Насоки № 3/2019 относно обработването на лични данни чрез видеоустройства

Версия 2.0

Прието на 29 януари 2020 г.

История на версиите

Версия 2.0	29 януари 2020 г.	Приемане на насоките след обществена консултация
Версия 1.0	10 юли 2019 г.	Приемане на насоките за обществена консултация

Съдържание

Европейският комитет по защита на данните

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство, и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,[1]

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ВЪВЕДЕНИЕ

1. Интензивната употреба на видеоустройства оказва въздействие върху поведението на гражданите. Значителното по обем въвеждане на такива инструменти в много сфери от живота на физическите лица ще ги подложи на допълнителен натиск за предотвратяване на откриването на обстоятелства, които могат бъдат оценени като аномалии. На практика тези технологии могат да ограничат възможностите за анонимно движение и анонимно използване на услуги и като цяло ограничават възможностите на лицата да останат незабелязани. Последиците по отношение на защитата на данните са големи.

2. Макар че лицата може да приемат осъществяване на видеонаблюдение за определена цел, например във връзка със сигурността, е необходимо да бъдат осигурени гаранции за избягване на несанкционирана употреба за съвършено различни и неочаквани за субекта на данните цели (например маркетинг, наблюдение на трудовото изпълнение на служители и др.). Наред с горното, понастоящем, се разработват множество инструменти за използване на записаните изображения и превръщане на обичайните камери в интелигентни камери. Обемите на данните, генерирани от видеосистемите, в съчетание с тези инструменти и техники повишават рисковете от вторично използване (свързано или не с първоначално определената цел на системата) и дори рисковете от злоупотреба. Общите принципи на ОРЗД (член 5) следва във всички случаи да се отчитат внимателно, когато става дума за видеонаблюдение.

3. Системите за видеонаблюдение променят на множество различни нива начина, по който специалистите от частния и публичния сектор си взаимодействат в частна обстановка или на публични места с цел повишаване на сигурността, анализ на аудиторията, персонализирана реклама и др. Ефективността на видеонаблюдението е значително повишена благодарение на все по-масовото въвеждане на интелигентен видео анализ. Тези техники могат да съдържат по-

[1] Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“.

висока (например- комплексни биометрични технологии) или по-ниска степен на намеса (например- прости алгоритми за отброяване). Запазването на анонимността и на неприкосновеността на личния живот като цяло става все по-трудно. Въпросите, свързани със защитата на данните, които се повдигат във всяка ситуация, могат да се различават, което важи и за правния анализ във връзка с използването на една или друга от тези технологии.

4. Наред с въпросите, свързани с неприкосновеността на личния живот, съществуват и рискове, свързани с възможно неправилно функциониране на тези устройства и с необективност, която те могат да породят. Според данните от научни изследвания, софтуерът, който се използва за идентифициране, разпознаване или анализ на лица, функционира с различна ефективност в зависимост от възрастта, пола и етническия произход на идентифицираното лице. Алгоритмите ще се използват по отношение на различни демографски групи, поради което наличието на необективност или отклонения при разпознаването на лица може да задълбочи предразсъдъците в обществото. С оглед на това, администраторите на данни трябва наред с другото да гарантират, че дейностите по обработване на биометрични данни, получени чрез видеонаблюдение, ще бъдат предмет на периодична оценка за тяхната необходимост и достатъчност на предоставените гаранции.

5. Видеонаблюдението не е необходимо по подразбиране, когато съществуват други начини за постигане на преследваната цел. В противен случай рискуваме промяна на културните норми, изразяваща се в това липсата на неприкосновеност на личния живот да бъде приета като нещо нормално.

6. Настоящите насоки са разработени, с цел да предоставят напътствия за прилагането на ОРЗД по отношение на обработването на лични данни чрез видеоустройства. Приведените примери не са изчерпателни, като общата аргументация може да се прилага към всички потенциални области на употреба.

2 ПРИЛОЖНО ПОЛЕ[2]

2.1 Лични данни

7. Систематичното автоматизирано наблюдение на определени зони посредством оптични или аудиовизуални устройства, най-често с цел защита на собствеността или на живота и здравето на физически лица, понастоящем е явление със значително разпространение. Тази дейност е свързана със събиране и запазване на образни или аудиовизуални данни за всички лица, влизащи в наблюдаваната зона, които подлежат на идентифициране въз основа на техния външен вид или други специфични елементи. Самоличността на въпросните лица може да бъде установена въз основа на тези данни. Също така те създават възможност за обработване на лични данни относно присъствието и поведението на лицата в съответната зона. Потенциалният риск от злоупотреба с тези данни нараства успоредно с размерите на наблюдаваната зона и броя на лицата, които я посещават. Този факт намира отражение в разпоредбата на член 35, параграф 3, буква в) от Общия регламент относно защитата на данните, съдържаща изискването за извършване на оценка на въздействието върху защитата на данните в случаи на систематично мащабно наблюдение на публично достъпна зона, както и в разпоредбата на член 37, параграф 1, буква б), която задължава обработващите лични данни да определят длъжностно лице по защита на данните, когато операцията по обработване поради по своето естество изисква редовно и систематично мащабно наблюдение на субектите на данни.

8. Регламентът не се прилага обаче по отношение на обработването на данни, които не се отнасят до лица, например, когато не е възможно да бъде идентифицирано, пряко или непряко, физическо лице.

> Пример: ОРЗД не се прилага по отношение на фалшиви камери (т.е. всяка камера, която не функционира като камера и следователно не обработва лични данни). *В някои държави членки обаче такива камери са предмет на други нормативни изисквания.*
>
> Пример: Видеозаписи, направени от голяма височина, попадат в обхвата на ОРЗД, само когато в конкретните обстоятелства обработените данни могат да бъдат свързани с конкретно физическо лице.
>
> Пример: Видеокамера е вградена в превозно средство с цел подпомагане на паркирането. Ако камерата е конструирана или настроена по такъв начин, че не събира никаква информация, свързана с физически лица (например- регистрационни табели на превозни средства или информация, позволяваща идентифициране на минувачи), ОРЗД не се прилага.

9.

2.2 Прилагане на Директивата относно правоприлагането (Директива (ЕС) 2016/680)

10. По-специално, в обхвата на Директива (ЕС) 2016/680 попада обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването и наказателното преследване на престъпления или изпълнението на наказателни санкции, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване.

[2] Европейският комитет по защита на данните отбелязва, че в случаите, когато това е допустимо съгласно ОРЗД, може да се прилагат специални изисквания, предвидени в националното законодателство.

2.3 Изключение във връзка с домашни занимания

11. Съгласно член 2, параграф 2, буква в) обработването на лични данни от физическо лице в хода на чисто лични или домашни занимания, които могат да включват и онлайн дейности, попада извън обхвата на ОРЗД.[3]

12. Тази разпоредба, известна като „изключение във връзка с домашни занимания“ в контекста на видеонаблюдението, трябва да се тълкува в тесен смисъл. Следователно, както изтъква Съдът на Европейския съюз, т.нар. „изключение във връзка с домашни занимания“ трябва „*да се тълкува като отнасящо се единствено до дейностите, които са част от личния или семейния живот на физическите лица, като очевидно не е такъв случаят с обработването на лични данни, което обхваща публикуването им в интернет, с което те стават достъпни за неопределен брой лица*“.[4] Освен това, ако система за видеонаблюдение, доколкото тя извършва постоянен запис и съхранение на лични данни и обхваща „*макар и частично, публични места и поради това е насочено извън личната сфера на лицето, което извършва по този начин обработване на данни, то не може да се счита за дейност, която е изцяло „лична или домашна“ по смисъла на член 3, параграф 2, второ тире от Директива 95/46*“[5].

13. Що се отнася до видеоустройства, функциониращи в помещения на частни лица, такова наблюдение може да попада в обхвата на изключението във връзка с домашни занимания. Това зависи от няколко фактора, които трябва да бъдат взети предвид при формулирането на заключение. Наред с посочените по-горе елементи, идентифицирани в решенията на Съда на Европейския съюз, ползвателите на видеонаблюдение в домашни условия трябва да отчитат дали имат някакви лични отношения със субекта на данните, дали мащабът и честотата на наблюдението предполагат някаква професионална дейност от тяхна страна, както и потенциалното отрицателно въздействие на наблюдението върху субектите на данните. Наличието на всеки един от посочените по-горе елементи не означава непременно, че обработването попада извън обхвата на изключението във връзка с домашните занимания — отговорът на този въпрос предполага извършване на цялостна оценка.

[3] Вж. също съображение 18.

[4] Съд на Европейския съюз, решение по дело C-101/01, *Bodil Lindqvist*, 6 ноември 2003 г., параграф 47.

[5] Съд на Европейския съюз, решение по дело C-212/13, *František Ryneš срещу Úřad pro ochranu osobních údajů*, 11 декември 2014 г., параграф 33.

Пример: Турист прави видеозаписи с мобилен телефон и видеокамера, за да документира своята ваканция. Той показва видеозаписите на приятели и близки, но не ги прави достъпни за неограничен кръг хора. Този случай попада в обхвата на изключението във връзка с домашните занимания.

Пример: Любителка на екстремните спортове, която се спуска по планински склонове с планински велосипед, желае да запише своите спускания със спортна видеокамера. Тя се спуска с велосипед в отдалечена област и планира да използва видеозаписите за собствено развлечение у дома си. Този случай попада в обхвата на изключението във връзка с домашните занимания, въпреки че в известна степен е налице обработване на лични данни.

Пример: Физическо лице извършва видеонаблюдение със запис в собствената си градина. Имотът е ограден и единствено администраторът на данните и неговото семейство влизат редовно в градината. Този случай попада в обхвата на изключението във връзка с домашните занимания, при условие че видеонаблюдението не обхваща дори частично обществени места или съседни имоти.

14.

3 ЗАКОНОСЪОБРАЗНОСТ НА ОБРАБОТВАНЕТО

15. Преди използване целите на обработването трябва да бъдат подробно описани (член 5, параграф 1, буква б)). Видеонаблюдение може да се осъществява с различни цели, например в помощ на защитата на имоти и други активи, защитата на живота и физическата неприкосновеност на физически лица, събиране на доказателства по граждански дела.[6] Тези цели на наблюдението трябва да бъдат документирани в писмена форма (член 5, параграф 2) и да бъдат посочени за всяка използвана камера за видеонаблюдение. Допуска се камери, които се използват за една и съща цел от един администратор на данни, да бъдат документирани заедно. Наред с горното, субектите на данните трябва да бъдат уведомени за целта (целите) на обработването в съответствие с член 13 (*вж. раздел 7, Задължения по отношение на прозрачността и информацията*). Посочването, че видеонаблюдението се извършва с цел „безопасност“ или „за вашата безопасност“, не е достатъчно конкретно (член 5, параграф 1, буква б)). Наред с това подобна практика противоречи на принципа, че личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните (вж. член 5, параграф 1, буква а)).

