори ако някои записани лица на практика не подлежат на идентификация.

Пример № 15: динамичен IP адрес

Работната група разгледа IP адресите като данни, свързани с подлежащи на идентификация лица. Тя заяви, че *доставчиците на интернет и управителите на локални мрежи могат, използвайки разумни средства, да идентифицират потребители на интернет, към които са отнесли IP адрес, тъй като обикновено системно „регистрират" във файл датата, часа, продължителността и динамичния IP адрес, даден на потребителя на интернет. Същото може да се каже за доставчиците на интернет услуги, които поддържат дневник на HTTP сървър. В тези случаи няма съмнение относно факта, че става дума за лични данни по смисъла на член 2, буква а) от директивата ...)*[12]

Особено в случаите, в които обработването на IP адреси се провежда с цел идентифициране на компютърните потребители (например от притежателите на авторски права, за да преследват компютърните потребители за нарушаване на правата за интелектуална собственост), администраторът очаква, че „средствата, които биха могли да бъдат използвани разумно" за идентифициране на лицата ще бъдат налични, например чрез внесените жалби в съдилищата (иначе събирането на информация няма никакъв смисъл), и следователно информацията трябва да се разглежда като лични данни.

Един специален случай би бил този на някои видове IP адреси, които при определени обстоятелства в действителност не позволяват идентифициране на потребителя поради разнообразни технически и организационни причини. Пример за това могат да бъдат IP адресите, определни на компютър в интернет кафе, където не се изисква идентификация на клиента. Може да се поддържа мнението, че събирането на данни за използването на компютър X през определен период от време не позволява идентифициране на потребителя с разумни средства и затова това не са лични данни. Обаче следва да се отбележи, че доставчиците на интернет услуги най-вероятно няма да знаят дали въпросният IP адрес позволява идентификация или не и ще обработват данните, свързани с този IP адрес, по същия начин, както обработват информацията, свързана с IP адреси на потребители, които са надлежно регистрирани и подлежат на идентификация. По този начин, освен ако доставчикът на интернет услуги е в състояние да определи с абсолютна сигурност, че данните съответстват на потребители, които не могат да бъдат идентифицирани, той ще трябва да разглежда цялата IP информация като лични данни, за всеки случай.

[12] РГ 37: Поверителност в интернет – Интегриран подход на ЕС към защита на данните он-лайн – приет на 21.11.2000 г.

Пример № 16: щета, причинена от графити

Моторни превозни средства за пътници, собственост на транспортна компания, понасят многократни щети като биват замърсявани с графити. За да оценят щетите и да улеснят подаването на правен иск срещу техните автори, компанията поддържа регистър, съдържащ информация за обстоятелствата на щетата, както и изображения на повредените предмети и на „надписите“ или „подписа“ на автора. Към момента на въвеждане на информацията в регистъра авторите на щетите не са известни, нито е известно на кого принадлежи „подписът“. Напълно е възможно това никога да не се узнае. Въпреки това целта на обработването е именно да се идентифицират лицата, за които се отнася информацията като автори на щетата, така че да бъде възможно подаването на правен иск срещу тях. Подобно обработване има смисъл, ако администраторът на данни очаква като „разумно възможно“, че един ден ще съществуват средства за идентифициране на лицето. Информацията, която се съдържа на снимките, би следвало да се разглежда като свързана с подлежащи на идентификация лица, информацията в регистъра – като лични данни, а обработването следва да бъде предмет на правилата за защита на личните данни, които позволяват подобно обработване като оправдано при определени обстоятелства и предмет на определени предпазни мерки.

Когато идентификацията на съответното физическо лице не е включена в целта на обработването, техническите мерки за предотвратяване на идентифицирането играят много важна роля. Използването на подходящи съвременни технически и организационни мерки за защита на данните срещу идентифициране може да е от значение, за да се счита, че лицата не подлежат на идентификация, като се вземат предвид *всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице* за идентифициране на лицата. В този случай осъществяването на тези мерки не е *следствие* от правно задължение, възникващо по силата на член 17 от директивата (който се прилага само, ако информацията представлява преди всичко лични данни), а по-скоро *условие* информацията именно да не бъде считана за лични данни, а обработването ѝ да не бъде предмет на директивата.

