Smernice 3/2019 o obdelavi osebnih podatkov z video napravami

Različica 2.0

Sprejete 29. januarja 2020

Zgodovina različic

Različica 2.1	26. februar 2020	Popravki vsebinskih napak
Različica 2.0	29. januar 2020	Sprejetje smernic po javnem posvetovanju
Različica 1.0	10. julij 2019	Sprejetje Smernic za javno posvetovanje

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE:

1 UVOD

1. Intenzivna uporaba video naprav vpliva na vedenje državljanov. Obsežno uvajanje takih orodij na številnih področjih življenja bo povzročilo dodaten pritisk na posameznike, da bodo preprečili odkrivanje tistega, kar bi se lahko štelo za anomalije. Te tehnologije lahko dejansko omejijo možnosti anonimnega gibanja in anonimne uporabe storitev ter na splošno omejijo možnost posameznikov, da ostanejo neopaženi. Posledice za varstvo podatkov so velikanske.

2. Čeprav posameznike morda ne moti video nadzor, ki je na primer vzpostavljen za določen varnostni namen, je treba zagotoviti jamstva, da se prepreči kakršna koli zloraba za povsem drugačne in, za posameznika, na katerega se nanašajo osebni podatki, nepričakovane namene (npr. trženje, spremljanje učinkovitosti zaposlenih itd.). Poleg tega se zdaj uporabljajo številna orodja za izkoriščanje posnetih slik in spreminjanje tradicionalnih kamer v pametne kamere. Količina podatkov, ustvarjenih z video posnetkom, v kombinaciji s temi orodji in tehnikami povečuje tveganja sekundarne uporabe (ki je ali ni povezana z namenom, ki je bil prvotno dodeljen sistemu) ali celo tveganja zlorabe. V zvezi z video nadzorom bi bilo treba vedno skrbno preučiti splošna načela iz Splošne uredbe o varstvu podatkov (člen 5).

3. Videonadzorni sistemi v več pogledih spreminjajo medsebojno interakcijo zaposlenih v zasebnem in javnem sektorju, v zasebnih prostorih ali na javnih mestih za namene povečanja varnosti, analize občinstva, pošiljanja osebno prilagojenih oglasov itd. S širitvijo izvajanja pametnih video analiz se je učinkovitost video nadzora znatno povečala. Te tehnike so lahko bolj vsiljive (npr. kompleksne biometrične tehnologije) ali manj vsiljive (npr. preprosti algoritmi štetja). Na splošno je čedalje težje ostati anonimen in ohraniti zasebnost. V različnih primerih se lahko pojavljajo različna vprašanja v zvezi z varstvom podatkov, zato se lahko razlikuje tudi pravna analiza pri uporabi ene ali druge tehnologije.

4. Poleg vprašanj v zvezi z zasebnostjo obstajajo tudi tveganja, povezana z možnimi napakami pri delovanju teh naprav in pristranskostjo, ki jo lahko povzročijo. Raziskovalci poročajo, da programska oprema, ki se uporablja za identifikacijo, prepoznavanje ali analizo obrazov, deluje različno glede na

[1] Sklicevanje na „države članice“ v tem mnenju je treba razumeti kot sklicevanje na „države članice EGP“.

starost, spol in narodnost osebe, ki jo identificira. Algoritmi bi delovali na podlagi različnih demografskih podatkov, zaradi česar obstaja nevarnost, da bi pristranskost pri prepoznavanju obrazov okrepila predsodke družbe. Zato morajo upravljavci podatkov zagotoviti, da se pri obdelavi biometričnih podatkov, pridobljenih z video nadzorom, redno ocenjujeta njena ustreznost in zadostnost zagotovljenih jamstev.

5. Video nadzor ni samodejno potreben, če obstajajo druga sredstva za doseganje osnovnega namena. Sicer tvegamo, da se bodo kulturne norme spremenile in da bo pomanjkanje zasebnosti postalo splošno sprejemljivo.

6. Te smernice so namenjene zagotavljanju napotkov za uporabo Splošne uredbe o varstvu podatkov v zvezi z obdelavo osebnih podatkov z video napravami. Primeri niso izčrpni in splošna obrazložitev se lahko uporabi za vsa morebitna področja uporabe.

2 PODROČJE UPORABE[2]

2.1 Osebni podatki

7. Sistematično avtomatizirano nadziranje določenega prostora z optičnimi ali avdiovizualnimi sredstvi, večinoma za zaščito lastnine ali življenja in zdravja posameznikov, je danes postal pomemben pojav. Ta dejavnost omogoča zbiranje in hrambo slikovnih ali avdiovizualnih informacij o vseh osebah, ki vstopajo v prostor, ki se nadzoruje, in jih je mogoče identificirati na podlagi njihovega videza ali drugih posebnih elementov. Na podlagi teh podrobnosti se lahko določi identiteta teh oseb. Omogoča tudi nadaljnjo obdelavo osebnih podatkov o prisotnosti in vedenju oseb v določenem prostoru. Morebitno tveganje zlorabe teh podatkov se povečuje glede na razsežnost prostora, ki se nadzoruje, in število oseb, ki zahajajo v prostor. To dejstvo se kaže v členu 35(3)(c) Splošne uredbe o varstvu podatkov, ki določa, da je treba izvesti oceno učinka v zvezi z varstvom podatkov v primeru obsežnega sistematičnega spremljanja javno dostopnega območja, in v členu 37(1)(b) navedene uredbe, ki določa, da morajo upravljavci imenovati pooblaščeno osebo za varstvo podatkov, če dejanja obdelave zaradi svoje narave vključujejo redno in sistematično spremljanje posameznikov, na katere se nanašajo osebni podatki.

8. Vendar se Splošna uredba o varstvu podatkov ne uporablja za obdelavo podatkov, ki se ne nanašajo na osebo, npr. če posameznika ni mogoče neposredno ali posredno identificirati.

[2] Evropski odbor za varstvo podatkov opozarja, da se lahko v primerih, v katerih to dovoljuje Splošna uredba o varstvu podatkov, uporabljajo posebne zahteve iz nacionalne zakonodaje.

Primer: Splošna uredba o varstvu podatkov se ne uporablja za lažne kamere (tj. vse kamere, ki ne delujejo kot kamera in zato ne obdelujejo osebnih podatkov). *Vendar lahko v nekaterih državah članicah zanje velja druga zakonodaja.*

Primer: Posnetki z velike višine spadajo na področje uporabe Splošne uredbe o varstvu podatkov samo, če je mogoče v zadevnih okoliščinah podatke, ki se obdelujejo, povezati s konkretno osebo.

Primer: Video kamera je vgrajena v avtomobil za zagotavljanje pomoči pri parkiranju. Če je kamera izdelana ali prilagojena tako, da ne zbira informacij v zvezi s fizično osebo (kot so registrske tablice ali informacije, ki bi se lahko uporabile za identifikacijo mimoidočih), se Splošna uredba o varstvu podatkov ne uporablja.

9.

2.2 Uporaba Direktive (EU) 2016/680 o kazenskem pregonu

10. Na področje uporabe Direktive (EU) 2016/680 spada zlasti obdelava osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.

2.3 Izjema obdelave za domače potrebe

11. V skladu s členom 2(2)(c) obdelava osebnih podatkov s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti, ki lahko vključuje tudi spletno dejavnost, ne spada na področje Splošne uredbe o varstvu podatkov[3].

12. To določbo, tako imenovano izjemo obdelave za domače potrebe, je treba v okviru video nadzora razlagati ozko. Zato je treba, kot meni Sodišče Evropske unije (v nadaljevanju: Sodišče), tako imenovano „izjemo obdelave za domače potrebe“ „razlagati tako, da se nanaša samo na dejavnosti, ki se izvajajo v zasebnem in družinskem življenju posameznikov, kar očitno ne velja za obdelavo osebnih podatkov, ki vključuje njihovo objavo na spletu, s čimer ti postanejo dostopni neopredeljenemu številu oseb“[4]. Poleg tega videonadzornega sistema, kadar vključuje stalno snemanje in shranjevanje osebnih podatkov ter zajema „čeprav delno, javni prostor in je tako usmerjen iz zasebnega okolja tistega, ki tako opravi obdelavo podatkov, [...] *ni mogoče šteti za popolnoma ‚osebno ali domačo‘ dejavnost v smislu člena 3(2), druga alinea, Direktive 95/46*“[5].

13. Kar zadeva video naprave, ki se uporabljajo v zasebnih prostorih osebe, lahko te spadajo v izjemo obdelave za domače potrebe. To je odvisno od več dejavnikov, katere je treba v celoti preučiti, da se lahko sprejme sklep. Poleg zgoraj navedenih elementov, opredeljenih v sodbi Sodišča, mora uporabnik video nadzora doma preučiti, ali je v kakršnem koli osebnem odnosu s posameznikom, na katerega se nanašajo osebni podatki, ali obseg ali pogostost nadzora nakazuje neko vrsto poklicne dejavnosti z njegove strani in morebiten škodljiv učinek nadzora na posameznike, na katere se nanašajo osebni podatki. Obstoj katerega koli od zgoraj navedenih elementov ne nakazuje nujno, da je obdelava zunaj področja uporabe izjeme obdelave za domače potrebe; za to ugotovitev je potrebna celovita ocena.

---

[3] Glej tudi uvodno izjavo 18.
[4] Sodba Sodišča z dne 6. novembra 2003 v zadevi C-101/01, *Bodil Lindqvist*, točka 47.
[5] Sodba Sodišča z dne 11. decembra 2014 v zadevi C-212/13, *František Ryneš zoper Úřad pro ochranu osobních údajů,* točka 33.

Primer: Turist snema video posnetke s svojim mobilnim telefonom in video kamero za dokumentiranje svojih počitnic. Posnetek pokaže prijateljem in sorodnikom, vendar ne omogoči dostopa do njega nedoločenemu številu ljudi. To bi spadalo v izjemo obdelave za domače potrebe.

Primer: Gorska kolesarka želi posneti svoj spust s športno kamero. Kolesari na odročnem območju in namerava uporabiti posnetke le za svoje osebno razvedrilo doma. To bi spadalo pod izjemo obdelave za domače potrebe, tudi če se v določenem obsegu obdelujejo osebni podatki.

Primer: Oseba spremlja in snema svoj vrt. Zemljišče je ograjeno in na vrt redno prihajajo le upravljavec sam in njegova družina. To bi spadalo v izjemo obdelave za domače potrebe, če video nadzor niti delno ne bi zajemal javnega prostora ali sosednjega zemljišča.

14.

3 ZAKONITOST OBDELAVE

15. Pred uporabo je treba podrobno opredeliti namene obdelave (člen 5(1)(b)). Video nadzor se lahko uporablja za številne namene, npr. pomoč pri varstva lastnine in drugega premoženja, pomoč pri varovanju življenja in telesne celovitosti posameznikov ter zbiranje dokazov za civilne tožbe[6]. Ti nameni spremljanja bi morali biti pisno dokumentirani (člen 5(2)) in morajo biti določeni za vsako nadzorno kamero v uporabi. Kamere, ki jih posamezen upravljavec uporablja za enak namen, se lahko dokumentirajo skupaj. Poleg tega morajo biti posamezniki, na katere se nanašajo osebni podatki, obveščeni o namenih obdelave v skladu s členom 13 (*glej oddelek 7, Obveznosti glede preglednosti in zagotavljanja informacij*). Video nadzor, ki je namenjen zgolj „varnosti“ ali „vaši varnosti“, ni dovolj specifičen (člen 5(1)(b)). Poleg tega je v nasprotju z načelom, da se osebni podatki obdelujejo zakonito, pošteno in pregledno v zvezi s posameznikom, na katerega se nanašajo osebni podatki (glej člen 5(1)(a)).