16. По принцип всяко предвидено основание съгласно член 6, параграф 1 може да представлява правно основание за обработване на данни от видеонаблюдение. Например, разпоредбата на член 6, параграф 1 се прилага в случаите, когато в националното законодателство е предвидено задължение за извършване на видеонаблюдение.[7] В практиката обаче е най-вероятно е да се използват следните разпоредби:

- Член 6, параграф 1, буква е) (законен интерес),
- Член 6, параграф 1, буква д) (необходимост за изпълнението на задача от обществен интерес или при упражняването на официални правомощия).

В някои изключителни случаи администраторът на данните може да използва като правно основание разпоредбата на член 6, параграф 1, буква а) (съгласие).

3.1 Законен интерес, член 6, параграф 1, буква е)

17. Правната оценка на член 6, параграф 1, буква е) следва да се основана на следните критерии в съответствие със съображение 47.

3.1.1 Наличие на законни интереси

18. Видеонаблюдението е законосъобразно, когато е необходимо за целите на законните интереси на администратора или на трета страна, освен когато пред такива интереси предимство имат интересите или основните права и свободи на субекта на данните (член 6, параграф 1, буква е)). Законните интереси на администратор или на трета страна могат да са правни[8], икономически или нематериални интереси.[9] Администраторът следва обаче да има предвид, че ако субектът

[6] Правилата за събиране на доказателства във връзка с граждански искове варират в отделните държави членки.

[7] Настоящите насоки не съдържат анализ или подробно описание на националното законодателство, което може да се различава в отделните държави членки.

[8] Съд на Европейския съюз, решение по дело C-13/16, *Rīgas satiksme*, 4 май 2017 г.

[9] вж. РД217, Работна група по член 29.

на данните възрази срещу видеонаблюдението на основание на член 21, администраторът може да предприеме такова видеонаблюдение на този субект на данни, ако е налице *неоспорим* законен интерес, който има предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

19. При наличие на реална и опасна ситуация целта за защита на имущество от обир с взлом, кражба или вандализъм може да представлява законен интерес за използване на видеонаблюдение.

20. Законният интерес трябва да е действителен и непосредствен (т.е. той не трябва да е теоретичен или предполагаем)[10]. За да бъде предприето видеонаблюдение, е необходимо да е налице реална ситуация на опасност, например, причинени в миналото вреди или възникнали сериозни инциденти. Във връзка с принципа на отчетност е препоръчително администраторите да документират съответните инциденти (дата, обстоятелства, финансови загуби) и свързаните с тях обвинения. Тези документирани инциденти могат да послужат като убедителни доказателства за наличието на законен интерес. Наличието на законен интерес, както и на необходимост от осъществяване на наблюдение следва да се подлага на периодична преоценка (например веднъж годишно, с оглед на обстоятелствата).

> Пример: Собственик на магазини желае да отвори нов магазин и да инсталира система за видеонаблюдение с цел предотвратяване на вандалски прояви. Той може да докаже със статистически данни, че в квартала съществува висока вероятност от вандализъм. Може да бъде приведен и опитът на съседните магазини. Не е необходимо въпросният администратор да е претърпял щети. Случаите на ощетяване на други търговци в квартала свидетелстват за наличие на опасност и могат да послужат за доказване на законен интерес. Не е достатъчно обаче да бъдат приведени национални или общи статистически данни за престъпността, без да е направен анализ на района, където е разположен магазинът, или на опасностите за този магазин.

21.

22. Ситуации на непосредствена опасност могат да оправдаят наличие на законен интерес: например банки или магазини, които продават ценни стоки (например бижутерийни магазини) или райони с повишени равнища на престъпления срещу собствеността (например срещу бензиностанции).

23. Освен това в ОРЗД ясно се посочва, че публични органи не могат да обосновават обработване на лични данни със законен интерес, когато изпълняват своите правомощия — член 6, параграф 1, второ изречение.

3.1.2 Необходимост на обработването

24. Личните данни следва да са подходящи, относими и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“), вж. член 5, параграф 1, буква в). Преди да предприеме инсталиране на система за видеонаблюдение, администраторът следва във всички случаи внимателно да анализира дали тази мярка е първо, подходяща за постигането на поставената цел и второ, адекватна, и необходима с оглед на неговите цели. Мерки за видеонаблюдение трябва да се предприемат единствено, ако целта на обработването

[10] Вж. РД217, Работна група по член 29, стр. 24 и сл. Вж. също Съд на Европейския съюз, решение по дело C-708/18, стр. 44.

не може да бъде постигната в достатъчна степен с други средства, които представляват по-малка намеса в основните права и свободи на субекта на данните.

25. С оглед на това, че администраторът на данни желае да предотврати престъпления срещу собствеността, а не да инсталира система за видеонаблюдение, той може да предприеме алтернативни мерки за сигурност като ограждане на имота, въвеждане на редовно патрулиране от служители по сигурността, назначаване на пазачи на входа, инсталиране на по-добро осветление, защитени ключалки, прозорци и врати или нанасяне на покритие или фолио срещу графити по стените. Тези мерки могат да бъдат не по-малко ефективни от системите за видеонаблюдение за предотвратяване на обири с взлом, кражби или вандализъм. Администраторът на данни трябва да оценява във всеки отделен случай дали подобни мерки са достатъчно ефективно решение.

26. Преди да започне да използва система от камери, администраторът е длъжен да оцени къде и в кои случаи мерките за видеонаблюдение са строго необходими. В повечето случаи система за видеонаблюдение, функционираща нощно време, както и извън обичайното работно време, ще удовлетвори нуждата на администратора да предотврати щети в своя имот.

27. По правило необходимостта от използване на видеонаблюдение за защита на имота на администратора на данни се ограничава в границите на имота.[11] Има обаче случаи, когато видеонаблюдението на имота не е достатъчно за осигуряване на ефективна защита. В отделни случаи може да се наложи видеонаблюдението да обхване и пространствата в непосредствено съседство с имота. В такива случаи администраторът следва да оцени необходимостта от физически и технически мерки, например блокиране или пикселизиране на зоните, където не се налага видеонаблюдение.

> Пример: Собственик на книжарница желае да защити имота от вандализъм. По правило камерите следва да заснемат само територията на имота, защото с оглед на преследваната цел не е необходимо да се наблюдават съседни имоти или обществени зони в близост до книжарницата.

28.

29. Въпроси, свързани с необходимостта от обработване на лични данни, възникват и по отношение на начина, по който се запазват доказателствата. В някои случаи се налага използване на решения от типа „черна кутия“, които осигуряват автоматично изтриване на видеозаписите след определен период на съхранение, а самите записи са достъпни само в случай на инцидент. В други случаи изобщо не е необходимо да се извършва видеозапис, а е достатъчно да се използва видеонаблюдение в реално време. Решението дали да се използва решение от типа „черна кутия“ или видеонаблюдение в реално време следва да се взема с оглед и на преследваната цел. Ако например целта на видеонаблюдението е запазване на доказателства, методите на наблюдение в реално време обикновено не са подходящи. В определени случаи наблюдението в реално време може да представлява по-голяма намеса от съхранението и автоматичното изтриване на видеозаписи след изтичане на определен срок (например- ако някой наблюдава постоянно монитора, наблюдението може да е по-голяма намеса в сравнение със ситуация, в която системата изобщо не е снабдена с монитор и видеозаписите се записват директно в черна кутия). Принципът на свеждане на данните до минимум трябва да се разглежда в този контекст

[11] Това може да е предмет на правно регулиране и от националното законодателство в някои държави членки.

(член 5, параграф 1, буква в)). Трябва също да се отчита обстоятелството, че администраторът на данни може да използва служители по сигурността вместо видеонаблюдение, тъй като служителите могат да реагират и да се намесват незабавно.

3.1.3 Търсене на баланс между интересите

30. В случаите, когато се приема, че видеонаблюдението е необходимо за защита на законните интереси на администратор на лични данни, въвеждане на система за видеонаблюдение се допуска само, когато пред законните интереси на администратора или на трета страна (например- защита на собствеността или на личната неприкосновеност) нямат предимство интересите или основните права и свободи на субекта на данните. Администраторът на данни трябва да вземе предвид: 1) в каква степен наблюдението засяга интересите, основните права и свободи на физически лица и 2) дали то нарушава или засяга отрицателно правата на субекта на данните. Всъщност постигането на баланс между интересите е задължително. Основните права и свободи от една страна и законните интереси на администратора на данни от друга страна трябва да бъдат внимателно оценени и балансирани.

> Пример: Дружество, което управлява частен паркинг за автомобили, документира трайни проблеми, свързани с кражби от паркираните автомобили. Паркингът е безпрепятствено достъпен за всички, но е ясно обозначен с табели и е ограден с устройства, препятстващи достъпа на автомобили. Дружеството, което управлява паркинга, има законен интерес (от предотвратяване на кражбите от автомобилите на своите клиенти) да извършва наблюдение в зоната на паркинга през тази част от денонощието, когато възникват проблеми. Субектите на данните се наблюдават за ограничено време, те не присъстват в зоната на наблюдение с цел развлечение, а освен това предотвратяването на кражби е и в техен интерес. В този случай законният интерес на администратора на данните има предимство пред интереса на субектите на данните да не бъдат наблюдавани.
>
> Пример: Управата на ресторант взема решение да инсталира видеокамери в тоалетните, за да контролира чистотата на тези санитарни помещения. В този случай правата на субектите на данните очевидно имат предимство пред интереса на администратора на данни, поради което не е допустимо инсталиране на камери в тези помещения.

31.

3.1.3.1 Вземане на решения индивидуално във всеки отделен случай

32. Тъй като съгласно Регламента постигането на баланс между интересите е задължително, решението трябва да се взема индивидуално във всеки отделен случай (вж. член 6, параграф 1, буква е)). Привеждането на теоретични ситуации или сравняването на сходни случаи не е достатъчно. Администраторът на данните трябва да оцени рисковете от намесата в правата на субектите на данните; в това отношение решаващият критерий е интензивността на намесата в правата и свободите на физическите лица.

33. Интензивността може да се определи наред с други начини с оглед на вида на събираната информация (съдържание на информацията), обхвата (плътност, пространствен и географски обхват на информацията), числеността на засегнатите субекти на данни, изразена като абсолютен брой или като дял от съответното население, конкретната ситуация, действителните интереси на групата субекти на данни, алтернативни способи, както и въз основа на характера и обхвата на оценката на данните.

34. Важни фактори за постигането на баланс между интересите са размерът на наблюдаваното пространство и броят на наблюдаваните субекти на данни. Използването на видеонаблюдение в отдалечена област (например- с цел наблюдение на диви животни или защита на критична инфраструктура, например частен радиопредавател) трябва да се оценява въз основа на различни критерии в сравнение с видеонаблюдението в пешеходна зона или в търговски център.