Псевдонимни данни

Поставянето на псевдоним е процес на прикриване на самоличността. Целта на този процес е да бъде възможно събиране на допълнителни данни, свързани с едно и също лице, без да е необходимо да се знае неговата самоличност. Това е особено необходимо в контекста на научноизследователската работа и статистиката.

Поставянето на псевдоним може да бъде осъществено по проследим начин, като се използва списък за съответствие на личностите и техните псевдоними, или като се използват алгоритми на двупосочна криптография за определяне на псевдоними. Прикриването на самоличността може също да бъде направено по такъв начин, че да не бъде възможно повторно идентифициране, например чрез еднопосочна криптография, която по принцип създава анонимни данни.

Ефективността на процедурата по поставяне на псевдоним зависи от редица фактори (на кой етап се използва, доколко надеждна е срещу обратно проследяване, брой на населението, от което е част лицето, възможност да се свържат отделни трансакции или записи с едно и също лице и т.н.) Псевдонимите

трябва да бъдат произволни и непредсказуеми. Броят на възможните псевдоними трябва да бъде толкова голям, че един и същи псевдоним никога да не бъде произволно избран два пъти. Ако се изисква високо ниво на защита, наборът от възможни псевдоними трябва да бъде поне равен на обхвата от стойности за надеждни криптографски хеш функции[13].

Проследимите псевдонимизирани данни могат да се разглеждат като информация за лица, които са *косвено подлежащи на идентификация.* Всъщност използването на псевдоним означава, че е възможно лицето да се проследи, така че самоличността му да може да бъде открита, но само при предварително определени обстоятелства. В този случай, въпреки че се прилагат правилата за защита на личните данни, рисковете за лицата по отношение на обработването на тази косвено подлежаща на идентификация информация най-често ще бъдат ниски, така че прилагането на тези правила с основание ще бъде по-гъвкаво, отколкото ако беше обработвана информация относно пряко подлежащи на идентификация лица.

Данни, кодирани с ключ

Кодираните данни са класически пример на поставяне на псевдоним. Информацията е свързана с лица, които са белязани с код, докато ключът, който извършва съответствието между кода и общите идентификатори на лицата (като име, дата на раждане, адрес), се съхранява отделно.

Пример № 17: необобщени данни за статистика

Един пример, който показва нагледно важността на отчитането на всички обстоятелства за оценяване на това дали средствата за идентификация „биха могли да бъдат разумно“ използвани, е този за информация за лица, обработвана националния статистически институт, където на определен етап информацията се държи в необобщена форма и е свързана с конкретни лица, но те са обозначени с код вместо с име (например лицето с код X1234 пие чаша вино повече от 3 пъти седмично). Статистическият институт съхранява отделно ключа за тези кодове (списъка, свързващ кодовете с имената на лицата). Този ключ може да се разглежда като такъв, „който би могъл да се използва разумно“ от статистическия институт, и затова наборът от информация, свързана с лица, може да се разглежда като лични данни от института и би трябвало да бъде предмет на правилата за защита на личните данни. Сега да предположим, че списъкът с данни за навиците на пиене на потребителите се изпраща на националната организация на винопроизводителите, за да им позволи да подкрепят позицията си със статистически цифри. За да се определи дали този списък с информация е все още лични данни, трябва да се прецени дали отделните потребители на вино могат да бъдат идентифицирани,*като се вземат предвид всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице*.

Ако използваните кодове са единствени за всяко конкретно лице, рискът от идентификация възниква винаги, когато е възможно да се получи достъп до

[13] Виж работен документ „подобряване на технологиите за защита на личния живот“ от Работната група по подобряване на технологиите за защита на личния живот на Комитета по техническите и арганизационни аспекти на защитата на данните на немските федерални и държавни комисари по защита на личните данни (октомври 1997 г.), публикуван на адрес: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

ключа, използван за криптиране. Следователно рискът от външен пробив, вероятността, че някой в организацията на изпращача въпреки професионалната тайна би предоставил ключа *и* осъществимостта на косвена идентификация са фактори, които трябва да бъдат взети под внимание, за да се определи дали лицата могат да бъдат идентифицирани, като се *вземат предвид всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице,* и следователно дали информацията следва да се разглежда като лични данни. Ако това е така, се прилагат правилата за защита на личните данни. Друг въпрос е, че в тези правила за защита на данните би могло да се отчете дали рисковете за лицата са намалени и да се направи така, че обработването да подлежи на повече или по-малко стриктни условия въз основа на гъвкавостта, позволена от правилата на директивата.