16. Načeloma lahko vsak pravni razlog iz člena 6(1) zagotavlja pravno podlago za obdelavo podatkov, pridobljenih z video nadzorom. Na primer, člen 6(1)(c) se uporablja, kadar nacionalno pravo določa obveznost izvajanja video nadzora[7]. Vendar se bosta v praksi najverjetneje uporabljali naslednji določbi:

- člen 6(1)(f) (zakoniti interes);
- člen 6(1)(e) (potreba po opravljanju naloge v javnem interesu ali pri izvajanju javne oblasti).

V izjemnih primerih lahko upravljavec kot pravno podlago uporabi člen 6(1)(a) (privolitev).

3.1 Zakoniti interes, člen 6(1)(f)

17. Pravna presoja člena 6(1)(f) bi morala temeljiti na naslednjih merilih v skladu z uvodno izjavo 47.

3.1.1 Obstoj zakonitih interesov

18. Video nadzor je zakonit, če je potreben za izpolnitev zakonitega interesa, za katerega si prizadeva upravljavec, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine

[6] Pravila o zbiranju dokazov za civilne tožbe se po državah članicah razlikujejo.
[7] Te smernice ne analizirajo nacionalnega prava, ki se lahko med državami članicami razlikuje, ali navajajo njegovih podrobnosti.

posameznika, na katerega se nanašajo osebni podatki (člen 6(1)(f)). Zakoniti interesi, za katere si prizadeva upravljavec ali tretja oseba, so lahko pravni[8], gospodarski ali nematerialni interesi[9]. Vendar bi moral upravljavec upoštevati, da če posameznik, na katerega se nanašajo osebni podatki, nasprotuje nadzoru v skladu s členom 21, lahko upravljavec nadaljuje video nadzor zadevnega posameznika, na katerega se nanašajo osebni podatki le, če gre za *nujen* zakoniti interes, ki prevlada nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

19. Glede na dejansko in nevarno situacijo lahko namen zaščite lastnine pred vlomom, tatvino ali vandalizmom pomeni zakoniti interes za video nadzor.

20. Zakoniti interes mora dejansko obstajati in mora biti aktualno vprašanje (tj. ne sme biti fiktiven ali špekulativen)[10]. Pred začetkom nadzora mora obstajati stiska v resničnem življenju, kot so poškodbe ali resni incidenti v preteklosti. Glede na načelo odgovornosti je priporočljivo, da upravljavci dokumentirajo ustrezne incidente (datum, način, finančna izguba) in z njimi povezane kazenske ovadbe. Taki dokumentirani incidenti so lahko trden dokaz obstoja zakonitega interesa. Obstoj zakonitega interesa in potrebo po spremljanju bi bilo treba vnovično ocenjevati periodično (npr. enkrat letno, odvisno od okoliščin).

> Primer: Lastnik trgovine želi odpreti novo trgovino in namestiti videonadzorni sistem za preprečevanje vandalizma. S predložitvijo statističnih podatkov lahko dokaže, da se v bližini trgovine pričakuje visoka stopnja vandalizma. Koristne so tudi izkušnje iz sosednjih trgovin. Ni nujno, da je nastala škoda zadevnemu upravljavcu, če škoda v soseski nakazuje nevarnost ali kaj podobnega in tako lahko kaže na zakoniti interes. Vendar ne zadošča, da se predloži nacionalna ali splošna statistika kaznivih dejanj, ne da bi se analizirali zadevno območje ali nevarnosti za konkretno trgovino.

21.

22. Primeri neposredne nevarnosti lahko pomenijo zakonit interes, kot so banke ali trgovine, ki prodajajo dragoceno blago (npr. draguljarji), ali območja, ki so znana kot značilni kraji izvršitve kaznivih dejanj zoper lastnino (npr. bencinske postaje).

23. V Splošni uredbi o varstvu podatkov je tudi jasno navedeno, da javni organi ne morejo utemeljevati obdelave z zakonitim interesom pri opravljanju svojih nalog, drugi stavek člena 6(1).

3.1.2 Potreba po obdelavi

24. Osebni podatki bi morali biti ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo („najmanjši obseg podatkov“), glej člen 5(1)(c). Upravljavec bi moral pred namestitvijo videonadzornega sistema vedno kritično preučiti, ali je ta ukrep, prvič, primeren za doseganje želenega cilja ter, drugič, ustrezen in potreben za njegove namene. Ukrepi v zvezi z video nadzorom bi morali biti izbrani, če namena obdelave ne bi bilo mogoče razumno doseči z drugimi sredstvi, ki manj posegajo v temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

25. Če želi upravljavec preprečiti kazniva dejanja, povezana z lastnino, bi lahko namesto namestitve videonadzornega sistema sprejel tudi alternativne varnostne ukrepe, kot so ograditev posesti,

[8] Sodba Sodišča z dne 4. maja 2017 v zadevi C-13/16, *Rīgas satiksme*.
[9] Glej WP217, Delovna skupina iz člena 29.
[10] Glej WP217, Delovna skupina iz člena 29, str. 24 in naslednje. Glej tudi sodbo Sodišča v zadevi C-708/18, str. 44.

uvedba rednih patrulj varnostnega osebja, uporaba vratarjev, zagotovitev boljše osvetlitve, namestitev varnostnih ključavnic, pred posegi varnih oken in vrat ali nanos antigrafitnega premaza ali folij na stene. Taki ukrepi so lahko enako učinkoviti pred vlomi, tatvinami in vandalizmom kot videonadzorni sistemi. Upravljavec mora za vsak primer posebej oceniti, ali so lahko taki ukrepi razumna rešitev.

26. Pred uporabo sistema kamer mora upravljavec oceniti, kje in kdaj so ukrepi video nadzora nujni. Običajno sistem nadzora, ki deluje ponoči in zunaj običajnega delovnega časa, zadovoljuje potrebe upravljavca po preprečevanju kakršne koli nevarnosti za njegovo lastnino.

27. Na splošno se potreba po uporabi video nadzora za zaščito prostorov upravljavca konča na mejah posesti.[11] Vendar obstajajo primeri, v katerih nadzor posesti ne zadošča za učinkovito zaščito. V nekaterih posameznih primerih je morda video nadzor treba razširiti na neposredno okolico prostorov. V zvezi s tem bi moral upravljavec razmisliti o fizičnih in tehničnih sredstvih, na primer blokiranju nepomembnih območij ali njihovi razdelitvi na slikovne točke.

> Primer: Knjigarna želi zaščititi svoje prostore pred vandalizmom. Običajno bi lahko kamere snemale le same prostore, saj za ta namen ni treba opazovati sosednjih prostorov ali javnih površin v okolici prostorov knjigarne.

28.

29. Pojavljajo se tudi vprašanja v zvezi s potrebo po obdelavi, ki se nanašajo na način zavarovanja dokazov. V nekaterih primerih je morda treba uporabiti rešitve s črno skrinjico, pri kateri se posnetek samodejno izbriše po določenem obdobju hrambe, dostop do njega pa je mogoč samo v primeru nesreče. V drugih primerih morda sploh ni treba posneti video materiala, ampak je namesto tega primerneje uporabiti nadzor v realnem času. Odločitev o izbiri med rešitvijo s črno skrinjico in nadzorom v realnem času bi morala prav tako temeljiti na namenu. Če je na primer namen video nadzora zavarovanje dokazov, metode v realnem času običajno niso primerne. Včasih je lahko nadzorovanje v realnem času tudi bolj vsiljivo od shranjevanja in samodejnega brisanja gradiva po določenem obdobju (npr. če nekdo stalno gleda v zaslon, je lahko to bolj vsiljivo, kot če zaslona ni in se gradivo neposredno shranjuje v črni skrinjici). V zvezi s tem je treba upoštevati načelo najmanjšega obsega podatkov (člen 5(1)(c)). Upoštevati bi bilo treba tudi, da bi bilo morda mogoče, da bi upravljavec namesto video nadzora lahko uporabljal varnostno osebje, ki bi se lahko takoj odzvalo in posredovalo.

3.1.3 Usklajevanje interesov

30. Ob predpostavki, da je video nadzor potreben za zaščito zakonitih interesov upravljavca, se videonadzorni sistem lahko začne uporabljati le, če interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladajo nad zakonitimi interesi upravljavca ali zakonitimi interesi tretje osebe (npr. varstvo lastnine ali zaščita telesne nedotakljivosti). Upravljavec mora upoštevati (1.) v kakšnem obsegu spremljanje vpliva na interese, temeljne pravice in svoboščine posameznikov ter (2.) ali to povzroča kršitve ali negativne posledice za pravice posameznika, na katerega se nanašajo osebni podatki. Usklajevanje interesov je obvezno. Natančno je treba oceniti in uskladiti temeljne pravice in svoboščine na eni strani ter zakonite interese upravljavca na drugi strani.

[11] To je lahko urejeno tudi v nacionalni zakonodaji v nekaterih državah članicah.

Primer: Zasebno parkirno podjetje je dokumentiralo ponavljajoče se težave s tatvinami v parkiranih avtomobilih. Parkirišče je odprt prostor in je zlahka vsakomur dostopno, vendar je jasno označeno z oznakami in cestnimi blokatorji, ki obkrožajo prostor. Parkirno podjetje ima zakoniti interes (preprečevanje tatvin v avtomobilih strank), da nadzoruje parkirišče v času dneva, ko se pojavljajo težave. Posameznike, na katere se nanašajo osebni podatki, se nadzoruje v omejenem obdobju, niso v območju za rekreativne namene in tudi v njihovem interesu je, da se tatvine preprečijo. Nad interesom posameznikov, na katere se nanašajo osebni podatki, da se jih ne nadzoruje, v tem primeru prevladuje zakoniti interes upravljavca.

Primer: Restavracija se odloči, da bo namestila video kamere v toaletnih prostorih, da bi nadzorovala čistočo sanitarnih prostorov. V tem primeru pravice posameznikov, na katere se nanašajo osebni podatki, jasno prevladajo nad interesom upravljavca, zato kamer tam ni mogoče namestiti.

31.

3.1.3.1 Odločanje za vsak primer posebej

32. Ker je v skladu z s Splošno uredbo o varstvu podatkov usklajevanje interesov obvezno, je treba odločitev sprejeti za vsak primer posebej (glej člen 6(1)(f)). Sklicevanje na abstraktne situacije ali primerjava podobnih primerov ne zadošča. Upravljavec mora oceniti tveganja poseganja v pravice posameznika, na katerega se nanašajo osebni podatki; pri tem je odločilno merilo intenzivnost poseganja v pravice in svoboščine posameznika.

33. Intenzivnost je med drugim mogoče opredeliti glede na vrsto informacij, ki se zbirajo (vsebina informacij), obseg (zgoščenost informacij, prostorski in geografski obseg), število zadevnih posameznikov, na katere se nanašajo osebni podatki, bodisi kot določeno število bodisi kot delež ustrezne populacije, zadevno situacijo, dejanske interese skupine posameznikov, na katere se nanašajo osebni podatki, alternativna sredstva ter naravo in obseg ocene podatkov.

34. Pomembna dejavnika usklajevanja sta lahko velikost območja, ki se nadzoruje, in število posameznikov, na katere se nanašajo osebni podatki, ki se nadzorujejo. Uporabo video nadzora na oddaljenem območju (npr. za opazovanje prostoživečih živali ali zaščito kritične infrastrukture, kot je radijska antena v zasebni lasti) je treba oceniti drugače kot video nadzor na območju za pešce ali v nakupovalnem središču.

Primer: Če je nameščena avtokamera (npr. za zbiranje dokazov v primeru nesreče), je treba zagotoviti, da ta kamera ne snema neprekinjeno prometa in oseb v bližini ceste. V nasprotnem primeru interes za video posnetke kot dokaz v razmeroma hipotetičnem primeru prometne nesreče ne more upravičiti tega resnega posega v pravice posameznikov, na katere se nanašajo osebni podatki[11].

