3/2019. számú iránymutatás a személyes adatok videoeszközökkel történő kezeléséről

2.0 változat

Elfogadás időpontja: 2020. január 29.

A változatok előzményei

2.0 változat	2020. január 29.	Az iránymutatás nyilvános konzultációt követő elfogadása
1.0 változat	2019. július 10.	Az iránymutatás nyilvános konzultáció céljából történő elfogadása

Tartalomjegyzék

Az Európai Adatvédelmi Testület

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel eljárási szabályzatának 12. és 22. cikkére,

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST

1 BEVEZETÉS

1. A videoeszközök gyakori használata befolyásolja a polgárok viselkedését. Az ilyen eszközök nagymértékű használata az egyének életének számos területén még inkább arra sarkallja az egyéneket, hogy elkerüljék az esetlegesen rendellenesnek tekinthető viselkedéseket. Ezek a technológiák ténylegesen korlátozhatják az névtelen módon történő mozgásnak és a szolgáltatások név nélküli igénybevételének lehetőségeit, általában korlátozzák az észrevétlenség megőrzésének lehetőségét. Ennek jelentős adatvédelmi vonzatai vannak.

2. Az egyéneket talán nem zavarja például a meghatározott biztonsági célra kiépített videokamerás megfigyelés, ugyanakkor garanciákat kell nyújtani a teljesen eltérő és – az érintett számára – előre nem várt céllal (például marketing, munkavállalói teljesítményfigyelés stb. céljából) való visszaélés elkerülése érdekében. Ráadásul számos eszköz már a rögzített képek felhasználására és a hagyományos kamerák okoskamerává alakítására szolgál. A videotechnológiával előállított adatmennyiség, valamint az említett eszközök és technikák együttesen növelik a másodlagos felhasználás (függetlenül attól, hogy kapcsolódik-e a rendszer eredeti rendeltetéséhez), sőt, akár visszaélés kockázatát. Az általános adatvédelmi rendeletben (5. cikk) megfogalmazott alapelveket mindig gondosan figyelembe kell venni a videokamerás megfigyelés során.

3. A videokamerás megfigyelőrendszerek sok szempontból megváltoztatják azt, hogy a magánszektorban és a közszférában dolgozó szakemberek magán- vagy közterületeken hogyan viselkednek egyebek mellett a biztonság fokozása, közönségelemzés készítése és személyre szabott reklámok megjelenítése céljából. A videokamerás megfigyelés az intelligens videoelemzés folyamatos alkalmazása révén már kiemelkedően eredményes. Ezek a technikák lehetnek magánszférára nagyobb behatással, (például összetett biometrikus technológiák), vagy magánszférára kevesebb behatással járóak is (például egyszerű számoló algoritmusok). A névtelenség megőrzése és a magánélet védelme általában véve egyre nehezebb. Az egyes helyzetek különböző adatvédelmi kérdéseket vethetnek fel,

[1] A jelen véleményben a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell érteni.

következésképpen az egyik vagy másik ilyen technológia használata esetén is eltérő jellegű jogi elemzésre lesz szükség.

4. A magánélet védelme mellett e készülékek esetleges üzemzavara és az abból eredő torzítás is kockázatokat vet fel. A kutatók szerint az arcazonosításra, -felismerésre vagy -elemzésre szolgáló szoftverek az azonosítandó személy életkorától, nemétől és etnikai hovatartozásától függően eltérően működnek. Az algoritmusok különböző demográfiai jellemzők alapján működnek, így az arcfelismerésben előforduló torzítás megerősítheti a társadalmi előítéleteket. Az adatkezelőknek ezért gondoskodniuk kell a videokamerás megfigyelésen alapuló biometrikus adatkezelés helyénvalóságának és a hozzá kapcsolódó garanciák elégséges voltának rendszeres értékeléséről is.

5. Alapértelmezés szerint nincs szükség videokamerás megfigyelésre, amikor a mögöttes cél más eszközökkel is elérhető. Ellenkező esetben felmerül a veszélye annak, hogy megváltoznak a kulturális normák, ami a magánélet hiányának mint alapállapotnak az elfogadásához vezethet.

6. Ezen iránymutatás célja, hogy útmutatással szolgáljon azzal kapcsolatosan, hogyan kell alkalmazni az általános adatvédelmi rendeletet a személyes adatok videoeszközökkel történő kezelésével összefüggésben. Az itt bemutatott példák nem kimerítő jellegűek, az általános okfejtés az összes lehetséges felhasználási területen alkalmazható.

2 HATÁLY[2]

2.1 Személyes adatok

7. Napjainkban elterjedt jelenséggé vált egy adott terület optikai vagy audiovizuális eszközökkel történő, módszeres, automatizált megfigyelése, elsősorban vagyonvédelem vagy az emberi élet és egészség védelme céljából. Ez a tevékenység képi vagy audiovizuális információk gyűjtésével és megőrzésével jár a megfigyelt területre belépő összes személy tekintetében, akik külső megjelenésük vagy egyéb sajátos elemek alapján azonosíthatóak. Az erre vonatkozó adatok felhasználhatók a személyazonosság megállapítására. Emellett lehetővé teszik a személyes adatok további kezelését a személyek adott területen való jelenlétével és viselkedésével összefüggésben. Az ilyen adatokkal való visszaélés esetleges kockázata a megfigyelt terület méretével és az ott megforduló személyek számával arányosan növekszik. Ez a tény tükröződik az általános adatvédelmi rendelet 35. cikke (3) bekezdésének c) pontjában, amely nyilvános helyek nagymértékű, módszeres megfigyelése esetén adatvédelmi hatásvizsgálat elvégzését írja elő, valamint ugyanezen rendelet 37. cikke (1) bekezdésének b) pontjában, amely adatvédelmi tisztviselő kijelölésére kötelezi az adatfeldolgozókat, amennyiben az adatkezelési művelet jellegénél fogva az érintettek rendszeres szisztematikus és nagymértékű megfigyelését teszik szükségessé.

8. A rendelet hatálya azonban nem terjed ki a nem személyeket érintő adatkezelésre, tehát például abban az esetben, ha az egyének sem közvetlenül, sem közvetetten nem azonosíthatóak.

> Példa: Az általános adatvédelmi rendelet nem vonatkozik az álkamerákra (vagyis olyan kamerákra, amelyek nem működnek kameraként, így semmilyen személyes adatot nem kezelnek). *Egyes tagállamokban azonban egyéb jogszabályok hatálya alá tartozhatnak.*
>
> Példa: A nagy magasságból történő felvételkészítés esetén az adatkezelésre csak akkor terjed ki az általános adatvédelmi rendelet hatálya, ha a kezelt adatok az adott körülmények között egy konkrét személyre vonatkozhatnak.
>
> Példa: Egy gépjárműben beépített kamera található a parkolás segítése céljából. Ha a kamerát úgy alakították ki vagy állították be, hogy semmilyen adatot ne gyűjtsön természetes személyekről (például rendszámokat, vagy járókelők azonosítását lehetővé tevő információkat), akkor az általános adatvédelmi rendelet nem alkalmazandó.

9.

2.2 A bűnüldözési irányelv (az (EU) 2016/680 irányelv) alkalmazása

10. Különösen az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – így többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából végzett személyesadat-kezelés az (EU) 2016/680 irányelv hatálya alá tartozik.

[2] Az Európai Adatvédelmi Testület megjegyzi, hogy amennyiben az általános adatvédelmi rendelet lehetővé teszi, a nemzeti jogszabályokban rögzített különös rendelkezések alkalmazhatók.

2.3 Az otthoni tevékenységek mentessége

11. A 2. cikk (2) bekezdésének c) pontja szerint a természetes személyek által kizárólag személyes vagy otthoni tevékenységük keretében végzett személyesadat-kezelésre – amely online tevékenységet is magában foglalhat – nem terjed ki az általános adatvédelmi rendelet hatálya.[3]

12. Ez a rendelkezést, vagyis az otthoni tevékenységek mentességét a videokamerás megfigyeléssel összefüggésben szűken kell értelmezni. Ahogy azt a Bíróság is megállapította, az otthoni tevékenységek mentességét „*úgy kell tehát értelmezni, hogy az kizárólag a magánszemélyek magán vagy családi élete keretébe tartozó tevékenységekre vonatkozik, nyilvánvalóan nem erről van azonban szó a személyes adatok interneten való közzétételét jelentő olyan feldolgozás esetében, amely során ezen adatok meghatározatlan számú személy számára válnak hozzáférhetővé*”.[4] Továbbá abban az esetben, ha a videokamerás megfigyelőrendszer személyes adatok folyamatos rögzítését és tárolását végzi, valamint „*ugyan csak részben, de közterületre is kiterjed, és így a kamerás megfigyelőrendszerrel adatkezelést végző személy magánszféráján kívülre irányul, nem tekinthető a 95/46 irányelv 3. cikke (2) bekezdésének második francia bekezdésében foglaltak értelmében kizárólag »személyes, illetve otthoni« tevékenységnek*”[5].

13. Ami a magánszemély területén és helyiségein belül üzemelő videoeszközöket illeti, kiterjedhet rájuk az otthoni tevékenységek mentességére vonatkozó rendelkezés. Ez több tényezőtől függ, megállapításához pedig mindegyik tényezőt figyelembe kell venni. A fent említett, a Bíróság ítéleteiben megjelölt elemek mellett az otthoni videokamerás megfigyelés felhasználójának azt is meg kell vizsgálnia, hogy valamilyen személyes kapcsolatban áll-e az érintettel, a megfigyelés terjedelme vagy gyakorisága valamilyen szakmai tevékenységet feltételez-e a részéről, és a megfigyelés kedvezőtlen hatást gyakorolhat-e az érintettekre. A fent említett elemek bármelyikének megléte még nem feltétlenül jelenti azt, hogy az adatkezelés nem tartozik az otthoni tevékenységek mentességének hatálya alá, ennek megállapításához tehát átfogó értékelésre van szükség.

[3] Lásd még a (18) preambulumbekezdést.

[4] A Bíróság C-101/01. sz., *Bodil Lindqvist elleni büntetőeljárás* ügyben 2003. november 6-án hozott ítéletének 47. pontja.

[5] A Bíróság C-212/13. sz., *František Ryneš kontra Úřad pro ochranu osobních údajů* ügyben 2014. december 11-én hozott ítéletének 33. pontja.

Példa: Egy turista nyaralása megörökítése céljából mobiltelefonjával és videokamerával is videókat rögzít. A felvételeket megmutatja barátainak és családtagjainak, de nem teszi hozzáférhetővé meghatározatlan számú személy számára. Ez az otthoni tevékenységek mentességének hatálya alá tartozik.

Példa: Egy hegyi kerékpáros akciókamerával szeretné rögzíteni, ahogy legurul a hegyről. Félreeső területen kerékpározik, a felvételeket pedig csak otthoni, személyes szórakozás céljára kívánja felhasználni. Ez még abban az esetben is az otthoni tevékenységek mentességének hatálya alá tartozik, ha bizonyos mértékben személyes adatok kezelésével jár.

Példa: Valaki a saját kertjét figyeli meg és rögzíti videofelvételeken videokamerás megfigyelőrendszerrel. Az ingatlant kerítés veszi körül, és csak maga az adatkezelő és a családja megy ki rendszeresen a kertbe. Ez az otthoni tevékenységek mentességének hatálya alá tartozik, feltéve, hogy a videokamerás megfigyelés részben sem terjed ki közterületre vagy szomszédos ingatlanra.

14.

3 AZ ADATKEZELÉS JOGSZERŰSÉGE

15. Használat előtt részletesen meg kell határozni az adatkezelés célját (az 5. cikk (1) bekezdésének b) pontja). A videokamerás megfigyelés számos célt szolgálhat, például ingatlan- és egyéb vagyonvédelem támogatását, az emberi élet és testi épség védelmének támogatását vagy polgári jogi igényhez kapcsolódó bizonyítékok gyűjtését.[6] Ezeket a megfigyelési célokat írásban kell rögzíteni (az 5. cikk (2) bekezdése), és mindegyik használatban lévő kamera vonatkozásában meg kell határozni. Az ugyanazon adatkezelő által azonos célra használt kamerák együtt dokumentálhatók. Ezenkívül az érintetteket a 13. cikknek megfelelően kell tájékoztatni az adatkezelés céljáról vagy céljairól (*lásd a 7. fejezetet [Átláthatósági és tájékoztatási kötelezettségek]*). A kizárólag a „biztonság" vagy a „saját biztonság" céljából folytatott videokamerás megfigyelés nem kellően konkrét (az 5. cikk (1) bekezdésének b) pontja). Ezenkívül ellentétes azzal az elvvel, miszerint a személyes adatok kezelését jogszerűen, tisztességesen és az érintett számára átlátható módon kell végezni (lásd az 5. cikk (1) bekezdésének a) pontját).