Ако кодовете не са единствени, а един и същ код (например 123) се използва за обозначаване на лица в различни градове и за данни от различни години (като се разграничава само конкретно лице в рамките на една година и в рамките на извадката в същия град), администраторът или трето лице биха могли да идентифицират определено лице, ако знаят годината и града, за които се отнасят данните. Ако тази допълнителна информация е изчезнала и няма вероятност да бъде по разумен начин възстановена, може да се счита, че информацията не се отнася за подлежащи на идентификация лица и не би била предмет на правилата за защита на данните.

Този тип данни често се използва при клинични изпитвания на лекарства. Директива 2001/20 от 4 април 2001 г. относно прилагането на добрата клинична практика при провеждането на клинични изпитвания на лекарствени продукти за хуманна употреба[14] създава правната рамка за осъществяване на тези дейности. Професионалното медицинско лице/научен изследовател (изследовател), изпитвайки лекарствата, събира информацията за резултатите от клиничните изпитвания върху всеки пациент, отбелязвайки го с код. Изследователят предоставя информацията на фармацевтична компания или на други заинтересовани лица (спонсори) само в тази кодирана форма, тъй като те се интересуват само от биостатистическа информация. Въпреки това изследователят пази отделно ключа, свързващ кода с общата информация, за идентифициране на пациентите отделно. За да се предпази здравето на пациентите в случай, че се окаже че лекарствата водят до опасности, изследователят е длъжен да пази този ключ, така че отделните пациенти да могат да бъдат идентифицирани в случай на необходимост и да получат съответно лечение.

Въпросът тук е дали данните, използвани за клинични изпитвания, може да се смятат за свързани с „подлежащи на идентификация“ физически лица, като по този начин са предмет на правилата за защита на данните. Според анализа, описан по-горе, за да се определи дали едно лице подлежи на идентификация, следва да се вземат предвид всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице, за да се идентифицира споменатото лице. В този случай идентификацията на лицата (за прилагане на подходящо лечение в случай на необходимост) е една от целите на обработката на данните, кодирани с ключ. Фармацевтичната компания тълкува средствата за обработване, включени в организационните мерки, и техните отношения с

[14] ОВ L 21, 1.5.2001 г., стр. 34.

изследователя, който съхранява ключа, по такъв начин, че идентифицирането на лицата да не е само нещо, което *би могло* да се случи, а е по-скоро нещо, което *трябва* да се случи при определени обстоятелства. Идентификацията на пациентите по този начин е включена в целите и средствата за обработка. В този случай може да се направи заключение, че подобни данни, кодирани с ключ, представляват информация, свързана с подлежащи на идентификация физически лица за всички страни, които биха могли да бъдат включени в евентуалното идентифициране, и следва да бъдат предмет на правилата на законодателството за защита на данните. Това не означава обаче, че всеки друг администратор на данни, обработващ същия набор от кодирани данни, би обработвал лични данни, ако в рамките на специфичната схема, в която работят тези други администратори, изрично е изключена повторна идентификация, като в това отношение са били взети съответните технически мерки.