> Пример: Когато се използва камера в превозно средство с преден обзор (например с цел събиране на доказателства в случай на злополука), е важно да се гарантира, че камерата не записва постоянно пътното движение, както и физическите лица, които се намират в близост до пътя. В противен случай интересът от наличието на видеозаписи като доказателства в по-теоретичния случай на пътна злополука не може да оправдае сериозната намеса в правата на субектите на данните.[11]

35.

3.1.3.2 Разумни очаквания на субектите на данните

36. Съгласно съображение 47 за установяването на законен интерес е необходима внимателна оценка. Тук трябва да се включат разумните очаквания на субекта на данните към момента и във връзка с обработването на неговите лични данни. По отношение на систематичното наблюдение отношенията между субекта и администратора на данните могат да се различават в значителна степен и да обусловят разумните очаквания на субекта на данните. Тълкуването на концепцията за разумните очаквания не следва да се основава само на въпросните субективни очаквания. Вместо това решаващият критерий трябва да е обстоятелството дали обективна трета страна може разумно да очаква и да заключи, че е обект на наблюдение в конкретната ситуация.

37. Например, в повечето случаи служител не очаква, че е обект на наблюдение на своето работно място от своя работодател.[12] Освен това, физическо лице не следва да очаква, че е обект на наблюдение в своята градина, в дома си или в помещения за медицински прегледи и лечение. Аналогично не следва разумно да се очаква извършване на наблюдение в санитарни помещения или сауни — извършването на наблюдение в такива помещения представлява интензивна намеса в правата на субекта на данните. Разумните очаквания на субектите на данните са, че на такива места не се извършва видеонаблюдение. От друга страна клиент на банка може да очаква, че е обект на наблюдение в помещенията на банката или когато ползва терминално устройство АТМ.

38. Субектите на данните могат да очакват, че не са обект на наблюдение на обществени места и особено на места, които обичайно се използват за почивка, възстановяване и дейности в свободното време, както и на места, където физически лица прекарват времето си и/или общуват, като места за почивка, маси в ресторанти, паркове, кина и зали за фитнес. В такива места интересите или свободите на субектите на данни често имат предимство пред законните интереси на администратора на данни.

> Пример: Субектите на данните очакват, че не са подложени на наблюдение в тоалетни помещения. В такива помещения видеонаблюдение, предприето например с цел предотвратяване на злополуки, не е пропорционална мярка.

39.

[12] Вж. също: Работна група по член 29, Становище № 2/2017 относно обработването на данни на работното място, РД249, прието на 8 юни 2017 г.

40. Наличието на информационни табели, които уведомяват субекта на данните, че се извършва видеонаблюдение, не е от значение за определянето на обективните очаквания на субекта на данните. Това означава, че например собственик на магазин не може да се позовава на обстоятелството, че клиентите *обективно* имат разумни очаквания, че ще бъдат подложени на наблюдение, само защото на входа е поставена табела, която уведомява физическите лица, че се извършва видеонаблюдение.

3.2 Необходимост от изпълнение на задача, която се осъществява в обществен интерес или при упражняване на официалните правомощия, които са предоставени на администратора, член 6, параграф 1, буква д)

41. Обработване на лични данни посредством видеонаблюдение се допуска съгласно член 6, параграф 1, буква д), когато е налице необходимост от изпълнението на задача от обществен интерес или при упражняването на официални правомощия.[13] Възможни са случаи, когато упражняването на официални правомощия не е основание за такова обработване, но наличието на други правни основания като „здраве и безопасност“ във връзка със защитата на посетителите и служителите може да даде ограничено основание за обработване при същевременно зачитане на задълженията съгласно ОРЗД и правата на субектите на данните.

42. Държавите членки могат да прилагат или въвеждат специално национално законодателство за видеонаблюдение, за да адаптират прилагането на правилата на ОРЗД, като определят по-конкретни изисквания за обработване, които трябва да отговарят на принципите, залегнали в ОРЗД (например за ограничение на съхранението или за пропорционалност).

3.3 Съгласие, член 6, параграф 1, буква а)

43. Съгласието трябва да е дадено свободно, да е конкретно, информирано и недвусмислено, както е описано в насоките относно съгласието.[14]

44. Що се отнася до систематичното наблюдение, съгласието на субекта на данните може да послужи като правно основание в съответствие с член 7 (вж. съображение 43) само в изключителни случаи. Същността на наблюдението предполага, че тази технология осъществява наблюдение едновременно върху неопределен брой хора. По правило администраторът на данните трудно може да докаже, че субектът на данните е дал своето съгласие преди обработването на неговите лични данни (член 7, параграф 1). В случай, че субектът на данните е оттеглил съгласието си, за администратора ще е трудно да докаже, че личните данни вече не се обработват (член 7, параграф 3).

[13] Използваното правно основание за обработване трябва да е предвидено в законодателството на Съюза или държавата членка и обработването трябва да е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора (член 6, параграф 3).

[14] Работна група по член 29, „Насоки относно съгласието в съответствие с Регламент 2016/679“ (РД 259 rev. 01). - одобрени от Европейския комитет по защита на данните

Пример: Спортисти могат да поискат осъществяване на видеонаблюдение по време на техните тренировки, за да анализират своята техника и резултати. От друга страна, когато спортен клуб осъществява по своя инициатива наблюдение на цял отбор със същата цел, в много случаи съгласието няма да е валидно, тъй като отделните спортисти може да считат, че са под натиск да дадат съгласието си, така че техният отказ да не се отрази неблагоприятно върху техните съотборници.

45.

46. Когато администраторът на данни желае да се позове на дадено съгласие, той е длъжен да се увери, че всеки субект на данни, който влиза в зоната, която е под видеонаблюдение, е дал своето съгласие. Това съгласие трябва да отговаря на условията по член 7. Влизането в обозначена наблюдавана зона (например, когато хора са приканвани да преминат през определен коридор или вход, за да влязат в наблюдавана зона), не се счита за изразено съгласие или ясно потвърждаващо действие, което изразява съгласие, освен ако отговаря на критериите, посочени в членове 4 и 7, както е посочено в насоките относно съгласието.[15]

47. С оглед на неравнопоставеността между работодателите и служителите в повечето случаи работодателите не следва да се позовават на дадено съгласие, когато извършват обработване на лични данни, тъй като е малко вероятно подобно съгласие да е свободно дадено. Във връзка с това следва да се вземат предвид насоките относно съгласието.

48. В законодателството на държавите членки или в колективни споразумения, включително „трудови споразумения“, може да са предвидени специфични правила за обработване на лични данни на служителите в контекста на трудовите правоотношения (вж. член 88).

[15] Работна група по член 29, „Насоки относно съгласието в съответствие с Регламент 2016/679“ (РД 259) — одобрени от Европейския комитет по защита на данните, които следва да бъдат взети предвид.

4 РАЗКРИВАНЕ НА ВИДЕОЗАПИСИ ПРЕД ТРЕТИ СТРАНИ

49. По принцип общите разпоредби на ОРЗД се прилагат към предаването на видеозаписи на трети страни.

4.1 Общи положения относно разкриването на видеозаписи пред трети страни

50. Разкриването е определено в член 4, параграф 2 като предаване (например- индивидуална комуникация), разпространяване (например- публикуване онлайн) или друг начин, по който данните стават достъпни. Третите страни са определени в член 4, параграф 10. Когато данните са разкрити пред трети държави или международни организации, се прилагат и специалните разпоредби на член 44 и следващи.

51. Всяко разкриване на лични данни е отделен вид обработване на лични данни, за което администраторът трябва да има правно основание съгласно член 6.

> Пример: Администратор на данни, който желае да публикува видеозапис в интернет, трябва да има правно основание за такова обработване, например като получи съгласието на субекта на данните в съответствие с член 6, параграф 1, буква а).

52.

53. Съгласно член 6, параграф 4 се допуска предаване на видеозаписи на трети страни за цели, различни от тези, за които данните са били събрани.

> Пример: Около бариера на паркинг е инсталирана система за видеонаблюдение с цел документиране на обстоятелствата, при които са причинени щети. Нанесени са щети и видеозаписът е предаден на адвокат, който е натоварен да заведе дело. В този случай целта на видеозаписа не се различава от целта на предаването.
>
> Пример: Около бариера на паркинг е инсталирана система за видеонаблюдение с цел документиране на обстоятелствата, при които са причинени щети. Видеозаписът е публикуван онлайн единствено с развлекателна цел. В този случай целта е променена и не е съвместима с първоначалната цел. Следователно трудно ще се намери правно основание за това обработване (публикуване).

54.

55. Третата страна получател трябва да извърши собствен правен анализ, по-конкретно, с цел да определи приложимото правно основание съгласно член 6 за обработването (например- получаване на материала).

4.2 Разкриване на видеозаписи пред правоприлагащи органи

56. Разкриването на видеозаписи пред правоприлагащи органи също е независим процес, за който изисква отделна обосновка от администратора на данните.

57. В съответствие с член 6, параграф 1, буква в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора. Въпреки че приложимото законодателство относно правомощия на полицейските органи е въпрос, който е от изключителната компетентност на държавите членки, най-вероятно съществуват общи правила, които регламентират предаването на доказателства на правоприлагащите органи във всяка държава членка. Обработването, изразяващо се в предаване на данните от страна на администратора, е предмет на правно регулиране от ОРЗД. Когато националното законодателство задължава администратора на данните да сътрудничи с правоприлагащите

органи (например във връзка с провеждано разследване), правното основание за предаването на данните е нормативно установено задължение съгласно член 6, параграф 1, буква в).

58. Във връзка с това предвиденото в член 6, параграф 4 ограничение на целите в много случаи не поражда затруднения, тъй като разкриването е изрично уредено от законодателството на държавата членка. С оглед на горното не е необходима преценка на специалните изисквания за промяна на целта, предвидени в букви а)—д).

59. Пример: Собственик на магазин прави видеозапис на пространството около входа на магазина. На видеозаписа е документирана кражба от физическо лице на портфейла на друго лице. Служителите на полицията изискват от администратора на данните да предаде видеозаписа в интерес на разследването. В този случай собственикът на магазина може да се позове на правното основание съгласно член 6, параграф 1, буква в) (правно задължение) във връзка с приложимите правила на националното законодателство относно обработването на данни чрез предаване.

60. Пример: Видеокамера е инсталирана в магазин с цел, свързана със сигурността. Собственикът на магазина смята, че е записал нещо подозрително и решава да изпрати видеозаписа в полицията (без да разполага с информация за текущо разследване). В този случай собственикът на магазина следва да прецени дали условията, предвидени в член 6, параграф 1, буква е), са изпълнени. Обикновено това е така, когато собственик на магазина има достатъчни основания да се съмнява, че е извършено престъпление.

61. Обработването на лични данни от правоприлагащите органи се извършва не по правилата на ОРЗД (вж. член 2, параграф 2, буква г)), а по правилата на Директивата относно правоприлагането ((ЕС) 2016/680).