16. Elvben a 6. cikk (1) bekezdése szerinti bármely jogalap alapul szolgálhat az adatok videokamerás megfigyeléssel történő kezelését illetően. Például a 6. cikk (1) bekezdésének c) pontja akkor alkalmazandó, amikor a nemzeti jog videokamerás megfigyelési kötelezettséget ír elő.[7] A gyakorlatban viszont a leggyakrabban az alábbi rendelkezésekre hivatkoznak:

- a 6. cikk (1) bekezdésének f) pontja (jogos érdek),
- a 6. cikk (1) bekezdésének e) pontja (az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges).

Meglehetősen kivételes esetekben az adatkezelő 6. cikk (1) bekezdésének a) pontját (hozzájárulás) is alkalmazhatja jogalapként.

3.1 Jogos érdek – a 6. cikk (1) bekezdésének f) pontja

17. A 6. cikk (1) bekezdése f) pontjának jogi értékelését a (47) preambulumbekezdéssel összhangban, az alábbi szempontok alapján kell elvégezni.

3.1.1 Jogos érdekek fennállása

18. A videokamerás megfigyelés jogszerű, amennyiben az adatkezelő vagy harmadik fél jogos érdekének érvényesítéséhez szükséges, kivéve, ha az ilyen érdekekkel szemben elsőbbséget élveznek az érintett érdekei vagy alapvető jogai és szabadságai (a 6. cikk (1) bekezdésének f) pontja). Az adatkezelő vagy harmadik fél jogos érdekei lehetnek jogi[8], gazdasági vagy nem vagyoni jellegűek.[9] Az adatkezelőnek azonban figyelembe kell vennie, hogy amennyiben az érintett a 21. cikk értelmében tiltakozik a megfigyelés ellen, akkor az adatkezelő csak akkor folytathatja az érintett videokamerás megfigyelését, ha azt *kényszerítő erejű* jogos érdek indokolja, amely elsőbbséget élvez az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amely jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

---

[6] Tagállamonként eltérő szabályok vonatkoznak a polgári jogi igényekkel kapcsolatos bizonyítékok gyűjtésére.

[7] Ez az iránymutatás nem elemzi és nem részletezi a tagállamonként esetlegesen eltérő nemzeti jogszabályokat.

[8] A Bíróság C-13/16. sz., *Rīgas satiksme*-ügyben 2017. május 4-én hozott ítélete.

[9] Lásd a 29. cikk szerinti munkacsoport WP217. sz. véleményét

19. Valós és veszélyes helyzetben a vagyon betörés, lopás vagy rongálás elleni védelmének célja a videokamerás megfigyeléshez fűződő jogos érdeknek minősülhet.

20. A jogos érdeknek valóban fenn kell állnia és ténylegesen léteznie kell (vagyis nem lehet kitalált vagy feltételezett)[10]. A megfigyelés megkezdése előtt tényleges veszélyhelyzetnek kell felmerülnie, amely lehet például korábbi káresemény vagy súlyos incidens. Az elszámoltathatóság elvére tekintettel az adatkezelőknek javasolt írásban rögzíteniük az ilyen incidenseket (dátum, módszer, pénzügyi veszteség) és a kapcsolódó büntetőjogi vádakat. Az írásban rögzített incidensek meggyőző bizonyítékként szolgálhatnak a jogos érdek fennállására vonatkozóan. A jogos érdek fennállását és a megfigyelés szükségességét rendszeres időközönként (a körülményektől függően például évente egyszer) újra kell értékelni.

> Példa: Egy üzlettulajdonos új üzletet kíván nyitni, és a rongálás megelőzése érdekében videokamerás megfigyelőrendszert szeretne telepíteni. A statisztikák bemutatásával bizonyíthatja, hogy a szűkebb környéken nagy a rongálás valószínűsége. Emellett a szomszédos üzletekben szerzett tapasztalatok is hasznosak. A szóban forgó adatkezelőnek nem kellett szükségszerűen kárt szenvednie, amennyiben a környéken felmerült károk veszélyre vagy hasonló helyzetre engednek következtetni, és ezáltal jogos érdekre utalnak. Nem elegendő azonban nemzeti vagy általános bűnügyi statisztikát bemutatni a szóban forgó terület vagy az adott üzletet fenyegető veszélyek elemzése nélkül.

21.

22. A közvetlen veszélyt jelentő helyzetek jogos érdeknek minősülhetnek többek között bankok vagy drága árukat értékesítő üzletek (például ékszerüzletek) számára, illetve a vagyon elleni bűncselekmények jellemző helyszíneként ismert területeken (például benzinkutakon).

23. Az általános adatvédelmi rendelet emellett a 6. cikk (1) bekezdésének második mondatában egyértelműen rögzíti, hogy a közhatalmi szervek feladataik ellátása körében nem alapíthatják az általuk végzett adatkezelést jogos érdekre.

3.1.2 Az adatkezelés szükségessége

24. A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsak kell lenniük, és a szükségesre kell korlátozódniuk („adattakarékosság”), lásd az 5. cikk (1) bekezdésének c) pontját. Videokamerás megfigyelőrendszer telepítése előtt az adatkezelőnek mindig érdemes alaposan megvizsgálnia, hogy ez az intézkedés elsősorban alkalmas-e a kitűzött cél elérésére, másodsorban pedig megfelelő és szükséges-e a céljaihoz. Csak abban az esetben érdemes videokamerás megfigyelési intézkedések mellett dönteni, ha az adatkezelés célját egyéb, az érintett alapvető jogait és szabadságait kevésbé csorbító eszközzel észszerű módon nem lehetséges elérni.

25. Abban a helyzetben, ha az adatkezelő vagyon elleni bűncselekményeket kíván megelőzni, videokamerás megfigyelőrendszer telepítése helyett más jellegű biztonsági intézkedéseket is tehet, például bekerítheti az ingatlant, rendszeres őrjárat teljesítésével bízhatja meg a biztonsági személyzetet, portásokat alkalmazhat, jobb világítást biztosíthat, biztonsági zárakat, betörésbiztos nyílászárókat szereltethet be, illetve graffiti elleni védőbevonattal vagy fóliával láthatja el a falakat. Ezek az intézkedések ugyanolyan hatékony védelmet nyújthatnak a betörés, a lopás és a rongálás ellen,

[10] Lásd a 29. cikk szerinti munkacsoport WP217. sz. véleményének 24. és azt követő oldalait. Lásd a Bíróság C-708/18. sz. ügyben hozott ítéletének 44. pontját.

mint a videokamerás megfigyelőrendszerek. Az adatkezelőnek eseti alapon kell értékelnie, hogy az ilyen intézkedések észszerű megoldást jelenthetnek-e.

26. A kamerarendszer üzembe helyezése előtt az adatkezelő köteles felmérni, hogy hol és mikor szükségesek feltétlenül a videokamerás megfigyelési intézkedések. Az éjszaka és a rendes munkaidőn kívül üzemelő megfigyelőrendszer általában megfelel az adatkezelő igényeinek a vagyonát fenyegető veszélyek elkerüléséhez.

27. Általában legfeljebb az ingatlan határáig szükséges videokamerás megfigyelést alkalmazni az adatkezelők területének és helyiségeinek védelmére.[11] Azonban előfordul, hogy az ingatlan megfigyelése nem elegendő a hatékony védelemhez. Bizonyos egyedi esetekben a környező területekre is szükség lehet kiterjeszteni a videokamerás megfigyelést. Ezzel összefüggésben az adatkezelőnek érdemes fizikai és technikai megoldásokhoz, például a nem releváns területek kitakarásához vagy kikockázásához folyamodnia.

> Példa: Egy könyvesbolt meg kívánja védeni helyiségeit a rongálástól. A kameráknak általában véve csak a helyiségekről kellene felvételt készíteniük, mivel a szomszédos helyiségeket vagy a könyvesbolt környékén található közterületeket e célból nem szükséges megfigyelni.

28.

29. A bizonyítékok megőrzésének módját illetően is felmerülnek az adatkezelés szükségességével kapcsolatos kérdések. Egyes esetekben szükség lehet feketedobozos megoldásokra, amelyeknél a felvétel meghatározott tárolási idő leteltével automatikusan törlődik, és kizárólag incidens esetén férhetők hozzá. Más esetekben előfordulhat, hogy egyáltalán nem szükséges videofelvételt rögzíteni, hanem megfelelőbb megoldás a valós idejű megfigyelés. A feketedobozos megoldás és a valós idejű megfigyelés közül szintén a kitűzött cél alapján kell választani. Ha például a videokamerás megfigyelés célja a bizonyítékok megőrzése, akkor általában nem megfelelőek a valós idejű módszerek. A valós idejű megfigyelés néha magánszférára nagyobb behatással járó lehet, mint a felvételek tárolása és korlátozott idő utáni automatikus törlése (például magánszférára nagyobb behatással járó lehet, ha valaki folyamatosan nézi a monitort, mint ha egyáltalán nem is lenne monitor, és az összes felvételt automatikusan a feketedobozban tárolnák). Ezzel összefüggésben tekintetbe kell venni az adattakarékosság elvét (az 5. cikk (1) bekezdésének c) pontja). Érdemes szem előtt tartani lehetőségként, hogy az adatkezelő videokamerás megfigyelés helyett azonnali reagálásra és beavatkozásra képes biztonsági személyzetet is foglalkoztathat.

3.1.3 Az érdekek kiegyensúlyozása

30. Feltételezve, hogy a videokamerás megfigyelés az adatkezelő jogos érdekeinek védelméhez szükséges, a videokamerás megfigyelőrendszer csak akkor helyezhető üzembe, ha az adatkezelő vagy harmadik fél jogos érdekeivel (például vagyon vagy testi épség védelme) szemben nem élveznek elsőbbséget az érintett érdekei vagy alapvető jogai és szabadságai. Az adatkezelőnek meg kell vizsgálnia a következőket: 1) milyen mértékben érinti a megfigyelés egyének alapvető jogait és szabadságait, és 2) az érintett jogainak sérelmével vagy e jogokra nézve hátrányos következményekkel jár-e. Tulajdonképpen kötelező egyensúlyt teremteni az érdekek között. Egyrészről az alapvető jogokat és szabadságokat, másrészről pedig az adatkezelő jogos érdekeit kell értékelni és gondosan kiegyensúlyozni.

[11] Ez egyes tagállamokban nemzeti jogszabályok tárgyát is képezheti.

Példa: Egy magánparkolót üzemeltető vállalkozás visszatérő problémaként jegyezte fel a parkoló gépkocsikból történt lopásokat. A parkoló bárki számára könnyen megközelíthető, nyitott terület, de jelzőtáblák és a körülötte lévő útakadályok egyértelműen jelölik. A parkolási társaságnak jogos érdeke (az ügyfelek gépkocsijából történő lopások megelőzése) fűződik ahhoz, hogy a területet megfigyelje abban a napszakban, amikor a problémák felmerülnek. Az érintetteket korlátozott ideig figyelik meg, nem kikapcsolódás céljából tartózkodnak a területen, és nekik is érdekükben áll a lopások megelőzése. Ebben az esetben az adatkezelő jogos érdeke elsőbbséget élvez az érintettek megfigyelés mellőzéséhez fűződő érdekével szemben.

Példa: Egy étterem úgy dönt, hogy a szaniterhelyiségek tisztaságának ellenőrzése céljából videokamerákat telepít a mosdókba. Ebben az esetben az érintettek jogai egyértelműen elsőbbséget élveznek az adatkezelő érdekével szemben, ezért nem telepíthetők kamerák ezekbe a helyiségekbe.

31.

3.1.3.1 Eseti döntéshozatal

32. Mivel az érdekek kiegyensúlyozása a rendelet értelmében kötelező, eseti alapon kell döntést hozni (lásd a 6. cikk (1) bekezdésének f) pontját). Nem elég elvont helyzetekre hivatkozni vagy hasonló eseteket összehasonlítani. Az adatkezelőnek értékelnie kell az érintettet megillető jogok csorbulásának kockázatait; ebben az esetben pedig a döntő szempont az egyént megillető jogok és szabadságok csorbulásának súlyossága.

33. A súlyosság egyebek mellett a gyűjtött információk jellege (információtartalom), terjedelme (információsűrűség, térbeli és földrajzi kiterjedés), az érintettek száma (konkrét számadatként vagy a releváns sokaság hányadában), a szóban forgó helyzet, az érintettek csoportjának tényleges érdekei, alternatív eszközök, valamint az adatértékelés jellege és terjedelme alapján határozható meg.

