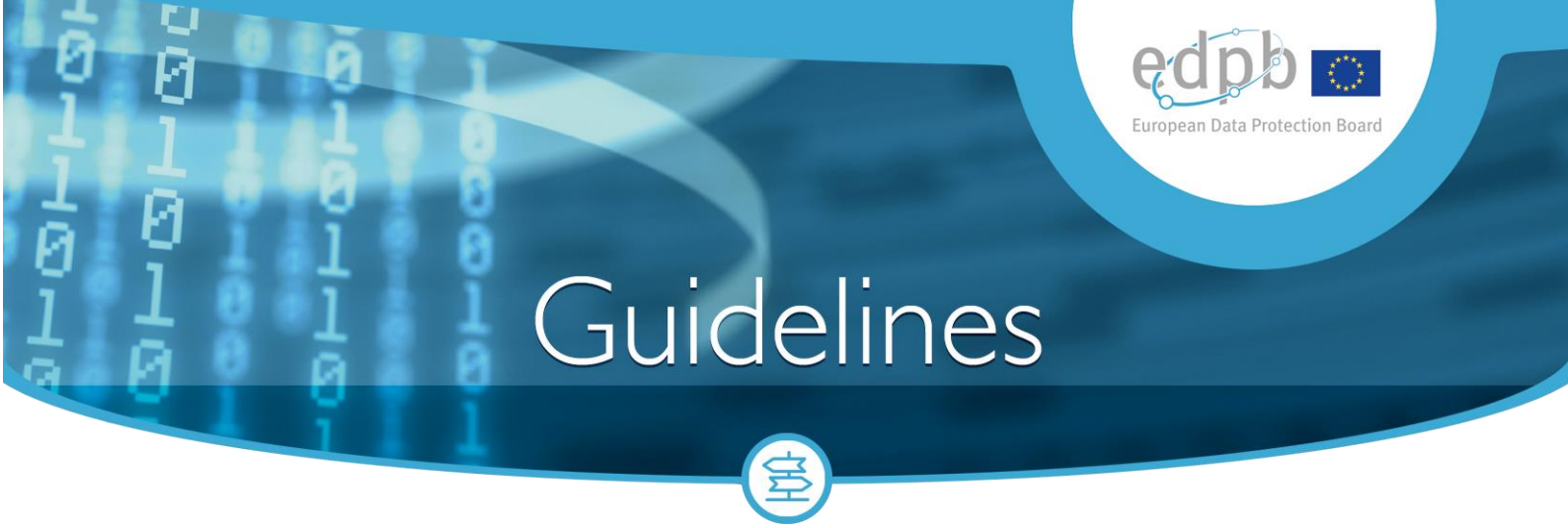

Smjernice 3/2019 o obradi osobnih podataka putem videouređaja

Verzija 2.0

Doneseno 29. siječnja 2020.

Povijest verzija

Verzija 2.0	29. siječnja 2020.	Donošenje Smjernica nakon javnog savjetovanja
Verzija 1.0	10. srpnja 2019.	Donošenje Smjernica za javno savjetovanje

Sadržaj

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe 2016/679/EU Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: Opća uredba o zaštiti podataka),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članak 12. i članak 22. svojeg Poslovnika,

DONIO JE SLJEDEĆE SMJERNICE:

1 UVOD

1. Intenzivna uporaba videouređaja utječe na ponašanje građana. Povećanom primjenom takvih alata u mnogim sferama svakodnevnog života stvara se dodatni pritisak na pojedinca koji će nastojati spriječiti da se otkrije nešto što bi se moglo smatrati nepravilnošću. Takve tehnologije zapravo mogu ograničiti mogućnosti anonimnog kretanja i anonimnog korištenja uslugama te općenito govoreći mogu ograničiti mogućnost da se ostane neprimijećen. To ima goleme posljedice kad je riječ o zaštiti osobnih podataka.

2. Premda pojedinci katkad nemaju ništa protiv videonadzora postavljenog, na primjer, u određene sigurnosne svrhe, potrebno je pružiti jamstva da će se spriječiti svaka zlouporaba takvog sustava u potpuno druge svrhe koje ispitanik ne očekuje (npr. u marketinške svrhe, u svrhe praćenja učinkovitosti zaposlenika itd.). Usto, sada su u uporabi i mnogi alati koji omogućuju iskorištavanje snimki i pretvaranje običnih kamera u pametne kamere. Zbog količine podataka koji nastanu snimanjem videouređajima, uz spomenute alate i tehnike, povećava se ne samo rizik od sekundarne uporabe (bez obzira na to je li ona povezana sa svrhom koja je izvorno pripisana sustavu), već i rizik od zlouporabe. Kad je riječ o videonadzoru, uvijek je potrebno pažljivo razmotriti opća načela iz Opće uredbe o zaštiti podataka (članak 5.).

3. Sustavi videonadzora u mnogim pogledima mijenjaju način interakcije stručnjaka iz privatnog i javnog sektora na privatnim i javnim mjestima u svrhu unapređenja sigurnosti, analiziranja potrošača, personaliziranog oglašavanja itd. Zahvaljujući sve većoj primjeni pametne videoanalitike videonadzor je postao visokoučinkovit. Takve tehnike mogu zadirati u privatnost u većoj mjeri (npr. složene biometrijske tehnologije) ili manjoj mjeri (npr. jednostavni algoritmi za prebrojavanje). Općenito je sve teže sačuvati anonimnost i privatnost. Pitanja u pogledu zaštite podataka koja se nameću mogu se razlikovati od situacije do situacije baš kao i pravna analiza koja se provodi kad je riječ o primjeni neke od navedenih tehnologija.

[1] Upućivanja na „države članice” u ovom mišljenju treba tumačiti kao upućivanja na „države članice EGP-a”.

4. Pored pitanja povezanih s privatnošću postoje i rizici povezani s mogućim neispravnostima tih uređaja i pristranostima do kojih mogu dovesti. Znanstvenici izvještavaju da se učinkovitost računalnih programa koji se upotrebljavaju za identifikaciju, prepoznavanje ili analizu lica razlikuje s obzirom na dob, spol i etničku skupinu osobe koja se identificira. Algoritmi funkcioniraju na temelju različitih demografskih podataka, zbog čega pristranost u prepoznavanju lica može dovesti do jačanja predrasuda već prisutnih u društvu. Upravo se zbog toga voditelji obrade podataka moraju pobrinuti da se redovito ocjenjuje relevantnost biometrijskih podataka prikupljenih videonadzorom, kao i dostatnost pruženih jamstava.

5. Videonadzor nije nužno potreban ako postoje druga sredstva s pomoću kojih je moguće ostvariti temeljnu svrhu. U protivnom prijeti opasnost da promijenimo kulturne norme, što bi moglo dovesti do prihvaćanja nedostatka privatnosti kao općenite polazišne točke.

6. Cilj je ovih smjernica pružiti savjete o primjeni Opće uredbe o zaštiti podatka na obradu osobnih podataka putem videouređaja. Ne daje se iscrpan popis primjera, ali se navedena opća razmatranja mogu primijeniti na sva potencijalna područja primjene.

2 PODRUČJE PRIMJENE[2]

2.1 Osobni podaci

7. Sustavni automatizirani nadzor određenog prostora optičkim ili audiovizualnim sredstvima, najčešće u svrhu zaštite imovine ili u svrhu zaštite života i zdravlja, česta je pojava u današnjem svijetu. Rezultat je toga prikupljanje i zadržavanje informacija u slikovnom obliku ili audiovizualnih informacija o svim osobama koje uđu u prostor pod nadzorom, a koje je moguće identificirati na temelju izgleda ili drugih specifičnih elemenata. Na temelju takvih pojedinosti moguće je utvrditi identitet tih osoba. To ujedno omogućuje daljnju obradu osobnih podataka koji se odnose na prisutnost i ponašanje osoba u određenom prostoru. Potencijalni rizik od zlouporabe takvih podataka povećava se razmjerno veličini prostora pod nadzorom te broju osoba koje posjećuju taj prostor. Ta se činjenica odražava u članku 35. stavku 3. točki (c) Opće uredbe o zaštiti podataka, u kojem se zahtijeva provedba procjene učinka na zaštitu podataka u slučaju sustavnog praćenja javno dostupnog područja u velikoj mjeri, te u članku 37. stavku 1. točki (b), u kojem se zahtijeva da izvršitelji obrade podataka imenuju službenika za zaštitu podataka ako postupci obrade zbog svoje prirode iziskuju redovito i sustavno praćenje ispitanika.

8. Međutim, Uredba se ne primjenjuje na obradu podataka koja se ne odnosi na određenu osobu, na primjer ako pojedinca nije moguće identificirati, ni izravno ni neizravno.

> Primjer: Opća uredba o zaštiti podataka nije primjenjiva kad je riječ o lažnim kamerama (kamere koje nemaju svrhu kamere, kojima se stoga ne obrađuju nikakvi osobni podatci). *Međutim, u nekim se državama članicama na tu situaciju mogu primjenjivati drugi zakoni.*
>
> Primjer: Snimke zabilježene s velike nadmorske visine obuhvaćene su područjem primjene Opće uredbe o zaštiti podataka samo ako je u predmetnim okolnostima obrađene podatke moguće povezati s određenom osobom.
>
> Primjer: U automobil je ugrađena videokamera za pomoć pri parkiranju. Ako je kamera ugrađena ili podešena na takav način da se njome ne prikupljaju nikakve informacije o pojedincima (kao što su oznake registarskih tablica ili informacije s pomoću kojih je moguće identificirati prolaznike), ne primjenjuje se Opća uredba o zaštiti podataka.

9.

2.2 Primjena Direktive o zaštiti podataka u području izvršavanja zakonodavstva ((EU) 2016/680)

10. Direktivom (EU) 2016/680 konkretno je obuhvaćena obrada osobnih podataka koju provode nadležna tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.

2.3 Izuzeće kućanstava

11. U skladu s člankom 2. stavkom 2. točkom (c) obrada osobnih podataka koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti, u što se mogu ubrojiti i aktivnosti na internetu, nije obuhvaćena područjem primjene Opće uredbe o zaštiti podataka[3].

---

[2] Europski odbor za zaštitu podataka napominje da se u slučajevima u kojima je to dopušteno Općom uredbom o zaštiti podataka u nacionalnom zakonodavstvu mogu primjenjivati posebni zahtjevi.

[3] Vidjeti i uvodnu izjavu 18.