5 ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ДАННИ

62. Системите за видеонаблюдение обикновено събират големи обеми данни, които могат да разкрият информация с подчертано личен характер, и дори специални категории данни. Трябва да се подчертае, че на пръв поглед събрани чрез видеонаблюдение данни без особено значение могат да се използват за получаване на друга информация за постигане на различни цели (например за анализ на навиците на физическо лице). Въпреки това, видеонаблюдението не във всички случаи се счита за обработване на специални категории лични данни.

> Пример: Видеозаписи, които изобразяват субект на данни, който носи очила или използва инвалидна количка, не се считат за специални категории лични данни.

63.

64. Ако обаче видеозаписите бъдат обработени с цел получаване на данни от специални категории, се прилага член 9.

> Пример: Например възможно е да бъдат определени политически възгледи въз основа на изображения на подлежащи на идентифициране субекти на данни, които участват в събития, стачки и т.н. Този случай попада в обхвата на член 9.
>
> Пример: Когато болница инсталира видеокамера, за да наблюдава здравословното състояние на пациент, се приема, че тя обработва специални категории лични данни (член 9).

65.

66. Като общ принцип винаги, когато се инсталира система за видеонаблюдение, следва внимателно да се отчита принципът на свеждане на данните до минимум. Следователно, дори в случаите, когато не се прилага разпоредбата на член 9, параграф 1, администраторът на данните следва във всички случаи да полага усилия за свеждане до минимум на риска от изготвяне на видеозаписи, които документират други чувствителни данни (извън обхвата на член 9), независимо от целта.

> Пример: Видеонаблюдение в църква не попада като такова в обхвата на член 9. Администраторът на данните обаче следва да прецени особено внимателно критериите по член 6, параграф 1, буква е), отчитайки характера на данните, както и риска от документиране на други чувствителни данни (извън обхвата на член 9), когато оценява интересите на субекта на данните.

67.

68. Когато система за видеонаблюдение се използва за обработване на специални категории данни, администраторът на данните трябва да определи както изключение за обработване на специални категории данни по член 9 (например изключение от общото правило за недопустимост на обработването на специални категории данни), така и правно основание по член 6.

69. Например разпоредбата на член 9, параграф 2, буква в) („[…] *обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице*[…]“) може да се използва, на теория и по изключение, но администраторът на данните би трябвало да обоснове прилагането ѝ с абсолютна необходимост за опазването на жизненоважни интереси на лице и да докаже, че този „[…] субект на данни *е физически или*

юридически неспособен да даде своето съгласие.“. Наред с горното администраторът на данните не може да използва системата за никаква друга цел.

70. Във връзка с това е важно да се отбележи, че което и да е изключение по член 9 най-вероятно няма да може да се използва за обосноваване на обработване на специални категории данни посредством видеонаблюдение. По-конкретно, администраторите на данни, които обработват тези данни в контекста на видеонаблюдение, не могат да се позовават на разпоредбата на член 9, параграф 2, буква д), която допуска обработване, свързано с лични данни, които са направени по явен начин обществено достояние от субекта на данните. Самият факт на влизането в зоната, наблюдавана от видеокамера, не означава, че субектът на данните има намерение да направи публично достояние специални категории данни, свързани с него или нея.

71. Освен това обработването на специални категории данни изисква повишена и постоянна бдителност за изпълнението на определени задължения, например осигуряване на високо ниво на сигурност и извършване на оценка на въздействието върху защитата на данните, когато е необходимо.

> Пример: Работодател не може да използва записи от видеонаблюдение на демонстрация, за да идентифицира стачниците.

72.

5.1 Общи съображения във връзка с обработването на биометрични данни

73. Използването на биометрични данни и по-конкретно на разпознаване на лица е свързано с повишени рискове за правата на субектите на данните. От решаващо значение е използването на такива технологии да се предприема при надлежно зачитане на залегналите в ОРЗД принципи на законосъобразност, необходимост, пропорционалност и свеждане на данните до минимум. Макар че използването на такива технологии може да се разглежда като особено ефективно, администраторите на данните следва преди всичко да оценят въздействието върху основните права и свободи, и да преценят възможностите за използване на алтернативи средства за постигане на законната цел на обработването, които представляват по-малка намеса.

74. За да отговаря на критериите за биометрични данни съгласно определението в ОРЗД, дейността по обработване на необработени данни като физически, физиологични или поведенчески характеристики на дадено физическо лице трябва да включва измерване на тези характеристики. Тъй като биометричните данни се получават в резултат на такива измервания, в член 4, параграф 14 от ОРЗД е предвидено, че те са *„[…] получени в резултат на специфично техническо обработване във връзка с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице […]“.* Видеозапис на физическо лице не може обаче да се счита сам по себе си за биометрични данни по смисъла на член 9, ако той не е

бил подложен на специфична техническа обработка, за да може да допринесе за идентифицирането на това лице. [16]

75. За да се счита обработването на биометрични данни за обработване на специални категории лични данни (по член 9), тези биометрични данни трябва да се обработват „с цел уникално идентифициране на физическо лице“.

76. В обобщение, с оглед на текста на член 4, параграф 14 и член 9 трябва да бъдат отчетени три критерия:

- **характер на данните:** данни, свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице,
- **средства и начин на обработване**: данни, „получени в резултат на специфично техническо обработване“,
- **цел на обработването:** данните трябва да се използват с цел уникално идентифициране на физическо лице.

77. Използването на видеонаблюдение, включващо функция за биометрично разпознаване, което е инсталирано от частни лица за техните цели (например- маркетинг, риск на статистически данни или дори сигурност), в повечето случаи изисква изричното съгласие на всички субекти на данни (член 9, параграф 2, буква а)), макар че може да се прилага и друго подходящо изключение от правилата на член 9.

[16] Текстът на съображение 51 към ОРЗД подкрепя този анализ, като посочва, че *„[…] обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице. […]*“.

Пример: За да подобри предлаганите от него услуги, частно дружество заменя пунктовете за идентифициране на пътниците на летище (чекиране на багаж, проверка преди качване на борда) със системи за видеонаблюдение, които използват техники за разпознаване на лица, за да удостоверят самоличността на пътниците, които са дали съгласието си за такава процедура. Тъй като обработването попада в обхвата на член 9, пътниците, които са дали своето изрично и информирано съгласие, трябва да се явят например пред автоматичен терминал, за да създадат и регистрират модел на своето лице, свързан с тяхната бордна карта и самоличност. Пунктовете за проверка, оборудвани с технология за разпознаване на лица, трябва да бъдат ефективно отделени, т.е. системата трябва да бъде инсталирана във визуално оградено място, така че да е невъзможно заснемането на биометрични модели на физическите лица, които не са дали своето съгласие за това. Само пътниците, които са дали предварително своето съгласие и са регистрирали лицевите си изображения, могат да използват портала, оборудван с биометричната система.

Пример: Администратор на данни контролира достъпа до своята сграда с помощта на технология за разпознаване на лица. Хората могат да използват тази технология за достъп, само ако са дали предварително своето изрично и информирано съгласие (съгласно член 9, параграф 2, буква а)). За да бъде гарантирано обаче, че никое лице, което не е дало предварително своето съгласие, няма да бъде заснето, технологията за разпознаване на лица следва да бъде стартирана от субекта на данните, например, посредством натискане на бутон. За да бъде осигурена законосъобразността на обработването, администраторът на данните трябва във всички случаи да предлага алтернативен способ за достъп до сградата, който не включва обработване на биометрични данни, например използване на баджове или ключове.

78.

79. В подобни случаи, когато се генерират биометрични модели, администраторите на данните трябва да гарантират, че след получаването на резултат, изразяващ се в съвпадение или несъвпадение, всички междинни модели, създадени в движение (с изричното и информирано съгласие на субекта на данните), с цел да бъдат сравнени с моделите, създадени от субектите на данните в момента на регистрацията в системата, се изтриват незабавно и необратимо. Моделите, създадени за регистрацията в системата, следва да се запазват за изпълнението на целта на обработването и не следва да се съхраняват или архивират.

80. Когато обаче целта на обработването е например да се разграничи една категория хора от друга, но не и да се извършва уникално идентифициране на отделни лица, обработването не попада в обхвата на член 9.

Пример: Собственик на магазин желае да индивидуализира своята реклама въз основа на характеристики като пола и възрастта на клиентите, които са документирани от система за видеонаблюдение. Ако тази система не генерира биометрични модели, за да осъществи уникално идентифициране на физическите лица, а само регистрира тези физически характеристики, за да категоризира лицата, обработването няма да попада в обхвата на член 9 (доколкото не се обработват други специални категории данни).

81.

82. Разпоредбата на член 9 се прилага обаче, когато администраторът съхранява биометрични данни (обикновено посредством модели, които се генерират чрез извличане на ключови характеристики от необработените биометрични данни (например- измерване на характеристики на лицата въз основа на изображение)), с цел уникално идентифициране на

физическо лице. Когато администратор на данни желае да установи повторно влизане на субект на данни в зоната под наблюдение или в друга зона (например с цел излъчване на продължаваща индивидуализирана реклама), целта би била уникално идентифициране на физическо лице, което означава, че от самото начало операцията попада в обхвата на член 9. Такъв би бил случаят, когато администратор на данни съхранява генерирани модели с цел изготвяне на допълнителни индивидуализирани реклами на няколко билборда, разположени на различни места в магазин. Тъй като системата използва физически характеристики, за да установи конкретни физически лица, които навлизат повторно в обхвата на камерата (например посетители на търговски център) и да ги проследява, се използва технология за биометрично идентифициране, тъй като целта е разпознаване посредством специфично техническо обработване.

Пример: Собственик на магазин е инсталирал система за разпознаване на лица в своя магазин, за да излъчва индивидуализирани реклами за определени физически лица. Администраторът на данните трябва да получи изричното и информирано съгласие на всички субекти на данни, преди да използва тази биометрична система и да излъчи индивидуализираните реклами. Системата ще бъде незаконосъобразна, ако заснема посетители на магазина или минувачи, които не са дали съгласието си за създаване на техни биометрични модели, дори ако техният модел се изтрива във възможно най-кратък срок. Тези временни модели представляват по съществото си биометрични данни, обработвани с цел уникално идентифициране на физически лица, които може да не желаят да получават индивидуално насочена реклама.

83.

84. Европейският комитет по защита на данните отбелязва, че някои биометрични системи са инсталирани в неконтролирана среда[17], което означава, че системата заснема в движение лицата на всички физически лица, които влизат в обхвата на камерата, включително лицата, които не са дали съгласието си за използване на биометричното устройство, и по този начин създава биометрични модели. Тези модели се сравняват с моделите, създадени за субект на данни, които са дали своето предварително съгласие по време на процеса на регистрация (например потребители на биометрични устройства), за да може администраторът на данните да установи дали съответното лице е потребител на биометричната технология. В подобни случаи често системата е настроена да разграничава физическите лица, които трябва да разпознава въз основа на база данни, от лицата, които не са регистрирани. Тъй като целта е уникално идентифициране на физически лица и в този случай е необходимо изключение от разпоредбата на член 9, параграф 2 от ОРЗД за всички лица, заснети от камерата.