34. Fontos egyensúlyozó tényező lehet a megfigyelt terület mérete és a megfigyelt érintettek száma. A félreeső területeken folytatott videokamerás megfigyelést (például vadvilág figyelése vagy kritikus infrastruktúrák, így magántulajdonú rádióantennák védelme) másképpen kell értékelni, mint a sétálóutcában vagy bevásárlóközpontban végzett videokamerás megfigyelést.

Példa: Menetrögzítő kamera telepítése esetén (például baleset bekövetkezésekor történő bizonyítékgyűjtés céljából) fontos gondoskodni arról, hogy ez a kamera ne rögzítse folyamatosan a forgalmat, valamint az út mellett tartózkodó személyeket. Ellenkező esetben az érintettek jogainak ez a csorbulása nem indokolható a videofelvételeknek egy inkább feltételezett balesetnél bizonyítékként való rendelkezésre állásához fűződő érdekkel.[11]

35.

3.1.3.2 Az érintettek észszerű elvárásai

36. A (47) preambulumbekezdés szerint a jogos érdek fennállásának megállapítása körültekintő vizsgálatot igényel. Ebben az esetben figyelembe kell venni az érintett észszerű elvárásait a személyes adatai kezelésének időpontjában és azzal összefüggésben. A módszeres megfigyelést illetően az érintett és az adatkezelő közötti kapcsolat jelentős különbségeket mutathat, és befolyásolhatja, hogy az érintettnek milyen észszerű elvárásai lehetnek. Az észszerű elvárások fogalmának értelmezése nem alapulhat kizárólag a szóban forgó szubjektív elvárásokon. A döntő szempontnak inkább annak kell lennie, hogy egy tárgyilagos harmadik fél az adott helyzetben észszerűen számíthat és következtethet arra, hogy megfigyelik.

37. Például egy munkavállaló a munkahelyén többnyire valószínűleg nem számít arra, hogy munkáltatója megfigyeli.[12] Ezenkívül jellemzően nem kell megfigyelésre számítani magánkertben, a lakóhelyen, illetve vizsgáló- és kezelőhelyiségekben. Ehhez hasonlóan nem észszerű megfigyelésre számítani szaniterhelyiségekben vagy szaunákban, az ilyen területek megfigyelése ugyanis súlyosan csorbítja az érintett jogait. Az érintettek észszerű elvárása, hogy ezeken a helyeken ne legyen videokamerás megfigyelés. Ugyanakkor a banki ügyfelek számíthatnak arra, hogy a bankon belül vagy a bankjegykiadó automatánál megfigyelik őket.

38. Az érintettek azt is elvárhatják, hogy ne figyeljék meg őket nyilvános helyeken, különösen akkor, ha ezeket a helyeket jellemzően lábadozás, pihenés és szabadidős tevékenységek céljára használják, valamint azokon a helyeken, ahol egyének tartózkodnak, illetve kommunikálnak, így például társalgókban, éttermi asztaloknál, parkokban, mozikban és fitneszlétesítményekben. Ebben az esetben az érintett érdekei vagy jogai és szabadságai gyakran elsőbbséget élveznek az adatkezelő jogos érdekeivel szemben.

> Példa: Az érintettek elvárják, hogy az illemhelyeken ne figyeljék meg őket. A videokamerás megfigyelés – például a balesetek megelőzése érdekében – itt nem arányos.

39.

40. Az érintettet a videokamerás megfigyelésről tájékoztató tábláknak nincs jelentőségük annak megállapításakor, hogy az érintettek tárgyilagosan milyen elvárásaik lehetnek. Következésképpen például az üzlettulajdonos nem hagyatkozhat arra, hogy a vevőknek *tárgyilagosan* az az észszerű elvárásuk, hogy megfigyelik őket, csak azért, mert a bejáratnál tábla tájékoztatja őket a megfigyelésről.

3.2 Az adatkezelés szükségessége közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, a 6. cikk (1) bekezdésének e) pontja

41. A 6. cikk (1) bekezdésének e) pontja szerint a személyes adatok akkor kezelhetők videokamerás megfigyelés útján, ha erre közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához van szükség.[13] Előfordulhat, hogy a közhatalmi jogosítvány nem teszi lehetővé az ilyen adatkezelést, de más jogalapok – például az „egészségvédelem és biztonság” a látogatók és a munkavállalók védelme érdekében – alkalmazásával korlátozott körű adatkezelés végezhető általános adatvédelmi rendelet szerinti kötelezettségek és az érintetteket megillető jogok tiszteletben tartása mellett.

42. Az általános adatvédelmi rendeletben foglalt szabályok alkalmazásának kiigazítása érdekében a tagállamok fenntarthatnak vagy bevezethetnek a videokamerás megfigyelésre vonatkozó különös nemzeti jogszabályokat, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, feltéve, hogy ezek a jogszabályok összhangban vannak az általános adatvédelmi rendeletben rögzített elvekkel (például korlátozott tárolhatóság, arányosság).

---

[12] Lásd még: a 29. cikk szerinti munkacsoport 2017. június 8-án elfogadott 2/2017. sz. véleménye a munkahelyi adatkezelésről (WP249).

[13] Az adatkezelés hivatkozott jogalapját az uniós jognak vagy valamely tagállam jogának kell megállapítania, és „szükségesnek kell lennie valamely közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához” (a 6. cikk (3) bekezdése).

3.3 Hozzájárulás, a 6. cikk (1) bekezdésének a) pontja

43. A hozzájárulásról szóló iránymutatásban foglaltak szerint a hozzájárulásnak önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie..[14]

44. A módszeres megfigyelést illetően az érintett hozzájárulása csak kivételes esetekben szolgálhat jogalapként a 7. cikk szerint (lásd a (43) preambulumbekezdést). A megfigyelés jellegéből adódóan ez a technológia egyszerre ismeretlen számú személyt figyel meg. Az adatkezelő aligha képes bizonyítani, hogy az érintett a személyes adatainak kezelése előtt hozzájárulását adta (a 7. cikk (1) bekezdése). Feltételezve, hogy az érintett visszavonja hozzájárulását, az adatkezelő nehezen tudja bizonyítani, hogy a továbbiakban nem kezeli a személyes adatokat (a 7. cikk (3) bekezdése).

> Példa: A sportolók kérhetik megfigyelésüket az egyéni edzés idejére, hogy kielemezhessék technikáikat és teljesítményüket. Ezzel szemben akkor, ha a sportegyesület kezdeményezi az egész csapat megfigyelését ugyanebből a célból, akkor a hozzájárulás gyakran nem érvényes, mivel az egyes sportolók kényszerítve érezhetik magukat a hozzájárulásra azért, hogy a hozzájárulásuk megtagadása ne érintse hátrányosan a csapattársaikat.

45.

46. Ha az adatkezelő hozzájárulásra kíván támaszkodni, akkor az ő kötelessége gondoskodni arról, hogy a videokamerával megfigyelt területre belépő összes érintett azt megelőzően a hozzájárulását adja. Ennek a hozzájárulásnak meg kell felelnie a 7. cikkben előírt feltételeknek. A kijelölt, megfigyelés alatt álló területre való belépés (ha például az embereket arra kérik, hogy meghatározott folyosón vagy kapun haladjanak keresztül a megfigyelt területre való belépéshez) nem minősül a hozzájáruláshoz szükséges nyilatkozatnak vagy a megerősítést félreérthetetlenül kifejező cselekedetnek, kivéve, ha – a hozzájárulásról szóló iránymutatásban leírt módon – a 4. és a 7. cikkben foglalt feltételeket egyaránt teljesíti.[15]

47. A munkáltatók és a munkavállalók közötti egyenlőtlen erőviszonyokra tekintettel a munkáltatóknak többnyire nem szabad hozzájárulásra támaszkodniuk a személyes adatok kezelését illetően, mivel valószínűsíthetően nem lesz önkéntes a hozzájárulás. Ezzel összefüggésben figyelembe kell venni a hozzájárulásról szóló iránymutatást.

48. A tagállami jog vagy kollektív szerződések – ideértve az üzemi megállapodásokat is – előírhatnak olyan konkrét szabályokat, amelyek a munkavállalók személyes adatainak a foglalkoztatással összefüggő kezelését szabályozzák (lásd a 88. cikket).

[14] A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról (WP259 rev.01). Az Európai Adatvédelmi Testület jóváhagyásával.

[15] Figyelembe kell venni a 29. cikk szerinti munkacsoportnak az (EU) 2016/679 rendelet szerinti hozzájárulásról szóló, az Európai Adatvédelmi Testület által jóváhagyott iránymutatását (WP 259).

4 VIDEOFELVÉTELEK KÖZLÉSE HARMADIK FELEK RÉSZÉRE

49. Elvben az általános adatvédelmi rendelet általános rendelkezései vonatkoznak a videofelvételek harmadik felekkel való közlésére.

4.1 Videofelvételek közlése általánosságban harmadik felek részére

50. A közlés a 4. cikk 2. pontjában szereplő fogalommeghatározás szerint továbbítás (például egyéni tájékoztatás), terjesztés (például online közzététel) vagy egyéb módon történő hozzáférhetővé tétel. A harmadik fél fogalmának meghatározását 4. cikk 10. pontja tartalmazza. Amennyiben a közlés harmadik országok vagy nemzetközi szervezetek részére irányul, a 44. és azt követő cikkekben foglalt különös rendelkezéseket is alkalmazni kell.

51. A személyes adatok bármilyen közlése a személyes adatok kezelésének külön típusa, amelyhez az adatkezelőnek a 6. cikk szerinti jogalappal kell rendelkeznie.

> Példa: Egy adatkezelő az internetre kíván feltölteni egy felvételt, ehhez az adatkezeléshez pedig jogalapra van szüksége, például a 6. cikk (1) bekezdésének a) pontja szerint be kell szereznie az érintett hozzájárulását.

52.

53. A 6. cikk (4) bekezdésében rögzített szabályoknak megfelelően továbbíthatók videofelvételek harmadik feleknek az adatgyűjtés céljától eltérő célból.

> Példa: Kárrendezés céljából videokamerás megfigyelés alatt tartanak egy sorompót (egy parkolóban). Kár keletkezik, és a videofelvételt továbbítják egy ügyvédnek, hogy járjon el az ügyben. Ebben az esetben a videofelvétel készítésének célja azonos a továbbításának céljával.
>
> Példa: Kárrendezés céljából videokamerás megfigyelés alatt tartanak egy sorompót (egy parkolóban). A felvételt kizárólag szórakoztatás céljából közzéteszik az interneten. Ebben az esetben a cél megváltozott és összeegyeztethetetlen az eredeti céllal. Ezenkívül nehezen lehetne meghatározni ennek az adatkezelésnek (közzétételnek) a jogalapját.

54.

55. A címzett harmadik félnek saját jogi elemzést kell végeznie, különösen azért, hogy meghatározza az általa végzett adatkezelés (például a felvétel átvétele) 6. cikk szerinti jogalapját.

4.2 Videofelvételek közlése bűnüldöző hatóságok részére

56. A videofelvételek bűnüldöző hatóságokkal való közlése szintén független folyamat, amelyet az adatkezelőnek külön indokolnia kell.

57. A 6. cikk (1) bekezdésének c) pontja szerint az adatkezelés akkor jogszerű, ha az adatkezelőre vonatkozó valamely jogi kötelezettség teljesítéséhez szükséges. Az erre vonatkozó rendőrségi jogszabályok ugyan a tagállamok kizárólagos hatáskörébe tartoznak, de nagy valószínűséggel mindegyik tagállamban vannak a bizonyítékok bűnüldöző hatóságoknak való továbbítására irányadó általános szabályok. Az adatokat átadó adatkezelő által végzett adatkezelést az általános adatvédelmi rendelet szabályozza. Ha a nemzeti jogszabályok arra kötelezik az adatkezelőt, hogy együttműködjön bűnüldöző hatóságokkal (például nyomozásban), akkor az adatok átadásának jogalapja a 6. cikk (1) bekezdésének c) pontjában említett jogi kötelezettség.

58. A 6. cikk (4) bekezdése szerinti célhoz kötöttség többnyire nem okoz problémát, mivel a közlés kifejezetten a tagállami jogból fakad. Ezért figyelembe kell venni a cél a)–e) pont értelmében vett megváltozására vonatkozó különös követelményeket.

> Példa: Egy üzlettulajdonos felvételt készít üzlete bejáratánál. A felvételen látható, hogy egy személy ellopja egy másik személy pénztárcáját. A rendőrség arra kéri az adatkezelőt, hogy a nyomozás segítése érdekében adja át a felvételt. Ebben az esetben az üzlettulajdonos a vonatkozó nemzeti jogszabályokkal összefüggésben a 6. cikk (1) bekezdésének c) pontja szerinti jogalapra (jogi kötelezettség) hivatkozhat a továbbítással megvalósuló adatkezeléshez.