35.

3.1.3.2 Razumna pričakovanja posameznikov, na katere se nanašajo osebni podatki

36. V skladu z uvodno izjavo 47 je treba obstoj zakonitega interesa natančno oceniti. Pri tem je treba vključiti razumna pričakovanja posameznika, na katerega se nanašajo osebni podatki, v času in v okviru obdelave njegovih osebnih podatkov. Glede sistematičnega nadzorovanjaa je lahko odnos med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem zelo različen in lahko vpliva na razumna pričakovanja posameznika, na katerega se nanašajo osebni podatki. Razlaga pojma razumnih pričakovanj ne bi smela temeljiti le na zadevnih subjektivnih pričakovanjih, temveč mora biti odločilno merilo, ali bi lahko objektivna tretja oseba razumno pričakovala in sklepala, da je v tem specifičnem primeru predmet nadzorovanja.

37. Na primer, zaposleni na svojem delovnem mestu verjetno ne pričakuje, da ga bo njegov delodajalec nadzoroval[12]. Poleg tega se nadzora ne pričakuje na zasebnem vrtu, v bivalnih prostorih ali v ordinacijah. Prav tako ni razumno pričakovati, da se bo nadzor izvajal v sanitarnih prostorih ali savni – nadzorovanje takih prostorov je velik poseg v pravice posameznika, na katerega se nanašajo osebni podatki. Posamezniki, na katere se nanašajo osebni podatki, razumno pričakujejo, da se v teh prostorih video nadzor ne bo izvajal. Po drugi strani pa bančni komitent lahko pričakuje, da se bo nadzor izvajal v banki ali pri bančnem avtomatu.

38. Posamezniki, na katere se nanašajo osebni podatki, lahko tudi pričakujejo, da se nadzorne izvaja na javno dostopnih območjih, zlasti če se ta območja običajno uporabljajo za počitek, regeneracijo in prostočasne dejavnosti, pa tudi na mestih, kjer se posamezniki zadržujejo in/ali komunicirajo, kot so prostori za sedenje, mize v restavracijah, parki, kinematografi in fitnesi. V takih primerih bodo interesi ali pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, pogosto prevladali nad zakonitimi interesi upravljavca.

> Primer: Posamezniki, na katere se nanašajo osebni podatki, ne pričakujejo, da se jih bo nadzorovalo v toaletnih prostorih. Video nadzor, na primer za preprečevanje nesreč, ni sorazmeren.

39.

40. Oznake, ki obveščajo posameznika, na katerega se nanašajo osebni podatki, o video nadzoru, niso pomembni pri določanju, kaj lahko posameznik, na katerega se nanašajo osebni podatki, objektivno pričakuje. To pomeni, da na primer lastnik trgovine ne more predpostavljati, da stranke *objektivno* razumno pričakujejo, da se jih bo spremljalo, zgolj zaradi oznake, ki na vhodu posameznika obvešča o nadzoru.

3.2 Potreba po opravljanju naloge v javnem interesu ali pri izvajanju javne oblasti, ki je dodeljena upravljavcu, člen 6(1)(e)

41. Osebni podatki se lahko obdelujejo z video nadzorom v skladu s členom 6(1)(e), če je to potrebno za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti[13]. Izvajanje javne oblasti morda ne dovoljuje take obdelave, vendar druge pravne podlage, kot sta „zdravje in varnost“ za zaščito obiskovalcev in zaposlenih, lahko zagotavljajo omejene možnosti za obdelavo, pri čemer se še vedno upoštevajo obveznosti in pravice posameznikov, na katere se nanašajo osebni podatki, iz Splošne uredbe o varstvu podatkov.

42. Države članice lahko ohranijo ali uvedejo posebno nacionalno zakonodajo za video nadzor, da prilagodijo uporabo pravil iz Splošne uredbe o varstvu podatkov z natančnejšo določitvijo posebnih zahtev za obdelavo, če je to v skladu z načeli, določenimi v Splošni uredbi o varstvu podatkov (npr. omejitev hrambe, sorazmernost).

[12] Glej tudi: Delovna skupina iz člena 29, Mnenje 2/2017 o obdelavi podatkov pri delu, WP 249, sprejeto 8. junija 2017.

[13] Ta podlaga za obdelavo je določena s pravom Unije ali pravom držav članic in je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je dodeljena upravljavcu (člen 6(3)).

3.3 Privolitev, člen 6(1)(a)

43. Privolitev mora biti prostovoljna, izrecna, informirana in nedvoumna, kot je opisano v smernicah o privolitvi[14].

44. Pri sistematičnem nadzoru se lahko privolitev posameznika, na katerega se nanašajo osebni podatki, uporablja kot pravna podlaga v skladu s členom 7 (glej uvodno izjavo 43) le v izjemnih primerih. Značilnost nadzora je, da ta tehnologija nadzoruje neznano število ljudi hkrati. Upravljavec bo težko dokazal, da je dal posameznik, na katerega se nanašajo osebni podatki, privolitev pred obdelavo njegovih osebnih podatkov (člen 7(1)). Ob predpostavki, da posameznik, na katerega se nanašajo osebni podatki, umakne svojo privolitev, bo upravljavec težko dokazal, da se osebni podatki ne obdelujejo več (člen 7(3)).

> Primer: Športniki lahko zahtevajo, da se jih nadzoruje med posameznimi vajami za analizo njihovih tehnik in rezultatov. Po drugi strani pa v primeru, če športni klub sprejme pobudo za nadzor celotne ekipe za enak namen, privolitev pogosto ne bo veljavna, saj lahko posamezni športniki privolijo v nadzor, da njihova zavrnitev privolitve ne bi negativno vplivala na preostale člane ekipe.

45.

46. Če se želi upravljavec sklicevati na privolitev, se mora prepričati, da je vsak posameznik, na katerega se nanašajo osebni podatki, ki vstopi na območje pod video nadzorom, dal svojo privolitev. Ta privolitev mora izpolnjevati pogoje iz člena 7. Vstop na območje, ki se nadzoruje (npr. osebe so pozvane, naj gredo po določenem hodniku ali skozi prehod, da vstopijo na območje, ki se nadzoruje), ne pomeni izjave ali jasnega pritrdilnega dejanja, potrebnih za privolitev, razen če izpolnjuje merila iz členov 4 in 7, kot je opisano v smernicah o privolitvi[15].

47. Glede na neravnovesje moči med delodajalci in zaposlenimi se delodajalci pri obdelavi podatkov v večini primerov ne bi smeli opirati na privolitev, saj je malo verjetno, da je bila dana prostovoljno. Glede tega bi bilo treba upoštevati smernice o privolitvi.

48. Pravo držav članic ali kolektivne pogodbe, vključno s „pogodbami na ravni podjetij“, lahko določajo posebna pravila o obdelavi osebnih podatkov zaposlenih v okviru zaposlitve (glej člen 88).

[14] Delovna skupina iz člena 29 „Smernice o privolitvi v skladu z Uredbo 2016/679“ (WP 259 rev. 01). – potrdil Evropski odbor za varstvo podatkov.
[15] Delovna skupina iz člena 29 „Smernice o privolitvi v skladu z Uredbo 2016/679“ (WP 259), ki jih je potrdil Evropski odbor za varstvo podatkov in jih je treba upoštevati.

4 RAZKRITJE VIDEO POSNETKOV TRETJIM OSEBAM

49. Načeloma se za razkritje video posnetkov tretjim osebam uporabljajo splošni predpisi iz Splošne uredbe o varstvu podatkov.

4.1 Razkritje video posnetkov tretjim osebam na splošno

50. Razkritje je opredeljeno v členu 4(2) kot posredovanje (npr. posameznega sporočila), razširjanje (npr. objavljanje na spletu) ali drugačno omogočanje dostopa. Tretje osebe so opredeljene v členu 4(10). V primeru razkritja tretjim državam ali mednarodnim organizacijam se uporabljajo posebne določbe člena 44 in naslednjih.

51. Vsako razkritje osebnih podatkov je ločena vrsta obdelave osebnih podatkov, za katero upravljavec potrebuje pravno podlago iz člena 6.

> Primer: Upravljavec, ki želi naložiti posnetek na internet, se mora za tako obdelavo opirati na pravno podlago, na primer s pridobitvijo privolitve posameznika, na katerega se nanašajo osebni podatki, v skladu s členom 6(1)(a).

52.

53. Posredovanje video posnetka tretjim osebam za namen, ki ni namen, za katerega se zbirajo podatki, je mogoč v skladu s pravili iz člena 6(4).

> Primer: Video nadzor ovire (na parkirišču) se uporablja za reševanje zahtevkov za povrnitev škode. Ko nastane škoda, se posnetek posreduje odvetniku, da sproži postopek. V tem primeru je namen snemanja enak namenu posredovanja.
>
> Primer: Video nadzor ovire (na parkirišču) se uporablja za reševanje zahtevkov za povrnitev škode. Posnetek se objavi na spletu zgolj v razvedrilne namene. V tem primeru se je namen spremenil in ni skladen s prvotnim namenom. Poleg tega bi bilo problematično opredeliti pravno podlago za tako obdelavo (objava).

54.

55. Prejemnik, ki je tretja oseba, bo moral izvesti svojo pravno analizo, zlasti opredeliti svojo pravno podlago v skladu s členom 6 za svojo obdelavo (npr. prejem gradiva).

4.2 Razkritje video posnetkov organom kazenskega pregona

56. Razkritje video posnetkov organom kazenskega pregona je prav tako neodvisen postopek, ki od upravljavca zahteva ločeno utemeljitev.

57. V skladu s členom 6(1)(c) je obdelava zakonita, če je potrebna za izpolnitev pravne obveznosti, ki velja za upravljavca. Čeprav veljavno policijsko pravo spada pod izključni nadzor držav članic, najverjetneje v vsaki državi članici obstajajo splošna pravila, ki urejajo prenos dokazov na organe kazenskega pregona. Postopek predaje podatkov s strani upravljavca ureja Splošna uredba o varstvu podatkov. Če nacionalna zakonodaja zahteva sodelovanje upravljavca z organi kazenskega pregona (npr. v preiskavi), je pravna podlaga za posredovanje podatkov pravna obveznost v skladu s členom 6(1)(c).

58. Omejitev namena iz člena 6(4) tako običajno ne povzroča težav, saj je razkritje izrecno utemeljeno na pravu države članice. Upoštevanje posebnih zahtev za spremembo namena v smislu točk (a)–(e) navedenega člena zato ni potrebna.

Primer: Lastnik trgovine naredi posnetek pri vhodu v trgovino. Na posnetku je vidno, kako neka oseba ukrade drugi osebi denarnico. Policija od upravljavca zahteva, naj ji izroči gradivo, ki ji bo v pomoč pri preiskavi. V tem primeru bi lastnik trgovine za postopek prenosa uporabil pravno podlago iz člena 6(1)(c) (pravna obveznost) v povezavi z ustreznim nacionalnim pravom.

59.

Primer: V trgovini je iz varnostnih razlogov nameščena kamera. Lastnik trgovine meni, da je posnel nekaj sumljivega, in se odloči, da bo gradivo poslal policiji (čeprav mu ni znano, da poteka morebitna preiskava). V tem primeru mora lastnik trgovine oceniti, ali so pogoji iz, v večini primerov, člena 6(1)(f) izpolnjeni. Tako je običajno v primeru, če lastnik trgovine utemeljeno sumi, da je bilo storjeno kaznivo dejanje.

60.

61. Za obdelavo osebnih podatkov s strani organov kazenskega pregona se ne uporablja Splošna uredba o varstvu podatkov (glej člen 2(2)(d)), ampak Direktiva (EU) 2016/680 o kazenskem pregonu.