12. Tu odredbu, takozvano „izuzeće kućanstava”, potrebno je usko tumačiti u kontekstu videonadzora. Prema tome, kako smatra Sud Europske unije, takozvano „izuzeće kućanstava” treba „*tumačiti na način da se odnosi isključivo na aktivnosti u okviru privatnog ili obiteljskog života pojedinaca, što očito nije slučaj s obradom osobnih podataka koja podrazumijeva njihovu objavu na internetu na način da se pristup tim podatcima omogući neodređenom broju osoba*”[4]. Nadalje, ako sustav videonadzora, koji uključuje stalno bilježenje i pohranu osobnih podataka, obuhvaća, „*iako djelomično, javni prostor, te je zbog te činjenice usmjeren prema eksterijeru privatne sfere onoga tko provodi obradu podataka tim sredstvom, ta se obrada ne može smatrati isključivo ‚osobnom ili domaćom' aktivnošću u smislu članka 3. stavka 2. drugog podstavka Direktive 95/46*”[5].

13. Kad je riječ o videouređajima kojima se nadzire unutrašnjost objekata privatne osobe, takva situacija može biti obuhvaćena izuzećem kućanstava. To će ovisiti o nekoliko čimbenika, koji se u donošenju zaključka cjelokupno uzimaju u obzir. Osim prethodno spomenutih elemenata utvrđenih u presudama Suda EU-a, korisnik kućnog videonadzora treba razmotriti i sljedeća pitanja: je li u nekoj vrsti osobnog odnosa s ispitanikom, upućuje li opseg ili učestalost nadzora na određenu vrstu njegove profesionalne aktivnosti, te može li nadzor imati nepovoljan učinak na ispitanike. Prisutnost bilo kojeg od prethodno spomenutih elemenata ne znači nužno da obrada nije obuhvaćena opsegom izuzeća kućanstava, naime za takav je zaključak potrebno provesti sveobuhvatnu procjenu.

Primjer: Da bi zabilježio svoj odmor, turist snima videozapise koristeći se i svojim mobilnim telefonom i videokamerom. Snimku je nakon toga pokazao prijateljima i obitelji, ali pristup snimci nije omogućio neodređenom broju osoba. Ta je situacija obuhvaćena izuzećem kućanstava.

Primjer: Biciklistica koja se bavi spustom brdskim biciklima želi akcijskom kamerom snimiti svoj spust. Vožnja se odvija na udaljenom području te se biciklistica snimkama planira koristiti u svrhu osobne zabave u privatnosti doma. Iako u određenoj mjeri uključuje obradu osobnih podataka, ta je situacija obuhvaćena izuzećem kućanstava.

Primjer: Osoba je postavila videonadzor kojim snima svoj vrt. Posjed je ograđen te samo voditelj obrade i njegova obitelj redovito ulaze u vrt. Ta je situacija obuhvaćena izuzećem kućanstava, pod uvjetom da videonadzorom nije pokriven ni jedan dio javnog prostora ni susjednog posjeda.

14.

[4] Sud Europske unije, presuda u predmetu C-101/01, *Bodil Lindqvist*, 6. studenoga 2003., t. 47.

[5] Sud Europske unije, presuda u predmetu C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11. prosinca 2014., t. 33.

3 ZAKONITOST OBRADE PODATAKA

15. Prije same obrade potrebno je detaljno utvrditi njezinu svrhu (članak 5. stavak 1. točka (b)). Videonadzor se može upotrebljavati u različite svrhe kao što je zaštita posjeda i druge imovine, zaštita života i tjelesnog integriteta pojedinaca, prikupljanje dokaza za potrebe privatnih tužbi[6]. Te je svrhe nadzora potrebno evidentirati u pisanom obliku (članak 5. stavak 2.) te je za svaku nadzornu kameru u uporabi potrebno navesti odgovarajuću svrhu. Kamere koje jedan voditelj obrade upotrebljava u istu svrhu mogu se evidentirati zajedno. Nadalje, u skladu s člankom 13. ispitanici moraju biti obaviješteni o svrhama obrade (*vidjeti odjeljak 7. – Obveze u pogledu transparentnosti i dostavljanja informacija*). Svrha videonadzora koja je formulirana s pomoću pojmova kao što su „sigurnost" ili „vaša sigurnost" nije dovoljno posebna svrha (članak 5. stavak 1. točka (b)). To je ujedno protivno načelu prema kojem se osobni podatci moraju obrađivati zakonito, pošteno i transparentno u odnosu na ispitanika (vidjeti članak 5. stavak 1. točka (a)).

16. U načelu, svi pravni razlozi propisani člankom 6. stavkom 1. mogu činiti pravnu osnovu za obradu podataka prikupljenih videonadzorom. Primjerice, u slučajevima u kojima nacionalno pravo propisuje obvezu provedbe videonadzora primjenjuje se članak 6. stavak 1. točka (c)[7]. Međutim, u praksi se najčešće primjenjuju sljedeće odredbe:

    - članak 6. stavak 1. točka (f) (legitimni interes)
    - članak 6. stavak 1. točka (e) (obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti).

    Iznimni su slučajevi u kojima voditelj obrade kao pravnu osnovu obrade navodi članak 6. stavak 1. točku (a) (privola).

3.1 Legitimni interes, članak 6. stavak 1. točka (f)

17. Pravna procjena iz članka 6. stavka 1. točke (f) trebala bi se temeljiti na kriterijima navedenima u nastavku u skladu s uvodnom izjavom 47.

3.1.1 Postojanje legitimnih interesa

18. Videonadzor je zakonit ako je nužan za potrebe ispunjavanja legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika (članak 6. stavak 1. točka (f)). Legitimni interesi voditelja obrade ili treće strane mogu biti pravni[8], ekonomski ili nematerijalni interesi[9]. Međutim, voditelj obrade trebao bi imati na umu da ako ispitanik uloži prigovor na videonadzor u skladu s člankom 21., voditelj obrade videonadzor takvog ispitanika može provoditi samo ako postoje *uvjerljivi* legitimni interesi koji nadilaze ispitanikove interese, prava i slobode ili ako je svrha takvog videonadzora postavljanje, ostvarivanje ili obrana pravnih zahtjeva.

---

[6] Pravila o prikupljanju dokaza za potrebe građanskih parnica razlikuju se među državama članicama.

[7] U ovim se smjernicama ne analiziraju niti detaljnije razmatraju eventualne razlike u nacionalnom pravu država članica.

[8] Sud Europske unije, presuda u predmetu C-13/16, *Rīgas satiksme*, 4. svibnja 2017.

[9] Vidjeti dokument WP 217 Radne skupine iz članka 29.

19. U slučaju stvarne i opasne situacije legitiman interes za videonadzor može biti svrha zaštite imovine od provale, krađe ili vandalizma.

20. Legitiman interes treba uistinu postojati te mora upućivati na postojeći problem (ne smije biti fiktivne ili špekulativne prirode)[10]. Upotreba videonadzora mora biti opravdavana stvarnom neprilikom kao što su nanesena šteta ili ozbiljan incident u prošlosti. U skladu s načelom odgovornosti voditeljima obrade se savjetuje da evidentiraju relevantne incidente (da zabilježe podatke kao što je datum, način počinjenja, financijski gubitak) i povezane kaznene prijave. Takvi evidentirani incidenti mogu biti snažni dokazi o postojanju legitimnog interesa. Postojanje legitimnog interesa te nužnost nadzora potrebno je iznova ocjenjivati u redovitim vremenskim razmacima (npr. jednom godišnje, ovisno o okolnostima).

> Primjer: Vlasnik trgovine želi otvoriti novu trgovinu te postaviti sustav videonadzora radi sprečavanja vandalizma. Služeći se statističkim podatcima, vlasnik trgovine može dokazati da u susjedstvu postoji visoka stopa učestalosti vandalizma. Iskustva drugih obližnjih trgovina isto tako mogu biti korisna. Nije nužno da je upravo taj voditelj obrade pretrpio štetu. Dovoljno je da šteta koja je počinjena u susjedstvu upućuje na postojanje opasnosti ili sličnih nepovoljnih okolnosti te to samo po sebi može biti naznaka legitimnog interesa. Međutim, nije dovoljno iznijeti opće statističke podatke o kriminalu ili nacionalne statističke podatke o kriminalu bez analize relevantnog područja i opasnosti koje prijete toj konkretnoj trgovini.

21.

22. Situacije neposredne opasnosti mogu predstavljati legitimni interes, a takvim situacijama izložene su primjerice banke ili trgovine koje prodaju skupocjenu robu (npr. draguljarnice) ili područja poznata po čestim kaznenim djelima protiv imovine (npr. benzinske postaje).

23. U Općoj uredbi o zaštiti podataka također se jasno navodi da tijela javne vlasti koja provode obradu pri izvršavanju svojih zadaća to ne mogu temeljiti na legitimnom interesu, kao što je propisano drugom rečenicom članka 6. stavka 1.

3.1.2 Nužnost obrade podataka

24. Osobni bi podatci trebali biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka”) u skladu s člankom 5. stavkom 1. točkom (c). Prije uvođenja sustava videonadzora voditelj obrade uvijek bi trebao kritički ispitati, kao prvo, je li ta mjera prikladna za postizanje željenog cilja te, kao drugo, je li ta mjera primjerena i nužna u odnosu na njezine svrhe. Mjerama videonadzora treba pribjeći samo ako se svrha obrade ne može na zadovoljavajući način postići drugim sredstvima kojima se u manjoj mjeri zadire u temeljna prava i slobode ispitanika.

25. Pod pretpostavkom da želi spriječiti kaznena djela povezana s imovinom, umjesto uvođenja sustava videonadzora voditelj obrade mogao bi poduzeti alternativne sigurnosne mjere kao što je postavljanje ograde oko posjeda, organizacija redovite ophodnje zaštitarskog osoblja, angažiranje vratara, postavljanje bolje rasvjete, postavljanje sigurnosnih brava, ugradnja protuprovalnih prozora i vrata ili nanošenje antigrafitnih premaza ili folija na zidove. Te mjere mogu biti jednako učinkovite u sprečavanju provale, krađe i vandalizma kao i sustav videonadzora. Voditelj obrade mora u svakom pojedinačnom slučaju ocijeniti jesu li takve mjere razumno rješenje.

26. Prije uvođenja sustava kamera voditelj obrade dužan je ocijeniti na kojim su mjestima i u koje vrijeme mjere videonadzora uistinu nužne. Obično će nadzorni sustav koji se aktivira noću ili izvan redovnog

[10] Vidjeti dokument WP 217 Radne skupine iz članka 29., str. 24. i sljedeće. Vidjeti također Sud EU-a, predmet C-708/18, t. 44.

radnog vremena zadovoljiti potrebe voditelja obrade u pogledu sprečavanja bilo kakvih opasnosti koje prijete njegovoj imovini.