59.

> Példa: Biztonsági okokból kamerát telepítenek egy üzletben. Az üzlettulajdonos úgy véli, hogy valamilyen gyanús cselekményről készített felvételt, és úgy dönt, hogy elküldi a rendőrségnek (miközben semmi nem utal arra, hogy bármilyen nyomozás lenne folyamatban). Ebben az esetben az üzlettulajdonosnak meg kell vizsgálnia, hogy többnyire a 6. cikk (1) bekezdésének f) pontjában rögzített feltételek teljesülnek-e. Rendszerint akkor áll fenn ez a helyzet, ha bűncselekmény alapos gyanúja merült fel az üzlettulajdonosban.

60.

61. A személyes adatok bűnüldöző hatóságok általi kezelésére nem az általános adatvédelmi rendelet vonatkozik (lásd a 2. cikk (2) bekezdésének d) pontját), hanem a bűnüldözési irányelv (az (EU) 2016/680 irányelv) hatálya alá tartozik.

5 ADATOK KÜLÖNLEGES KATEGÓRIÁINAK KEZELÉSE

62. A videokamerás megfigyelőrendszerek általában jelentős mennyiségű személyes adatot gyűjtenek, amelyek között fokozottan személyes jellegű, sőt, akár különleges kategóriájú adatok is lehetnek. Tulajdonképpen az eredetileg videorögzítéssel gyűjtött, lényegtelennek tűnő adatokból is kikövetkeztethetők eltérő célt (például az egyéni szokások feltérképezését) szolgáló információk. A videokamerás megfigyelés azonban nem mindig minősül különleges kategóriájú személyes adatok kezelésének.

> Példa: A szemüveget viselő vagy kerekesszéket használó érintettet ábrázoló videofelvétel önmagában nem tekinthető a személyes adatok különleges kategóriájának.

63.

64. Ha azonban a videofelvételt különleges kategóriájú adatok kinyerésére használják fel, akkor a 9. cikk alkalmazandó.

> Példa: Politikai vélemények következtethetők ki például azokból a felvételekből, amelyek alapján a rendezvényen részt vevő, sztrájkoló stb. érintettek azonosíthatók. Ez a 9. cikk hatálya alá tartozik.
>
> Példa: Ha egy kórház videokamerákat telepített azért, hogy a betegek egészségi állapotát figyelemmel kísérje, akkor ez különleges kategóriájú személyes adatok kezelésének tekinthető (9. cikk).

65.

66. Videokamerás megfigyelőrendszer telepítése esetén elvileg körültekintően figyelembe kell venni az adattakarékosság elvét. Így még ha a 9. cikk (1) bekezdése nem is alkalmazandó, az adatkezelőnek mindig törekednie kell arra, hogy a (9. cikken túlmenően) egyéb különleges adatokat tartalmazó videofelvételek rögzítésének kockázata a lehető legkisebb legyen.

> Példa: A videokamerás megfigyelés keretében egy templomról készített felvételek önmagukban nem tartoznak a 9. cikk hatálya alá. Az adatkezelőnek azonban különösen körültekintő vizsgálatot kell végeznie a 6. cikk (1) bekezdésének f) pontja alapján, figyelembe véve az adatok jellegét és a (9. cikken túlmenően) egyéb különleges adatokat tartalmazó videofelvételek rögzítésének kockázatát, amikor az érintett érdekeit vizsgálja.

67.

68. Ha különleges kategóriájú adatok kezelésére használnak videokamerás megfigyelőrendszert, az adatkezelőnek a 9. cikk értelmében a személyes adatok különleges kategóriáinak kezelésére vonatkozó kivételt (vagyis a különleges kategóriájú adatok kezelésének tilalmát rögzítő főszabály alóli kivételt) és a 6. cikk szerinti jogalapot egyaránt meg kell határoznia.

69. Például elméletben és kivételesen lehet hivatkozni a 9. cikk (2) bekezdésének c) pontjára („*[…] az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges[…]*”), de ez esetben az adatkezelőnek indokolnia kellene, hogy az adatkezelés valamely személy létfontosságú érdekeinek védelméhez elengedhetetlenül szükséges, és bizonyítania kellene, hogy ez „*[…] az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni*”. Ezenkívül az adatkezelő semmilyen egyéb okból nem használhatná a rendszert.

70. Ezzel összefüggésben megjegyzendő, hogy valószínűleg a 9. cikkben felsorolt kivételek egyikével sem indokolható a különleges kategóriájú adatok videokamerás megfigyelés útján történő kezelése.

Konkrétabban azok az adatkezelők, akik a videokamerás megfigyelés keretében ilyen adatokat kezelnek, nem hagyatkozhatnak a 9. cikk (2) bekezdésének e) pontjára, amely lehetővé teszi az érintett által kifejezetten nyilvánosságra hozott személyes adatok kezelését. Pusztán a kamera látóterébe való belépés tényéből nem következik az, hogy az érintett a rá vonatkozó különleges kategóriájú adatokat nyilvánosságra kívánja hozni.

71. Ezenkívül a különleges kategóriájú adatok kezeléséhez kiemelt és folyamatos figyelmet kell fordítani bizonyos kötelezettségek teljesítésére, így például szükség esetén magas szintű biztonságról kell gondoskodni, és adatvédelmi hatásvizsgálatot kell végezni.

> Példa: A munkáltatónak tilos felhasználnia a videokamerás megfigyelés során egy tüntetésről készült felvételeket arra, hogy a sztrájkolókat beazonosítsa.

72.

5.1 Általános szempontok biometrikus adatok kezelésekor

73. A biometrikus adatok felhasználása, különösen az arcfelismerés az érintettek jogaira nézve fokozott kockázatokkal jár. Elengedhetetlenül fontos, hogy az ilyen technológiák csak a jogszerűség, a szükségesség, az arányosság és az adattakarékosság általános adatvédelmi rendeletben rögzített elvének tiszteletben tartása mellett vehetők igénybe. Mivel ezeknek a technológiáknak a használata különösen hatékonynak tekinthető, az adatkezelőknek először az alapvető jogokra és szabadságokra gyakorolt hatást kell vizsgálniuk, és mérlegelniük kell, hogy az adatkezelés jogszerű célja elérhető-e magánszférára kevesebb behatással járó megoldásokkal.

74. A nyers adatok, például egy természetes személy testi, fiziológiai vagy viselkedési jellemzői az általános adatvédelmi rendeletben foglalt fogalommeghatározás szerint akkor minősülnek biometrikus adatnak, ha kezelésük magában foglalja az említett jellemzők mérését. Mivel a biometrikus adatok ilyen mérések eredményeként jönnek létre, az általános adatvédelmi rendelet a 4. cikkének 14. pontjában rögzíti, hogy a biometrikus adat *„[…] egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását […]”.* Egy egyénről készített videofelvétel azonban a 9. cikk szerint önmagában nem tekinthető biometrikus adatnak, ha nem sajátos technikai eljárásokkal nyerték azzal a céllal, hogy elősegítse az egyén azonosítását.[16]

75. Ahhoz, hogy különleges kategóriájú személyes adatok kezelésének legyen tekinthető (9. cikk), a biometrikus adatok kezelésének a „természetes személyek egyedi azonosítását” kell céloznia.

76. Összefoglalva tehát a 4. cikk 14. pontjára és a 9. cikkre tekintettel az alábbi három szempontot kell figyelembe venni:

- **az adatok jellege:** egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó adatok,
- **az adatkezelés eszköze és módja:** az adatokat „sajátos technikai eljárásokkal” kell kinyerni,
- **az adatkezelés célja:** az adatokat természetes személy egyedi azonosítására kell felhasználni.

[16] Az általános adatvédelmi rendelet (51) preambulumbekezdése a következőképpen rendelkezik: *„[a] fényképek kezelését nem szükséges szisztematikusan különleges adatkezelésnek tekinteni, mivel azokra csak azokban az esetekben vonatkozik a biometrikus adatok fogalommeghatározása, amikor a természetes személy egyedi azonosítását vagy hitelesítését lehetővé tevő speciális eszközzel kezelik őket. […]*”.

77. A magánszervezetek által saját (például értékesítési, statisztikai vagy akár biztonsági) célra kiépített, biometrikus azonosítást magában foglaló videokamerás megfigyeléshez többnyire szükséges az összes érintett kifejezett hozzájárulása (a 9. cikk (2) bekezdésének a) pontja), azonban a 9. cikk alapján egyéb megfelelő kivétel is vonatkozhat rá.

> Példa: Egy magánvállalkozás a szolgáltatása fejlesztése céljából a reptéren belüli utasazonosítási ellenőrző pontokat (poggyászfeladás, beszállás) videokamerás megfigyelőrendszerre cseréli, amely arcfelismerési technikákat alkalmaz az utasok személyazonosságának ellenőrzésére, akik úgy döntöttek, hozzájárulnak ehhez az eljáráshoz. Mivel az adatkezelés a 9. cikk hatálya alá tartozik, azoknak az utasoknak, akik előzőleg kifejezett és megfelelő tájékoztatáson alapuló hozzájárulásukat adták, fel kell iratkozniuk például egy automata terminálnál, hogy létrehozzák és nyilvántartásba vegyék a beszállókártyájukhoz és a személyazonosságukhoz társított arcsablonjukat. Az arcfelismeréses ellenőrzési pontokat egyértelműen el kell különíteni, például a rendszert beléptető kapun belülre kell telepíteni, hogy elkerülhető legyen azon személyek biometrikus sablonjának a rögzítése, akik ehhez nem adták hozzájárulásukat. Csak azok az utasok használják a biometrikus rendszerrel felszerelt beléptető kaput, akik előzőleg hozzájárulásukat adták, és feliratkoztak.
>
> Példa: Egy adatkezelő arcfelismeréses módszert alkalmaz az épületébe történő beléptetéshez. Az emberek csak így léphetnek be, ha előzetesen kifejezett és megfelelő tájékoztatáson alapuló hozzájárulásukat adták (a 9. cikk (2) bekezdésének a) pontja). Azonban annak elkerülésére, hogy bárkit az előzetes hozzájárulása nélkül rögzítsenek, az arcfelismerést magának az érintettnek kell elindítania, például gombnyomással. Az adatkezelés jogszerűségének biztosítása érdekében az adatkezelőnek mindig kínálnia kell alternatív, biometrikus adatkezelés nélküli lehetőséget az épületbe való belépéshez, például belépőkártya vagy kulcs formájában.

78.

79. Az ilyen esetekben, amikor biometrikus sablonok készülnek, az adatkezelőknek gondoskodniuk kell arról, hogy miután eredményként egyezést vagy nem egyezést kaptak, az érintettek által a feliratkozáskor létrehozott sablonnal való összehasonlítás céljából menet közben (az érintettek kifejezett és megfelelő tájékoztatáson alapuló hozzájárulásával) készített összes sablont azonnal és biztonságosan törlik. A feliratkozás céljából készített sablonokat kizárólag az adatkezelés céljának megvalósításához szabad megőrizni, és tilos tárolni vagy archiválni.

80. Ha azonban az adatkezelés célja például a személyek kategóriáinak egymástól való megkülönböztetése, és nem az egyének egyedi azonosítása, akkor az adatkezelés nem tartozik a 9. cikk hatálya alá.

> Példa: Egy üzlettulajdonos személyre szabott reklámokat szeretne készíteni a vevők videokamerás megfigyelőrendszerrel rögzített nemi és életkori sajátosságai alapján. Ha a rendszer nem hoz létre biometrikus sablonokat, hogy egyedileg azonosítsa a személyeket, hanem csak az említett testi jellemzőket észleli a személyek besorolása érdekében, akkor az adatkezelés nem tartozik a 9. cikk hatálya alá (amennyiben nem kezelnek semmilyen egyéb, különleges kategóriájú adatot).

81.

82. Azonban a 9. cikk irányadó akkor, ha az adatkezelő tárolja a biometrikus adatokat (leggyakrabban a nyers formában létező biometrikus adatokból [például kép alapján készített arcmérésekből] kinyert főbb sajátosságokból készített sablonokként) a személyek egyedi azonosítása céljából. Ha az adatkezelő szeretné észlelni, hogy az érintettek újra belépnek a területre vagy másik területre lépnek

be (például azért, hogy folyamatosan személyre szabott reklámokat jelenítsen meg nekik), akkor ebben az esetben a cél a természetes személyek egyedi azonosítása, tehát a tevékenység kezdettől fogva a 9. cikk hatálya alá tartozik. Előállhat ez a helyzet akkor, ha az adatkezelő azért tárolja a létrehozott sablonokat, hogy még inkább személyre szabott reklámokat helyezzen el az üzlet különböző pontjain található hirdetőtáblákon. Mivel a rendszer testi jellemzőket használ a kamera látóterébe visszatérő konkrét egyének (például a bevásárlóközpont látogatói) észlelésére és nyomon követésére, ez biometrikus azonosítási módszernek minősül, mivel sajátos technikai eljárásokkal történő felismerésre irányul.