5 OBDELAVA POSEBNIH VRST PODATKOV

62. Videonadzorni sistemi običajno zbirajo ogromne količine osebnih podatkov, ki lahko razkrivajo zelo osebne podatke in celo posebne vrste podatkov. Dejansko se lahko na videz nepomembni podatki, ki so bili prvotno zbrani z video nadzorom, uporabijo za sklepanje o drugih informacijah za doseganje drugega namena (npr. za spremljanje navad posameznika). Vendar video nadzor ne pomeni vedno, da se z njim obdelujejo posebne vrste osebnih podatkov.

Primer: Video posnetek, na katerem je posameznik, na katerega se nanašajo osebni podatki, ki nosi očala ali uporablja invalidski voziček, se sam po sebi ne šteje za posebno vrsto osebnih podatkov.

63.

64. Toda, če se video posnetek obdela za sklepanje o posebnih vrstah podatkov, se uporablja člen 9.

Primer: O političnih mnenjih bi se lahko na primer sklepalo iz slik, na katerih je mogoče identificirati posameznike, na katere se nanašajo osebni podatki, ki sodelujejo na prireditvi, stavkajo itd. To bi spadalo na področje uporabe člena 9.

Primer: Namestitev video kamere v bolnišnici za spremljanje zdravstvenega stanja pacienta bi se štela za obdelavo posebnih vrst osebnih podatkov (člen 9).

65.

66. Na splošno bi bilo treba načeloma ob vsaki namestitvi videonadzornega sistema skrbno upoštevati načelo najmanjšega obsega podatkov. Tako bi si moral upravljavec podatkov tudi v primerih, v katerih se ne uporablja člen 9(1), vedno prizadevati zmanjšati tveganje, da bi posnetek razkril druge občutljive podatke (poleg tistih iz člena 9), ne glede na cilj.

Primer: Video nadzor cerkve sam po sebi ne spada na področje uporabe člena 9. Vendar mora upravljavec pri presoji interesov posameznika, na katerega se nanašajo osebni podatki, izvesti zelo natančno oceno v skladu s členom 6(1)(f), ob upoštevanju narave podatkov in tveganja zajetja drugih občutljivih podatkov (poleg tistih iz člena 9).

67.

68. Če se videonadzorni sistem uporablja za obdelavo posebnih vrst podatkov, mora upravljavec podatkov opredeliti izjemo za obdelavo posebnih vrst podatkov iz člena 9 (tj. izjemo od splošnega pravila, da se posebnih vrst podatkov ne sme obdelovati) in pravno podlago iz člena 6.

69. Na primer, člen 9(2)(c) („[…] *obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugega posameznika* […]“) bi se teoretično in izjemoma lahko uporabil, vendar bi moral upravljavec podatkov to upravičiti kot nujno potrebno za zaščito življenjskih interesov osebe in dokazati, da ta „[…] *posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno ni sposoben dati privolitve.*“ Poleg tega upravljavec podatkov sistema ne bi smel uporabljati za noben drug namen.

70. Pri tem je treba opozoriti, da vsake izjeme, navedene v členu 9, verjetno ne bo mogoče uporabiti za utemeljitev obdelave posebnih vrst podatkov z video nadzorom. Natančneje, upravljavci podatkov, ki obdelujejo take podatke v okviru video nadzora, se ne morejo sklicevati na člen 9(2)(e), ki dovoljuje obdelavo, povezano z osebnimi podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi. Sam vstop na območje dosega kamere ne pomeni, da namerava posameznik, na katerega se nanašajo osebni podatki, objaviti posebne vrste podatkov, povezane z njim.

71. Poleg tega obdelava posebnih vrst podatkov zahteva poostreno in stalno spremljanje nekaterih obveznosti, kot sta visoka raven varnosti in po potrebi ocena učinka v zvezi z varstvom podatkov.

> Primer: Delodajalec ne sme uporabiti posnetkov demonstracij, pridobljenih z video nadzorom, za identifikacijo stavkajočih.

72.

5.1 Splošni premisleki pri obdelavi biometričnih podatkov

73. Uporaba biometričnih podatkov in zlasti prepoznavanje obrazov vključujeta večja tveganja za posameznike, na katere se nanašajo osebni podatki. Ključno je, da se take tehnologije uporabljajo ob ustreznem spoštovanju načel zakonitosti, potrebnosti, sorazmernosti in najmanjšega obsega podatkov, kot so določena v Splošni uredbi o varstvu podatkov. Čeprav se uporaba teh tehnologij lahko šteje za posebej učinkovito, bi morali upravljavci najprej oceniti vpliv na temeljne pravice in svoboščine ter razmisliti o manj vsiljivih sredstvih za doseganje njihovega zakonitega namena obdelave.

74. Da se podatki lahko štejejo za biometrične podatke, kot so opredeljeni v Splošni uredbi o varstvu podatkov, mora obdelava neobdelanih podatkov, kot so fizične, fiziološke ali vedenjske značilnosti posameznika, vključevati meritev teh značilnosti. Ker so biometrični podatki rezultat takih meritev, je v členu 4(14) Splošne uredbe o varstvu podatkov navedeno, da so „[…] *rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika* […]“. Vendar se video posnetek posameznika sam po sebi ne more šteti za biometrični podatek v skladu s členom 9, če ni bil posebej tehnično obdelan, da bi pripomogel k identifikaciji posameznika[16].

75. Da bi se obdelava štela za obdelavo posebnih vrst osebnih podatkov (člen 9), bi se morali biometrični podatki obdelovati „za namene edinstvene identifikacije posameznika“.

76. Na kratko, glede na člena 4(14) in 9 je treba upoštevati tri merila:

[16] To analizo podpira uvodna izjava 51 Splošne uredbe o varstvu podatkov, v kateri je navedeno, da se „ *obdelava fotografij […] ne bi smela sistematično šteti za obdelavo posebnih vrst osebnih podatkov, saj spadajo v opredelitev biometričnih podatkov le, kadar so obdelane s posebnimi tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika.* […]“.

- **narava podatkov:** podatki, povezani s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika;
- **sredstva in način obdelave:** podatki, „ki so rezultat posebne tehnične obdelave“;
- **namen obdelave:** podatke je treba uporabljati za namene edinstvene identifikacije posameznika.

77. Uporaba video nadzora, ki vključuje funkcijo biometričnega prepoznavanja, ki jo zasebni subjekti namestijo za lastne namene (npr. trženje, statistične ali celo varnostne namene), bo v večini primerov zahtevala izrecno privolitev vseh posameznikov, na katere se nanašajo osebni podatki (člen 9(2)(a)), vendar bi se lahko uporabila tudi druga ustrezna izjema iz člena 9.

Primer: Zasebno podjetje za izboljšanje svojih storitev nadomešča kontrolne točke za identifikacijo potnikov na letališču (oddaja prtljage, vkrcanje) z videonadzornimi sistemi, ki uporabljajo tehnike prepoznavanja obraza za preverjanje identitete tistih potnikov, ki so se odločili, da bodo privolili v tak postopek. Ker obdelava spada na področje uporabe člena 9, se bodo morali potniki, ki so predhodno dali svojo izrecno in informirano privolitev, prijaviti na, na primer, avtomatskem terminalu, da bodo ustvarili in registrirali svojo predlogo obraza, povezano z njihovim vstopnim kuponom in identiteto. Kontrolne točke s prepoznavanjem obraza morajo biti jasno ločene, npr. sistem mora biti nameščen znotraj zamejenega prehoda, tako da biometrične predloge oseb, ki niso dale svoje privolitve, ne bodo zajete. Samo potniki, ki so predhodno dali svojo privolitev in se nato prijavili, bodo uporabljali zamejeni prehod, opremljen z biometričnim sistemom.

Primer: Upravljavec upravlja dostop do svoje stavbe z uporabo metode prepoznavanja obrazov. Osebe lahko uporabljajo ta način dostopa le, če so pred tem podale izrecno in informirano privolitev (v skladu s členom 9(2)(a)). Da bi zagotovili, da ni zajet nihče, ki ni predhodno dal svoje privolitve, pa bi moral metodo prepoznavanja obraza sprožiti sam posameznik, na katerega se nanašajo osebni podatki, na primer s pritiskom na gumb. Za zagotovitev zakonitosti obdelave mora upravljavec vedno ponuditi alternativen način dostopa do stavbe, brez biometrične obdelave, kot so izkaznice ali ključi.

78.

79. V primerih, ko se ustvarjajo biometrične predloge, upravljavci zagotovijo, da se po pridobitvi rezultata ujemanja ali neujemanja takoj in varno izbrišejo vse vmesne predloge, ki se ustvarjajo sprotno (na podlagi izrecne in informirane privolitve posameznika, na katerega se nanašajo osebni podatki), da se primerjajo s tistimi, ki jih ob prijavi ustvarijo posamezniki, na katere se nanašajo osebni podatki. Predloge, ustvarjene za prijavo, se lahko zadržijo samo za uresničitev namena obdelave in se ne smejo shraniti ali arhivirati.

80. Če pa je namen obdelave, na primer, razlikovanje ene kategorije ljudi od druge, ne pa edinstvena identifikacija posameznika, obdelava ne spada na področje uporabe člena 9.

Primer: Lastnik trgovine želi prilagoditi svoje oglaševanje na podlagi spola in starosti strank, ki se snemajo z videonadzornim sistemom. Če tak sistem ne ustvarja biometričnih predlog za edinstveno identifikacijo oseb, ampak le zaznava te fizične značilnosti za razvrstitev oseb, obdelava ne spada na področje uporabe člena 9 (če se ne obdelujejo druge posebne vrste podatkov).

81.

82. Vendar pa se člen 9 uporablja, če upravljavec hrani biometrične podatke (običajno s predlogami, ki se ustvarijo s pridobivanjem ključnih značilnosti iz neobdelanih biometričnih podatkov (npr. meritve obraza s slike)za edinstveno identifikacijo osebe. Če želi upravljavec odkriti posameznika, na katerega se nanašajo osebni podatki, ki vnovič vstopa na območje ali vstopa na drugo območje (na primer za načrtovanje stalnega prilagojenega oglaševanja), je namen edinstvena identifikacija posameznika, kar pomeni, da bi dejanje od vsega začetka spadalo na področje člena 9. To je morda v primeru, kadar upravljavec hrani ustvarjene predloge za zagotavljanje nadaljnjega prilagojenega oglaševanja na več panojih na različnih mestih v trgovini. Ker sistem uporablja fizične značilnosti za odkrivanje določenih posameznikov, ki se vračajo na območje, ki ga zajema kamera (kot so obiskovalci nakupovalnega središča), in njihovo sledenje, bi pomenil metodo biometrične identifikacije, saj je namenjen prepoznavanju z uporabo tehnične obdelave.

> Primer: Lastnik trgovine je v trgovini namestil sistem za prepoznavanje obrazov, da bi prilagodil svoje oglaševanje posameznikom. Upravljavec podatkov mora pred uporabo tega biometričnega sistema in izvajanjem prilagojenega oglaševanja pridobiti izrecno in informirano privolitev vseh posameznikov, na katere se nanašajo osebni podatki. Sistem bi bil nezakonit, če bi snemal obiskovalce ali mimoidoče, ki niso privolili v ustvarjanje svoje biometrične predloge, tudi če se njihova predloga izbriše v najkrajšem možnem času. Dejansko te začasne predloge pomenijo biometrične podatke, ki se obdelujejo za edinstveno identifikacijo osebe, ki morda ne želi prejemati ciljno usmerjenih oglasov.

83.