27. Općenito govoreći, uporaba videonadzora u svrhu zaštite objekata voditelja obrade smatra se nužnom samo unutar granica njegova posjeda.[11] Međutim, postoje slučajevi u kojima nadzor posjeda nije dovoljan za učinkovitu zaštitu. U nekim pojedinačnim slučajevima može biti potrebno proširiti videonadzor na neposredno okruženje posjeda. U tom bi kontekstu voditelj obrade trebao razmotriti mogućnost uporabe fizičkih i tehničkih sredstava poput prekrivanja ili pikselizacije nerelevantnih područja.

> Primjer: Vlasnik knjižare želi zaštititi svoj objekt od vandalizma. Općenito govoreći, kamere bi trebale pokrivati isključivo sâm objekt jer u tu svrhu nije potrebno snimati susjedne objekte kao ni javne površine koje se nalaze u blizini knjižare.

28.

29. Pitanja u pogledu nužnosti obrade postavljaju se i u vezi s načinom na koji se dokazi čuvaju. U određenim slučajevima može biti potrebno rješenje koje uključuje primjenu uređaja za snimanje podataka („crne kutije”), pri čemu se snimka automatski briše nakon određenog razdoblja pohrane te se snimci pristupa samo u slučaju incidenta. U drugim slučajevima postoji mogućnost da snimanje videomaterijala uopće nije potrebno, već je umjesto toga prikladnije primjenjivati nadzor u stvarnom vremenu. Odluka o tome hoće li se odabrati rješenje koje uključuje primjenu uređaja za snimanje podataka („crne kutije”) ili nadzor u stvarnom vremenu treba se temeljiti na svrsi koja se želi ostvariti. Ako je svrha primjene videonadzora, na primjer, čuvanje dokaza, metode nadzora u stvarnom vremenu obično nisu prikladne. Nadzor u stvarnom vremenu katkad može biti više nametljiv nego pohrana materijala koji se automatski briše nakon određenog razdoblja (npr. situacija u kojoj netko neprestano promatra zaslon može biti nametljivija za pojedinca nego situacija u kojoj zaslona uopće nema te se snimljeni materijal izravno pohranjuje na uređaj za snimanje podataka („crnu kutiju”)). U tom je kontekstu potrebno voditi računa o načelu smanjenja količine podataka (članak 5. stavak 1. točka (c)). Isto tako valja imati na umu da voditelj obrade, umjesto da se koristi videonadzorom, može angažirati zaštitarsko osoblje koje može odmah reagirati i intervenirati.

3.1.3 Odvagivanje interesa

30. Pod pretpostavkom da je videonadzor potreban radi zaštite legitimnih interesa voditelja obrade, sustav videonadzora smije se postaviti samo ako nad legitimnim interesima voditelja obrade ili oni treće strane (npr. zaštita imovine ili tjelesnog integriteta) ne prevladavaju interesi ili temeljna prava i slobode ispitanika. Voditelj obrade treba razmotriti: 1) do koje mjere nadzor utječe na interese te temeljna prava i slobode pojedinaca te 2) dovodi li to do povrede ispitanikovih prava ili negativnih posljedica na njegova prava. Naime, odvagivanje je interesa obvezno. Potrebno je pažljivo ocijeniti te uskladiti, s jedne strane, temeljna prava i slobode ispitanika i, s druge strane, legitimne interese voditelja obrade.

[11] U nekim državama članicama i to može ovisiti o nacionalnom zakonodavstvu.

Primjer: Privatno društvo koje upravlja parkiralištem više je puta zabilježilo probleme s krađom imovine iz parkiranih automobila. Parkiralište je otvoren prostor kojem svatko može lako pristupiti te je jasno označeno prometnim znakovima i okruženo prometnim barijerama. Nadzor prostora tijekom razdoblja dana u kojem se problemi događaju legitiman je interes društva koje upravlja parkiralištem (sprečavanje krađe imovine iz automobila klijenata). Osim što se nadzor ispitanika odvija u ograničenom razdoblju, oni ne provode vrijeme na tom prostoru te je sprečavanje krađa ujedno u njihovu vlastitom interesu. Legitimni interesi voditelja obrade u ovom slučaju prevladavaju nad interesima ispitanika da ih se ne nadzire.

Primjer: Rukovodstvo restorana odluči postaviti videokamere u zahode radi kontrole urednosti sanitarnih objekata. U tom slučaju prava ispitanika očigledno nadilaze interes voditelja obrade te se prema tome ondje ne smiju postaviti kamere.

31.

3.1.3.1 Odlučivanje na pojedinačnoj osnovi

32. Budući da je u skladu s Uredbom odvagivanje interesa obvezno, odluke je potrebno donositi na pojedinačnoj osnovi (vidjeti članak 6. stavak 1. točku (f)). Nije dovoljno pozvati se na hipotetske situacije ili iznijeti usporedbu sličnih slučajeva. Voditelj obrade mora procijeniti rizike u pogledu zadiranja u prava ispitanika, a u tom je slučaju odlučujući kriterij intenzivnost zadiranja u prava i slobode pojedinca.

33. Intenzivnost se između ostalog može odrediti s obzirom na vrstu informacija koje se prikupljaju (sadržaj informacija), opseg (gustoću informacija te prostorni i zemljopisni opseg), broj uključenih ispitanika (određen konkretnom brojkom ili kao udio u relevantnoj populaciji), s obzirom na predmetnu situaciju, stvarne interese skupine ispitanika, alternativna sredstva te s obzirom na prirodu i opseg ocjene podataka.

34. Važni čimbenici u pogledu odvagivanja različitih interesa mogu biti veličina područja koje se nalazi pod nadzorom te broj nadziranih ispitanika. Uporaba videonadzora na udaljenim područjima (npr. radi promatranja biljnog i životinjskog svijeta ili radi zaštite kritične infrastrukture kao što je radijska antena u privatnom vlasništvu) mora se ocijeniti na drukčiji način nego uporaba videonadzora u pješačkoj zoni ili u trgovačkom centru.

Primjer: Ako je u vozilu postavljena kamera za snimanje vožnje (npr. za potrebe prikupljanja dokaza u slučaju nesreće), važno je zajamčiti da se tom kamerom ne snima stalno promet kao ni osobe koje se nalaze u blizini ceste. U protivnom interes koji podrazumijeva snimanje videozapisa koji mogu poslužiti kao dokaz u teoretskom slučaju prometne nesreće ne može opravdati ozbiljno zadiranje u prava ispitanika[11].

35.

3.1.3.2 Razumna očekivanja ispitanika

36. U skladu s uvodnom izjavom 47. postojanje legitimnog interesa zahtijeva pažljivu procjenu. Pritom je potrebno uzeti u obzir razumna očekivanja ispitanika u vrijeme i u kontekstu obrade njegovih osobnih podataka. Kad je riječ o sustavnom nadzoru, odnos između ispitanika i voditelja obrade može se znatno razlikovati i može utjecati na razumna očekivanja koja ispitanik ima. Tumačenje koncepta razumnih očekivanja ne bi se trebalo temeljiti samo na takvim subjektivnim očekivanjima. Umjesto toga, odlučujući kriterij treba se temeljiti na pitanju može li objektivna treća strana razumno očekivati da će biti predmet nadzora u određenoj situaciji i može li takva objektivna treća strana to zaključiti.

37. Na primjer, u većini slučajeva zaposlenik ne očekuje da će ga poslodavac nadzirati na radnom mjestu[12]. Nadalje, nadzor se ne očekuje u privatnom vrtu, stambenim prostorima ili u prostorijama za preglede i liječenje. Isto tako, nije razumno očekivati nadzor u sanitarnim objektima ili u sauni jer nadzor u takvim prostorima čini snažno zadiranje u prava ispitanika. Razumno je očekivanje ispitanika da se u takvim prostorima videonadzor ne primjenjuje. S druge strane, klijent banke očekuje da ga se nadzire unutar banke ili za vrijeme korištenja bankomata.

38. Ispitanici isto tako mogu očekivati da neće biti nadzirani na javno dostupnim prostorima, osobito ako takvi prostori obično služe za odmor, opuštanje i bavljenje aktivnostima u slobodno vrijeme te ako je riječ o mjestima na kojima se pojedinci zadržavaju i/ili komuniciraju kao što su prostori namijenjeni za sjedenje, stolovi u restoranima, parkovi, kina i objekti za rekreaciju. U takvim slučajevima interesi ili prava i slobode ispitanika često nadilaze legitimne interese voditelja obrade.

> Primjer: Ispitanici ne očekuju nadzor u zahodima. Na primjer, videonadzor u svrhu sprečavanja nezgoda nije razmjeran opasnosti od nezgode.

39.

40. Znakovi kojima se ispitanici obavještavaju o primjeni videonadzora nisu relevantni pri utvrđivanju onoga što ispitanik može objektivno očekivati. To na primjer znači da se vlasnik trgovine ne može osloniti na to da kupci *objektivno* imaju razumna očekivanja da će biti nadzirani samo zato što je na ulazu postavljen znak kojim se pojedinac obavještava o nadzoru.

3.2 Nužnost obrade za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade, u skladu s člankom 6. stavkom 1. točkom (e)

41. Osobni podatci mogu se obrađivati primjenom videonadzora u skladu s člankom 6. stavkom 1. točkom (e) ako je to nužno za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti[13]. Može se dogoditi da takva obrada nije dopuštena u okviru samog izvršavanja službene ovlasti, ali da druge zakonodavne osnove kao što je zaštita „zdravlja i sigurnosti" posjetitelja i zaposlenika omogućuju ograničenu obradu, u skladu s obvezama iz Opće uredbe o zaštiti podataka i pravima ispitanika.

42. Države članice mogu zadržati ili uvesti posebne odredbe nacionalnog zakonodavstva u pogledu videonadzora kako bi prilagodile primjenu pravila iz Opće uredbe o zaštiti osobnih podataka na način da se preciznije odrede posebni uvjeti za obradu pod uvjetom da je ona usklađena s načelima propisanima Uredbom (npr. ograničenje pohrane, proporcionalnost).

[12] Vidjeti i: Radna skupina iz članka 29., Mišljenje 2/2017 o obradi podataka na radnome mjestu, WP 249, doneseno 8. lipnja 2017.

[13] Pravna osnova za obradu „utvrđuje se u pravu Unije ili pravu države članice" te ona „mora biti nužna za izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade" (članak 6. stavak 3.).