Példa: Egy üzlettulajdonos arcfelismerő rendszert telepített üzletébe, hogy személyre szabott reklámokat jelenítsen meg az egyének számára. Az adatkezelőnek be kell szereznie az összes érintett kifejezett és megfelelő tájékoztatáson alapuló hozzájárulását, mielőtt a biometrikus azonosító rendszert használná, és személyre szabott reklámokat jelenítene meg. A rendszer jogszerűtlen lenne, ha azokat a látogatókat vagy járókelőket is rögzítené, akik nem járultak hozzá biometrikus sablonjuk létrehozásához, még abban az esetben is, ha a sablont a lehető legrövidebb időn belül törlik. Ezek az ideiglenes sablonok valójában olyan személyek egyéni azonosítása céljából kezelt biometrikus adatokat tartalmaznak, akik nem feltétlenül kívánnak célzott reklámokat kapni.

83.

84. Az Európai Adatvédelmi Testület megjegyzi, hogy bizonyos biometrikus rendszereket ellenőrizetlen környezetben telepítenek[17], ami azt jelenti, hogy a rendszer menet közben rögzíti és biometrikus sablonok létrehozására használja fel a kamera látóterében elhaladó összes egyén arcát, köztük azokét is, akik nem járultak hozzá a biometrikus eszköz használatához. Ezek a sablonok hasonlóak azokhoz a sablonokhoz, amelyek az érintettek (vagyis a biometrikus eszközt használók) feliratkozás során adott előzetes hozzájárulásával készültek azért, hogy az adatkezelő azonosíthassa, kik a biometrikus eszközt használók és kik nem. Ebben az esetben a rendszert gyakran úgy alakítják ki, hogy az adatbázis alapján azonosítandó egyéneket megkülönböztesse azoktól, akik nem iratkoztak fel. Mivel a cél természetes személyek egyedi azonosítása, változatlanul szükség van az általános adatvédelmi rendelet 9. cikkének (2) bekezdése szerinti kivételre mindazok számára, akikről felvételt készít a kamera.

[17] Tehát a biometrikus eszköz nyilvános helyen található, és minden elhaladó személyen működik, ellentétben az ellenőrzött környezetben üzemelő biometrikus rendszerekkel, amelyek kizárólag a hozzájáruló személyek közreműködésével használhatók.

Példa: Egy szálloda arra használja a videokamerás megfigyelést, hogy automatikusan figyelmeztesse a szállodaigazgatót a kiemelten fontos (VIP) vendégek érkezésére az arcuk felismerése alapján. Ezek a kiemelten fontos vendégek előzőleg kifejezetten hozzájárultak az arcfelismerés használatához, mielőtt bekerültek volna az e célra létrehozott adatbázisba. Ezek a biometrikus adatokat kezelő rendszerek jogszerűtlenek lennének, ha az összes többi (a kiemelten fontos vendégek azonosítása céljából) megfigyelt vendég nem járulna hozzá az adatkezeléshez az általános adatvédelmi rendelet 9. cikke (2) bekezdésének a) pontja szerint.

Példa: Egy adatkezelő arcfelismeréssel ellátott videokamerás megfigyelőrendszert telepít az általa üzemeltetett koncertterem bejáratához. Az adatkezelőnek egyértelműen elkülönített bejáratokat kell kialakítania: egyet biometrikus rendszerrel, egyet pedig anélkül (ahol például leolvassák a jegyeket). A biometrikus eszközökkel felszerelt bejáratokat úgy kell kialakítani és megközelíthetővé tenni, hogy a rendszer ne rögzíthesse azoknak a nézőknek a biometrikus sablonját, akik nem adták hozzájárulásukat.

85.

86. Végezetül pedig abban az esetben, ha az általános adatvédelmi rendelet 9. cikke értelmében hozzájárulásra van szükség, az adatkezelő nem kötheti szolgáltatásai igénybevételét a biometrikus adatkezeléshez való hozzájáruláshoz. Tehát különösen akkor, ha a biometrikus adatkezelést hitelesítés céljára használja, az adatkezelőnek biometrikus adatkezeléssel nem járó, alternatív megoldást kell kínálnia anélkül, hogy az érintettre korlátozásokat vagy többletköltséget róna. Erre az alternatív megoldásra van szükség a biometrikus eszközre vonatkozó kikötéseknek meg nem felelő személyeknél is (a feliratkozás vagy a biometrikus adatok olvasása nem lehetséges, használatát fogyatékosság nehezíti stb.), a biometrikus eszköz működésképtelenségére (például meghibásodására) való felkészülés céljából pedig „tartalékmegoldásról" kell gondoskodni a kínált szolgáltatás folytonosságának biztosítása érdekében, de használata csak kivételes esetekre korlátozódhat. Kivételes esetekben előfordulhat, hogy a biometrikus adatok kezelése a szerződés alapján nyújtott szolgáltatás szerinti fő tevékenység. Ha például egy múzeum az arcfelismerő eszköz használatát bemutató kiállítást szervez, az érintett nem tagadhatja meg a biometrikus adatok kezelését, amennyiben részt kíván venni a kiállításon. Ez esetben a 9. cikkében előírt hozzájárulás akkor is érvényes, ha a 7. cikkben rögzített követelmények teljesülnek.

5.2 A biometrikus adatok kezelésével járó kockázatok minimalizálására javasolt intézkedések

87. Az adatkezelőknek az adattakarékosság elvével összhangban gondoskodniuk kell arról, hogy a digitális képről sablon létrehozása céljából kinyert adatok köre ne legyen túlzottan széles, és csak az adott célra szükséges információkra korlátozódjon, ezzel elkerülve az esetleges további adatkezelést. Intézkedéseket kell hozni annak biztosítása érdekében, hogy ne lehessen sablonokat továbbítani biometrikus rendszerek között.

88. Az azonosításhoz és a hitelesítéshez vagy ellenőrzéshez valószínűleg tárolni kell a sablonokat a későbbi összehasonlítás céljából. Az adatkezelőnek a legmegfelelőbb helyet kell megtalálnia az adatok tárolására. Ellenőrzött környezetben (elkerített folyosók vagy ellenőrző pontok) a sablonokat külön eszközön kell tárolni, amelyet a felhasználó magánál tart, és amely felett kizárólagos ellenőrzést gyakorol (okostelefon vagy személyazonosító igazolvány), vagy amennyiben konkrét célokra és objektív igények megléte esetén szükségesek, akkor központi adatbázisban, titkosított formában kell tárolni őket úgy, hogy a rejtjelkulcs vagy titkos kód a sablonhoz vagy a tárolási helyhez való jogosulatlan hozzáférés megelőzése érdekében az adott személynél legyen. Ha elkerülhetetlen, hogy az adatkezelő

hozzáférjen a sablonokhoz, akkor az adatkezelőnek megfelelő intézkedésekkel kell gondoskodnia a tárolt adatok biztonságáról. Ilyen intézkedés lehet a sablon titkosítása kriptográfiai algoritmussal.

89. Az adatkezelőnek minden esetben meg kell tennie minden szükséges óvintézkedést a kezelt adatok rendelkezésre állásának, integritásának és bizalmas jellegének megőrzése érdekében. Ebből a célból az adatkezelőnek különösen a következő intézkedéseket kell meghoznia: az adatok elkülönítése továbbítás és tárolás során, a biometrikus sablonok és a nyers adatok vagy személyazonossági adatok különálló adatbázisban tárolása, a biometrikus adatok, különösen a biometrikus sablonok titkosítása, továbbá a titkosításra és a rejtjelkulcskezelésre vonatkozó szabályzat kidolgozása, a csalás feltárására irányuló szervezeti és technikai intézkedés integrálása, integritási kód (például aláírás vagy hash) társítása az adatokhoz, valamint a biometrikus adatokhoz való külső hozzáférés letiltása. Az ilyen intézkedéseknek követniük kell a technológia fejlődését.

90. Ezenkívül az adatkezelőknek törölniük kell a nyers adatokat (arcképeket, beszédjeleket, járásmódokat stb.), és meg kell győződniük a törlés eredményességéről. Ha az adatkezelés jogalapja megszűnik, a nyers anyagokat törölni kell. Sőt, amennyiben biometrikus sablonok készültek ilyen adatok alapján, akkor az adatbázisok összeállítása ugyanakkora, de talán még nagyobb veszélynek tekinthető (mivel a biometrikus sablon nem mindig olvasható könnyen annak ismerete nélkül, hogy hogyan programozták, mivel minden sablon nyers adatokból épül fel). Amennyiben az adatkezelőnek meg kellene őriznie az ilyen adatokat, akkor érdemes megvizsgálni a „zaj” hozzáadásának (például vízjelezésnek) a lehetőségét, ami eredménytelenné tenné a sablon létrehozását. Az adatkezelőnek emellett akkor is törölnie kell a biometrikus adatokat és sablonokat, ha az olvasó-összehasonlító terminálhoz vagy a tárkiszolgálóhoz való illetéktelen hozzáférés merül fel, továbbá törölnie kell mindazokat az adatokat, amelyek további adatkezeléshez már nem hasznosak a biometrikus eszköz élettartamának végén.

6 AZ ÉRINTETT JOGAI

91. A videokamerás megfigyelés keretében végzett adatkezelés jellegéből adódóan az érintettek általános adatvédelmi rendeletben biztosított jogainak egy része alaposabb tisztázást igényel. Ez a fejezet azonban nem kimerítő jellegű, az általános adatvédelmi rendelet szerinti összes jog érvényesül a személyes adatok videokamerás megfigyeléssel történő kezelésére.

6.1 Hozzáféréshez való jog

92. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. A videokamerás megfigyelés esetében ez azt jelenti, hogy amennyiben semmilyen módon nem tárolnak vagy továbbítanak adatokat, akkor a valós idejű megfigyelés idejének letelte után az adatkezelő csak arról adhat tájékoztatást, hogy személyes adatok kezelése már nincs folyamatban (a 13. cikk szerinti általános tájékoztatási kötelezettségek mellett, lásd a *7. fejezetet [Átláthatósági és tájékoztatási kötelezettségek]*). Ha azonban a kérelem benyújtásakor még mindig folyamatban van az adatkezelés (vagyis az adatokat tárolják vagy bármilyen más módon folyamatosan kezelik), akkor az érintettnek a 15. cikk szerint hozzáférést és tájékoztatást kell kapnia.

93. Létezik azonban több olyan korlátozás, amely egyes esetekben érintheti a hozzáférési jogot.

- Az általános adatvédelmi rendelet 15. cikkének (4) bekezdése, mások jogaira gyakorolt hátrányos hatás

94. Mivel ugyanazon a videokamerás megfigyelésről készített felvételen bármennyi érintett megörökíthető, a szűrés más érintettek személyes adatainak további kezelését eredményezné. Hátrányosan érintheti a videofelvételen szereplő más érintettek jogait és szabadságait, ha az érintett szeretné megkapni a felvétel másolati példányát (a 15. cikk (3) bekezdése). Ennek elkerülése érdekében ezért az adatkezelőnek figyelembe kell vennie, hogy bizonyos esetekben előfordulhat, hogy a videofelvételt annak magánszférára nagy behatással járó jellege miatt nem adhatja ki, ha más érintettek is felismerhetők rajta. A harmadik felek jogainak védelme azonban nem használható kifogásként az egyének hozzáférés iránti jogos igényének megtagadására, ezért az adatkezelőnek technikai intézkedéseket (például képszerkesztés, ezen belül elfedés vagy eltorzítás) kell hoznia ilyen esetekre, hogy teljesíteni tudja a hozzáférési kérelmet. Az adatkezelők azonban nem kötelesek ilyen technikai intézkedéseket végrehajtani, ha más módon is gondoskodhatnak arról, hogy a 15. cikk szerinti kérelemre a 12. cikk (3) cikkében előírt határidőn belül válaszolni tudnak.

- Az általános adatvédelmi rendelet 11. cikkének (2) bekezdése, az adatkezelő nem tudja azonosítani az érintettet

95. Ha a videofelvételen nem kereshetők személyes adatok (vagyis az adatkezelőnek valószínűleg nagy mennyiségű tárolt anyagot kellene feldolgoznia ahhoz, hogy megtalálja a kérdéses érintettet), akkor előfordulhat, hogy az adatkezelő nem tudja azonosítani az érintettet.