[17] Това означава, че биометричното устройство е инсталирано в пространство с обществен достъп и може да регистрира всички лица, които преминават през неговия обсег, за разлика от биометричните системи, функциониращи в контролирана среда, които могат да се използват само с участието на лицата, които са дали съгласието си за това.

Пример: Хотел използва видеонаблюдение за автоматично сигнализиране на управителя на хотела за пристигането на важен гост в резултат на разпознаване на лицето на госта. Тези важни гости са дали предварително своето изрично съгласие за използването на технология за разпознаване на лица, преди да бъдат регистрирани в база данни, създадена за тази цел. Такива системи за обработване на биометрични данни биха били незаконосъобразни, освен ако всички останали гости, които са обект на наблюдение (с цел идентифицирането на важните гости) са дали съгласието си за обработването в съответствие с член 9, параграф 2, буква а) от ОРЗД.

Пример: Администратор на данни инсталира система за видеонаблюдение с функция за разпознаване на лица на входа на концертната зала, която управлява. Администраторът трябва да изгради ефективно разделени входове, единият от които е оборудван с биометричната система, а другият не е оборудван с такава система (където посетителите например сканират билетите си). Входовете, оборудвани с биометрични устройства, трябва да са оформени и достъпни по такъв начин, че системата да не може да заснема биометрични модели на зрителите, които не са дали съгласието си за това.

85.

86. И накрая, в случаите, когато съгласно член 9 от ОРЗД се изисква съгласие, администраторът на данните не може да предоставя своите услуги единствено под условие за изразяване на съгласие с обработването на биометрични данни. Казано по друг начин, особено в случаите, когато се използва обработване на биометрични данни с цел идентифициране на физически лица, администраторът на данните трябва да предлага алтернативно решение, което не включва обработване на биометрични данни, без ограничения или допълнителни разходи за субектите на данните. Такова алтернативно решение е необходимо и за лица, които не отговарят на ограниченията, характерни за биометричното устройство (невъзможност за регистрация или разчитане на биометричните данни, наличие на увреждане, което затруднява използването на устройството и др.), както и с оглед на възможно излизане от строя на биометричното устройство (например поради повреда), като с оглед на тези случаи трябва да бъде въведено в експлоатация „резервно решение“, с цел да се осигури непрекъснатостта на предлагането на услугите, което трябва да се използва само в изключителни случаи. В изключителни случаи са възможни ситуации, когато обработването на биометрични данни е основна дейност в рамките на услуги, предоставяни по договор, например музей, който урежда изложба, демонстрираща използването на устройство за разпознаване на лица. В този случай, субектът на данните няма възможност да откаже обработването на биометрични данни, ако желае да участва в изложбата. В такива случаи, съгласието, което се изисква съгласно член 9, е валидно, ако са изпълнени изискванията по член 7.

5.2 Подходящи мерки за свеждане до минимум на рисковете при обработване на биометрични данни

87. В съответствие с принципа за свеждане на данните до минимум администраторите на данни трябва да гарантират, че данните, извлечени от цифрово изображение с цел изграждане на модел, не надхвърлят необходимото и съдържат само информацията, необходима за посочената цел, с което се предотвратява възможно по-нататъшно обработване. Следва да бъдат въведени мерки, чрез които да се гарантира, че моделите не могат да се прехвърлят от една биометрична система в друга.

88. За целите на идентифицирането и удостоверяването/ проверката на самоличността на физически лица обикновено е необходимо съхраняване на моделите, с цел да бъдат използвани за последващо сравнение. Администраторът на данните трябва да прецени кое е най-подходящото място за съхранение на данните. В контролирана среда (обозначени коридори или пунктове за проверка) моделите се съхраняват на отделно устройство, което се пази от потребителя и е под негов изключителен контрол (смартфон или карта за самоличност) или, когато е необходимо за специфични цели, и при обективна необходимост, моделите се съхраняват в криптирана форма, ключът за която е достъпен единствено за лицето с цел предотвратяване на неразрешен достъп до модела или мястото, където се съхранява той. Когато администраторът на данните по необходимост има достъп до моделите, той трябва да предприеме подходящи стъпки за гарантиране на сигурността на съхраняваните данни. Това може да включва криптиране на моделите с помощта на криптографски алгоритъм.

89. Във всички случаи администраторът предприема всички необходими мерки, за да осигури наличността, целостта и поверителността на обработваните данни. По-конкретно за тази цел администраторът предприема следните мерки: разделяне на данните при тяхното предаване и съхранение, съхранение на биометрични модели и необработени данни или данни за самоличност в отделни бази данни, криптиране на биометричните данни, и по-специално на биометричните модели, определяне на политика за криптиране и управление на ключовете, интегриране на организационни и технически мерки за разкриване на измами, изготвяне на код за цялост на данните (например подпис или хеш функция), които забраняват всякакъв външен достъп до биометричните данни. Тези мерки следва да се развиват успоредно с развитието на технологиите.

90. Наред с горното, администраторите на данни следва да изтриват необработените данни (изображения на лица, реч, походка и т.н.) и да осигурят ефективността на това изтриване. Когато вече няма правно основание за обработването, необработените данни се изтриват. Доколкото биометричните модели са генерирани въз основа на такива данни, може да се счита, че създаването на бази данни представлява не по-малка или дори по-голяма заплаха (тъй като не във всички случаи е лесно да се разчете биометричен модел без познаване на начина на неговото програмиране, докато необработените данни са градивните елементи на всеки модел). В случаите, когато се налага администраторът на данните да съхранява тези данни, трябва да се проучи възможността за прилагане на методи за добавяне на шум (например водни знаци), с което създаването на модела ще стане неефективно. Освен това, администраторът на данните трябва да изтрие биометричните данни и модели в случай на неразрешен достъп до терминала за четене, и сравнение или сървъра за съхранение на данните, както и да изтрие всички данни, които не са приложими за по-нататъшното обработване в края на жизнения цикъл на биометричното устройство.

6 ПРАВА НА СУБЕКТА НА ДАННИ

91. С оглед на характера на обработването на данни във връзка с видеонаблюдението някои права на субекта на данните съгласно ОРЗД се нуждаят от допълнително изясняване. Тази глава обаче не е изчерпателна, като всички права съгласно ОРЗД се прилагат към обработването на лични данни посредством видеонаблюдение.

6.1 Право на достъп

92. Субектът на данните има право да получи от администратора на данните потвърждение дали се обработват негови или нейни лични данни. По отношение на видеонаблюдението това означава, че когато под никаква форма не се осъществява съхранение или предаване на данни, след провеждането на наблюдението в реално време, администраторът може да предостави единствено информацията, че вече не се обработват никакви лични данни (в допълнение към общите изисквания за предоставяне на информация съгласно член 13, вж. *раздел 7, Задължения по отношение на прозрачността и информацията*). Ако обаче в момента на запитването все още се извършва обработване на данни (т.е. ако данните се съхраняват или обработват текущо по друг начин), субектът на данните следва да получи достъп и информация в съответствие с член 15.

93. Предвидени са обаче редица ограничения, които в някои случаи се прилагат по отношение на правото на достъп.

- член 15, параграф 4 от ОРЗД, неблагоприятно въздействие върху правата на други лица

94. Предвид обстоятелството, че при видеозапис е възможно да бъдат заснети произволен брой субекти на данни, преглеждането ще бъде свързано с допълнително обработване на лични данни на други субекти на данни. Ако субектът на данните желае да получи копие от записа ((член 15, параграф 3)), това може да засегне неблагоприятно правата и свободите на други лица, заснети на записа. За да не допусне този резултат, администраторът на данните следва да отчита, че с оглед на обстоятелството, че видеозаписите представляват намеса в права, в някои случаи, той не следва да предава видеозаписи, в които е възможно да бъдат идентифицирани други субекти на данни. Защитата на правата на трети страни обаче не следва да се използва като претекст за възпрепятстване на законни искания за достъп от физически лица, като в такива случаи администраторът трябва да предприеме технически мерки за удовлетворяване на исканията за достъп (например посредством редактиране на изображенията като покриване или замъгляване). Администраторите обаче не са длъжни да изпълняват такива технически мерки, ако могат да осигурят по друг начин изпълнението на искане по член 15 в срока, предвиден в член 12, параграф 3.

- Член 11, параграф 2 от ОРЗД, администраторът не е в състояние да идентифицира субекта на данните

95. Ако видеозаписът не позволява търсене на лични данни (което означава, че администраторът трябва да прегледа голям обем съхранявани записи, за да намери съответния субект на данни), може да се приеме, че администраторът не е в състояние да идентифицира субекта на данните.

96. По тези причини субектът на данните следва (освен изискването да се идентифицира, включително с помощта на документ за самоличност или лично) да посочи в своето искане до администратора кога, в рамките на разумен период с оглед на общия брой на заснетите субекти на данни, е влизал в наблюдаваната зона. Администраторът е длъжен да уведоми субекта на данните от каква информация се нуждае, за да може да изпълни искането му. Ако администраторът на данните може да докаже, че не е в състояние да идентифицира субекта на данни, администраторът уведомява съответно субекта на данни, ако това е възможно. В такива случаи в своя отговор до физическото лице администраторът следва да му предостави информация за точната зона на видеонаблюдение, камерите, които са се използвали, и т.н., така че субектът на данните да разбира правилно какви негови лични данни може да са обработени.

> Пример: Когато субект на данни иска копие от своите лични данни, които са обработени посредством видеонаблюдение на входа на търговски център, който се посещава от 30 000 души на ден, той следва да посочи кога е преминал през наблюдаваната зона в рамките на приблизително един час. Ако администраторът все още съхранява записите, трябва да предостави копие от тях. Ако записите позволяват да бъдат идентифицирани други субекти на данни, съответната част от тях следва да бъде анонимизирана (например посредством замъгляване на копието или на част от него), преди то да бъде предоставено на физическото лице, което е подало искането.
>
> Пример: Ако администраторът на данните изтрива автоматично всички видеозаписи, например в срок от 2 дни, той не е в състояние да предостави видеозапис на субекта на данните след изтичането на тези 2 дни. Ако администраторът получи искане след изтичането на този двудневен срок, субектът на данните следва да бъде уведомен.

97.

- Член 12 от ОРЗД, прекомерни искания

98. В случай на прекомерни или явно неоснователни искания, подадени от субект на данни, администраторът на данните може да наложи разумна такса в съответствие с член 12, параграф 5, буква а) от ОРЗД или да откаже да изпълни искането (член 12, параграф 5, буква б) от ОРЗД). Администраторът трябва да може да докаже явно неоснователния или прекомерен характер на искането.