84. Evropski odbor za varstvo podatkov ugotavlja, da so nekateri biometrični sistemi nameščeni v nenadzorovanih okoljih[17], kar pomeni, da sistem vključuje sprotno snemanje obrazov vseh posameznikov, ki vstopijo na območje, ki ga zajema kamera, vključno z osebami, ki niso dale privolitve za uporabo biometrične naprave, in tako ustvarja biometrične predloge. Te predloge se primerjajo s tistimi, ki jih ustvarijo posamezniki, na katere se nanašajo osebni podatki, ki so med postopkom prijave dali predhodno privolitev (tj. uporabnik biometrične naprave), da bi lahko upravljavec podatkov prepoznal, ali je oseba uporabnik biometrične naprave ali ne. V tem primeru je sistem pogosto zasnovan za razlikovanje posameznikov, ki jih želi prepoznati iz podatkovne zbirke, od tistih, ki niso prijavljeni. Ker je namen edinstvena identifikacija posameznikov, je izjema iz člena 9(2) Splošne uredbe o varstvu podatkov še vedno potrebna za vsakogar, ki ga kamera posname.

[17] To pomeni, da je biometrična naprava v prostoru, ki je odprt za javnost, in lahko posname vsakega mimoidočega, v nasprotju z biometričnimi sistemi v nadzorovanih okoljih, ki se lahko uporabljajo samo s sodelovanjem osebe, ki je dala soglasje.

Primer: Hotel uporablja video nadzor za samodejno opozarjanje vodje hotela, da je prispel zelo pomemben gost, ko je prepoznan obraz takega gosta. Ti zelo pomembni gostje so predhodno dali svojo privolitev za uporabo prepoznavanja obrazov, preden so bili evidentirani v podatkovni zbirki, vzpostavljeni v ta namen. Ti sistemi obdelave biometričnih podatkov bi bili nezakoniti, razen če bi vsi preostali gostje (v namene identifikacije zelo pomembnih gostov) privolili v obdelavo v skladu s členom 9(2)(a) Splošne uredbe o varstvu podatkov.

Primer: Upravljavec na vhodu v koncertno dvorano, ki jo upravlja, namesti videonadzorni sistem s prepoznavanjem obrazov. Zagotoviti mora jasno ločena vhoda: enega z biometričnim sistemom in enega brez njega (kjer je na primer mogoče skenirati vstopnico). Vhodi, opremljeni z biometričnimi napravami, morajo biti nameščeni in dostopni tako, da preprečujejo, da bi sistem snemal biometrične predloge obiskovalcev, ki niso dali svoje privolitve.

85.

86. Nazadnje, če se zahteva privolitev v skladu s členom 9 Splošne uredbe o varstvu podatkov, upravljavec podatkov ne pogojuje dostopa do svojih storitev s sprejetjem biometrične obdelave. Povedano drugače in zlasti, kadar se biometrična obdelava uporablja za avtentikacijo, mora upravljavec podatkov ponuditi alternativno rešitev, ki ne vključuje biometrične obdelave, brez omejitev ali dodatnih stroškov za posameznika, na katerega se nanašajo osebni podatki. Ta alternativna rešitev je potrebna tudi za osebe, ki ne izpolnjujejo zahtev, povezanih z biometrično napravo (prijava ali odčitavanje biometričnih podatkov nista mogoča, invalidnost otežuje uporabo itd.), za primer nerazpoložljivosti biometrične naprave (kot je okvara naprave) pa je treba pripraviti nadomestno rešitev za neprekinjeno delovanje ponujene storitve, ki pa je omejena na izredno uporabo. V izjemnih primerih je lahko obdelava podatkov glavna dejavnost storitve, ki se opravlja po pogodbi, npr. muzej, ki pripravi razstavo, da bi predstavil uporabo naprave za prepoznavanje obrazov; v takem primeru posamezniki, na katere se nanašajo osebni podatki, ne morejo zavrniti obdelave biometričnih podatkov, če želijo sodelovati pri razstavi. V takem primeru je privolitev, ki se zahteva v skladu s členom 9, še vedno veljavna, če so izpolnjene zahteve iz člena 7.

5.2 Predlagani ukrepi za zmanjšanje tveganj pri obdelavi biometričnih podatkov

87. V skladu z načelom najmanjšega obsega podatkov morajo upravljavci podatkov zagotoviti, da podatki, pridobljeni iz digitalne slike za oblikovanje predloge, ne bodo preobsežni in bodo vključevali le informacije, ki so potrebne za določeni namen, da se prepreči morebitna nadaljnja obdelava. Sprejeti bi bilo treba ukrepe za zagotovitev, da predlog ni mogoče prenašati med biometričnimi sistemi.

88. Za identifikacijo in avtentikacijo/preverjanje bo verjetno potrebno shranjevanje predloge za uporabo pri poznejši primerjavi. Upravljavec podatkov mora razmisliti o najprimernejšem mestu za shranjevanje podatkov. V nadzorovanem okolju (razmejeni hodniki ali kontrolne točke) se predloge shranjujejo v samostojni napravi, ki jo hrani uporabnik in je pod njegovim nadzorom (v pametnem telefonu ali na osebni izkaznici), ali, če je to potrebno za posebne namene in če obstajajo objektivne potrebe, v centralizirani podatkovni zbirki v šifrirani obliki s ključem/skrivno kodo izključno v rokah osebe, da se prepreči nepooblaščen dostop do predloge ali mesta hrambe. Če se upravljavec podatkov ne more izogniti dostopu do predlog, mora sprejeti ustrezne ukrepe za zagotovitev varstva shranjenih podatkov. To lahko vključuje šifriranje predloge z uporabo kriptografskega algoritma.

89. V vsakem primeru upravljavec podatkov sprejme vse potrebne previdnostne ukrepe za ohranitev razpoložljivosti, celovitosti in zaupnosti podatkov, ki se obdelujejo. V ta namen upravljavec sprejme zlasti naslednje ukrepe: segmentacija podatkov med posredovanjem in shranjevanjem, shranjevanje

biometričnih predlog in neobdelanih podatkov ali identifikacija podatkov v različnih podatkovnih zbirkah, šifriranje biometričnih podatkov, zlasti biometričnih predlog, ter opredelitev politike za šifriranje in upravljanje ključev, vključitev organizacijskega in tehničnega ukrepa za odkrivanje goljufij, povezovanje kode celovitosti s podatki (na primer podpis ali zgoščevalna funkcija) in prepoved vsakršnega zunanjega dostopa do biometričnih podatkov. Taki ukrepi se bodo morali razvijati z napredkom tehnologij.

90. Poleg tega bi morali upravljavci podatkov brisati neobdelane podatke (slike obrazov, govorni signali, način hoje itd.) in zagotoviti učinkovitost tega brisanja. Če ni več pravne podlage za obdelavo, je treba neobdelane podatke izbrisati. Dejansko je mogoče v primeru, če je biometrična predloga pridobljena iz takih podatkov, predpostavljati, da bi vzpostavitev podatkovne zbirke lahko pomenila enako ali celo večjo nevarnost (saj morda ni vedno preprosto prebrati biometrične predloge, ne da bi vedeli, kako je bila programirana, neobdelani podatki pa so gradniki vsake predloge). Če bi moral upravljavec podatkov hraniti take podatke, bi bilo treba preučiti metode dodajanja šumov (kot je vodni tisk), zaradi katerih bi predloga postala neučinkovita. Upravljavec mora izbrisati biometrične podatke in predloge tudi v primeru nepooblaščenega dostopa do terminala za primerjavo z odčitavanjem ali strežnika za shranjevanje in ob koncu življenjske dobe biometrične naprave izbrisati vse podatke, ki niso koristni za nadaljnjo obdelavo.

6 PRAVICE POSAMEZNIKA, NA KATEREGA SE NANAŠAJO OSEBNI PODATKI

91. Zaradi narave obdelave podatkov pri uporabi video nadzora je treba nekatere pravice posameznikov, na katere se nanašajo osebni podatki, iz Splošne uredbe o varstvu podatkov dodatno pojasniti. Vendar to poglavje ni izčrpno, za obdelavo osebnih podatkov z video nadzorom se uporabljajo vse pravice iz Splošne uredbe o osebnih podatkih.

6.1 Pravica do dostopa

92. Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da pridobi potrditev od upravljavca, ali se njegovi osebni podatki obdelujejo ali ne. Za video nadzor to pomeni, da če se podatki na noben način ne shranjujejo ali prenašajo, lahko upravljavec po izteku časa nadzora v realnem času posreduje le informacijo, da se noben osebni podatek ne obdeluje več (poleg obveznosti glede splošnih informacij iz člena 13, glej *razdelek 7 – Obveznosti glede preglednosti in zagotavljanja informacij*). Če pa se podatki v času zahteve še vedno obdelujejo (tj., če se podatki kakor koli drugače shranjujejo ali stalno obdelujejo), bi moral posameznik, na katerega se nanašajo osebni podatki, pridobiti dostop in informacije v skladu s členom 15.

93. Vendar obstaja več omejitev, ki se lahko v nekaterih primerih uporabljajo v zvezi s pravico do dostopa.

Člen 15(4) Splošne uredbe o varstvu podatkov: negativen vpliv na pravice drugih

94. Glede na to, da se lahko v eni sekvenci video nadzora posname poljubno število posameznikov, na katere se nanašajo osebni podatki, bi ogled posnetka sprožil dodatno obdelavo osebnih podatkov drugih posameznikov, na katere se nanašajo osebni podatki. Če želi posameznik, na katerega se nanašajo osebni podatki, prejeti kopijo gradiva (člen 15(3)), lahko to negativno vpliva na pravice in svoboščine drugih posameznikovv gradivu. Za preprečitev takega vpliva bi moral upravljavec upoštevati, da zaradi vsiljive narave video posnetka v nekaterih primerih ne bi smel predati video posnetka, na katerem je mogoče identificirati druge posameznike, na katere

se nanašajo osebni podatki. Vendar pa se varstvo pravic tretjih oseb ne bi smelo uporabljati kot izgovor za preprečevanje upravičenih zahtevkov posameznikov po dostopu; upravljavec bi moral v takih primerih izvesti tehnične ukrepe za izpolnitev zahteve po dostopu (na primer urejanje slik s tehnikami, kot sta maskiranje ali premešanje). Vendar upravljavci niso obvezani izvesti takih tehničnih ukrepov, če se lahko drugače odzovejo na zahtevo v skladu s členom 15 v časovnem okviru, določenem v členu 12(3).

- Člen 11(2) Splošne uredbe o varstvu podatkov: upravljavec ne more identificirati posameznika, na katerega se nanašajo osebni podatki

95. Če video posnetek ne omogoča iskanja osebnih podatkov (tj., če mora upravljavec pregledati veliko količino shranjenega gradiva, da najde zadevnega posameznika, na katerega se nanašajo osebni podatki), upravljavec morda ne bo mogel identificirati posameznika, na katerega se nanašajo osebni podatki.

96. Zato bi moral posameznik, na katerega se nanašajo osebni podatki (poleg tega, da se sam identificira, lahko tudi osebno ali z osebnim dokumentom), v svoji zahtevi, naslovljeni na upravljavca, navesti, kdaj (v razumnem roku glede na število posameznikov, na katere se nanašajo osebni podatki, ki so bili posneti) je vstopil na območje, ki se nadzoruje. Upravljavec bi moral vnaprej obvestiti posameznika, na katerega se nanašajo osebni podatki, katere informacije potrebuje, da izpolni zahtevo. Če upravljavec lahko dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki, ga mora, če je to mogoče, o tem ustrezno obvestiti. V takem primeru bi moral upravljavec v svojem odgovoru posamezniku, na katerega se nanašajo osebni podatki, zagotoviti informacije o natančnem območju nadzora, preverjanju kamer, ki so se uporabljale, itd., da bi posameznik, na katerega se nanašajo osebni podatki, v celoti razumel, kateri njegovi osebni podatki so bili morda predmet obdelave.