96. Következésképpen az érintettnek az adatkezelőhöz intézett kérelmében (önmaga személyazonosító okmánnyal, személyesen vagy egyéb módon történő azonosítása mellett) azt is meg kell adnia, hogy a felvételen szereplő érintettek számával arányos, észszerű időkereten belül mikor lépett be a megfigyelt területre. Az adatkezelőnek előzetesen tájékoztatnia kell az érintettet arról, milyen információkra lesz szüksége a kérelem teljesítéséhez. Ha az adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint megfelelő módon tájékoztatnia kell őt. Ilyen helyzetben az adatkezelőnek az érintett részére adott

válaszában tájékoztatást kell nyújtania a megfigyeléssel érintett területről, a használt kamerák ellenőrzéséről stb., hogy az érintett teljesen tisztában legyen azzal, hogy az adatkezelő mely személyes adatait kezelhette.

> Példa: Ha az érintett a napi 30 000 látogatót fogadó bevásárlóközpont bejáratánál folytatott videokamerás megfigyelés útján kezelt személyes adatairól kér másolatot, akkor megközelítőleg egyórás időkereten belül kell megadnia, mikor haladt át a megfigyelt területen. Ha az adatkezelő még kezeli az anyagot, akkor át kell adnia a videofelvétel másolati példányát. Ha ugyanazon felvétel alapján más érintettek is azonosíthatók, akkor az adatkezelőnek az anyag adott részét felismerhetetlenné kell tennie (például a teljes másolati példány vagy bizonyos részei elhomályosításával), mielőtt átadná a példányt a kérelmet benyújtó érintettnek.
>
> Példa: Ha az adatkezelő például két napon belül automatikusan töröl minden felvételt, akkor e két nap elteltével nem tudja biztosítani a felvételt az érintettnek. Ha az adatkezelő e két nap eltelte után kapja meg a kérelmet, akkor ennek megfelelően kell tájékoztatnia az érintettet.

97.

- Az általános adatvédelmi rendelet 12. cikke, túlzó kérelmek

98. Amennyiben az érintett kérelme túlzó vagy egyértelműen megalapozatlan, az adatkezelő az általános adatvédelmi rendelet 12. cikke (5) bekezdésének a) pontja szerint észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést (az általános adatvédelmi rendelet 12. cikke (5) bekezdésének b) pontja). Az adatkezelőnek tudnia kell bizonyítani a kérelem egyértelműen megalapozatlan vagy túlzó jellegét.

6.2 A törléshez való jog és a tiltakozáshoz való jog

6.2.1 A törléshez való jog (az elfeledtetéshez való jog)

99. Ha az adatkezelő a valós idejű megfigyelésen túl is folytatja a személyes adatok kezelését (például tárolás útján), akkor az érintett az általános adatvédelmi rendelet 17. cikke szerint kérelmezheti a személyes adatok törlését.

100. Az adatkezelő a kérelem alapján köteles a személyes adatokat indokolatlan késedelem nélkül törölni, ha az általános adatvédelmi rendelet 17. cikkének (1) bekezdésében felsorolt körülmények valamelyike fennáll (és az általános adatvédelmi rendelet 17. cikkének (3) bekezdésében felsorolt kivételek közül pedig egyik sem alkalmazható). E körbe tartozik az a kötelezettség is, miszerint a személyes adatokat törölni kell, ha már nincs rájuk szükség arra a célra, amelyre eredetileg tárolták őket, vagy az adatkezelés jogszerűtlen (lásd még a *8. fejezetet [Az adattárolás időtartama és törlési kötelezettség]*). Ezenfelül az adatkezelés jogalapjától függően a személyes adatokat törölni kell:

- *hozzájárulás esetén*: akkor, ha a hozzájárulást visszavonják (és az adatkezelésnek nincs más jogalapja);
- *jogos érdekkel összefüggésben*:
    - akkor, ha az érintett gyakorolja a tiltakozáshoz való jogát (lásd a *6.2.2. alszakaszt*), és az adatkezelésnek nincs elsőbbséget élvező, kényszerítő erejű jogos oka; vagy
    - közvetlen üzletszerzés esetén (ideértve a profilalkotást is) akkor, ha az érintett tiltakozik az adatkezelés ellen.

101. Ha az adatkezelő nyilvánosságra hozta a videofelvételt (például internetes sugárzás vagy közvetítés útján), akkor meg kell tennie az észszerűen elvárható lépéseket annak érdekében, hogy az általános

adatvédelmi rendelet 17. cikkének (2) bekezdése szerint tájékoztasson más (a szóban forgó személyes adatokat aktuálisan kezelő) adatkezelőket a kérelemről. Az elérhető technológia és a megvalósítás költségeinek figyelembevételével észszerűen elvárható lépések között lenniük kell technikai intézkedéseknek. Amennyiben lehetséges, az adatkezelőnek az általános adatvédelmi rendelet 19. cikke értelmében a személyes adatok törlésekor értesítenie kell mindenkit, akivel a személyes adatokat előzőleg közölte.

102. A személyes adatok érintett kérelmére történő törlésére vonatkozó kötelezettségén túlmenően az adatkezelő az általános adatvédelmi rendelet alapelvei szerint köteles korlátozni a tárolt személyes adatok körét (lásd a *8. fejezetet*).

103. A videokamerás megfigyeléssel kapcsolatosan érdemes megjegyezni, hogy a személyes adatok az általános adatvédelmi rendelet értelmében töröltnek minősülnek, ha a képet például elhomályosítják úgy, hogy visszamenőlegesen nem nyerhetők ki a korábban a képen látható személyes adatok.

> Példa: Egy vegyeskereskedésnek problémát okoz a rongálás, amely főként a külsejét érinti, ezért videokamerás megfigyelést alkalmaz a bejáratán kívül, közvetlenül a falaknál. Egy járókelő kérelmezi személyes adatai törlését attól a pillanattól kezdve. Az adatkezelő köteles a kérelemre indokolatlan késedelem nélkül, de legkésőbb egy hónapon belül válaszolni. Mivel a szóban forgó felvétel már nem felel meg a célnak, amelyre eredetileg tárolták (nem történt rongálás, miközben az érintett elhaladt), ezért az adatok tárolásához a kérelem időpontjában nem fűződik jogos érdek, amely elsőbbséget élvezne az érintettek érdekeivel szemben. Az adatkezelőnek törölnie kell a személyes adatokat.

104.

6.2.2 A tiltakozáshoz való jog

105. A *jogos érdeken* (az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontján) alapuló videokamerás megfigyelés vagy *közérdekű* feladat (az általános adatvédelmi rendelet 6. cikke (1) bekezdésének e) pontja) végrehajtásának szükségessége esetén az érintett az általános adatvédelmi rendelet 21. cikke értelmében jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon. Ha az adatkezelő nem bizonyítja az érintett jogaival és érdekeivel szemben elsőbbséget élvező, kényszerítő erejű jogos okok meglétét, akkor fel kell hagynia a tiltakozó egyén adatainak kezelésével. Az adatkezelő az érintett kérelmére köteles indokolatlan késedelem nélkül, de legkésőbb egy hónapon belül válaszolni.

106. A videokamerás megfigyeléssel összefüggésben ez a tiltakozás megfogalmazható a megfigyelt területre való belépéskor, az ott-tartózkodás során vagy az onnan való távozás után. A gyakorlatban ez azt jelenti, hogy amennyiben az adatkezelőnek nincs kényszerítő erejű jogos oka, akkor csak az alábbi esetekben jogszerű annak a területnek a megfigyelése, ahol természetes személyek azonosíthatóak:

(1) az adatkezelő kérelemre azonnal gondoskodni tud arról, hogy a kamera ne kezeljen személyes adatokat, vagy

(2) a megfigyelt terület olyan részletesen korlátozott, hogy az adatkezelő még a területre való belépés előtt be tudja szerezni az érintett hozzájárulását, és az érintett polgárként nem jogosult belépni erre a területre.

107. Ennek az iránymutatásnak nem célja meghatározni, mi minősül *kényszerítő erejű* jogos érdeknek (az általános adatvédelmi rendelet 21. cikke).

108. A videokamerás megfigyelés közvetlen üzletszerzésre való használata esetén az érintett jogosult saját belátása szerint tiltakozni az adatkezelés ellen, mivel a tiltakozáshoz való jog ebben az összefüggésben abszolút jog (az általános adatvédelmi rendelet 21. cikkének (2) és (3) bekezdése).

> Példa: Egy vállalkozásnak gondot okoznak a nyilvános bejáratán keresztüli illetéktelen behatolások, ezért jogos érdek alapján videokamerás megfigyelést folytat azzal a céllal, hogy tetten érje a jogellenesen belépőket. Az egyik látogató saját helyzetével kapcsolatos okokból tiltakozik személyes adatai videokamerás megfigyelőrendszerrel való kezelése ellen. A vállalkozás viszont ez esetben visszautasítja a kérelmet azzal az indoklással, hogy a tárolt felvételre szüksége van egy folyamatban lévő belső vizsgálathoz, tehát kényszerítő erejű jogos oka van a személyes adatok kezelésének folyatására.

109.

7 ÁTLÁTHATÓSÁGI ÉS TÁJÉKOZTATÁSI KÖTELEZETTSÉGEK[18]

110. Az európai adatvédelmi jogból régóta következik, hogy az érintetteknek tisztában kell lenniük azzal, hogy videokamerás megfigyelés folyik. A megfigyelt helyekről részletes tájékoztatást kell kapniuk.[19] Az általános adatvédelmi rendeletben az általános átláthatósági és tájékoztatási kötelezettségeket a 12. és azt követő cikkek rögzítik. Részletesebb felvilágosítást nyújt a 29. cikk szerinti munkacsoport (EU) 2016/679 rendelet szerinti átláthatóságról szóló iránymutatása (WP260), amelyet az Európai Adatvédelmi Testület 2018. május 25-én hagyott jóvá. A WP260. sz. dokumentum 26. pontjával összhangban az általános adatvédelmi rendelet 13. cikke alkalmazandó abban az esetben, ha „[…] az érintettől megfigyelés útján […] (pl. automatizált adatgyűjtő eszközök vagy adatgyűjtő szoftverek, például kamerák […] használata)” gyűjtenek személyes adatokat.

111. Az érintett által közlendő információk mennyiségére tekintettel az adatkezelő többszintű megközelítést követhet, amely esetben az átláthatóság biztosítása érdekében több módszer kombinációjának alkalmazása mellett dönthet (WP260, 35. pont; WP89, 22. pont). A videokamerás megfigyelést illetően a legfontosabb információkat a figyelmeztető táblán (első szint) kell feltüntetni, a további kötelező adatok pedig közölhetők más módon (második szint).

7.1 Első szintű tájékoztatás (figyelmeztető tábla)

112. Az első szint az érintettel való első kapcsolatfelvétel elsődleges módja. Ebben a szakaszban az adatkezelők a lényeges információkat megjelenítő figyelmeztető táblákat használhatnak. A megjelenített információkat ikonnal is ki lehet egészíteni annak érdekében, hogy az érintett a tervezett adatkezelésről jól látható, könnyen érthető és jól olvasható formában általános tájékoztatást kapjon (az általános adatvédelmi rendelet 12. cikkének (7) bekezdése). Az információk formátumának az adott helyhez kell igazodnia (WP89, 22. pont).

7.1.1 A figyelmeztető tábla kihelyezése

113. A tájékoztatást úgy kell kihelyezni, hogy az érintett a megfigyelt területre való belépés előtt könnyen felismerhesse a megfigyelés körülményeit (megközelítőleg szemmagasságban). Nem szükséges közölni a kamera helyét, amennyiben nincs kétség azzal kapcsolatosan, mely területek állnak megfigyelés alatt, és a megfigyelés körülményeit egyértelműen tisztázzák (WP89, 22. pont). Az érintettnek fel kell tudnia mérni, mely területet figyeli kamera, hogy elkerülhesse a megfigyelést, vagy szükség esetén ahhoz igazíthassa viselkedését.

7.1.2 Az első szintű tájékoztatás tartalma

114. Az első szintű tájékoztatásnak (figyelmeztető tábla) általában a legfontosabb információkat kell tartalmaznia, így például az adatkezelés céljaira, az adatkezelő kilétére és az érintett jogainak meglétére vonatkozó részletes tudnivalókat, valamint az adatkezelés legnagyobb hatásaival kapcsolatos információkat.[20] Ide tartozhatnak például az adatkezelő (vagy harmadik fél) jogos érdekei és (adott esetben) az adatvédelmi tisztviselő elérhetőségei. Emellett utalni kell a részletesebb, második szintű tájékoztatásra, valamint elérhetőségének helyére és módjára.