В други области на изследване или на същия проект повторната идентификация на физическото лице, субект на данните, може да е била изключена при създаването на протоколите и процедурата, защото например няма включени терапевтични аспекти. Поради технически или други причини може все още да има начин да се открие кои лица съответстват на дадени клинични данни, но идентификацията не се предполага или не се очаква да бъде осъществена при каквото и да е обстоятелство, като са били приложени съответните технически мерки (например криптографски, необратимо хеширане) за предотвратяване на това. В този случай, дори ако може да се осъществи идентификация на определени физически лица въпреки всички тези протоколи и мерки (поради непредвидени обстоятелства като например случайно съчетаване на качества на физическото лице, които разкриват неговата самоличност), информацията, обработена от първоначалния администратор, не може да се смята за свързана с идентифицирани или подлежащи на идентификация лица, като се вземат предвид *всички средства, които разумно биха могли да бъдат използвани от администратора или от друго лице.* Нейното обработване по този начин не може да бъде предмет на разпоредбите на директивата. Отделен въпрос е факта, че за новия администратор, който ефективно е получил достъп до информация, подлежаща на идентификация, тя безспорно ще се разглежда като „лични данни“.

ЧЗВ 14, параграф 7 от схемата за сфера на неприкосновеност

Въпросът за данните, кодирани с ключ, при фармацевтичните изследвания беше адресиран в рамките на споразумението за сферата на неприкосновеност[15]. ЧЗВ 14, параграф 7 гласи следното:

ЧЗВ 14 – Фармацевтични и медицински продукти

7. В: Данните от изследването са обикновено кодирани още на изхода и то единствено от основния изследовател, за да се предпази самоличността на заинтересованите лица. Фармацевтичните дружества, които възлагат подобни изследвания, не получават ключа на кода. Единствено изследователят съхранява един екземпляр от ключа за кода, за да може да идентифицира субекта на изследването при извънредни обстоятелства (например, ако се налага медицинска помощ). Предаването от ЕС за Съединените щати на лични

[15] Решение 2000/520/ЕО на Комисията от 26.7.2000 г., ОВ L 215/7, 25.8.2000 г.

данни, които са били кодирани по този начин, представлява ли предаване на данни, подчинено на принципите „сфера на неприкосновеност на личния живот“?

7. О: Не. Това не представлява предаване на лични данни, които са предмет на принципите..

Работната група смята, че това становище в споразумението за сфера на неприкосновеност на личния живот не е противоречи на обосновката, изяснена по-горе в полза на съображението за разглеждане на подобна информация като лични данни, предмет на директивата. Всъщност този често задаван въпрос не е достатъчно прецизен, тъй като не посочва на кого и при какви условия се прехвърлят данните. Работната група разбира, че този често задаван въпрос се отнася за случаи, когато данните, кодирани с ключ, се изпращат на получател в САЩ (например фармацевтичната компания), който получава само данните, кодирани с ключ, и никога няма да разбере самоличността на пациентите, която е известна и ще бъде известна при необходимост от лечение единствено на професионалното медицинско лице/изследовател в ЕС, но никога на компанията в САЩ.

Анонимни данни

„Анонимни данни“ по смисъла на директивата могат да бъдат определени като информация, свързана с физическо лице, когато то не може да бъде идентифицирано, независимо дали от администратора на данни или от друго лице, *като се вземат предвид всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице* за идентифициране на физическото лице. „Анонимизирани данни“ следователно биха били анонимни данни, които преди това са се отнасяли за подлежащо на идентификация лице, но тази идентификация повече не е възможна. Съображение 26 също се отнася до това понятие като гласи, че *принципите на защита не се отнасят до данни, които са направени анонимни по начин, който прави невъзможно идентифицирането на съответното физическо лице*. Оценката на това дали данните позволяват идентифициране на дадено лице и дали информацията може да се разглежда като анонимна или не зависи от обстоятелствата, като трябва да бъде проведен анализ на всеки отделен случай с конкретно споменаване на степента, до която средствата биха могли да бъдат използвани разумно за идентифициране, както е описано в съображение 26. Това се отнася особено за случая със статистическата информация, където въпреки факта, че информацията може да бъде представена като обединени данни, първоначалната извадка не е достатъчно голяма и друга информация може да направи възможно идентифицирането на лицата.