Primer: Če posameznik, na katerega se nanašajo osebni podatki, zahteva kopijo svojih osebnih podatkov, ki so se obdelali z video nadzorom ob vhodu v nakupovalno središče s 30.000 obiskovalci na dan, bi moral navesti, kdaj je prešel območje, ki se spremlja, v približno enournem obdobju. Če upravljavec še vedno obdeluje gradivo, bi bilo treba zagotoviti kopijo video posnetka. Če je mogoče v istem gradivu identificirati druge posameznike, na katere se nanašajo osebni podatki, je treba zadevni del gradiva anonimizirati (na primer z zameglitvijo kopije ali njenih delov), preden se izroči posamezniku, na katerega se nanašajo osebni podatki, ki je vložil zahtevo.

Primer: Če upravljavec samodejno izbriše vse posnetke, na primer v dveh dneh, ne more predložiti posnetka posamezniku, na katerega se nanašajo osebni podatki, po izteku teh dveh dni. Če upravljavec prejme zahtevo po teh dveh dneh, je treba posameznika, na katerega se nanašajo osebni podatki, o tem ustrezno obvestiti.

97.

- Člen 12 Splošne uredbe o varstvu podatkov: pretirane zahteve

98. V primeru pretiranih ali očitno neutemeljenih zahtev posameznika, na katerega se nanašajo osebni podatki, lahko upravljavec bodisi zaračuna razumno pristojbino v skladu s členom 12(5)(a) Splošne uredbe o varstvu podatkov bodisi zavrne ukrepanje glede zahteve (člen 12(5)(b) Splošne uredbe o varstvu podatkov). Upravljavec mora biti sposoben dokazati, da je zahteva očitno neutemeljena ali pretirana.

6.2 Pravica do izbrisa in pravica do ugovora

6.2.1 Pravica do izbrisa (pravica do pozabe)

99. Če upravljavec nadaljuje obdelavo osebnih podatkov po izvajanju nadzora v realnem času (npr. shranjevanje), lahko posameznik, na katerega se nanašajo osebni podatki, zahteva izbris osebnih podatkov v skladu s členom 17 Splošne uredbe o varstvu podatkov.

100. Upravljavec mora na zahtevo brez nepotrebnega odlašanja izbrisati osebne podatke, če je izpolnjena ena od okoliščin, navedenih v členu 17(1) Splošne uredbe o varstvu podatkov (in ne velja nobena od izjem, navedenih v členu 17(3) Splošne uredbe o varstvu podatkov). To vključuje obveznost izbrisa osebnih podatkov, če niso več potrebni za namen, za katerega so se prvotno hranili, ali če je obdelava nezakonita (glej tudi *razdelek 8 – Obdobja hrambe in obveznost izbrisa*). Poleg tega bi bilo treba glede na pravno podlago osebne podatke izbrisati:

- zaradi *privolitve*, kadar je privolitev umaknjena (in ni druge pravne podlage za obdelavo);
- zaradi *zakonitega interesa*:
    - kadar posameznik, na katerega se nanašajo osebni podatki, uveljavlja pravico do ugovora (glej *razdelek 6.2.2*), za njihovo obdelavo pa ne obstajajo nobeni prevladujoči nujni zakoniti razlogi, ali
    - v primeru neposrednega trženja (vključno z oblikovanjem profilov), kadar posameznik, na katerega se nanašajo podatki, ugovarja obdelavi.

101. Če je upravljavec objavil video posnetek (npr. ga je predvajal ali prenašal prek spleta), je treba sprejeti razumne ukrepe, da se o zahtevi obvesti druge upravljavce (ki zdaj obdelujejo zadevne osebne podatke) v skladu s členom 17(2) Splošne uredbe o varstvu podatkov. Razumni ukrepi bi morali vključevati tehnične ukrepe, ob upoštevanju razpoložljive tehnologije in stroškov izvajanja. Če je to mogoče, bi moral upravljavec po izbrisu osebnih podatkov obvestiti vse, ki so jim bili osebni podatki pred tem razkriti, in sicer v skladu s členom 19 Splošne uredbe o varstvu podatkov.

102. Poleg obveznosti upravljavca, da na zahtevo posameznika, na katerega se nanašajo osebni podatki, izbriše osebne podatke, mora upravljavec v skladu s splošnimi načeli Splošne uredbe o varstvu podatkov omejiti osebne podatke, ki se hranijo (glej *razdelek 8*).

103. Glede video nadzora je treba opozoriti, da se na primer z zamegljevanjem slike brez možnosti retroaktivne obnovitve osebnih podatkov, ki jih je slika vsebovala prej, osebni podatki štejejo za izbrisane v skladu s Splošno uredbo o varstvu podatkov.

> Primer: Prodajalna z nujnimi življenjskimi potrebščinami ima težave z vandalizmom, zlasti v zunanjem delu prodajalne, zato uporablja video nadzor pred vhodom, ki je neposredno povezan s stenami. Mimoidoči zahteva, da se njegovi osebni podatki takoj izbrišejo. Upravljavec mora odgovoriti na zahtevo brez nepotrebnega odlašanja in najpozneje v enem mesecu. Ker zadevni posnetek ne izpolnjuje več namena, za katerega se je prvotno hranil (v času, ko je šel posameznik, na katerega se nanašajo osebni podatki, mimo prodajalne, ni prišlo do vandalizma), v času zahteve ni zakonitega interesa za hrambo podatkov, ki bi prevladal nad interesi posameznikov, na katere se nanašajo osebni podatki. Upravljavec mora osebne podatke izbrisati.

104.

6.2.2 Pravica do ugovora

105. Zaradi izvajanja video nadzora na podlagi *zakonitega interesa* (člen 6(1)(f) Splošne uredbe o varstvu podatkov) ali zaradi potreb pri izvajanju naloge v *javnem interesu* (člen 6(1)(e) Splošne uredbe o varstvu podatkov) ima posameznik, na katerega se nanašajo osebni podatki, pravico, da iz razlogov, povezanih z njegovim posebnim položajem, kadar koli ugovarja obdelavi v skladu s členom 21 Splošne uredbe o varstvu podatkov. Obdelavo njegovih podatkov je treba nato ustaviti, razen če upravljavec dokaže nujne zakonite razloge za obdelavo, ki prevladajo nad pravicami in interesi posameznika, na katerega se nanašajo osebni podatki. Upravljavec mora odgovoriti na zahtevo posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja in najpozneje v enem mesecu.

106. V zvezi z video nadzorom je ta ugovor mogoč bodisi ob vstopu na območje, ki se spremlja, v času, ko se oseba nahaja na tem območju, ali po odhodu s tega območja. V praksi to pomeni, da je razen v primeru, ko ima upravljavec nujne zakonite razloge za to, spremljanje območja, na katerem bi bilo posameznike mogoče identificirati, zakonito le, če

    (1) lahko upravljavec na zahtevo takoj ustavi obdelavo osebnih podatkov s kamero ali

    (2) če je območje, ki se spremlja, tako natančno omejeno, da lahko upravljavec zagotovi privolitev posameznika, na katerega se nanašajo osebni podatki, pred njegovim vstopom na območje in to ni območje, do katerega je posameznik, na katerega se nanašajo osebni podatki, kot državljan upravičen dostopati.

107. Te smernice niso namenjene opredelitvi *nujnega* zakonitega interesa (člen 21 Splošne uredbe o varstvu podatkov).

108. Kadar se video nadzor uporablja za namene neposrednega trženja, ima posameznik, na katerega se nanašajo osebni podatki, pravico ugovarjati obdelavi na diskrecijski podlagi, saj je pravica do ugovora v tem okviru absolutna (člen 21(2) in (3) Splošne uredbe o varstvu podatkov).

> Primer: Podjetje se srečuje s težavami v zvezi s kršitvami varnosti pri javnem vhodu in uporablja video nadzor na podlagi razlogov zakonitega interesa z namenom ujeti tiste, ki vstopajo nezakonito. Obiskovalec ugovarja obdelavi njegovih podatkov z videonadzornim sistemom na podlagi razlogov, povezanih z njegovim posebnim položajem. Vendar podjetje v tem primeru zahtevo zavrne z obrazložitvijo, da je shranjeni posnetek potreben zaradi notranje preiskave, ki poteka, zaradi česar obstajajo nujni zakoniti razlogi za nadaljnjo obdelavo osebnih podatkov.

109.

7 OBVEZNOSTI GLEDE PREGLEDNOSTI IN ZAGOTAVLJANJA INFORMACIJ[18]

110. Evropska zakonodaja o varstvu podatkov že dolgo določa, da bi morali biti posamezniki, na katere se nanašajo osebni podatki, seznanjeni z dejstvom, da se izvaja video nadzor. Natančno bi morali biti obveščeni o prostorih, ki se nadzorujejo[19]. V Splošni uredbi o varstvu podatkov so obveznosti glede preglednosti in zagotavljanja informacij določene v členu 12 in naslednjih. Več podrobnosti je v „Smernicah o preglednosti v skladu z Uredbo 2016/679 (WP260)“, ki jih je pripravila Delovna skupina iz člena 29 in jih je Evropski odbor za varstvo podatkov potrdil 25. maja 2018. V skladu z odstavkom 26 WP260 se člen 13 Splošne uredbe o varstvu podatkov uporablja, če „[…] *posameznik, na katerega se nanašajo osebni podatki [zbira podatke] z opazovanjem (npr. z uporabo avtomatiziranih naprav za zbiranje podatkov ali programsko opremo za zbiranje podatkov, kot so kamere* […])“.

111. Glede na količino informacij, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, lahko upravljavci podatkov uporabijo pristop, ki vključuje več ravni in pri katerem se odločijo za uporabo kombinacije metod, da se zagotovi preglednost (WP260, odstavek 35; WP89, odstavek 22). Glede video nadzora je treba najpomembnejše informacije prikazati na samem opozorilnem znaku (prva raven), nadaljnji obvezni podatki pa se lahko zagotovijo z drugimi sredstvi (druga raven).

7.1 Informacije prve ravni (opozorilni znak)

112. Prva raven se nanaša na primarni način prvega stika upravljavca s posameznikom, na katerega se nanašajo osebni podatki. V tej fazi lahko upravljavci uporabijo opozorilni znak z ustreznimi informacijami. Prikazane informacije se lahko navedejo skupaj z uporabo ikone, da se na jasno razviden, razumljiv in berljiv način zagotovi smiseln pregled načrtovane obdelave (člen 12(7) Splošne uredbe o varstvu podatkov). Oblika informacij mora biti prilagojena posamezni lokaciji (odstavek 22 WP89).

7.1.1 Položaj opozorilnega znaka

113. Informacije bi morale biti na takem mestu, da lahko posameznik, na katerega se nanašajo osebni podatki, enostavno prepozna okoliščine nadzora, preden vstopi na območje, ki se spremlja (približno na višini oči). Položaja kamere ni treba razkriti, če ni dvoma glede tega, katera območja se spremljajo, in je okvir nadzora nedvoumno pojasnjen (odstavek 22 WP 89). Posameznik, na katerega se nanašajo osebni podatki, mora biti sposoben oceniti, katero območje snema kamera, tako da se lahko izogne nadzoru ali da lahko po potrebi prilagodi svoje vedenje.

7.1.2 Vsebina prve ravni

114. Informacije prve ravni (opozorilni znak) bi morale načeloma vsebovati najpomembnejše informacije, npr. podrobnosti o namenih obdelave, identiteto upravljavca in obstoj pravic posameznika, na katerega se nanašajo osebni podatki, skupaj z informacijami o največjih učinkih obdelave[20]. To lahko na primer vključuje zakonite interese upravljavca (ali tretje osebe) in kontaktne podatke pooblaščene osebe za varstvo podatkov (če je to ustrezno). Poleg tega je treba opozoriti na podrobnejše informacije druge ravni ter navesti, kje in kako jih je mogoče najti.