3.3 Privola, članak 6. stavak 1. točka (a)

43. Privola mora biti dobrovoljna, posebna, informirana i nedvosmislena, kako se navodi u smjernicama o privoli[14].

44. Kad je riječ o sustavnom nadzoru, ispitanikova privola može služiti kao pravna osnova u skladu s člankom 7. (vidjeti uvodnu izjavu 43.) samo u iznimnim slučajevima. Takva tehnologija nadzora po svojoj prirodi podrazumijeva nadzor neodređenog broja ljudi odjednom. Voditelj obrade teško će moći dokazati da je ispitanik dao privolu prije obrade njegovih osobnih podataka (članak 7. stavak 1.). Ako ispitanik povuče svoju privolu, vršitelj obrade teško će moći dokazati da se osobni podatci više ne obrađuju (članak 7. stavak 3.).

> Primjer: Sportaši mogu zatražiti nadzor tijekom pojedinačnog vježbanja u svrhu analize tehnika i uspješnosti. S druge strane, u slučaju u kojem sportski klub odluči nadzirati cijeli tim u istu svrhu, privola često neće biti valjana jer se pojedinačni sportaši mogu osjećati primoranima dati privolu kako njihovo odbijanje da to učine ne bi negativno utjecalo na ostale članove tima.

45.

46. Ako se voditelj obrade želi osloniti na privolu, njegova je dužnost pobrinuti se da svaki ispitanik koji uđe u prostor pod videonadzorom da svoju privolu. Ta privola mora ispunjavati uvjete propisane člankom 7. Ulazak u označeni prostor koji je pod nadzorom (npr. osobe se pozove da prođu kroz poseban hodnik ili vrata kako bi ušli u prostor pod nadzorom) ne predstavlja izjavu ni jasnu potvrdnu radnju koju zahtijeva privola, osim ako to ispunjava kriterije propisane člancima 4. i 7., kako je opisano u smjernicama o privoli[15].

47. S obzirom na neravnotežu između poslodavaca i zaposlenika u pogledu ovlasti, u većini se slučajeva poslodavci ne bi trebali oslanjati na privole kad je riječ o obradi osobnih podataka jer je malo vjerojatno da su takve privole dobrovoljne. U tom bi kontekstu trebalo uzeti u obzir smjernice o privoli.

48. Države članice mogu zakonom ili kolektivnim ugovorima, uključujući „ugovore o radovima”, predvidjeti posebna pravila za obradu osobnih podataka zaposlenikâ u kontekstu zaposlenja (vidjeti članak 88.).

[14] Radna skupina iz članka 29., „Smjernice o privoli u skladu s Uredbom 2016/679” (WP 259 rev. 01), koje je potvrdio EDPB.

[15] Radna skupina iz članka 29., „Smjernice o privoli u skladu s Uredbom 2016/679” (WP 259), koje je potvrdio Europski odbor za zaštitu podataka, i koje je potrebno uzeti u obzir.

4 OTKRIVANJE VIDEOZAPISA TREĆIM STRANAMA

49. Opće odredbe Opće uredbe o zaštiti podataka u načelu se primjenjuju na otkrivanje videozapisa trećim stranama.

4.1 Otkrivanje videozapisa trećim stranama općenito

50. U članku 4. točki 2. otkrivanje se definira kao prijenos (npr. pojedinačnim priopćenjem), širenje (npr. objavom na internetu) ili stavljanje na raspolaganje na drugi način. Treće strane definirane su u članku 4. točki 10. U slučaju otkrivanja osobnih podataka trećim zemljama ili međunarodnim organizacijama, primjenjuju se i posebne odredbe članka 44. i sljedećih članaka.

51. Svako otkrivanje osobnih podataka čini posebnu vrstu obrade za koju voditelj obrade mora imati jednu od pravnih osnova navedenih u članku 6.

> Primjer: Voditelj obrade koji želi objaviti snimku na internetu mora imati pravnu osnovu za takvu obradu kao što je na primjer privola dobivena od ispitanika u skladu s člankom 6. stavkom 1. točkom (a).

52.

53. Videozapis je moguće prenijeti trećim stranama u svrhu koja je različita od svrhe u koju su podatci prikupljeni u skladu s pravilima iz članka 6. stavka 4.

> Primjer: Postavljen je videonadzor rampe (na parkiralištu) u svrhu rješavanja sporova za naknadu štete. Nakon nastanka štete snimka se prenosi pravniku za potrebe postupka. U tom slučaju svrha u koju je snimka zabilježena jednaka je svrsi prijenosa.
>
> Primjer: Postavljen je videonadzor rampe (na parkiralištu) u svrhu rješavanja sporova za naknadu štete. Snimka je objavljena na internetu iz razloga isključivo povezanih sa zabavom. U tom se slučaju svrha mijenja te je u raskoraku s izvornom svrhom. Nadalje, za takvu obradu (objavu) problematično je utvrditi pravnu osnovu.

54.

55. Treća strana koja čini primatelja treba provesti vlastitu pravnu analizu; točnije, treba utvrditi pravnu osnovu za svoju obradu (npr. primanje materijala) u skladu s člankom 6.

4.2 Otkrivanje videozapisa tijelima za izvršavanje zakonodavstva

56. Otkrivanje videozapisa tijelima za izvršavanje zakonodavstva također je zaseban postupak koji od voditelja obrade zahtijeva posebno obrazloženje.

57. U skladu s člankom 6. stavkom 1. točkom (c) obrada je zakonita ako je nužna radi poštovanja pravnih obveza voditelja obrade. Iako je primjenjivo policijsko pravo pitanje koje se nalazi pod isključivom nadležnošću država članica, sve države članice vjerojatno imaju opća pravila kojima se uređuje prijenos dokaza tijelima za izvršavanje zakonodavstva. Obrada koju obavlja voditelj obrade koji predaje podatke uređena je Općom uredbom o zaštiti podataka. Ako je u skladu s nacionalnim zakonodavstvom voditelj obrade obvezan surađivati s tijelima za izvršavanje zakonodavstva (npr. u istragama), pravna je osnova za predaju podataka pravna obveza u skladu s člankom 6. stavkom 1. točkom (c).

58. Ograničenje u pogledu svrhe propisano člankom 6. stavkom 4. u tom slučaju najčešće nije problematično jer se otkrivanje izričito temelji na pravu države članice. Razmatranje posebnih zahtjeva u pogledu promjene svrhe u smislu točaka od (a) do (e) prema tome nije potrebno.

Primjer: Vlasnik trgovine snima ulaz u trgovinu. Na snimci se vidi kako jedna osoba drugoj krade novčanik. Policija traži od voditelja obrade da preda videomaterijale jer mogu pomoći u istrazi. U tom se slučaju vlasnik trgovine može pozvati na pravnu osnovu propisanu člankom 6. stavkom 1. točkom (c) (pravna obveza), koja se tumači u vezi s relevantnim nacionalnim pravom u pogledu obrade prijenosom.

59.

Primjer: U trgovini je postavljena kamera zbog sigurnosnih razloga. Vlasniku trgovine se čini da je kamerom zabilježeno sumnjivo ponašanje te odluči poslati materijal policiji (a da nije dobio obavijest da je u tijeku ikakva istraga). U tom slučaju vlasnik trgovine najčešće mora ocijeniti jesu li ispunjeni uvjeti propisani člankom 6. stavkom 1. točkom (f). Ta situacija obično nastaje kad vlasnik trgovine opravdano sumnja na počinjenje kaznenog djela.

60.

61. Obrada osobnih podataka koju obavljaju sama tijela za izvršavanje zakonodavstva ne podliježe Općoj uredbi o zaštiti podataka (vidjeti članak 2. stavak 2. točku (d)), već podliježe Direktivi o zaštiti podataka u području izvršavanja zakonodavstva ((EU) 2016/680).

5 OBRADA POSEBNIH KATEGORIJA PODATAKA

62. Sustavima videonadzora obično se prikupljaju goleme količine osobnih podataka koje mogu otkrivati podatke krajnje osobne prirode te posebne kategorije podataka. Naime, naizgled nevažni podatci koji se prvotno prikupe videouređajima mogu se upotrebljavati kako bi se iz njih izvele druge informacije radi postizanja nekog drugog cilja (npr. utvrđivanja navika određene osobe). Međutim, videonadzor se ne smatra uvijek obradom posebnih kategorija osobnih podataka.

> Primjer: Videozapisi s ispitanicima koji nose naočale ili se koriste invalidskim kolicima same se po sebi ne smatraju posebnim kategorijama osobnih podataka.

63.

64. Međutim, ako se videozapis obrađuje radi izvođenja posebnih kategorija podataka, primjenjivat će se članak 9.

> Primjer: Na primjer, na temelju snimaka koje prikazuju ispitanike čiji se identitet može utvrditi kako sudjeluju u štrajku, nekom drugom događaju itd. mogao bi se izvesti zaključak o njihovim političkim mišljenjima. Takvi bi slučajevi bili obuhvaćeni člankom 9.
>
> Primjer: Slučaj u kojem bolnica postavi videokameru radi praćenja zdravstvenog stanja pacijenta smatrao bi se obradom posebnih kategorija osobnih podataka (članak 9.).

65.

66. U načelu bi pri svakom postavljanju sustava videonadzora općenito trebalo pažljivo razmotriti načelo smanjenja količine podataka. Stoga bi voditelj obrade, čak i u slučajevima u kojima se ne primjenjuje članak 9. stavak 1., uvijek trebao pokušati smanjiti mogućnost snimanja koje otkriva druge osjetljive podatke (izvan okvira članka 9.), neovisno o cilju prikupljanja tih podataka.

> Primjer: Slučajevi u kojima se videonadzorom snima crkva sami po sebi nisu obuhvaćeni člankom 9. Međutim, voditelj obrade mora provesti posebno pažljivu procjenu interesa ispitanika u skladu s člankom 6. stavkom 1. točkom (f) kojom se uzima u obzir priroda podataka te rizik od prikupljanja drugih osjetljivih podataka (izvan okvira članka 9.).

67.

68. Ako se sustav videonadzora upotrebljava radi obrade posebnih kategorija podataka, voditelj obrade mora, na temelju članka 9. utvrditi iznimku u skladu s kojom se obrađuju posebne kategorije podataka (tj. izuzeće od općeg pravila koje nalaže da se posebne kategorije podataka ne smiju obrađivati) i pravnu osnovu na temelju članka 6.