6.2 Право на изтриване и право на възражение

6.2.1 Право на изтриване (Право „да бъдеш забравен“)

99. Ако администраторът продължава да обработва лични данни след извършването на наблюдението в реално време (например съхранява данните), субектът на данните може да поиска личните данни да бъдат изтрити в съответствие с член 17 от ОРЗД.

100. При съответно искане, администраторът на данните е длъжен да изтрие личните данни без необосновано забавяне, когато е налице някое от обстоятелствата, описани в член 17, параграф 1 от ОРЗД (и не се прилага никое от изключенията, изброени в член 17, параграф 3 от ОРЗД). Това включва задължението за изтриване на лични данни, когато те вече не са необходими за целта, за която са били първоначално съхранени, или когато обработването и незаконосъобразно (вж. също *Раздел 8: Срокове на съхранение и задължение за изтриване*). Освен в горните случаи, в зависимост от правното основание за обработването, личните данни следва да бъдат изтрити:

- *при дадено съгласие:* винаги, когато съгласието е оттеглено (и липсва друго правно основание за обработването),
- в случаи на *законен интерес*:
    - винаги, когато субектът на данните упражнява правото си на възражение (вж. *раздел 6.2.2*) и липсват убедителни законови основания за обработването, или
    - в случаи на директен маркетинг (включително профилиране) винаги, когато субектът на данните възразява срещу обработването.

101. Ако администраторът е направил видеозаписите публично достояние (например- те са били излъчени или са достъпни онлайн), е необходимо да бъдат предприети разумни стъпки за уведомяване на други администратори (които притежават съответните лични данни) за искането по член 17, параграф 2 от ОРЗД. Разумните стъпки следва да включват технически мерки при отчитане на наличните технологии и разходите за изпълнението. Доколкото е възможно, администраторът трябва да уведоми след изтриването на личните данни всички лица, на които са били разкрити тези лични данни, в съответствие с член 19 от ОРЗД.

102. Освен задължението на администратора да изтрие личните данни в отговор на искане от субекта на данните, администраторът е длъжен съгласно общите принципи на ОРЗД да ограничи съхраняваните лични данни (вж. *раздел 8*).

103. По отношение на случаите на видеонаблюдение следва да се отбележи, че например посредством замъгляване на картината без възможност за последващо възстановяване на личните данни, които са се съдържали в нея, личните данни се считат за изтрити в съответствие с ОРЗД.

> Пример: Малък магазин за хранителни продукти има проблеми, свързани с вандализъм, най-вече пред витрините и поради това използва система за видеонаблюдение пред входа, която е монтирана на стените. Минувач иска неговите лични данни да бъдат изтрити незабавно. Администраторът на данните е длъжен да удовлетвори искането без ненужно забавяне и най-късно в рамките на един месец. Тъй като видеозаписът, който е предмет на искането, вече не отговаря на целта, за която е първоначално съхранен (по време на присъствието на минувача не са извършени вандалски прояви), към момента на подаване на искането липсва законен интерес от съхранение на данните, който да има предимство пред интересите не субектите на данните. Администраторът трябва да изтрие личните данни.

104.

6.2.2 Право на възражение

105. В случаи на видеонаблюдение на основание на *законен интерес* (член 6, параграф 1, буква е) от ОРЗД) или в случаи на необходимост за изпълнение на задача от *обществен интерес* (член 6, параграф 1, буква д) от ОРЗД) субектът на данните има право, по всяко време и на основания, свързани с конкретната ситуация, на възражение срещу обработването в съответствие с член 21 от ОРЗД. В такъв случай, администраторът прекратява обработването на личните данни на лицето, подало възражението, освен ако докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред правата и интересите на субекта на данните. Администраторът на данните е длъжен да удовлетвори искането на субекта на данните без ненужно забавяне и най-късно в рамките на един месец.

106. В случаи на видеонаблюдение това възражение може да бъде отправено при влизане или престой в наблюдаваната зона или след излизането от нея. На практика това означава, че ако администраторът няма убедителни законови основания за обработването, наблюдението на зона, в която е възможно да бъдат идентифицирани физически лица, е законосъобразно, само ако

    (1) администраторът на данните може да изключи камерата незабавно в отговор на искане, с което да прекрати обработването на личните данни, или

    (2) наблюдаваната зона е ограничена по такъв начин, че администраторът може да получи одобрението на субекта на данните, преди последният да влезе в тази зона, и тя не е зона, до която субектът на данните има като гражданин право на достъп.

107. Настоящите насоки нямат за цел да определят понятието *убедителен* законов интерес (член 21 от ОРЗД).

108. В случаи, когато се използва видеонаблюдение за целите на директен маркетинг, субектът на данните има право на възражение срещу обработването по своя преценка, тъй като при това положение правото на възражение е абсолютно (член 21, параграфи 2 и 3 от ОРЗД).

> Пример: Дружество изпитва проблеми, свързани с нарушения на сигурността около входа за посетители и използва видеонаблюдение на основание на законен интерес, с цел да залови лицата, които влизат незаконно в имота. Посетител възразява срещу обработването на личните му данни чрез системата за видеонаблюдение на основания, свързани с конкретната му ситуация. В този случай обаче дружеството отхвърля искането с обяснението, че съхраняваният видеозапис е необходим за целите на активно вътрешно разследване, което означава, че има убедителни законови основания да продължи да обработва личните данни.

109.

7 ЗАДЪЛЖЕНИЯ ПО ОТНОШЕНИЕ НА ПРОЗРАЧНОСТТА И ИНФОРМАЦИЯТА[18]

110. В европейското право за защита на данните от дълго време е застъпен принципът, че субектите на данни следва да са информирани за функционирането на система за видеонаблюдение. Те трябва да получават подробна информация за наблюдаваните зони.[19] В рамките на правната уредба на ОРЗД общите задължения по отношение на прозрачността и информацията са уредени в член 12 и следващите членове от Регламента. По-подробна информация може да се намери в документа на Работната група по член 29 „Насоки относно прозрачността в съответствие с Регламент 2016/679“ (РД260)“, одобрен от Европейския комитет по защита на данните на 25 май 2018 г. В съответствие с параграф 26 от Насоки РД260, разпоредбата на член 13 от ОРЗД е приложима към ситуации на събиране на лични данни „[…] от субект на данни посредством наблюдение (например използване на автоматизирани устройства или софтуер за събиране на данни, например камери […].“.

111. С оглед на обема на информацията, която трябва да бъде предоставена на субекта на данните, администраторите на данните могат на прилагат подход, структуриран в различни нива, съгласно който те могат да използват съчетание от методи, за да осигурят прозрачност (РД260, параграф 35; РД89, параграф 22). В случаите, когато се използва видеонаблюдение, най-важната информация следва да е поставена на самата предупредителна табела (първо ниво), а останалите задължителни детайли може да бъдат предоставени по различни начини (второ ниво).

7.1 Информация на първо ниво (предупредителна табела)

112. Първото ниво се отнася до основния начин, по който администраторът на данните взаимодейства със субектите на данните. На този етап администраторите могат да използват предупредителна табела, на която е изобразена съответната информация. Тази писмена информация може да бъде придружена с пиктограма, чрез която по лесно видим, разбираем и ясно четим начин да се представи смислен преглед на планираното обработване (член 12, параграф 7 от ОРЗД). Форматът на информацията следва да бъде адаптиран към конкретното място, на което е изобразена (РД89, параграф 22).

7.1.1 Излагане на предупредителната табела

113. Информацията следва да бъде изложена по такъв начин, че субектът на данните да може лесно да възприеме обстоятелствата, при които се осъществява видеонаблюдението, преди да влезе в наблюдаваната зона (приблизително на нивото на очите). Не е необходимо да се разкрива местоположението на камерата, доколкото няма съмнение по отношение на това кои зони са обхванати от видеонаблюдението и целта на наблюдението е разяснена недвусмислено (РД 89, параграф 22). Субектът на данните трябва да може да оцени каква площ се обхваща от камерата, за да може да избегне да бъде наблюдаван или да адаптира съответно своето поведение.

[18] Възможно е да се прилагат специфични изисквания, предвидени в националното законодателство.

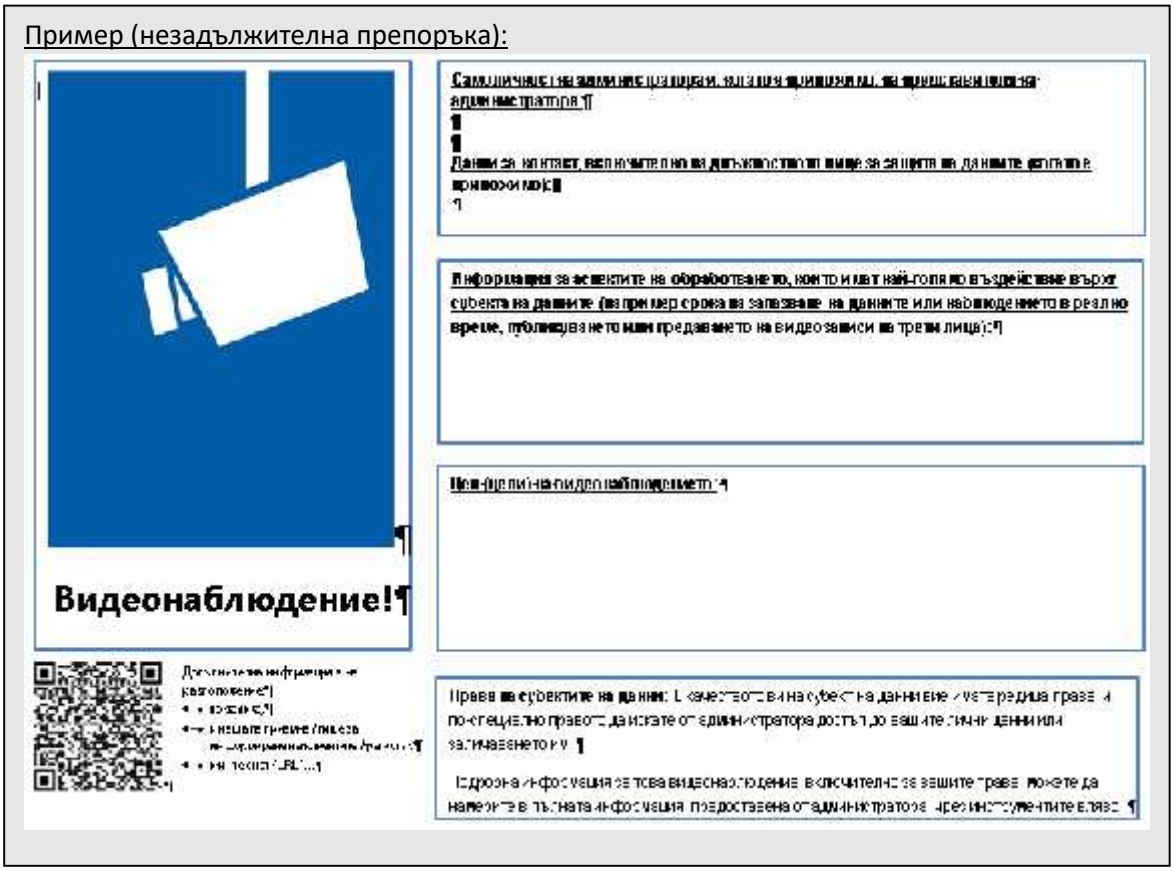
[19] Вж. РД89, Становище № 4/2004 относно обработването на лични данни посредством видеонаблюдение на Работната група по член 29).