---

[18] A nemzeti jogszabályokban rögzített különös rendelkezések alkalmazhatók.

[19] Lásd a 29. cikk szerinti munkacsoport 4/2004. számú véleményét a személyes adatok videokamerás megfigyeléssel történő kezeléséről (WP89).

[20] Lásd a WP260. sz. dokumentum 38. pontját.

115. A táblának ezenkívül az érintett számára esetleg meglepő információkat is tartalmaznia kell (WP260, 38. pont). Ilyen lehet például a harmadik – különösen az Unión kívüli – feleknek történő adattovábbítás ténye és az adattárolás időtartama. Ezen információk hiányában az érintett bízhat abban, hogy csak élő megfigyelés folyik (adatrögzítés vagy harmadik feleknek történő adattovábbítás nélkül).

116.

Példa (nem kötelező erejű javaslat):

Videokamerás megfigyelés!

Az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte:

Elérhetőségek, többek között az adatvédelmi tisztviselő (ha van ilyen) elérhetőségei:

Tájékoztatás az érintettre legnagyobb hatást gyakorló adatkezelésről (például megőrzési időszak vagy élő megfigyelés, a videófelvétel közzététele vagy harmadik feleknek történő továbbítása):

A videokamerás megfigyelés célja(i):

További tájékoztatás kapható:
- értesítés útján,
- a recepciónál/az ügyfélinformációs pultnál/pénztárnál,
- az interneten (URL)…

Az érintettek jogai: Önt, mint érintettet számos jog megilleti, közülük kiemelendő az a jog, hogy kérelmezze az adatkezelőtől a személyes adataihoz való hozzáférést vagy azok törlését.

Ha szeretne többet megtudni a videokamerás megfigyelésről, egyebek mellett megismerné a jogait, tekintse meg az adatkezelő által a bal oldali lehetőségek útján nyújtott, teljes körű tájékoztatást.

7.2 Második szintű tájékoztatás

117. A második szintű tájékoztatást is az érintett számára könnyen hozzáférhető helyen kell rendelkezésre bocsátani, például központi helyen (információs pultnál, recepción vagy pénztárnál) kihelyezett teljes körű tájékoztató lap vagy könnyen észrevehető plakát formájában. A fentieknek megfelelően az első szintű figyelmeztető táblának egyértelműen utalnia kell a második szintű tájékoztatásra. Ezenkívül az első szintű tájékoztatásban érdemes a második szintű tájékoztatás digitális forrására hivatkozni (például QR-kóddal vagy webhely címével). A tájékoztatást ugyanakkor nem digitális formában is könnyen hozzáférhetővé kell tenni. A második szintű tájékoztatásnak a megfigyelt területre való belépés nélkül is rendelkezésre kell állnia, különösen akkor, ha digitálisan bocsátják rendelkezésre (ez megoldható például hivatkozás megadásával). További elfogadható lehetőség a hívható telefonszám megadása. Bármilyen formában is nyújtják a tájékoztatást, annak tartalmaznia kell az általános adatvédelmi rendelet 13. cikke értelmében kötelező összes információt.

118. Az említett lehetőségeken kívül és azok hatékonyabbá tétele érdekében az Európai Adatvédelmi Testület támogatja a technológiai eszközök használatát az érintettek tájékoztatására. E körbe tartozhat például a földrajzi helymeghatározással felszerelt kamerák használata, és az információk térképes alkalmazásokban vagy webhelyeken való feltüntetése, hogy az egyének egyrészről könnyen azonosíthassák és meghatározhassák a jogaik gyakorlásához kapcsolódó videoforrásokat, másrészről részletesebb felvilágosítást kapjanak az adatkezelési műveletről.

Példa: Egy üzlettulajdonos megfigyeli az üzletét. A 13. cikknek megfelelően elegendő az első szintű tájékoztatást nyújtó figyelmeztető táblát kihelyezni az üzlet bejáratánál jól látható helyen. Ezenkívül a második szintű tájékoztatást tartalmazó tájékoztató lapot kell kihelyeznie a pénztárnál vagy az üzleten belül bármilyen egyéb, központi és könnyen megközelíthető helyen.

119.

8 AZ ADATTÁROLÁS IDŐTARTAMA ÉS TÖRLÉSI KÖTELEZETTSÉG

120. A személyes adatok csak a kezelésük céljainak eléréséhez szükséges ideig tárolhatóak (az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) és e) pontja). Egyes tagállamokban az általános adatvédelmi rendelet 6. cikkének (2) bekezdése szerint külön rendelkezések vonatkozhatnak az adattárolás időtartamára a videokamerás megfigyeléssel összefüggésben.

121. Függetlenül attól, hogy a személyes adatok tárolása szükséges-e vagy sem, kezelésüknek szűk időtartamra kell korlátozódnia. Általában véve a videokamerás megfigyelés jogszerű céljai közül gyakran fordul elő a vagyonvédelem és a bizonyítékmegőrzés. A keletkezett károk rendszerint egy vagy két napon belül felismerhetők. Az adatvédelmi keret előírásainak való megfelelés bizonyításának megkönnyítése céljából az adatkezelő érdeke, hogy előzetesen szervezeti intézkedéseket hozzon (például szükség esetén felelős kinevezése a videofelvételek szűrésére és biztonságának szavatolására). Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) és e) pontjában foglalt elvekre, nevezetesen az adattakarékosság és a korlátozott tárolhatóság elvére figyelemmel a személyes adatok az esetek többségében (például rongálás észlelése céljából) néhány nap elteltével – lehetőleg automatikusan – törölhetők. Minél hosszabb a megadott adattárolási időtartam (különösen akkor, ha 72 óránál több), annál több érvvel kell alátámasztani a cél jogszerűségét és az adattárolás szükségességét. Ha az adatkezelő nemcsak a helyiségei és területei ellenőrzése céljából folytat videokamerás megfigyelést, hanem tárolni is kívánja az adatokat, akkor gondoskodnia kell arról, hogy az adattárolásra ténylegesen szükség legyen a cél eléréséhez. Ebben az esetben az adattárolás időtartamát mindegyik cél tekintetében egyértelműen és külön meg kell határozni. Az adatkezelő feladata, hogy a szükségesség és az arányosság elvével összhangban megállapítsa a megőrzési időszakot, és bizonyítsa az általános adatvédelmi rendelet rendelkezéseinek teljesülését.

> Példa: Egy kis üzlet tulajdonosa rendszerint még aznap észreveszi, ha rongálás történik. Következésképpen 24 órás rendes adattárolási időtartam elegendő. A hétvégi zárva tartás vagy hosszabb munkaszüneti időszakok esetén azonban hosszabb adattárolási időtartam lehet indokolt. Kár észlelése esetén előfordulhat, hogy a tulajdonosnak hosszabb ideig kell tárolnia a videofelvételt, hogy az elkövetővel szemben jogi lépéseket tegyen.

122.

9 TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK

123. Az általános adatvédelmi rendelet 32. cikkének (1) bekezdésében foglaltak szerint a videokamerás megfigyelés során végzett személyesadat-kezelésnek nemcsak jogilag megengedettnek kell lennie, hanem az adatkezelőknek és az adatfeldolgozóknak gondoskodniuk kell a megfelelő biztonságáról is. A végrehajtott **szervezési és technikai intézkedéseknek arányosnak** kell lenniük **a természetes személyek jogait és szabadságait érintő kockázatokkal**, amelyek a videokamerás megfigyelési adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan közléséből vagy az azokhoz való jogosulatlan hozzáférésből erednek. Az általános adatvédelmi rendelet 24. és 25. cikke szerint az adatkezelőknek azért is technikai és szervezési intézkedéseket kell hozniuk, hogy az adatkezelés során gondoskodjanak az összes adatvédelmi elv tiszteletben tartásáról, és lehetőséget kell teremteniük arra, hogy az érintettek gyakorolják a 15–22. cikkben meghatározott jogaikat. Az adatkezelőknek belső keretet és szabályzatokat kell bevezetniük, amelyekkel mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során biztosítható a fentiek megvalósítása, ideértve szükség esetén az adatvédelmi hatásvizsgálatok végrehajtását is.

9.1 A videokamerás megfigyelőrendszer áttekintése

124. A videokamerás megfigyelőrendszer[21] analóg és digitális eszközökből, valamint szoftverekből áll, amelyek célja egy adott helyszín képi rögzítése, a képek kezelése és a kezelő számára történő megjelenítése. Összetevői az alábbi kategóriákba sorolhatók:

- videokörnyezet: képrögzítés, összeköttetések és képkezelés:
  - a képrögzítés célja a valós világot ábrázoló kép előállítása a rendszer többi része által használható formátumban,
  - az összeköttetések a videokörnyezeten belüli összes adattovábbítást, vagyis a kapcsolatokat és adatközléseket határozzák meg. A kapcsolatok körébe tartoznak például a kábelek, a digitális hálózatok és a vezeték nélküli adattovábbítás. Az adatközlések közé tartozik az összes video- és vezérlőadat-jel, amely lehet digitális vagy analóg,
  - a képkezelés magában foglalja a kép vagy képsor elemzését, tárolását és ábrázolását;
- rendszerkezelés szempontjából a videokamerás megfigyelőrendszer a következő logikai funkciókkal rendelkezik:
  - adatgazdálkodás és tevékenységirányítás, amely magában foglalja a kezelői parancsok és a rendszer által létrehozott tevékenységek (riasztási eljárások, a kezelő figyelmeztetése) kezelését,
  - a más rendszerekkel fennálló interfészek között lehetnek más biztonsági (beléptető, tűzvédelmi) és nem biztonsági (létesítményüzemeltetési, automatikus rendszámfelismerő) rendszerekkel létesített kapcsolatok;
- a videokamerás megfigyelőrendszer biztonsági eleme a rendszer és az adatok bizalmas jellegére, integritására és rendelkezésre állására terjed ki:
  - a rendszerbiztonság körébe tartozik az összes rendszerösszetevő fizikai biztonsága és a videokamerás megfigyelőrendszerhez való hozzáférés ellenőrzése,
  - az adatbiztonság az adatok elvesztésének vagy manipulálásának megelőzését foglalja magában.

[21] Az általános adatvédelmi rendelet nem tartalmazza a fogalommeghatározását, műszaki leírását például a „Videokamerás megfigyelőrendszerek biztonsági alkalmazásokhoz – 1-1. rész: Rendszerkövetelmények” című EN 62676-1-1:2014 szabvány tartalmazza.

125.

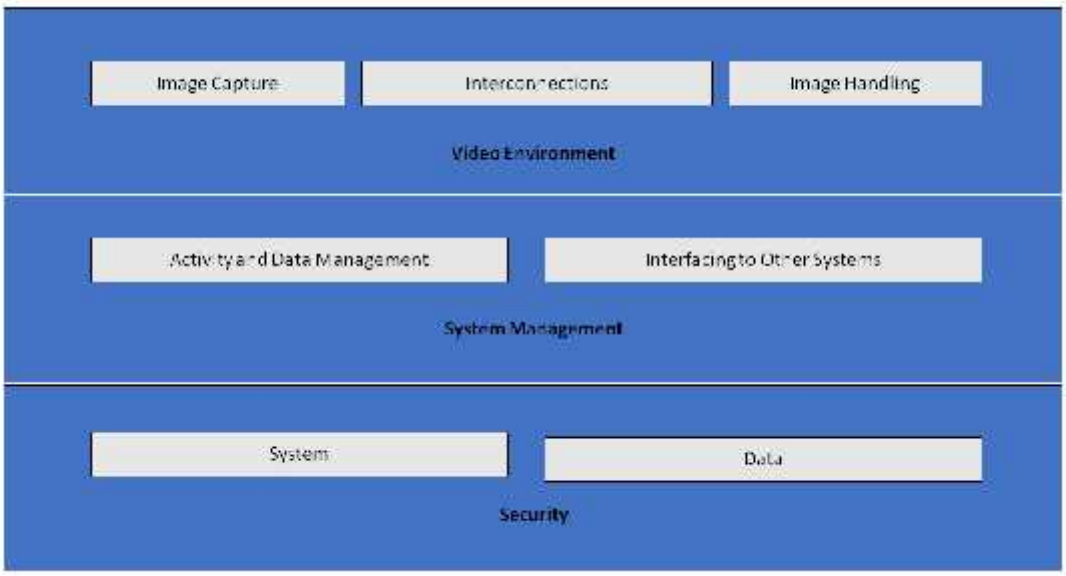

Image Capture	Képrögzítés
Interconnections	Összeköttetések
Image Handling	Képkezelés
Video Environment	Videokörnyezet
Activity and Data Management	Tevékenységirányítás és adatgazdálkodás
Interfacing to Other Systems	Interfészek más rendszerekkel
System Management	Rendszerkezelés
System	Rendszer
Data	Adatok
Security	Biztonság

1. ábra: Videokamerás megfigyelőrendszer

9.2 Beépített és alapértelmezett adatvédelem

126. Az általános adatvédelmi rendelet 25. cikkében foglaltak szerint az adatkezelőknek megfelelő technikai és szervezési intézkedéseket kell hozniuk az adatvédelem érdekében, amikor videokamerás megfigyelést terveznek, még a videofelvételek gyűjtésének és kezelésének megkezdése előtt. Ezek az elvek rávilágítanak arra, hogy a beépített adatvédelmet fokozó technológiákra, az adatkezelést minimalizáló alapértelmezett beállításokra és a személyes adatok lehető legmagasabb szintű védelméhez szükséges eszközök biztosítására van szükség[22].