69. Na primjer, članak 9. stavak 2. točka (c) („[…] *obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca* […]") mogao bi se, teoretski i iznimno, primjenjivati, ali bi voditelj obrade to morao opravdati apsolutnom nužnošću da se zaštite životno važni interesi osobe i da se dokaže da taj „[…] ispitanik *fizički ili pravno nije u mogućnosti dati privolu*". Osim toga, voditelju obrade neće biti dopušteno da iskoristi taj sustav zbog bilo kojeg drugog razloga.

70. Važno je naglasiti da se za opravdanje obrade posebnih kategorija podataka primjenom videonadzora vjerojatno neće moći primijeniti svaka iznimka iz članka 9. Konkretnije, voditelji obrade koji u okviru videonadzora obrađuju te podatke ne mogu se oslanjati na članak 9. stavak 2. točku (e), kojim se omogućuje obrada koja se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik. Sam čin ulaska u vidno polje objektiva kamere ne znači da ispitanik želi da posebne kategorije podataka koji se na njega odnose budu dostupne javnosti.

71. Nadalje, obrada posebnih kategorija podataka zahtijeva posvećivanje pojačane i stalne pozornosti određenim obvezama, na primjer visokoj razini sigurnosti i procjeni učinka na zaštitu podataka, gdje je to potrebno.

> Primjer: Poslodavac se ne smije koristiti snimkama videonadzora koje prikazuju prosvjed kako bi utvrdio identitete štrajkaša.

72.

5.1 Opća razmatranja prilikom obrade biometrijskih podataka

73. Korištenje biometrijskim podatcima, a posebno podatcima povezanima s prepoznavanjem lica, podrazumijeva povećani rizik za prava ispitanika. Ključno je da se takve tehnologije upotrebljavaju uz poštovanje načela zakonitosti, nužnosti, proporcionalnosti i smanjenja količine podataka, kako je utvrđeno u Općoj uredbi o zaštiti podataka. Iako se uporaba takvih tehnologija može smatrati posebno učinkovitom, voditelji obrade najprije bi trebali procijeniti njihov utjecaj na temeljna prava i slobode te razmotriti mogućnost uporabe sredstava kojima se u manjoj mjeri zadire u privatnost pojedinca kako bi ostvarili zakonitu svrhu obrade podataka.

74. Da bi se podatci mogli smatrati biometrijskim podatcima u skladu s Općom uredbom o zaštiti podataka, obrada neobrađenih podataka, kao što su fizička ili fiziološka obilježja ili obilježja ponašanja pojedinca, mora podrazumijevati mjerenje tih obilježja. Budući da su biometrijski podatci rezultat takvih mjerenja, u članku 4. točki 14. Opće uredbe o zaštiti podataka navodi se da su to podatci „[…] *dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca […]”*. Međutim, videozapisi koji prikazuju pojedince sami se po sebi ne mogu smatrati biometrijskim podatcima u skladu s člankom 9. ako nisu posebno tehnički obrađeni kako bi pridonijeli identifikaciji tih pojedinaca[16].

75. Kako bi se obrada smatrala obradom posebnih kategorija osobnih podataka (članak 9.), biometrijske se podatke mora obrađivati „u svrhu jedinstvene identifikacije pojedinca”.

76. Kao zaključak, s obzirom na članak 4. točku 14. i članak 9., potrebno je razmotriti sljedeća tri kriterija:

- **prirodu podataka:** podatci koji se odnose na fizička ili fiziološka obilježja ili obilježja ponašanja pojedinca
- **sredstva i način obrade:** podatci „dobiveni posebnom tehničkom obradom”
- **svrhu obrade:** podatci se moraju upotrebljavati u svrhu jedinstvene identifikacije pojedinca**.**

77. Za uporabu videonadzora koji uključuje funkciju biometrijskog prepoznavanja kojim se privatni subjekti koriste za vlastite potrebe (npr. marketinške, statističke ili čak sigurnosne potrebe) u većini će slučajeva biti potrebno da svi ispitanici daju svoju izričitu privolu (članak 9. stavak 2. točka (a)), ali bi se mogla primjenjivati i neka druga odgovarajuća iznimka iz članka 9.

[16] U prilog toj analizi, u uvodnoj izjavi 51. Opće uredbe o zaštiti podataka navodi se sljedeće: „[…] Obradu fotografija ne bi trebalo sustavno smatrati obradom posebnih kategorija osobnih podataka jer su one u biti obuhvaćene samo definicijom biometrijskih podataka pri obradi posebnim tehničkim sredstvima kojima se omogućuje jedinstvena identifikacija ili autentifikacija pojedinca. *[…]”.*

Primjer: Kako bi poboljšao svoju uslugu, privatni zračni prijevoznik kontrolne točke za identifikaciju putnika u zračnoj luci (predaja prtljage, ukrcaj) zamjenjuje sustavima videonadzora koji primjenjuju tehnike prepoznavanja lica radi provjere identiteta putnika koji su za takav postupak dali svoju privolu. Budući da je takva obrada podataka obuhvaćena člankom 9., putnici koji su za to prethodno dali svoju izričitu i informiranu privolu morat će se prijaviti putem, na primjer, automatskog terminala kako bi izradili i registrirali svoj predložak lica koji je povezan s njihovom ukrcajnom propusnicom i njihovim identitetom. Kontrolne točke s funkcijom prepoznavanja lica moraju se jasno odvojiti, npr. sustav se mora postaviti unutar okvira za prolaz kako se ne bi registrirali biometrijski predlošci osoba koje nisu dale svoju privolu. Samo će putnici koji su prethodno dali svoju privolu i izvršili prijavu ući u okvir u koji je postavljen biometrijski sustav.

Primjer: Voditelj obrade upravlja pristupom svojoj zgradi primjenjujući metodu prepoznavanja lica. Osobe se tim pristupom mogu koristiti samo ako su prethodno dale svoju izričitu informiranu privolu (u skladu s člankom 9. stavkom 2. točkom (a)). Međutim, kako bi se osiguralo da se ne registriraju lica osoba koje prethodno nisu dale svoju privolu, metodu prepoznavanja lica trebao bi pokrenuti sam ispitanik, na primjer pritiskom na gumb. Kako bi se zajamčila zakonitost obrade, voditelj obrade u svakom slučaju mora omogućiti alternativni način pristupa zgradi pri kojem se ne primjenjuje obrada biometrijskih podataka, kao što su identifikacijske oznake ili ključevi.

78.

79. U slučajevima u kojima se izrađuju biometrijski predlošci voditelji obrade moraju se pobrinuti da nakon što se zabilježi rezultat podudaranja ili nepodudaranja, svi privremeni predlošci koji su zabilježeni u tijeku postupka (uz izričitu i informiranu privolu ispitanika) radi uspoređivanja s predlošcima koje su ispitanici izradili prilikom prijave, izbrisat će se sigurno i bez odgode. Predlošci koji su izrađeni prilikom prijave čuvat će se samo za potrebe obrade te se neće pohraniti ili arhivirati.

80. Međutim, obrada nije obuhvaćena člankom 9. ako je njezina svrha, na primjer, razlikovanje jedne kategorije ljudi od druge, a ne jedinstvena identifikacija određene osobe.

Primjer: Vlasnik trgovine želio bi oglasni sadržaj prilagoditi spolu i dobi kupca koji je snimljen s pomoću sustava videonadzora. Ako se tim sustavom videonadzora ne izrađuju biološki predlošci u svrhu jedinstvene identifikacije osobe već se samo utvrđuju navedena fizička obilježja te osobe radi njezine kategorizacije (a pritom se ne obrađuju druge vrste posebnih kategorija podataka), obrada neće biti obuhvaćena člankom 9.

81.

82. Međutim, članak 9. primjenjuje se ako voditelj obrade pohranjuje biometrijske podatke (najčešće u obliku predložaka koji se izrađuju izdvajanjem ključnih obilježja iz neobrađenih biometrijskih podataka (npr. mjerenje lica na temelju snimke)) u svrhu jedinstvene identifikacije određene osobe**.** Ako voditelj obrade želi utvrditi ispitanika koji ponovo ulazi u prostor ili ulazi u drugi prostor (na primjer, radi kontinuiranog prikazivanja oglasa prilagođenog sadržaja), namjera bi tada bila jedinstvena identifikacija pojedinca čime bi ta aktivnost od početka bila obuhvaćena člankom 9. To može biti slučaj ako voditelj obrade pohranjuje izrađene predloške kako bi se oglasi prilagođenog sadržaja nastavili prikazivati na oglasnim panelima na različitim lokacijama u trgovini. Budući da se u okviru tog sustava fizička obilježja upotrebljavaju kako bi se utvrdili i pratili određeni pojedinci koji ponovno ulaze u vidno polje objektiva kamere (kao što su posjetitelji trgovačkog centra), riječ je o metodi biometrijske identifikacije s obzirom na to da je namijenjena prepoznavanju primjenom posebne tehničke obrade.

Primjer: Vlasnik trgovine u svoju je trgovinu postavio sustav prepoznavanja lica kako bi sadržaj oglasa koji se u njoj prikazuju prilagodio pojedinačnim osobama. Voditelj obrade prije uporabe biometrijskog sustava i prikazivanja oglasa prilagođenog sadržaja mora pribaviti izričitu i informiranu privolu svih ispitanika. Sustav se smatra nezakonitim ako se njime snimaju posjetitelji ili prolaznici koji nisu dali svoju privolu za izradu biometrijskog predloška, čak i ako se taj predložak izbriše u najkraćem mogućem roku. Ti privremeni predlošci čine biometrijske podatke koji se obrađuju u svrhu jedinstvene identifikacije određene osobe koja možda ne želi da joj se prikazuju oglasi prilagođenog sadržaja.

83.

84. Europski odbor za zaštitu podataka napominje da su neki biometrijski sustavi postavljeni u nekontroliranom okruženju[17], što znači da sustav snima i lice svakog prolaznika koji se nađe u vidnom polju objektiva kamere, uključujući osobe koje za to nisu dale svoju privolu, te izrađuje njegov biometrijski predložak. Ti se predlošci uspoređuju s onima koji su se izradili za ispitanike koji su dali svoju privolu u postupku prijave (korisnike biometrijskog uređaja) kako bi voditelj obrade utvrdio je li dotična osoba korisnik biometrijskog uređaja. U tom je slučaju sustav često dizajniran na način da omogući razlikovanje pojedinaca koje želi prepoznati u određenoj bazi podataka od pojedinaca koji nisu prijavljeni. Budući da je svrha jedinstvena identifikacija pojedinca, još uvijek je za svaku osobu koju kamera snimi potrebno utvrditi iznimku iz članka 9. stavka 2. Opće uredbe o zaštiti podataka.