7.1.2 Съдържание на първото ниво

114. Информацията на първо ниво (предупредителна табела) следва като цяло да предава най-важната информация, например информация за целите на обработването, самоличност на администратора на данните и наличието на права на субекта на данните, заедно с информация за най-значимото въздействие от обработването.[20] Тази информация може да включва например данни за законните интереси на администратора (или на трета страна) и данни за контакт на длъжностното лице за защита на данните (ако е приложимо). Също така трябва да е дадена информация за по-подробното второ ниво на информация и къде, и как тя може да бъде намерена.

115. Наред с горното, табелата трябва да съдържа информация, която може да изненада субекта на данните (РД260, параграф 38). Това може например да включва информация за предавания на данни на трети страни, особено ако те са извън ЕС, както и за срока на съхранение. Ако тази информация не е посочена, субектът на данните следва да има основания да вярва, че се извършва само наблюдение в реално време (без запис или предаване на данни на трети страни).

116. Пример (незадължителна препоръка):



7.2 Информация на второ ниво

117. Информацията на второ ниво също трябва да е изобразена на място, което е лесно достъпно за субекта на данните, например под формата на подробен информационен документ, достъпен на централно място (бюро за информация, рецепция или каса) и изложен върху лесно достъпен плакат. Както е посочено по-горе, предупредителната табела, съдържаща информация на първо ниво, трябва да съдържа ясно позоваване на информацията на второ ниво. Освен това е най-добре, ако информацията на първо ниво съдържа препратка към цифров източник (например

[20] Вж. РД260, параграф 38.

QR-код или адрес на уебсайт), съдържащ информацията на второ ниво. Същевременно обаче информацията следва да е лесно достъпна и в нецифров формат. Трябва да е възможно да се получи достъп до информацията на второ ниво, без да се влиза в наблюдаваната зона, особено когато информацията е предоставена в цифров формат (това може да се постигне например чрез предоставяне на връзка към информацията). Друг подходящ начин за предоставяне на информацията е посочване на телефонен номер, който субектът на данните може да набере. Независимо по какъв начин е предоставена информацията, тя трябва да съдържа всички данни, които се предоставят задължително съгласно член 13 от ОРЗД.

118. В допълнение към тези възможности и с цел те да бъдат по-ефективни, ОРЗД насърчава използването на технологични средства за предоставяне на информация на субектите на данните. Това може да включва например: камери с геолокация и включване на информация в приложения или уебсайтове с картографска информация, което би позволило на физическите лица от една страна лесно да идентифицират и посочат източниците на видео данни, които са свързани с упражняването на техните права, а от друга страна, да могат да получат по-подробна информация за операцията по обработване.

> Пример: Собственик на магазин извършва наблюдение в магазина. За да бъдат изпълнени изискванията по член 13, е достатъчно да се постави предупредителна табела на лесно видимо място при входа на магазина, която съдържа информацията на първо ниво. Наред с това собственикът на магазина трябва да предостави при касата или друго централно и лесно достъпно място в магазина информационен документ, съдържащ информацията на второ ниво.

119.

8 СРОКОВЕ НА СЪХРАНЕНИЕ И ЗАДЪЛЖЕНИЕ ЗА ИЗТРИВАНЕ

120. Не се допуска съхранение на лични данни за период, по-дълъг от необходимия за целите, за които се обработват данните (член 5, параграф 1, букви в) и д) от ОРЗД). В някои държави членки може да се прилагат специални разпоредби относно сроковете на съхранение на данни от видеонаблюдение в съответствие с член 6, параграф 2 от ОРЗД.

121. Контролът на необходимостта от съхранение на личните данни следва да се осъществява в тесни времеви рамки. Като цяло законните цели за осъществяване на видеонаблюдение често са защита на собствеността или запазване на доказателства. Обикновено е възможно нанесените щети да бъдат установени в срок от един или два дни. За да се улесни доказването на съответствие с рамката за защита на данните, в интерес на администратора на данни е да се погрижи предварително за необходимата организация (например да определи, ако е необходимо, представител, натоварен с извършването на преглед и запазване на видеозаписи). При отчитане на принципите, прогласени в член 5, параграф 1, букви в) и д) от ОРЗД, и по-конкретно на принципите на свеждане на данните до минимум и ограничаване на съхранението, личните данни следва в повечето случаи (например когато целта е откриване на прояви на вандализъм) да бъдат изтрити, най-добре автоматично, до няколко дни. Колкото е по-дълъг определеният срок на съхранение (и особено когато той надхвърля 72 часа), толкова по-убедителни аргументи трябва да бъдат предоставени за законността на целта и необходимостта от съхранението. Когато администраторът използва видеонаблюдение, не само за да наблюдава своя имот, но също така планира да съхранява данните, той следва да се увери, че съхранението на данните е необходимо за постигането на съответната цел. Когато това е така, срокът на съхранение трябва да бъде ясно и индивидуално определен за всяка отделна цел. Задължение на администратора на данни е да определи срока за запазване на данните в съответствие с принципите на необходимост и пропорционалност, както и да докаже съответствие с разпоредбите на ОРЗД.

> Пример: Собственик на малък магазин обикновено открива прояви на вандализъм още същия ден. С оглед на това е достатъчно данните да се съхраняват за срок от 24 часа. Уикендите или по-продължителни почивни дни обаче може да са основание за по-дълъг срок на съхранение. При установяване на нанесени щети може също така да се наложи собственикът да съхрани видеозаписите за по-дълъг период, за да може да заведе дело срещу извършителя.

122.

9 ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

123. Както е посочено в член 32, параграф 1 от ОРЗД, обработването на лични данни посредством видеонаблюдение не само трябва да е правно допустимо, но администраторите и обработващите лични данни трябва да обезпечат адекватно тяхната сигурност. Изпълнените **организационни и технически мерки** трябва да са **пропорционални на рисковете за правата и свободите на физическите лица**, произтичащи от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до данни от видеонаблюдение. В съответствие с членове 24 и 25 от ОРЗД, администраторите трябва да предприемат технически и организационни мерки за спазването на всички принципи на защитата на данните в процеса на обработване, както и да осигурят на субектите на данните възможности да упражняват правата си в съответствие с членове 15—22 от ОРЗД. Администраторите на данни следва да приемат

вътрешни рамки и политики, гарантиращи спазването на тези принципи, както по време на определянето на средствата за обработване, така и по време на самото обработване, което включва изготвянето на оценки на въздействието върху защитата на данните при необходимост.

9.1 Обща информация за системите за видеонаблюдение

124. Системата за видеонаблюдение (СВ)[21] се състои от аналогови и цифрови устройства, както и от софтуер, предназначени за заснемане на изображения на дадена обстановка, обработване на изображенията и извеждането им на екран за оператора. Компонентите на системата са групирани в следните категории:

- Видео среда: заснемане на изображения, системни връзки и обработване на изображенията:
  - целта на заснемането на изображенията е да се генерира изображение на реалния свят във формат, позволяващ използването на изображението от останалата част от системата;
  - системните връзки описват всички случаи на предаване на данни във видео средата, т.е. свързващите елементи и комуникациите. Примерите за свързващи елементи включват кабели, цифрови мрежи и безжично предаване. Комуникациите описват всички видео и контролни сигнали за предаване на данни, които могат да са цифрови или аналогови;
  - обработването на изображения включва анализ, съхранение и представяне на изображение или поредица от изображения.
- От гледната точка на управлението на системата всяка система за видеонаблюдение изпълнява следните логически функции:
  - управление на данните и дейностите, което включва изпълнение на команди на оператора и генерирани от системата дейности (процедури за предупреждение, уведомяване на операторите);
  - интерфейсите с други системи могат да включват връзка с други системи за сигурност (контрол на достъпа, пожароизвестителна система) и системи, които не са свързани със сигурността (системи за управление на сгради, автоматично разпознаване на регистрационни табели на превозни средства).
- Изискванията за сигурност на системите за видеонаблюдение включват поверителност, цялостност и наличност на системата и данните:
  - сигурността на системата включва физическа сигурност на всички компоненти на системата и контрол на достъпа до ВС;
  - сигурността на данните включва предотвратяване на загуба или манипулиране на данните.

[21] ОРЗД не съдържа определение за такава система, а техническо описание може да се намери например в стандарт EN 62676-1-1:2014: Системи за видеонаблюдение за използване в рамките на приложения за сигурност — част 1-1: Изисквания към системите за видеонаблюдение.

125.

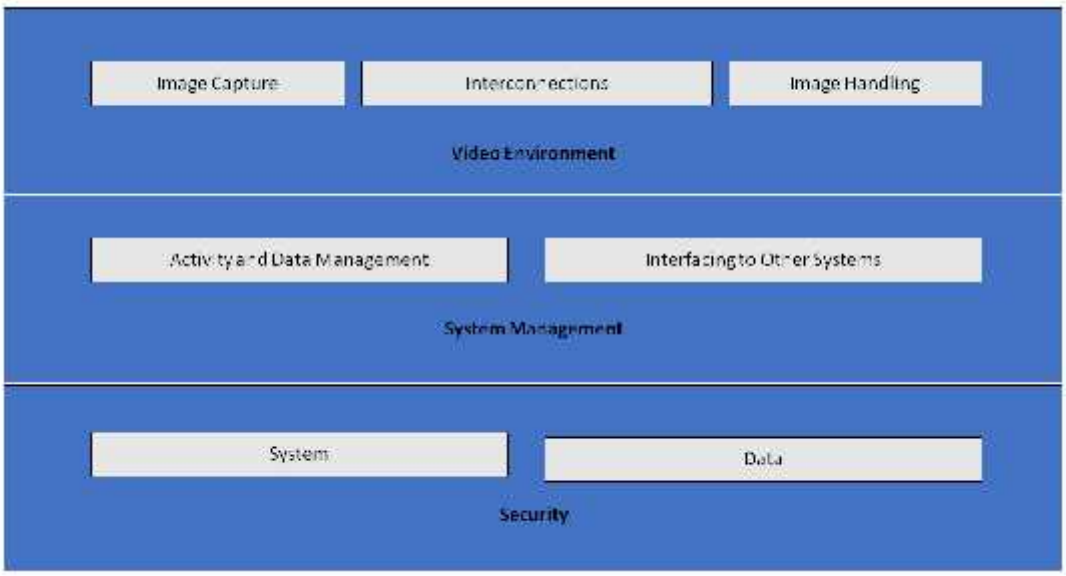


Image Capture	Заснемане на изображения
Interconnections	Системни връзки
Image Handling	Обработване на изображения
Video Environment	Видео среда
Activity and Data Management	Управление на дейностите и данните
Interfacing to Other Systems	Интерфейси с други системи
System Management	Управление на системата
System	Система
Data	Данни
Security	Сигурност

Фигура 1: Система за видеонаблюдение

9.2 Защита на данните на етапа на проектирането и по подразбиране

126. Както е посочено в член 25 от ОРЗД, администраторите на данни трябва да предприемат подходящи технически и организационни мерки за защита на данните още на етапа на планирането на видеонаблюдението и преди да започнат да събират и обработват видео данни. Тези принципи подчертават необходимостта от вградени технологии за обезпечаване на неприкосновеността на личния живот, настройки по подразбиране, които свеждат до минимум обработването на лични данни и осигуряване на необходимите инструменти, които обезпечават възможно най-голяма степен на защита на личните данни[22].