Пример № 18: статистически изследвания и комбиниране на разпръсната информация

Освен общоприетото задължение за спазване на правилата за защита на данните, за да се гарантира анонимността на статистическите изследвания, статистиците са подчинени на специфично задължение за спазване на професионална тайна, като съгласно тези правила им е забранено да публикуват неанонимни данни. Това ги задължава да публикуват обединени статистически данни, които няма вероятност да бъдат отнесени към идентифицирано лице зад статистиката. Това

правило е особено важно по отношение на публикуване на статистически данни от преброяване на населението. Във всяка ситуация трябва да бъде определен праг, под който се счита за възможно да се идентифицират засегнатите лица. Ако се появи критерий, който да доведе до идентификация при дадена категория лица, независимо колко голяма (т.е. само един лекар работи в град от 6000 жители), този „отличителен“ критерий трябва да отпадне изцяло или да бъдат добавени други критерии, за да „размият“ резултатите за дадено лице, така че да позволят запазването на статистическа тайна.

Пример № 19: публикуване на видеонаблюдение

Собственик на магазин инсталира система за наблюдение с камера в своя магазин. Той разпространява в своя магазин снимките на крадците, които са били хванати посредством системата за видеонаблюдение с камера. След намеса на полицията той заличава лицата на крадците, като ги потъмнява. Въпреки това, дори след това действие, все още съществува възможност лицата на снимките да бъдат разпознати от техните приятели, роднини или съседи, поради факта, че например все още могат да бъдат разпознати фигурата, прическата и дрехите им.

4. ЧЕТВЪРТИ ЕЛЕМЕНТ: „ФИЗИЧЕСКО ЛИЦЕ“

Защита, осигурена от правилата на директивата, се прилага към физически лица, т.е. към човешки същества. Правото на защита на личните данни е в този смисъл универсално, неограничено само до поданици или пребиваващи в определена държава. Съображение 2 от директивата изрично посочва това, като заявява, че *системите за обработка на данни са създадени с цел да служат на хората* и че *независимо от националността или местожителството на физическите лица, те трябва да зачитат техните основни права и свободи*.

Понятието „физическо лице“ се споменава в член 6 от Всеобщата декларация за правата на човека, съгласно който *всеки човек, където и да се намира, има право на признаване на неговата правосубектност*. Законодателствата на държавите-членки, обикновено в областта на гражданското право, излагат по-точно понятието за личностния характер на човешките същества, която се разбира като способност да бъде предмет на правни отношения, започвайки от раждането на личността и завършвайки с нейната смърт. Личните данни следователно са данни, свързани с идентифицирани или подлежащи на идентификация по принцип *живи личности*. Това повдигна редица въпроси за целите на този анализ.

Данни за мъртви лица

Информацията, свързана с мъртви лица, следователно по принцип не се счита за лични данни, подлежащи на правилата на директивата, тъй като мъртвите лица вече не са физически лица в гражданското право. Обаче данните за починалите могат все пак да получат някаква косвена защита в определени случаи.

От друга страна, администраторът на данните може да не е в състояние да установи дали лицето, за което се отнасят данните е все още живо или може би мъртво. Дори ако може да направи това, информацията за починалото лице може да бъде обработвана при същия режим като този за живите лица без разграничение. Тъй като администраторът на данните подлежи на задълженията

за защита на данните, наложени от директивата по отношение на данните за живите лица, вероятно за него ще бъде по-лесно на практика да обработва също и данните на починалите по начина, наложен от правилата за защита на данните, отколкото да разделя двете групи данни.

От друга страна, информацията за мъртвите лица може също да се отнася за живи лица. Например информацията, че починалата N е страдала от хемофилия показва, че нейният син X страда от същото заболяване, тъй като то е свързано с ген, съдържащ се в X-хромозомата. По този начин, когато информацията, която представлява данни за мъртвото лице, може да се разглежда като свързана в същото време и с живо лице и да бъде лични данни, предмет на директивата, личните данни на починалото лице могат непряко да се възползват от защитата на правилата за защита на данните.

На трето място информацията за мъртви лица може да бъде предмет на особена защита, предоставена от група правила, различни от законодателството за защита на данните, очертавайки това, което някои наричат *personalitas praeterita*. Задължението за конфиденциалност за медицинския персонал не приключва със смъртта на пациента. Националното законодателство относно правото на собствен образ и достойнство може също да предостави защита на паметта на мъртвото лице.