Primjer: U hotelu se upotrebljava videonadzor kako bi upravitelj hotela automatski dobio obavijest u slučaju da sustav prepozna lice vrlo važnog gosta. Ti su gosti prethodno dali svoju izričitu privolu za primjenu prepoznavanja lica te su upisani u za to predviđenu bazu podataka. Ti sustavi za obradu biometrijskih podataka ne bi bili nezakoniti samo u slučaju da svi drugi gosti koji se nadziru (kako bi se identificirali vrlo važni gosti) daju svoju privolu za obradu u skladu s člankom 9. stavkom 2. točkom (a) Opće uredbe o zaštiti podataka.

Primjer: Voditelj obrade postavlja sustav videonadzora s funkcijom prepoznavanja lica na ulazu u koncertnu dvoranu kojom upravlja. Voditelj obrade mora postaviti jasno odvojene ulaze; jedan na kojem se primjenjuje biometrijski sustav i jedan na kojem se takav sustav ne primjenjuje (na primjer, ulaz s uređajima za očitavanje karte). Ulazi opremljeni biometrijskim uređajima moraju biti postavljeni i dostupni na način koji sustavu onemogućuje da izradi biometrijske predloške gledatelja koji za to nisu dali svoju privolu.

85.

86. Naposljetku, ako je privola obvezna na temelju članka 9. Opće uredbe o zaštiti podataka, voditelj obrade ne smije uvjetovati pristup uslugama koje pruža prihvaćanjem biometrijske obrade. Drugim riječima, a posebno ako se biometrijska obrada primjenjuje u svrhe autentifikacije, voditelj obrade mora ponuditi alternativno rješenje koje ne uključuje biometrijsku obradu, bez ograničenja ili dodatnog troška za ispitanika. To alternativno rješenje potrebno je i kada je riječ o osobama koje ne ispunjavaju uvjete ograničenja povezane s biometrijskim uređajem (nemogućnost prijave ili očitavanja podataka, otežana uporaba zbog invaliditeta osobe itd.) i kada se očekuje neraspoloživost biometrijskog uređaja (na primjer, uslijed kvara uređaja). Tada će biti potrebno primijeniti „rezervno rješenje” kako bi se osigurala neprekinuta usluga, koje je, međutim, ograničeno na iznimnu primjenu.

[17] To znači da je biometrijski uređaj postavljen u javnom prostoru i može snimiti svakog prolaznika, za razliku od biometrijskih sustava koji su postavljeni u kontroliranom okruženju i koji se smiju upotrebljavati samo na osobama koje su za to dale svoju privolu.

U iznimnim se slučajevima može dogoditi da je obrada biometrijskih podataka glavna aktivnost ugovorene usluge, npr. muzej koji organizira izložbu na kojoj se predstavlja primjena uređaja za prepoznavanje lica. U tom slučaju ispitanik koji želi sudjelovati u izložbi neće moći odbiti obradu biometrijskih podataka. U tom se slučaju i dalje primjenjuje zahtjev za davanje privole iz članka 9. ako su ispunjeni uvjeti iz članka 7.

5.2 Mjere predložene za smanjenje na najmanju mjeru rizika povezanih s obradom biometrijskih podataka

87. U skladu s načelom smanjenja količine podataka voditelji obrade dužni su osigurati da podatci dobiveni iz digitalne snimke u svrhu izrade predložaka ne budu preopsežni te da sadržavaju samo one informacije koje su potrebne za tu svrhu, čime se izbjegava moguća dodatna obrada. Potrebno je uvesti mjere kojima bi se zajamčilo da se predlošci ne mogu prenositi u druge biometrijske sustave.

88. Vjerojatno je da će pri identifikaciji i autentifikaciji/provjeri biti potrebno pohraniti predložak kako bi se kasnije mogao upotrebljavati u usporedbi s drugim predlošcima. Voditelj obrade mora razmotriti najpogodniju lokaciju za pohranu podataka. U kontroliranom okruženju (ograničeni hodnici ili kontrolne točke) predlošci se pohranjuju na zasebnom uređaju koji je u posjedu i pod nadzorom korisnika (u pametnom telefonu ili na identifikacijskoj iskaznici) ili se, kada su potrebni za posebne namjene i ako postoji objektivna potreba, pohranjuju u centraliziranoj bazi podataka u šifriranom obliku pri čemu ključ/lozinku zna samo korisnik radi sprečavanja neovlaštenog pristupa predlošku ili lokaciji pohrane. Ako voditelj obrade ne može izbjeći da ima omogućen pristup predlošcima, mora poduzeti odgovarajuće mjere kako bi osigurao zaštitu pohranjenih podataka. To može uključivati enkripciju predložaka primjenom kriptografskog algoritma.

89. Voditelj obrade u svakom slučaju mora poduzeti sve potrebne mjere opreza kako bi očuvao dostupnost, cjelovitost i povjerljivost obrađenih podataka. Voditelj obrade u tu svrhu posebno poduzima sljedeće mjere: kategorizacija podataka tijekom prijenosa i pohrane, pohrana biometrijskih predložaka i neobrađenih podataka ili podataka o identitetu u zasebnim bazama podataka, enkripcija biometrijskih podataka, a posebno biometrijskih predložaka, utvrđivanje politike za upravljanje enkripcijom i ključevima, uvođenje organizacijske i tehničke mjere za otkrivanje prijevara, pridruživanje koda za očuvanje cjelovitosti podataka (na primjer, potpis ili *„hash”*-funkcija) te zabrana vanjskog pristupa biometrijskim podatcima. Potrebno je osigurati razvoj takvih mjera usporedno s napretkom tehnologije.

90. Osim toga, voditelji obrade trebali bi brisati neobrađene podatke (snimke lica, govorne signale, hod itd.) i osigurati djelotvorno brisanje. Ako za obradu više nema pravne osnove, neobrađene je podatke potrebno izbrisati. Naime, ako se biometrijski predlošci izvode iz takvih podataka, izrada baze podataka može predstavljati jednaku, ako ne i veću prijetnju (jer je moguće da biometrijski predložak neće biti lako očitati bez znanja o načinu programiranja tog predloška, a od neobrađenih će se podataka sastavljati svaki predložak). U slučaju potrebe da voditelj obrade zadrži takve podatke moraju se razmotriti metode dodavanja šuma (npr. dodavanje vodenog žiga), uz čiju primjenu ne bi bilo moguće izraditi predložak. Voditelj obrade također mora izbrisati biometrijske podatke i predloške u slučaju neovlaštenog pristupa terminalu za očitavanje/usporedbu ili poslužitelju za pohranu te na kraju životnog vijeka biometrijskog uređaja izbrisati sve podatke koji nisu potrebni za daljnju obradu.

6 PRAVA ISPITANIKA

91. S obzirom na prirodu obrade podataka pri primjeni videonadzora, potrebno je dodatno pojasniti neka od prava ispitanika iz Opće uredbe o zaštiti podataka. Međutim, ovo poglavlje nije iscrpno. Sva prava koja se navode u Općoj uredbi o zaštiti podataka odnose se i na obradu osobnih podataka primjenom videonadzora.

6.1 Pravo na pristup

92. Ispitanik ima pravo od voditelja obrade zatražiti da mu potvrdi obrađuju li se njegovi osobni podatci. Kad je riječ o videonadzoru, to znači da ako se podatci ne pohranjuju ili prenose na bilo koji način, nakon što je proveden nadzor u stvarnom vremenu, voditelj informacija jedino može dostaviti informaciju o tome da se nikakvi osobni podatci više ne obrađuju (osim općih informacija koje je obvezan pružiti na temelju članka 13., vidjeti *odjeljak 7. – Obveze u pogledu transparentnosti i dostavljanja informacija*). Međutim, ako se podatci u trenutku podnošenja zahtjeva za informacije još obrađuju (tj. ako su podatci pohranjeni ili se kontinuirano obrađuju na bilo koji drugi način), ispitaniku bi u skladu s člankom 15. trebalo dodijeliti pristup i pružiti informacije.

93. Međutim, postoji niz ograničenja koji u nekim slučajevima mogu biti povezani s pravom na pristup.

- Članak 15. stavak 4. Opće uredbe o zaštiti podataka: negativan utjecaj na prava drugih

94. Budući da bilo koji broj ispitanika može biti snimljen videonadzorom u istoj sekvenciji, probiranje bi stoga uključivalo dodatnu obradu osobnih podataka drugih ispitanika. Ako ispitanik želi kopiju materijala (članak 15. stavak 3.), to bi moglo negativno utjecati na prava i slobode drugih ispitanika čiji su podatci zabilježeni u tom materijalu. Kako bi se to spriječilo, voditelj bi obrade stoga trebao razmotriti mogućnost da zbog nametljive prirode videosnimki u nekim slučajevima ne preda videosnimku na kojoj se mogu utvrditi identiteti drugih ispitanika. Međutim, zaštita prava trećih strana ne bi se smjela upotrebljavati kao izgovor za odbijanje zakonitog zahtjeva pojedinca za pristup, a voditelj bi obrade u tim slučajevima trebao poduzeti tehničke mjere radi ispunjavanja zahtjeva za pristup (na primjer, uređivanje slike kao što je maskiranje (engl. „masking”) ili premetanje dijelova slike (engl. „scrambling”)). Ipak, voditelji obrade nisu dužni poduzeti takve tehničke mjere ako na neki drugi način mogu osigurati da će moći odgovoriti na zahtjev iz članka 15. u roku koji se propisuje u članku 12. stavku 3.

- Članak 11. stavak 2. Opće uredbe o zaštiti podataka: voditelj obrade nije u mogućnosti utvrditi identitet ispitanika

95. Ako na videosnimci nije moguće pretraživati osobne podatke (tj. voditelj obrade vjerojatno bi trebao pregledati veliku količinu pohranjenog materijala kako bi pronašao dotičnog ispitanika), voditelj obrade možda neće biti u mogućnosti identificirati ispitanika.

96. Zbog tog bi razloga ispitanik pri podnošenju zahtjeva voditelju obrade trebao (uz potvrđivanje svojeg identiteta, među ostalim dostavljanjem identifikacijske iskaznice ili osobnim dolaskom) odrediti kada je točno – u razumnom vremenskom okviru razmjernom broju snimljenih ispitanika – ušao u nadzirano područje. Voditelj obrade trebao bi prethodno obavijestiti ispitanika o tome koje informacije treba dostaviti kako bi se mogao ispuniti njegov zahtjev. Ako voditelj obrade može dokazati da nije u mogućnosti identificirati ispitanika, voditelj obrade o tome na odgovarajući način obavješćuje ispitanika, ako je to moguće. U takvom bi slučaju voditelj obrade u svojem odgovoru ispitaniku trebao dati informacije o točnom području nadzora, potvrditi koje

su se kamere upotrebljavale itd. kako bi ispitanik bio potpuno upoznat s time koji su se njegovi osobni podatci možda obrađivali.