---

[18] Uporabljajo se lahko posebne zahteve iz nacionalne zakonodaje.
[19] Glej WP89, Mnenje 4/2004 Delovne skupine iz člena 29 o obdelavi osebnih podatkov z video nadzorom.
[20] Glej odstavek 38 WP260.

115. Znak bi moral vsebovati tudi vse informacije, ki bi lahko posameznika, na katerega se nanašajo osebni podatki, presenetile (odstavek 38 WP260). To bi lahko bile na primer informacije o prenosu tretjim osebam, zlasti če so le te zunaj EU, in o obdobju hrambe. Če te informacije niso navedene, bi lahko posameznik, na katerega se nanašajo osebni podatki, utemeljeno predpostavljal, da spremljanje poteka samo v živo (brez snemanja podatkov ali njihovega posredovanja tretjim osebam).

116.

Primer (nezavezujoč predlog):

Identiteta upravljavca in, če je ustrezno, predstavnika upravljavca:

Kontaktni podatki, vključno s podatki pooblaščene osebe za varstvo podatkov (če je ustrezno):

Informacije o obdelavi, ki imajo največji vpliv na posameznika, na katerega se nanašajo osebni podatki (npr. obdobje hrambe ali spremljanje v živo, objava ali posredovanje video posnetkov tretjim osebam):

Namen(i) video nadzora:

Pravice posameznikov, na katere se nanašajo osebni podatki:

7.2 Informacije druge ravni

117. Informacije druge ravni morajo biti na voljo tudi na mestu, ki je posamezniku, na katerega se nanašajo osebni podatki, enostavno dostopno, na primer kot celovit informativni list, ki je na voljo na osrednji lokaciji (npr. na informativnih točkah, recepciji ali blagajni) ali prikazan na zlahka dostopnem plakatu. Kot je navedeno zgoraj, je treba na opozorilnem znaku prve ravni jasno opozoriti na informacije druge ravni. Poleg tega je najbolje, če se informacije prve ravni sklicujejo na digitalni vir (npr. koda QR ali naslov spletnega mesta) druge ravni. Vendar bi morale biti informacije zlahka dostopne tudi v nedigitalni obliki. Dostop do informacij druge ravni bi moral biti mogoč brez vstopa na nadzorovano območje, zlasti če se informacije zagotovijo digitalno (to se lahko na primer doseže s povezavo). Drugo ustrezno sredstvo je lahko telefonska številka, na katero je mogoče poklicati. Ne glede na to, kako se informacije zagotovijo, morajo vsebovati vse, kar je obvezno v skladu s členom 13 Splošne uredbe o varstvu podatkov.

118. Poleg teh možnosti in za njihovo večjo učinkovitost Evropski odbor za varstvo podatkov spodbuja uporabo tehnoloških sredstev za zagotavljanje informacij posameznikom, na katere se nanašajo osebni podatki. To lahko na primer vključuje kamere za določanje zemljepisnega položaja in informacije v aplikacijah ali spletnih mestih za kartiranje, tako da lahko posamezniki enostavno na eni strani identificirajo in določijo vire video posnetkov, povezane z uveljavljanjem svojih pravic, na drugi strani pa pridobijo podrobnejše informacije o dejanju obdelave.

Primer: Lastnik trgovine spremlja dogajanje v svoji trgovini. Za skladnost s členom 13 zadostuje, da namesti opozorilni znak na dobro vidnem mestu ob vhodu v trgovino, ki vsebuje informacije prve ravni. Poleg tega mora na blagajni ali katerem koli drugem osrednjem in zlahka dostopnem mestu v trgovini zagotoviti informativni list.

119.

8 OBDOBJA HRAMBE IN OBVEZNOST IZBRISA

120. Osebni podatki se ne smejo hraniti dlje, kot je potrebno za namene, za katere se obdelujejo (člen 5(1)(c) in (e) Splošne uredbe o varstvu podatkov). V nekaterih državah članicah morda obstajajo posebne določbe za obdobja hrambe, kar zadeva video nadzor po členu 6(2) Splošne uredbe o varstvu podatkov.

121. Potrebo po hrambi osebnih podatkov bi bilo treba presojati za čim krajše obdobje. Na splošno je zakoniti namen video nadzora pogosto varstvo lastnine ali zavarovanje dokazov. Običajno se nastala škoda lahko ugotovi v enem ali dveh dneh. Za lažje dokazovanje skladnosti z okvirom varstva podatkov je v interesu upravljavca, da vnaprej poskrbi za organizacijsko ureditev (npr. po potrebi imenuje predstavnika za pregledovanje in varovanje video gradiva). Ob upoštevanju načel iz člena 5(1)(c) in (e) Splošne uredbe o varstvu podatkov, tj. načel najmanjšega obsega podatkov in omejitve shranjevanja, bi bilo treba osebne podatke v večini primerov (npr. za namen odkrivanja vandalizma) po nekaj dneh izbrisati, v idealnem primeru samodejno. Daljše kot je določeno obdobje hrambe (zlasti, če je daljše od 72 ur), bolj je treba utemeljiti zakonitost namena in potrebo po shranjevanju. Če upravljavec video nadzora ne uporablja le za spremljanje svojih prostorov, ampak namerava podatke tudi shranjevati, mora zagotoviti, da je shranjevanje dejansko potrebno za dosego namena. V takem primeru mora biti obdobje hrambe jasno opredeljeno in določeno za vsak posamezen namen. Odgovornost upravljavca je, da določi obdobje hrambe v skladu z načeloma potrebnosti in sorazmernosti ter dokaže skladnost z določbami Splošne uredbe o varstvu podatkov.

Primer: Lastnik majhne trgovine bi običajno še v istem dnevu opazil, da je prišlo do vandalizma. Zato zadošča običajno 24-urno obdobje hrambe. Vendar pa so konci tedna, ko je trgovina zaprta, in daljša obdobja dopusta lahko razlog za daljše obdobje hrambe. Če se odkrije škoda, mora video posnetek morda hraniti daljše obdobje, da se zoper kršitelja sproži sodni postopek.

122.

9 TEHNIČNI IN ORGANIZACIJSKI UKREPI

123. Kot je navedeno v členu 32(1) Splošne uredbe o varstvu podatkov, mora biti obdelava osebnih podatkov med video nadzorom ne le zakonsko dovoljena, ampak jo morajo upravljavci in obdelovalci tudi ustrezno zavarovati. Izvedeni **organizacijski in tehnični ukrepi** morajo biti **sorazmerni s tveganji za pravice in svoboščine posameznikov**, ki izhajajo iz nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do podatkov video nadzora. V skladu s členoma 24 in 25 Splošne uredbe o varstvu podatkov morajo upravljavci izvesti tehnične in organizacijske ukrepe tudi za zaščito vseh načel varstva podatkov med obdelavo ter vzpostaviti sredstva, s katerimi lahko posamezniki, na katere se nanašajo osebni podatki, uveljavljajo pravice, kot so opredeljene v členih 15–22 Splošne uredbe o varstvu podatkov. Upravljavci podatkov bi morali sprejeti notranji okvir in notranje politike, ki bi zagotavljali to izvajanje ob določitvi sredstev za

obdelavo in med izvajanjem obdelave, vključno z izvedbo ocene učinka v zvezi z varstvom podatkov, če je potrebna.

9.1 Pregled videonadzornega sistema

124. Videonadzorni sistem[21] sestavljajo analogne in digitalne naprave ter programska oprema za snemanje slik dogajanja, upravljanje slik in njihovo prikazovanje operaterju. Njegovi sestavni deli so razvrščeni v naslednje kategorije:

- Video okolje: snemanje slik, medsebojne povezave in upravljanje slik:
  - namen snemanja slik je ustvarjanje slike realnega sveta v taki obliki, da jo lahko uporablja preostali sistem,
  - medsebojne povezave opisujejo vse prenose podatkov v video okolju, tj. povezave in komunikacije. Primeri povezav so kabli, digitalna omrežja in brezžični prenosi. Komunikacije opisujejo vse video signale in kontrolne podatkovne signale, ki so lahko digitalni ali analogni,
  - upravljanje slik vključuje analizo, shranjevanje in predstavitev slike ali zaporedja slik.
- Z vidika upravljanja sistema ima videonadzorni sistem naslednje logične funkcije:
  - upravljanje podatkov in upravljanje dejavnosti, kar vključuje upravljanje ukazov operaterja in dejavnosti, ki jih ustvari sistem (alarmni postopki, opozarjanje upravljavcev);
  - vmesniki do drugih sistemov lahko vključujejo povezavo z drugimi varnostnimi (nadzor dostopa, požarni alarm) in nevarnostnimi sistemi (sistemi za upravljanje stavb, samodejno prepoznavanje registrskih tablic).
- Varnost videonadzornega sistema sestavljajo zaupnost sistema in podatkov, celovitost in razpoložljivost:
  - varnost sistema vključuje fizično varnost vseh sestavnih delov sistema in nadzor nad dostopom do videonadzornega sistema,
  - varnost podatkov vključuje preprečevanje izgube podatkov ali manipulacije z njimi.

[21] Splošna uredba o varstvu podatkov ne vsebuje opredelitve videonadzornega sistema; tehnični opis je na primer mogoče najti v standardu EN 62676-1-1:2014 Sistemi za video nadzor za uporabo v varnostnih aplikacijah – del 1-1: Zahteve za video sistem.

125.

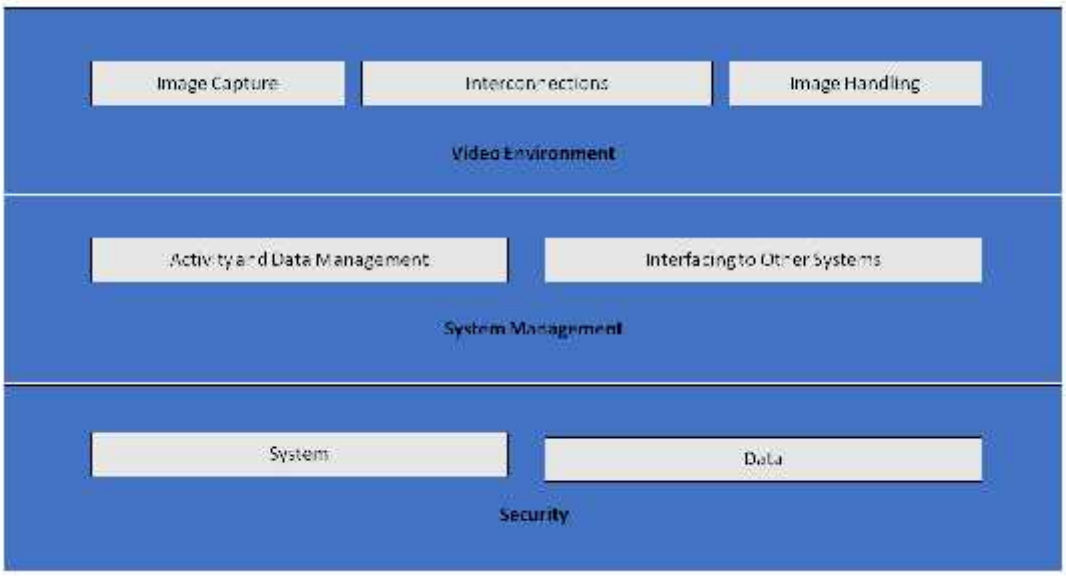

Image Capture	Snemanje slik
Interconnections	Medsebojne povezave
Image Handling	Upravljanje slik
Video Environment	Video okolje
Activity and Data Management	Upravljanje dejavnosti in podatkov
Interfacing to Other Systems	Povezovanje z drugimi sistemi
System Management	Upravljanje sistema
System	Sistem
Data	Podatki
Security	Varnost

Slika 1-–videonadzorni sistem

9.2 Vgrajeno in privzeto varstvo podatkov

126. Kot je navedeno v členu 25 Splošne uredbe o varstvu podatkov, morajo upravljavci uvesti ustrezne tehnične in organizacijske ukrepe, takoj ko začnejo načrtovati video nadzor, tj. pred začetkom zbiranja in obdelave video posnetkov. Ta načela poudarjajo potrebo po vgrajenih tehnologijah za boljše varovanje zasebnosti, privzetih nastavitvah, ki zmanjšujejo obdelavo podatkov, in zagotavljanju potrebnih orodij, ki omogočajo največje možno varstvo osebnih podatkov[22].