И на четвърто място нищо не пречи на държава-членка да разшири обхвата на националното законодателство, прилагащо разпоредбите на Директива 95/46/ЕО, върху области, невключени в обхвата ѝ, при условие че никоя друга разпоредба от правото на Общността не възпрепятства това, както напомня Съда на ЕО[16]. Възможно е някой национален законодател да реши да разшири разпоредбите на националното законодателство за защита на данните върху някои аспекти, отнасящи се до обработването на данните относно починали лица, когато това е оправдано от легитимен интерес[17].

Неродени деца

Степента, до която могат да се прилагат правилата за защита на данните преди раждането, зависи от общото състояние на националните правни системи относно защитата на неродените деца. Главно за да се вземат предвид наследствените права, някои държави-членки признават принципа, че заченати, но все още неродени деца, се считат за родени, доколкото става въпрос за облаги (като по този начин могат да получат наследство или да приемат дарение), при условие, че те действително могат да бъдат родени. В други държави-членки се предоставя специфична защита чрез конкретни правни разпоредби, също подлежащи на това условие. За да се определи дали националните разпоредби за защита на данните защитават също и информацията за неродени деца, трябва да се вземе предвид този общ подход на националната правна система, заедно с идеята, че целта на правилата за защита на данните е да защитава личността.

---

16 Решение на Съда на Европейските общности C-101/2001 от 06.11.2003 г. (Lindqvist), § 98

17 Протокол на заседание на Съвета на Европейския съюз, 8.2.1995 г., документ 4730/95: „Re член 2(a) *Съветът и Комисията потвърждават, че държавите-членки постановят дали и до каква степен настоящата директива ще се прилага по отношение на починали лица*.“

Втори въпрос се поставя от съображението, че общият отговор на правната система зависи от очакването, че положението на неродените деца е ограничено във времето за периода на бременността. Не се отчита фактът, че това положение може всъщност да продължи значително по-дълго, както е случаят със замразените ембриони. Накрая, конкретен правен отговор може да бъде намерен в съответните разпоредби за репродуктивните техники, занимаващи се с използването на медицинска или генетична информация за ембрионите.

Юридически лица

Тъй като определението за личните данни се отнася към отделни лица, т.е. физически лица, информацията, свързана с юридическите лица по принцип не се покрива от директивата и предоставената от нея защита не се прилага[18]. Въпреки това в редица случаи определени правила за защита на данните могат все пак да се приложат косвено по отношение на информация, свързана с предприятия или с юридически лица.

Някои разпоредби на Директива 2002/58/ЕО за защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации се отнасят за юридическите лица. Член 1 от тази директива предвижда, че *разпоредбите на настоящата директива конкретизират и допълват Директива 95/46/ЕО, за целите, упоменати в параграф 1. Освен това, те се грижат за защита на легитимните интереси на абонати, които са юридически лица*. Съответно, членове 12 и 13 разширяват приложението на някои разпоредби, отнасящи се до указателите на абонатите и нежеланите съобщения, също върху юридически лица.

Информацията за юридическите лица може също да се разглежда по същество като „свързана с“ физически лица съгласно критериите, изложени в настоящия документ. Това може да е така, когато името на юридическото лице произлиза от това на физическо лице. Друг случай може да бъде свързан с фирмената електронна поща, която обикновено се използва от определен служител, или с информация за малък бизнес (казано на правен език по-скоро „субект“, отколкото юридическо лице), която да описва поведението на собственика. Във всички случаи, когато критериите за съдържание, цел, или резултат позволяват информацията за юридическото лице или предприятието да се разглежда като свързана с физическо лице, тя следва да се смята за лични данни и следва да се прилагат правилата за защита на личните данни.

Съдът на Европейските общности поясни, че няма пречки за държавите-членки да разширят обхвата на тяхното национално законодателство, прилагащо разпоредбите на директивата, върху области, които не са включени в нея, при условие, че това не противоречи на никоя друга разпоредба на правото на Общността[19]. Съответно държави-членки като Италия, Австрия или Люксембург разшириха приложението на определени разпоредби на националното законодателство, прието в съответствие с директивата (като тези за мерките за сигурност), като включиха в него обработването на данни за юридически лица.