> Primjer: Ako ispitanik podnosi zahtjev za kopiju svojih osobnih podataka koji su se obrađivali primjenom videonadzora postavljenog na ulazu u trgovački centar koji bilježi 30 000 posjetitelja dnevno, trebao bi utvrditi kada se nalazio u nadziranom području, i to u vremenskom okviru od otprilike jednog sata. Ako voditelj obrade i dalje obrađuje materijal, ispitaniku je potrebno dostaviti kopiju videosnimke. Ako se u istom materijalu mogu identificirati i drugi ispitanici, tada bi prije davanja kopije ispitaniku koji je podnio zahtjev taj dio materijala trebalo anonimizirati (na primjer, zamagljivanjem cijele kopije ili njezinih dijelova).
>
> Primjer: Ako voditelj obrade sve snimke automatski briše, na primjer u roku od dva dana, po isteku ta dva dana neće biti u mogućnosti ispitaniku dostaviti snimku. Ako voditelj obrade zahtjev primi po isteku ta dva dana, treba o tome obavijestiti ispitanika.

97.

- Članak 12. Opće uredbe o zaštiti podataka: pretjerani zahtjevi

98. Ako su zahtjevi ispitanika pretjerani ili očito neutemeljeni, voditelj obrade može naplatiti razumnu naknadu u skladu s člankom 12. stavkom 5. točkom (a) Opće uredbe o zaštiti podataka ili odbiti postupiti po zahtjevu (članak 12. stavak 5. točka (b) Opće uredbe o zaštiti podataka. Voditelj obrade treba moći dokazati očiglednu neutemeljenost ili pretjeranost zahtjeva.

6.2 Pravo na brisanje i pravo na prigovor

6.2.1 Pravo na brisanje (pravo na zaborav)

99. Ako voditelj obrade nastavi obrađivati osobne podatke povrh obrade prilikom nadzora u stvarnom vremenu (npr. pohrana), ispitanik može zatražiti brisanje osobnih podataka u skladu s člankom 17. Opće uredbe o zaštiti podataka.

100. Ako nastupi jedna od okolnosti iz članka 17. stavka 1. Opće uredbe o zaštiti podataka (i ako se ne primjenjuje ni jedna od iznimaka iz članka 17. stavka 3. Opće uredbe o zaštiti podataka), voditelj obrade na zahtjev dužan je bez nepotrebnog odgađanja obrisati osobne podatke. To uključuje i obvezu brisanja osobnih podataka u slučaju da više nisu potrebni za svrhe za koje su prvotno pohranjeni ili u slučaju da je njihova obrada nezakonita (vidjeti i *odjeljak 8. – Razdoblja pohrane i obveza brisanja).* Nadalje, ovisno o pravnoj osnovi obrade, osobne je podatke potrebno izbrisati u sljedećim slučajevima:

- kad je riječ o *privoli,* u slučaju da ispitanik povuče svoju privolu (a za obradu ne postoji druga pravna osnova)
- kad je riječ o *legitimnom interesu:*
    - u slučaju da ispitanik iskoristi svoje pravo na prigovor (vidjeti *odjeljak 6.2.2.*) i ne postoje jači legitimni razlozi za obradu, ili
    - u slučaju izravnog marketinga (uključujući izradu profila) ako ispitanik podnese prigovor na obradu.

101. Ako je voditelj obrade videosnimku objavio (npr. emitiranjem ili internetskim prijenosom), potrebno je poduzeti razumne mjere kako bi se druge voditelje obrade (koji sada obrađuju predmetne osobne podatke) obavijestilo o zahtjevu ispitanika u skladu s člankom 17. stavkom 2. Opće uredbe o zaštiti podataka. Te bi razumne mjere trebale uključivati tehničke mjere, uzimajući u obzir dostupnu tehnologiju i trošak provedbe. U skladu s člankom 19. Opće uredbe o zaštiti podataka, voditelj bi

obrade nakon brisanja osobnih podataka trebao, u mjeri u kojoj je to moguće, obavijestiti sve osobe kojima su ti osobni podatci prethodno otkriveni.

102. Osim obveze voditelja obrade da na zahtjev ispitanika izbriše osobne podatke, on je u skladu s općim načelima Opće uredbe o zaštiti podataka dužan i ograničiti pohranjene osobne podatke (vidjeti *odjeljak 8.*).

103. Kad je riječ o videonadzoru, treba napomenuti da će se, na primjer, zamagljivanjem slike bez mogućnosti retroaktivnog obnavljanja osobnih podataka koje je ta slika prethodno sadržavala, osobni podatci u skladu s Općom uredbom o zaštiti podataka smatrati izbrisanima.

> Primjer: Trgovina prehrambenih proizvoda ima probleme s vandalizmom, posebno u vanjskom dijelu trgovine, te je ispred ulaza u trgovinu na zid postavljen videonadzor. Prolaznik traži da se odmah izbrišu njegovi osobni podatci. Voditelj obrade dužan je odgovoriti na zahtjev bez nepotrebnog odgađanja i u roku od najviše jednog mjeseca. Budući da predmetna snimka više ne ispunjava svrhu za koju je prvotno pohranjena (prilikom prolaska ispitanika nije se odvijao vandalizam), u trenutku podnošenja zahtjeva ne postoji legitiman interes za pohranu tih podataka koji nadilazi interese ispitanika. Voditelj obrade dužan je obrisati osobne podatke.

104.

6.2.2 Pravo na prigovor

105. Kad je riječ o videonadzoru koji se temelji na *legitimnom interesu* (članak 6. stavak 1. točka (f) Opće uredbe o zaštiti podataka) ili nužnosti obrade za izvršavanje zadaće od *javnog interesa* (članak 6. stavak 1. točka (e) Opće uredbe o zaštiti podataka), ispitanik ima pravo, na temelju svoje posebne situacije, u svakom trenutku podnijeti prigovorna obradu u skladu s člankom 21. Opće uredbe o zaštiti podataka. Osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze prava i interese tog ispitanika, obrada podataka koji se odnose na pojedinca koji je podnio prigovor mora se prekinuti. Voditelj obrade trebao bi biti dužan odgovoriti na zahtjeve ispitanika bez nepotrebnog odgađanja i u roku od najviše jednog mjeseca.

106. Kad je riječ o videonadzoru, ispitanik taj prigovor može podnijeti pri ulasku u nadzirano područje, dok se nalazi u tom području ili kada napusti to područje. U praksi to znači da, osim ako voditelj obrade dokaže da ima uvjerljive legitimne razloge, nadziranje područja u kojem je moguće utvrđivati identitet pojedinaca zakonito je samo

(1) ako voditelj obrade na zahtjev može odmah zaustaviti kameru kako se ne bi obrađivali osobni podatci, ili

(2) ako je nadzirano područje ograničeno u takvoj mjeri da voditelj obrade može osigurati pribavljanje privole ispitanika prije nego što ispitanik stupi u nadzirano područje, a to nije područje kojem je ispitanik kao građanin ovlašten pristupiti.

107. Cilj ovih smjernica nije utvrditi što se smatra *uvjerljivim* legitimnim interesom (članak 21. Opće uredbe o zaštiti podataka).

108. Kada se videonadzor upotrebljava za potrebe izravnog marketinga, ispitanik ima diskrecijsko pravo podnijeti prigovor na obradu s obzirom na to da je njegovo pravo na prigovor u tom smislu apsolutno (članak 21. stavci 2. i 3. Opće uredbe o zaštiti podataka).

Primjer: Društvo ima probleme s povredama sigurnosti na ulazu za javnost i na temelju legitimnih interesa primjenjuje videonadzor kako bi se uhvatile osobe koje ulaze u objekt nezakonito. Posjetitelj objekta na temelju svoje posebne situacije podnosi prigovor na obradu podataka koji se na njega odnose u okviru sustava videonadzora. Međutim, društvo u tom slučaju odbija zahtjev uz obrazloženje da je pohranjena snimka nužna s obzirom na to da se provodi interna istraga, što znači da postoje uvjerljivi legitimni razlozi za nastavak obrade osobnih podataka.

109.

7 OBVEZE U POGLEDU TRANSPARENTNOSTI I DOSTAVLJANJA INFORMACIJA[18]

110. U europskom pravu u području zaštite podataka već je davno utvrđeno da ispitanike treba obavijestiti o primjeni videonadzora. Ispitanike je potrebno detaljno obavijestiti o prostorima koji su pod nadzorom.[19] Opće obveze u pogledu transparentnosti i dostavljanja informacija utvrđene su u članku 12. Opće uredbe o zaštiti podataka i navode se u nastavku. U „Smjernicama o transparentnosti na temelju Uredbe 2016/679 (WP 260)" Radne skupine iz članka 29., koje je Europski odbor za zaštitu podataka potvrdio 25. svibnja 2018., navode se dodatne pojedinosti. U skladu s točkom 26. dokumenta WP 260, ako se osobni podatci prikupljaju „[…] od ispitanika na temelju opažanja (npr. upotrebom automatiziranih uređaja za prikupljanje podataka ili softvera za prikupljanje podataka kao što su kamere […])", primjenjivat će se članak 13. Opće uredbe o zaštiti podataka.

111. Uzimajući u obzir količinu informacija koja se mora dostaviti ispitaniku, voditelji obrade mogu primjenjivati višeslojni pristup u skladu s kojim mogu kombinirati metode za osiguravanje transparentnosti (točka 35. dokumenta WP 260, točka 22. dokumenta WP 89). Kad je riječ o videonadzoru, najvažnija bi se informacija trebala prikazati na samom znaku upozorenja (prvi sloj), dok se druge obvezne pojedinosti mogu pružiti na druge načine (drugi sloj).

7.1 Informacije prvog sloja (znak upozorenja)

112. Prvi se sloj odnosi na primarni način na koji voditelj obrade uspostavlja prvu komunikaciju s ispitanikom. Voditelji se obrade u toj fazi mogu koristiti znakom upozorenja na kojem se prikazuju relevantne informacije. Prikazana se informacija može pružiti u kombinaciji s ikonom kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio smislen pregled namjeravane obrade (članak 12. stavak 7. Opće uredbe o zaštiti podataka). Format informacije potrebno je prilagoditi pojedinačnoj lokaciji (točka 22. dokumenta WP 89).