127. Az adatkezelőknek az adatok és a magánélet védelmét szolgáló garanciákat kell beépíteniük nemcsak a technológiai tervezési előírásokba, hanem a szervezeti gyakorlatokba is. A szervezeti gyakorlatokat illetően az adatkezelőnek megfelelő irányítási keretet kell bevezetnie, továbbá szabályzatokat és eljárásokat kell meghatároznia és érvényesítenie a videokamerás megfigyeléssel összefüggésben. A rendszerekre vonatkozó előírásoknak és terveknek technikai szempontból tartalmazniuk kell a személyes adatok kezelésével kapcsolatos követelményeket az általános adatvédelmi rendelet 5. cikkében foglalt elvekkel összhangban (az adatkezelés jogszerűsége, célhoz kötöttség, korlátozott

[22] Vélemény a magánélet jövőjéről (WP168), a 29. cikk szerinti munkacsoport és a rendőrségi és igazságügyi munkacsoport (2009. december 1-jén elfogadott) közös hozzájárulása az Európai Bizottság által a személyes adatok védelméhez való alapvető jogra vonatkozó jogi keretről folytatott konzultációhoz.

tárolhatóság, az általános adatvédelmi rendelet 25. cikkének (2) bekezdése szerint alapértelmezett adattakarékosság, integritás és bizalmas jelleg, elszámoltathatóság stb.). Amennyiben az adatkezelő kereskedelmi videokamerás megfigyelőrendszer beszerzését tervezi, ezt fel kell tüntetnie a vásárlási leírásban. Az adatkezelőnek oly módon kell gondoskodnia ezeknek a követelményeknek a teljesüléséről, hogy a követelményeket a rendszer összes összetevőjére és a vele feldolgozott összes adatra alkalmazza a teljes élettartamuk alatt.

9.3 Konkrét példák releváns intézkedésekre

128. A videokamerás megfigyelés biztonságának szavatolásához végrehajtható intézkedések többsége – különösen digitális berendezések és szoftverek használata esetén – nem tér el a más informatikai rendszereknél alkalmazott intézkedésektől. Ugyanakkor az adatkezelőnek a kiválasztott megoldástól függetlenül gondoskodnia kell a videokamerás megfigyelőrendszer összetevőinek és az adatoknak a megfelelő védelméről minden szakaszban, vagyis a tárolás (inaktív adatok), a továbbítás (átvitel alatt lévő adatok) és a kezelés (aktív adatok) során. Ehhez szükség van arra, hogy az adatkezelők és az adatfeldolgozók szervezési és technikai intézkedéseket egyaránt alkalmazzanak.

129. A technikai megoldások kiválasztásakor az adatkezelőnek a magánélet védelme szempontjából előnyös technológiákat érdemes választania, egyebek mellett azért, mert fokozzák a biztonságot. Ilyen technológiák közé tartoznak például azok a rendszerek, amelyek a videofelvétel érintetteknek való átadása esetén lehetővé teszik a megfigyelés szempontjából lényegtelen területek maszkolását vagy eltorzítását, illetve harmadik felek képekről való kiszerkesztését.[23] Másrészről viszont a kiválasztott megoldások nem tartalmazhatnak szükségtelen funkciókat (például a kamerák korlátlan mozgatása, nagyítási képesség, rádiós átvitel, elemzés és hangfelvétel-készítés). A meglévő, de nem szükséges funkciókat ki kell kapcsolni.

130. Ennek a témakörnek gazdag szakirodalma van, ide sorolhatók például a multimédia-rendszerekre[24] és az általános informatikai rendszerek biztonságára[25] vonatkozó nemzetközi szabványok és műszaki leírások. Ez a szakasz tehát csak nagy vonalakban nyújt áttekintést erről a témakörről.

9.3.1 Szervezési intézkedések

131. Az esetlegesen szükséges adatvédelmi hatásvizsgálaton kívül (lásd a *10. fejezetet*) az adatkezelőknek az alábbi kérdéseket érdemes mérlegelniük saját videokamerás megfigyelési szabályzataik és eljárásaik kidolgozása során:

- ki felelős a videokamerás megfigyelőrendszer kezeléséért és üzemeltetéséért;
- a videokamerás megfigyelési beruházás célja és terjedelme;
- megfelelő és tiltott használat (hol és mikor megengedett a videokamerás megfigyelés, illetve hol és mikor nem; például rejtett kamerák használata és hangrögzítés a videofelvétel készítésén túl)[26];
- a *7. fejezetben (Átláthatósági és tájékoztatási kötelezettségek)* foglaltak szerinti átláthatósági intézkedések;

[23] Ilyen technológiák használata egyes esetekben még kötelező is lehet az 5. cikk (1) bekezdésének c) pontjában foglalt rendelkezések teljesítése érdekében. Mindenesetre példaként szolgálhatnak bevált módszerekre.

[24] IEC TS 62045 szabvány: Multimédiás biztonság – Iránymutatás a magánélet védelméhez használatban lévő és használaton kívüli berendezések és rendszerek esetében.

[25] ISO/IEC 27000 szabványsorozat: Információbiztonság-irányítási rendszerek.

[26] Ez a nemzeti jogszabályoktól és ágazati szabályozásoktól függhet.

- a videofelvételek rögzítésének módja és időtartama, ideértve a biztonsági incidensekhez kapcsolódó videofelvételek archiválását;
- kinek és mikor kell elvégeznie a vonatkozó képzést;
- ki férhet hozzá a videofelvételekhez és milyen céllal;
- működési eljárások (például ki és honnan végzi a videokamerás megfigyelést, mi a teendő adatvédelmi incidens esetén);
- milyen eljárásokat kell követniük külső feleknek a videofelvételek kérelmezéséhez, és milyen eljárások vonatkoznak az ilyen kérelmek megtagadására vagy teljesítésére;
- a videokamerás megfigyelőrendszer beszerzésére, telepítésére és karbantartására vonatkozó eljárások;
- incidenskezelési és helyreállítási eljárások.

9.3.2 Technikai intézkedések

132. A **rendszerbiztonság** az összes rendszerösszetevő **fizikai biztonsága**, a rendszer integritása, vagyis **a rendszer rendes működésébe való szándékos vagy nem szándékos beavatkozással szembeni védelem és ellenálló képesség** és a **hozzáférés szabályozása**. Az adatbiztonság a **bizalmasságot** (az adatokhoz kizárólag azok férhetnek hozzá, akik erre jogosultságot kaptak), az **integritást** (az adatok elvesztésének vagy manipulálásának megelőzése) és a **rendelkezésre állást** (az adatok hozzáférhetőek, amikor szükség van rájuk) jelenti.

133. A **fizikai biztonság** az adatvédelem elengedhetetlen része, és az első védelmi vonalat képezi, mivel védi a videokamerás megfigyelőrendszer berendezéseit lopás, rongálás, természeti katasztrófa, ember okozta katasztrófa és véletlen kár (például túlfeszültség, szélsőséges hőmérséklet vagy kiöntött kávé miatti kár) ellen. Analóg rendszerek esetében a fizikai biztonság a legfontosabb a védelem szempontjából.

134. A **rendszer- és az adatbiztonság**, vagyis a rendes működésébe való szándékos vagy akaratlan beavatkozással szembeni védelem körébe az alábbiak tartozhatnak:

- a videokamerás megfigyelőrendszer teljes infrastruktúrájának (ideértve a távműködtetésű kamerákat, a vezetékeket és a tápellátást) védelme fizikai manipulálás és lopás ellen;
- a felvételek továbbításának védelme lehallgatás ellen védett kommunikációs csatornákon keresztül;
- adattitkosítás;
- hardver- és szoftveralapú megoldások, például tűzfalak, vírusirtók vagy behatolásjelző rendszerek használata kibertámadások ellen;
- összetevők, szoftverek és összeköttetések meghibásodásának észlelése;
- fizikai vagy műszaki incidens esetén a rendszer rendelkezésre állásának és hozzáférhetőségének helyreállítására szolgáló eszközök.

135. A **hozzáférés szabályozásával** biztosítható, hogy csak az arra jogosult személyek férhessenek hozzá a rendszerhez és az adatokhoz, mások pedig ne tehessék meg. A hozzáférés fizikai és logikai szabályozását támogató intézkedések közé tartoznak az alábbiak:

- annak biztosítása, hogy a videokamerás megfigyeléssel érintett és a videofelvétel tárolására használt összes terület és helyiség védelmet élvezzen a harmadik felek általi, felügyelet nélküli hozzáféréssel szemben;
- a monitorok oly módon történő elhelyezése (különösen nyitott terekben, például recepción), hogy azokat csak az arra jogosult kezelők láthassák;
- a fizikai és logikai hozzáférés megadására, módosítására és visszavonására vonatkozó eljárások meghatározása és érvényesítése;

- a felhasználói hitelesítésre és engedélyezésre szolgáló módszerek és eszközök bevezetése, például a jelszavak hosszának és módosítási gyakoriságának meghatározására;
- a felhasználók által (a rendszerben és az adatokon egyaránt) végrehajtott műveletek rögzítése és rendszeres felülvizsgálata;
- a sikertelen hozzáférések folyamatos figyelemmel kísérése és észlelése, valamint a feltárt hiányosságok mielőbbi orvoslása.

10 ADATVÉDELMI HATÁSVIZSGÁLAT

136. Az általános adatvédelmi rendelet 35. cikkének (1) bekezdése szerint az adatkezelőknek adatvédelmi hatásvizsgálatot kell végezniük, ha valamilyen adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az általános adatvédelmi rendelet 35. cikke (3) bekezdésének c) pontja rögzíti, hogy az adatkezelőknek adatvédelmi hatásvizsgálatot kell végezniük, ha az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelésének minősül. Ezenkívül az általános adatvédelmi rendelet 35. cikke (3) bekezdésének b) pontja szerint akkor is szükség van adatvédelmi hatásvizsgálatra, ha az adatkezelő nagy számban kíván kezelni különleges kategóriájú személyes adatokat.

137. Az adatvédelmi hatásvizsgálatról szóló iránymutatás[27] további tanácsokkal és részletesebb példákkal szolgál a videokamerás megfigyeléssel összefüggésben (például „kamerarendszer használata az autóvezetői magatartás megfigyelésére az autópályákon"). Az általános adatvédelmi rendelet 35. cikkének (4) bekezdése előírja, hogy mindegyik felügyeleti hatóságnak közzé kell tennie az olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan kötelező adatvédelmi hatásvizsgálatot végezni az országukban. Ezek a jegyzékek rendszerint a hatóságok honlapján találhatók meg. A videokamerás megfigyelés jellemző céljaira (személy- és vagyonvédelem, bűncselekmények felderítése, megelőzése és megfékezése, bizonyítékok gyűjtése és gyanúsítottak biometrikus azonosítása) tekintettel észszerű feltételezni, hogy a videokamerás megfigyelés számos esetben adatvédelmi hatásvizsgálatot igényel. Az adatkezelőknek ezért érdemes alaposan áttanulmányozniuk ezeket a dokumentumokat annak megállapításához, hogy szükség van-e ilyen vizsgálatra, és szükség esetén elvégezzék azt. Az adatkezelőnek az elvégzett adatvédelmi hatásvizsgálat eredménye alapján kell döntenie arról, milyen adatvédelmi intézkedéseket vezet be.

138. Emellett fontos megjegyezni, hogy amennyiben az adatvédelmi hatásvizsgálat eredményei alapján az adatkezelés az adatkezelő által tervezett biztonsági intézkedések ellenére magas kockázattal járna, akkor az adatkezelés előtt egyeztetni kell az illetékes felügyeleti hatósággal. Az előzetes konzultációval kapcsolatos részletes tudnivalók a 36. cikkben találhatók.

Az Európai Adatvédelmi Testület nevében

Az elnök

(Andrea Jelinek)

[27] Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e (WP248 rev.01). Az Európai Adatvédelmi Testület jóváhagyásával.