---

[18] Съображение 24 от директивата: *като имат предвид, че законодателството, отнасящо се до защитата на юридически лица при обработването на данни, които се отнасят до тях, не се обхваща от настоящата директива*.

[19] Решение на Съда на Европейските общности C-101/2001 от 06.11.2003 г. (Lindqvist), § 98

Както в случая с информацията за починалите лица практическите мерки на администратора на данни може също да доведат до това данни за юридическите лица да подлежат де факто на правилата за защита на личните данни. Когато администраторът на данни събира данни за физически и юридически лица без разграничение и ги включва в една и съща група данни, структурата на механизмите за обработване на данните и системата за одит може да бъде установена така, че да се спазват правилата за защита на данните. Всъщност може да бъде по-лесно за администратора да прилага правилата за защита на данните към всички видове информация в своите папки, отколкото да се опитва да я разпредели за физически и за юридически лица.

IV. КАКВО СЕ СЛУЧВА, АКО ДАННИТЕ ПОПАДАТ ИЗВЪН ОПРЕДЕЛЕНИЕТО?

Както видяхме в настоящия документ, при различни обстоятелства информацията може да счита, че не представлява лични данни. Това е така, когато данните не могат да се разглеждат като свързани с отделно лице, или защото лицето не може да се разглежда като идентифицирано или подлежащо на идентификация. Когато обработваната информация не попада в рамките на понятието „лични данни“, последствието е, че директивата не се прилага съгласно член 3 от нея. Това не означава обаче, че лицата могат да бъдат лишени от всякаква защита в конкретната ситуация. Следва да се вземат под внимание следните съображения.

Ако директивата не се прилага, може да се приложи националното законодателство за защита на личните данни. Както е посочено в член 34, адресати на директивата са държавите-членки. Извън нейния обхват държавите-членки не са подчинени на задълженията, които тя налага, а именно да влязат в сила законовите, подзаконовите и административните разпоредби, които са необходими за да се съобразят с нея. Обаче, както Съдът на Европейските общности разясни, няма пречки за държавите-членки да разширят обхвата на националното законодателство за прилагане на разпоредбите на директивата върху области, които не са включени в нея, при условие че това не противоречи на никоя друга разпоредба на правото на Общността. Следователно е напълно възможно определени ситуации, които не включват обработване на лични данни, както е определено в директивата, да бъдат подчинени въпреки това на предпазни мерки по национален закон. Това може например да се приложи към данни, кодирани с ключ, независимо от това дали са лични данни или не.

Когато правилата за защита на данните не се прилагат, някои действия могат все пак да противоречат на член 8 от Европейската конвенция за правата на човека, която защитава правото на личен и семеен живот в светлината на особено значимата юриспруденция на Европейския съд по правата на човека. Друг комплекс от правила като законодателството за гражданските правонарушения, наказателното право или антидискриминационното законодателство също могат да осигурят защита на лицата в онези случаи, когато правилата за защита на личните данни не се прилагат и става дума за различни легитимни интереси.

V. ЗАКЛЮЧЕНИЯ

В настоящото становище работната група предостави насоки за начина, по който понятието за лични данни в Директива 95/46/ЕО и свързаното законодателство на

Общността следва да бъдат разбирани и за начина, по който те трябва да бъдат прилагани в различни ситуации.

Като основно съображение бе отбелязано, че европейският законодател е имал намерение да приеме широко понятие за личните данни, но това понятие не е неограничено. Винаги трябва да се взима предвид, че целта на правилата, съдържащи се в директивата, е да защитава основните права и свободи на лицата, по-конкретно тяхното право на личен живот по отношение на обработването на данните. Затова тези правила бяха създадени, така че да се прилагат в ситуации, в които правата на лицата могат да бъдат изложени на риск и следователно имат нужда от защита. Обхватът на правилата за защита на данните не бива да е прекалено разширен, но и прекомерно ограничаване на понятието „лични данни“ също трябва да се избягва. Директивата определи обхвата си, като изключи редица дейности и позволява гъвкавост при приложението на правилата по отношение на дейности, които са в обхвата ѝ. Органите за защита на данните играят основна роля при намирането на подходящото равновесие в това приложение (виж точка II).