127. Администраторите на данни следва да включат гаранции за защита на данните и неприкосновеността на личния живот не само в техническите спецификации за разработване на технологиите, но и в организационните практики. По отношение на организационните практики, администраторът на данни следва да приеме подходяща рамка за управление и да въведе, и прилага политики, и процедури, свързани с видеонаблюдението. От техническа гледна точка

[22] РД168, Становище относно документа „Бъдещето на неприкосновеността на личния живот“, съвместен принос на Работната група по защитата на данните по член 29 и Работната група по полицейско и съдебно сътрудничество относно консултацията на Европейската комисия относно правната уредба на основното право на защита на личните данни (прието на 1 декември 2009 г.).

спецификациите и структурата на системата следва да включват изисквания за обработване на лични данни в съответствие с принципите, залегнали в член 5 от ОРЗД (законосъобразност на обработването, ограничаване на целта и данните, свеждане на данните до минимум по подразбиране по смисъла на член 25, параграф 2 от ОРЗД, цялост и поверителност, отчетност и др.). Когато даден администратор на данни планира да придобие търговска система за видеонаблюдение, той следва да включи тези изисквания в спецификациите за придобиване на системата. Администраторът е длъжен да осигури съответствието с тези изисквания, като ги прилага към всички компоненти на системата и към всички данни, обработвани от нея, през целия им жизнен цикъл.

9.3 Конкретни примери за подходящи мерки

128. По-голямата част от мерките, които могат да се прилагат за обезпечаване на сигурността на видеонаблюдението, особено в случаите, когато се използва цифрово оборудване и софтуер, не се различават от мерките, прилагани във връзка с другите информационни системи. Независимо от избраното решение обаче администраторът на данни е длъжен да осигури достатъчна защита на всички компоненти на системата за видеонаблюдение и данните на всички етапи, т.е. по време на съхранението (данни в покой), предаването (данни в движение), и обработването (данни в употреба). За тази цел е необходимо администраторите и обработващите лични данни да съчетават организационните и техническите мерки.

129. При избора на технически решения администраторът следва да анализира и технологии, гарантиращи неприкосновеността на личния живот, включително, защото те подобряват сигурността. Примери за такива технологии са системите, които позволяват покриване или замъгляване на зоните, където не следва да се извършва видеонаблюдение, или заличаване на изображенията на трети лица, когато видеозаписите се предоставят на субекти на данните.[23] От друга страна избраните решения не следва да включват функции, които не са необходими (например неограничено насочване на камерите, възможност за приближаване на изображението, предаване на изображения по радио канал, анализ и звукозаписи). Функциите, които са налични, но не са необходими, трябва да бъдат деактивирани.

130. На тази тема са налични множество публикации, включително международни стандарти и технически спецификации за физическа сигурност на мултимедийни системи[24] и сигурност на информационни системи с общо предназначение[25]. С оглед на това в настоящия раздел е даден само общ преглед на тази тема.

9.3.1 Организационни мерки

131. Отделно от потенциално необходимата оценка на въздействието върху защитата на данните (вж. *раздел 10*), администраторите на данни следва да вземат предвид следните аспекти, когато изготвят своите политики и процедури за видеонаблюдение:

- Кой отговаря за управлението и експлоатацията на системата за видеонаблюдение?

[23] Използването на такива технологии в някои случаи може да е дори задължително с оглед осигуряване на съответствие с член 5, параграф 1, буква в). Във всеки случай те могат да се използват като примери за най-добра практика.

[24] IEC TS 62045 — Сигурност на мултимедийни системи: Насоки за защита на неприкосновеността на личния живот във връзка с оборудване и системи във или извън експлоатация.

[25] ISO/IEC 27000 — поредица „Системи за управление на информационната сигурност“.

- Цел и обхват на проекта за видеонаблюдение.
- Допустима и забранена употреба (къде и кога се допуска или не се допуска видеонаблюдение; например използване на скрити камери и звукозапис в допълнение към видеозаписите)[26].
- Мерки за прозрачност, посочени в *раздел 7 (Задължения по отношение на прозрачността и информацията).*
- Как се извършва видеозаписът и с каква продължителност, включително архивно съхранение на видеозаписи, свързани с инциденти по сигурността?
- Кой и кога трябва да премине съответно обучение?
- Кой има достъп до видеозаписите и за какви цели?
- Оперативни процедури (например от кого и откъде се контролира видеонаблюдението, какво следва да се предприеме в случай на нарушение на защитата на данните?).
- Какви процедури следва да изпълняват външните страни, за да поискат достъп до видеозаписи и процедури за отказ или удовлетворяване на такива искания.
- Процедури за възлагане на изграждането, инсталирането и поддръжката на системи за видеонаблюдение.
- Процедури за управление на инциденти и възстановяване.

9.3.2 Технически мерки

132. **Сигурност на системите** означава **физическа сигурност** на всички компоненти на системите и цялост на системите, т.е. **защита и устойчивост на преднамерена и непреднамерена намеса в нормалното им функциониране,** и **контрол на достъпа**. Сигурност на данните означава **поверителност** (данните са достъпни само за лицата, на които е предоставен достъп), **цялост** (предотвратяване на загуба или манипулиране на данни) и **наличност** (данните са достъпни винаги, когато са необходими).

133. **Физическата сигурност** е жизненоважна част от защитата на данните и е първата линия на защита, тъй като това е защита на оборудването на системите за видеонаблюдение от кражби, вандализъм, природни бедствия, антропогенни катастрофи и случайни повреди (например в резултат на токови удари, екстремни температури или разлято кафе). При системи, базирани на аналогова технология, физическата сигурност е основният елемент от тяхната защита.

134. **Сигурността на системите и данните**, т.е. защита от преднамерена или непреднамерена намеса в нормалното им функциониране може да включва:

- защита на цялата инфраструктура на СВ (включително отдалечени камери, кабели и захранване с енергия) от физическа намеса и кражба;
- защита на предаването на видео изображения чрез комуникационни канали, които са защитени от копиране;
- криптиране на данните.
- Използване на хардуерни и софтуерни решения като пожарни стени, антивирусен софтуер или системи за откриване на кибератаки, изразяващи се в проникване в системата.
- Откриване на откази на компоненти, софтуер и системни връзки.
- Способи за възстановяване на наличността и достъпа до системата в случай на физически или технически инцидент.

[26] Това може да зависи от националното законодателство и секторната регулаторна рамка.

135. **Контролът на достъпа** гарантира, че само оправомощени лица могат да получат достъп до системата и данните, докато всички останали лица нямат такъв достъп. Мерките, които обезпечават контрола на физическия и логическия достъп, включват:

- гарантиране, че всички помещения, където се извършва контрол чрез видеонаблюдение и където се съхраняват видеозаписи, са защитени от неконтролиран достъп на трети страни;
- разполагане на мониторите по такъв начин (особено, когато те са инсталирани в достъпни помещения като приемна), че да са видими само за оправомощените оператори;
- определени са и се прилагат процедури за предоставяне, промяна и оттегляне на физически и логически достъп;
- въведени са методи и средства за удостоверяване и оправомощаване на потребителите, например относно дължината на паролите и честотата на смяната им;
- изпълняваните от потребителите действия (засягащи както системата, така и данните) се документират и подлежат на периодичен преглед;
- наблюдението и откриването на неуспешни опити за достъп се осъществява непрекъснато, а установените слабости се отстраняват във възможно най-кратък срок.

10 ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

136. В съответствие с член 35, параграф 1 от ОРЗД, администраторите на данни са длъжни да извършват оценка на въздействието върху защитата на данните (ОВЗД), когато дадена дейност по обработване на данни е съпроводена с висок риск за правата и свободите на физически лица. В член 35, параграф 3, буква в) от ОРЗД е предвидено, че администраторите на данни са длъжни да извършват оценки на въздействието върху защитата на данните, когато обработването се изразява в мащабно и систематично наблюдение на зона с обществен достъп. Нещо повече, в съответствие с член 35, параграф 3, буква б) от ОРЗД оценка на въздействието върху защитата на данните се изисква и когато администраторът планира мащабно обработване на специални категории данни.

137. „Насоките относно оценката на въздействието върху защитата на данните“[27] съдържат допълнителни съвети и по-подробни примери, приложими във връзка с видеонаблюдението (например относно „използването на система от камери за наблюдение на поведението на водачи на моторни превозни средства“). В член 35, параграф 4 от ОРЗД се съдържа изискването всеки надзорен орган да публикува списък на видовете операции по обработване, които подлежат на задължителна оценка на въздействието върху защитата на данните в съответната държава. Обикновено тези списъци са публикувани на уебсайтовете на съответните органи. С оглед на типичните цели на видеонаблюдението (защита на физическите лица и собствеността, откриване, предотвратяване и контрол на правонарушения, събиране на доказателства и биометрична идентификация на заподозрени лица) е обосновано да се приеме, че в много случаи на видеонаблюдение е наложително извършването на ОВЗД. Поради това, администраторите на данни следва внимателно да проучват тези документи, за да определят дали в конкретния случай се изисква такава оценка и да я извършат при необходимост. Резултатът от извършената ОВЗД следва да обуслови избора на администратора на данни на мерки за защита на данните.

138. Също така е важно да се отбележи, че когато резултатите от ОВЗД показват, че обработването ще породи висок риск въпреки планираните от администратора мерки за сигурност, преди да се предприеме обработването, е необходимо да се извърши консултация с компетентния надзорен орган. Информация по отношение на предишни консултации се съдържа в член 36.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)

[27] Работна група по член 29, „Насоки относно оценката на въздействието върху защитата на данните (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679“. - одобрени от Европейския комитет по защита на данните