127. Upravljavci bi morali vključiti zaščitne ukrepe glede varstva podatkov in zasebnosti ne le v specifikacije tehnologije glede zasnove, ampak tudi v organizacijske prakse. Glede organizacijskih praks bi moral upravljavec sprejeti ustrezen okvir upravljanja ter vzpostaviti in izvajati politike in postopke, povezane z video nadzorom. S tehničnega vidika bi morala specifikacija in zasnova sistema vključevati zahteve za obdelavo osebnih podatkov v skladu z načeli, navedenimi v členu 5 Splošne uredbe o varstvu podatkov (zakonitost obdelave, omejitev namena in podatkov, privzeti najmanjši obseg podatkov v smislu člena 25(2) Splošne uredbe o varstvu podatkov, celovitost in zaupnost, odgovornost itd.). Če upravljavec načrtuje nakup komercialnega videonadzornega sistema, mora vključiti te zahteve v specifikacijo nakupa. Zagotoviti mora skladnost s temi zahtevami ter jih

[22] WP 168, Mnenje o prihodnosti zasebnosti, skupni prispevek Delovne skupine za varstvo podatkov iz člena 29 in Delovne skupine Evropske komisije za policijo in pravosodje o pravnem okviru za temeljno pravico do varstva osebnih podatkov (sprejeto 1. decembra 2009).

uporabljati za vse sestavne dele sistema in vse podatke, ki jih sistem obdela, in sicer vso njihovo celotno življenjsko dobo.

9.3 Konkretni primeri ustreznih ukrepov

128. Večina ukrepov, ki se lahko uporabljajo za zaščito video nadzora, zlasti kadar se uporabljata digitalna in programska oprema, se ne bo razlikovala od tistih, ki se uporabljajo pri drugih sistemih IT. Vendar mora upravljavec ne glede na izbrano rešitev ustrezno zaščititi vse sestavne dele videonadzornega sistema in podatke v vseh fazah, tj. med shranjevanjem (podatki v mirovanju), prenosom (podatki med prenašanjem) in obdelavo (podatki v uporabi). Za to morajo upravljavci in obdelovalci združiti organizacijske in tehnične ukrepe.

129. Pri izbiri tehničnih rešitev bi moral upravljavec razmisliti o tehnologijah, ki upoštevajo zasebnost, tudi zato, ker povečujejo varnost. Primeri takih tehnologij so sistemi, ki omogočajo maskiranje ali premešanje delov, ki niso pomembni za nadzor, ali obdelavo slik tretjih oseb pri posredovanju video posnetkov posameznikom, na katere se nanašajo osebni podatki[23]. Po drugi strani pa izbrane rešitve ne bi smele zagotavljati funkcij, ki niso potrebne (npr. neomejeno premikanje kamer, možnost spreminjanja velikosti prikaza, radijsko oddajanje, analiza in zvočni posnetki). Zagotovljene funkcije, ki niso nujne, je treba deaktivirati.

130. V zvezi s tem vprašanjem je na voljo veliko literature, vključno z mednarodnimi standardi in tehničnimi specifikacijami o fizični varnosti multimedijskih sistemov[24] in varnosti splošnih sistemov IT[25]. Zato ta razdelek vključuje samo splošen pregled te teme.

9.3.1 Organizacijski ukrepi

131. Poleg morebitne potrebne ocene učinka v zvezi z varstvom podatkov (glej *razdelek 10*) bi morali upravljavci pri oblikovanju svojih politik in postopkov na področju video nadzora obravnavati naslednje teme:

- kdo je odgovoren za upravljanje in delovanje videonadzornega sistema;
- namen in področje uporabe projekta video nadzora;
- ustrezna in prepovedana uporaba (kje in kdaj je video nadzor dovoljen ter kje in kdaj ni; npr. uporaba skritih kamer in snemanja zvoka poleg snemanja slike)[26];
- ukrepi v zvezi s preglednostjo iz *razdelka 7 (Obveznosti glede preglednosti in zagotavljanja informacij)*;
- kako se video snema in koliko časa, vključno z arhivsko hrambo video posnetkov, povezanih z varnostnimi incidenti;
- kdo mora opraviti ustrezno usposabljanje in kdaj;
- kdo ima dostop do video posnetkov in za kakšne namene;
- operativni postopki (npr. kdo spremlja video nadzor in od kod, kaj storiti v primeru kršitve varstva podatkov);
- katere postopke morajo zunanje strani uporabiti, da zahtevajo video posnetke, in postopki za zavrnitev ali odobritev takih zahtev;
- postopki za nabavo, namestitev in vzdrževanje videonadzornega sistema;

---

[23] Uporaba takih tehnologij je lahko v nekaterih primerih celo obvezna, da se zagotovi skladnost s členom 5(1)(c). V vsakem primeru se lahko uporabljajo kot primeri dobre prakse.

[24] IEC TS 62045 – Multimedijska varnost – Smernice za zaščito zasebnosti opreme in sistemov, ki so v uporabi ali umaknjeni iz uporabe.

[25] ISO/IEC 27000 – Serija sistemov za upravljanje informacijske varnosti.

[26] To je lahko odvisno od nacionalne zakonodaje in sektorskih predpisov.

- obvladovanje incidentov in postopki izterjave.

9.3.2 Tehnični ukrepi

132. **Varnost sistema** pomeni **fizično varnost** vseh sestavnih delov sistema in celovitost sistema, tj. **zaščito pred namernimi in nenamernimi posegi v normalno delovanje** in **odpornost nanje** ter **nadzor nad dostopom**. Varnost podatkov pomeni **zaupnost** (podatki so dostopni le tistim, ki jim je odobren dostop), **celovitost** (preprečevanje izgube podatkov in manipulacije z njimi) in **razpoložljivost** (dostop do podatkov je mogoč na zahtevo).

133. **Fizična varnost** je ključni del varstva podatkov in prva obrambna črta, saj ščiti opremo videonadzornega sistema pred tatvinami, vandalizmom, naravnimi nesrečami, nesrečami, ki jih povzroči človek, in naključno škodo (npr. zaradi električnih udarov, skrajnih temperatur in razlite kave). V primeru analognih sistemov ima fizična varnost glavno vlogo pri njihovi zaščiti.

134. **Varnost sistema in podatkov**, tj. zaščita pred namerno in nenamerno motnjo normalnega delovanja, lahko vključuje:

- zaščito celotne infrastrukture videonadzornega sistema (vključno z daljinsko vodenimi kamerami, kabli in oskrbo z električno energijo) pred fizičnimi posegi in tatvino;
- zaščito pri posredovanju posnetkov s komunikacijskimi kanali, ki so zavarovani pred prestrezanjem;
- šifriranje podatkov;
- uporabo rešitev, ki temeljijo na strojni in programski opremi, kot so požarni zidovi, protivirusna zaščita in sistemi za zaznavanje vsiljivcev proti kibernetskim napadom;
- odkrivanje okvar sestavnih delov, programske opreme in medsebojnih povezav;
- sredstva za vnovično vzpostavitev razpoložljivosti sistema in dostopa do njega v primeru fizičnega ali tehničnega incidenta.

135. **Nadzor nad dostopom** zagotavlja, da lahko do sistema in podatkov dostopajo samo pooblaščene osebe, drugim pa je to onemogočeno. Ukrepi, ki podpirajo fizični in logični nadzor nad dostopom, vključujejo:

- zagotavljanje, da so vsi prostori, v katerih se izvaja spremljanje z video nadzorom in v katerih se hranijo video posnetki, zaščiteni pred nenadzorovanim dostopom tretjih oseb;
- taka namestitev zaslonov (zlasti če so v odprtih prostorih, kot je recepcija), da jih lahko vidijo samo pooblaščeni upravljavci;
- opredelitev in izvajanje postopkov za odobritev, spremembo in preklic fizičnega in logičnega dostopa;
- uporabo metod in sredstev za avtentikacijo uporabnikov in izdajanje dovoljenj uporabnikom, med drugim z dolžino in pogostostjo spreminjanja gesel;
- evidentiranje in redno pregledovanje ukrepov, ki jih izvajajo uporabniki (v zvezi s sistemom in podatki);
- stalno spremljanje in zaznavanje neuspešnih dostopov, pri čemer se ugotovljene pomanjkljivosti čim prej odpravijo.

10 OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV

136. V skladu s členom 35(1) Splošne uredbe o varstvu podatkov morajo upravljavci izvesti ocene učinka v zvezi z varstvom podatkov, kadar obstaja verjetnost, da bo vrsta obdelave podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov. Člen 35(3)(c) Splošne uredbe o varstvu podatkov določa, da morajo upravljavci izvesti ocene učinka v zvezi z varstvom podatkov, če obdelava pomeni obsežno sistematično spremljanje javno dostopnega območja. Poleg tega se v skladu s členom 35(3)(b) Splošne uredbe o varstvu podatkov ocena učinka v zvezi z varstvom podatkov zahteva tudi, kadar upravljavec načrtuje obsežno obdelavo posebne vrste podatkov.

137. Smernice o oceni učinka v zvezi z varstvom podatkov[27] zagotavljajo nadaljnje nasvete in podrobnejše primere, ki se nanašajo na video nadzor (npr. v zvezi z „uporabo sistema kamer za spremljanje vedenja voznikov na avtocestah“). Člen 35(4) Splošne uredbe o varstvu podatkov določa, da mora vsak nadzorni organ objaviti seznam vrste dejanj obdelave, za katera velja zahteva po oceni učinka v zvezi z varstvom podatkov v njegovi državi. Ti seznami so običajno na voljo na spletiščih organov. Glede na značilne namene video nadzora (zaščita ljudi in lastnine, odkrivanje, preprečevanje in nadzor nad kaznivimi dejanji, zbiranje dokazov in biometrična identifikacija osumljencev) je razumno predvidevati, da bo v številnih primerih video nadzora potrebna ocena učinka v zvezi z varstvom podatkov. Zato bi morali upravljavci podatkov te dokumente skrbno pregledati, da bi določili, ali je taka ocena potrebna, in jo po potrebi izvedli. Na podlagi rezultata ocene učinka v zvezi z varstvom podatkov bi moral upravljavec določiti ukrepe za varstvo podatkov, ki jih je treba izvesti.

138. Prav tako je pomembno poudariti, da če rezultati ocene učinka v zvezi z varstvom podatkov kažejo, da bi obdelava povzročila veliko tveganje, kljub varnostnim ukrepom, ki jih načrtuje upravljavec, se je treba pred obdelavo posvetovati z ustreznim nadzornim organom. Podrobnosti o predhodnem posvetovanju so navedene v členu 36.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

[27] WP248 rev.01, Smernice o oceni učinka v zvezi z varstvom podatkov (DPIA) in določanjem, ali „obstaja verjetnost, da bo dejanje obdelave povzročilo visoko tveganje“ za namene Uredbe 2016/679 – potrdil Evropski odbor za varstvo podatkov.