Анализът на работната група е основан на четири основни „градивни елемента“, които могат да бъдат разграничени в определението за лични данни, а именно „всяка информация“, „свързана с“, „идентифицирано или подлежащо на идентификация“, „физическо лице“. Тези елементи са тясно преплетени и взаимозависими, но заедно определят дали една информация следва да се разглежда като лични данни. Анализът е подкрепен от примери от националната практика на европейските органи за защита на данните.

- Първият елемент – „всяка информация“ – изисква широко тълкуване на понятието, независимо от характера или съдържанието на информацията и техническия формат, в който е представена. Това означава, че както обективната, така и субективната информация за дадено лице в каквото и да е негово качество може да бъде разглеждана като лични данни и независимо от техническия носител, на който се съдържа. Становището също така обсъжда биометричните данни и правни различия при човешки проби, от които могат да бъдат извлечени (виж III.1).

- Вторият елемент – „свързана с“ – досега е бил пренебрегван, но има решаващо значение при определянето на съществения обхват на понятието, особено по отношение на предмети и нови технологии. Становището предвижда три алтернативни елемента – т.е. съдържание, цели и резултат, за да се определи дали информацията е „свързана с“ определено лице. Това също обхваща информация, която може да има очевидно въздействие върху начина, по който лицето бива третирано или оценявано. (виж III.2).

- Третият елемент – „идентифицирано или подлежащо на идентификация“ – е насочен върху условията, при които едно лице следва да се разглежда като „подлежащо на идентификация“ и особено върху „средствата, които биха могли да бъдат разумно използвани“ от администратора или от друго лице за идентифициране на това лице. Конкретният контекст и обстоятелствата на специфичния случай играят важна роля в този анализ. Съображението също така се занимава с „псевдонимизирани данни“ и използването на „данни, кодирани с ключ“ при статистическите и фармацевтичните изследвания (виж III.3).

- Четвъртият елемент – "физическо лице" – се занимава с изискването личните данни да са за живи лица. Становището също така обсъжда допирните точки с данни за починали лица, неродени деца и юридически лица (виж III.4).

Становището накрая разглежда това какво се случва, ако данните попадат извън обхвата на определението за лични данни. Може да има различни решения за справяне с проблеми в тези случаи, включително националното законодателство извън обхвата на директивата, при условие че се зачитат другите закони на общността (виж IV).

Работната група приканва всички заинтересовани лица внимателно да изучат насоките, предвидени в настоящото становище, и да ги имат предвид, когато тълкуват и прилагат разпоредбите на националното законодателство в съответствие с Директива 95/46/ЕО.

Членовете на работната група, главно представители на надзорните органи за защита на данните на национално ниво, се ангажират да разработят допълнително предоставените насоки в това становище в рамките на тяхната юрисдикция и да гарантират правилното прилагане на националното законодателство в съответствие с Директива 95/46/ЕС.

Работната група възнамерява да прилага и разработва насоките в настоящото становище винаги когато е уместно, както и да ги взима под внимание в бъдещата си работа, особено когато се занимава с теми като управление на самоличността, в контекста на електронното управление и електронното здравеопазване, както и в контекста на радиочестотната идентификация (RFID). Що се отнася до последната тема, работната група има намерение да допринесе за допълнителен анализ на начина, по който правилата за защита на данните могат да въздействат върху използването на радиочестотната идентификация и на необходимостта от допълнителни мерки, за да се гарантира съответното зачитане на правата за защита на личните данни и интереси в този контекст.

Работната група накрая приканва заинтересованите лица и надзорните органи да предоставят обратна връзка въз основа на техния практически опит на предоставените насоки в настоящото становище, включително всякакви примери, допълващи споменатите в настоящия документ. Тя възнамерява да се върне към този въпрос своевременно с оглед на по-нататъшното подобряване на общото разбиране на ключовото понятие за личните данни, както и с цел гарантиране на хармонизирано прилагане и по-добро изпълнение на Директива 95/46/ЕО и свързаното законодателство на тази основа.

За работната група

Председател:
Peter SCHAAR