7.1.1 Položaj znaka upozorenja

113. Informacije bi trebale biti prikazane na takav način da ispitanik može lako prepoznati okolnosti nadzora prije ulaska u nadzirano područje (otprilike u razini očiju). Položaj kamere nije potrebno utvrditi ako nema dvojbi o tome koja su područja pod nadzorom i ako su okolnosti nadzora jasno pojašnjene (točka 22. dokumenta WP 89). Ispitanik mora biti u mogućnosti procijeniti koje je područje obuhvaćeno vidnim poljem objektiva kamere kako bi mogao izbjeći nadzor ili prilagoditi svoje ponašanje, ako je to potrebno.

7.1.2 Sadržaj informacija prvog sloja

114. Informacije prvog sloja (znak upozorenja) općenito bi trebale prenositi najvažnije informacije, npr. pojedinosti o svrhama obrade, identitetu voditelja obrade i postojanju prava ispitanika, zajedno s informacijama o najvećim učincima obrade.[20] One, na primjer, mogu uključivati legitimne interese voditelja obrade (ili treće strane) i kontaktne podatke službenika za zaštitu podataka (ako je to primjenjivo). One moraju upućivati i na detaljniji drugi sloj informacija te gdje i kako ga pronaći.

---

[18] U nacionalnom se zakonodavstvu mogu primjenjivati posebni zahtjevi.

[19] Vidjeti dokument WP 859 Radne skupine iz članka 29., „Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance" (Mišljenje 4/2004 o obradi osobnih podataka s pomoću videonadzora).

[20] Vidjeti točku 38. dokumenta WP 260.

115. Osim toga, znak bi trebao sadržavati i informacije koje bi mogle iznenaditi ispitanika (točka 38. dokumenta WP 260). To bi moglo uključivati, na primjer, prenošenje podataka trećim stranama, posebno ako se one nalaze izvan EU-a te razdoblje pohrane. Ako te informacije nisu navedene, ispitanik bi se trebao moći pouzdati u to da se nadzor odvija samo uživo (bez bilježenja podataka i prenošenja tih podataka trećim stranama).

116.

Primjer (neobvezujući prijedlog):

7.2 Informacije drugog sloja

117. Informacije drugog sloja isto se tako moraju nalaziti na mjestu koje je lako dostupno ispitaniku, na primjer, kao cjelovito navedene na informativnom letku dostupnom na centralnom mjestu (npr. informacijskom pultu, recepciji ili blagajni) ili prikazane na lako dostupnom plakatu. Kako je prethodno navedeno, znak upozorenja prvog sloja mora jasno upućivati na informacije drugog sloja. Osim toga, najbolje bi bilo da informacije prvog sloja upućuju na digitalni izvor drugog sloja (npr. QR kod ili internetske stranice). Međutim, informacije bi trebale biti lako dostupne i u nedigitalnom obliku. Pristupanje informacijama drugog sloja trebalo bi omogućiti bez ulaska u nadzirano područje, posebno ako se informacije pružaju u digitalnom obliku (to se može ostvariti, na primjer, pružanjem poveznice). Druga prikladna sredstva mogu biti broj telefona koji je moguće nazvati. Neovisno o načinu na koji se te informacije pruže, one moraju sadržavati sve stavke obvezne na temelju članka 13. Opće uredbe o zaštiti podataka.

118. Kad je riječ o pružanju informacija ispitanicima, osim navedenih mogućnosti te u svrhu povećanja djelotvornosti, Europski odbor za zaštitu podataka promiče i uporabu tehnoloških sredstava. To može uključivati, na primjer, kamere s mogućnošću geografskog lociranja te pružanje informacija u aplikacijama i na internetskim stranicama s prikazima zemljovida kako bi pojedinci lako mogli identificirati i utvrditi videoizvore povezane s ostvarivanjem svojih prava te dobiti detaljnije informacije o postupku obrade.

Primjer: Vlasnik trgovine u svojoj je trgovini postavio videonadzor. Da bi se ispunili uvjeti iz članka 13., dovoljno je na lako vidljivom mjestu na ulazu u trgovinu postaviti znak upozorenja koji sadržava informacije prvog sloja. Osim toga, vlasnik trgovine mora izložiti informativni letak koji sadržava informacije drugog sloja i to na mjestu blagajne ili bilo kojem drugom centralnom i lako dostupnom mjestu u trgovini.

119.

8 RAZDOBLJA POHRANE I OBVEZA BRISANJA

120. Osobni se podatci u svrhe za koje se obrađuju smiju pohranjivati samo onoliko dugo koliko je potrebno (članak 5. stavak 1. točke (c) i (e) Opće uredbe o zaštiti podataka). U skladu s člankom 6. stavkom 2. Opće uredbe o zaštiti podataka, u nekim državama članicama mogu postojati posebne odredbe o razdobljima pohrane povezanima s videonadzorom.

121. Trebaju li se osobni podatci pohranjivati potrebno je utvrditi u kratkom roku. Općenito govoreći, zakonite svrhe videonadzora često uključuju zaštitu vlasništva ili čuvanje dokaza. Nastala se šteta obično može utvrditi u roku od jednog ili dva dana. Radi lakšeg dokazivanja usklađenosti s okvirom za zaštitu podataka, u interesu je voditelja obrade da organizacijske mjere poduzme unaprijed (npr. prema potrebi imenuje predstavnika za pregled i pribavljanje videomaterijala). Uzimajući u obzir načela iz članka 5. stavka 1. točaka (c) i (e) Opće uredbe o zaštiti podataka, odnosno načela smanjenja količine podataka i ograničenja pohrane, osobni podatci u većini bi se slučajeva (npr. radi utvrđivanja vandalskih činova) trebali izbrisati, u idealnom slučaju automatski, nakon nekoliko dana. Što je razdoblje pohrane dulje (posebno ako premašuje 72 sata), to će se trebati iznijeti jači dokazi o legitimnosti svrhe i nužnosti pohrane. Ako voditelj obrade videonadzor ne upotrebljava samo u svrhe nadzora objekta u svojem vlasništvu već podatke namjerava i pohranjivati, tada će morati dokazati da je pohrana uistinu nužna radi ostvarivanja određene svrhe. Razdoblje pohrane u tom se slučaju mora jasno definirati i utvrditi za svaku pojedinačnu svrhu. Odgovornost je voditelja obrade utvrditi razdoblje zadržavanja podataka u skladu s načelima nužnosti i proporcionalnosti te dokazati usklađenost s odredbama Opće uredbe o zaštiti podataka.

> Primjer: Vlasnik male trgovine posljedice bi vandalizma obično primijetio istog dana. Stoga se uobičajeno razdoblje pohrane u trajanju od 24 sata smatra dovoljnim. Međutim, mogući su razlozi za dulje razdoblje pohrane zatvaranje trgovine tijekom vikenda ili dulji praznici. Ako vlasnik trgovine utvrdi štetu, moguće je da će videosnimku trebati pohranjivati i tijekom duljeg razdoblja radi pokretanja postupka protiv počinitelja.

122.

9 TEHNIČKE I ORGANIZACIJSKE MJERE

123. Kao što se navodi u članku 32. stavku 1. Opće uredbe o zaštiti podataka, obrada osobnih podataka u okviru videonadzora mora biti zakonom dopuštena te voditelji obrade i izvršitelji obrade moraju na odgovarajući način osigurati njezinu sigurnost. Provedene **organizacijske i tehničke mjere** moraju biti **razmjerne rizicima za prava i slobode pojedinaca** koji se odnose na slučajno ili nezakonito uništenje, gubitak, izmjenu i neovlašteno otkrivanje podataka dobivenih u okviru videonadzora ili pristup takvim podatcima. U skladu s člancima 24. i 25. Opće uredbe o zaštiti podataka, voditelji obrade dužni su provoditi tehničke i organizacijske mjere i kako bi osigurali da se tijekom obrade poštuju sva načela zaštite podataka te utvrditi načine na koje ispitanici mogu ostvariti svoja prava utvrđena člancima od 15. do 22. Opće uredbe o zaštiti podataka. Voditelji obrade trebali bi donijeti unutarnji okvir i politike kojima se ta provedba osigurava u trenutku utvrđivanja sredstava za obradu i u trenutku same obrade, uključujući provedbu procjena učinka na zaštitu podataka, kada je to potrebno.

9.1 Pregled sustava videonadzora

124. Sustav videonadzora[21] sastoji se od analognih i digitalnih uređaja te softvera namijenjenih za snimanje slika određenog prostora, upravljanje tim slikama i njihovo prikazivanje operatoru. Njegove su sastavnice razvrstane u kategorije navedene u nastavku:

- Videookruženje: snimanje snimke, međusobno povezivanje i upravljanje snimkom:
    - svrha snimanja snimki jest izraditi sliku stvarnog svijeta u formatu u kojem će se njome moći koristiti ostatak sustava;
    - međusobno povezivanje odnosi se na sve prijenose podataka u videookruženju, tj. veze i komunikacije. Primjeri veza su kablovi, digitalne mreže i bežični prijenos. Komunikacije se odnose na sve videosignale i kontrolne podatkovne signale, koji mogu biti digitalni ili analogni;
    - upravljanje slikama uključuje analizu, pohranu i prikaz slike ili slijeda slika.
- Kad je riječ o upravljanju sustavom, sustav videonadzora ima sljedeće logičke funkcije:
    - upravljanje podatcima i upravljanje aktivnostima, uključujući upravljanje naredbama operatora i aktivnostima koje generira sustav (postupci alarmiranja, uzbunjivanje operatora)
    - povezivanje s drugim sustavima koje može uključivati povezivanje s drugim sigurnosnim (kontrola pristupa, protupožarni alarm) i nesigurnosnim sustavima (sustavi upravljanja objektom, automatsko prepoznavanje oznaka registarskih tablica).
- Sigurnost sustava videonadzora sastoji se od povjerljivosti, cjelovitosti i dostupnosti sustava i podataka:
    - sigurnost sustava odnosi se na fizičku sigurnost svih sastavnih dijelova sustava i kontrolu pristupa sustavu videonadzora
    - sigurnost podataka odnosi se na sprečavanje gubitka podataka ili manipulacije podatcima.

[21] U Općoj uredbi o zaštiti podataka ne navodi se definicija sustava videonadzora, ali njegov se tehnički opis može pronaći, na primjer, u normi EN 62676-1-1:2014 „Videonadzorni sustavi za uporabu u primjenama zaštite – Dio 1-1: Zahtjevi za sustav”.

125.

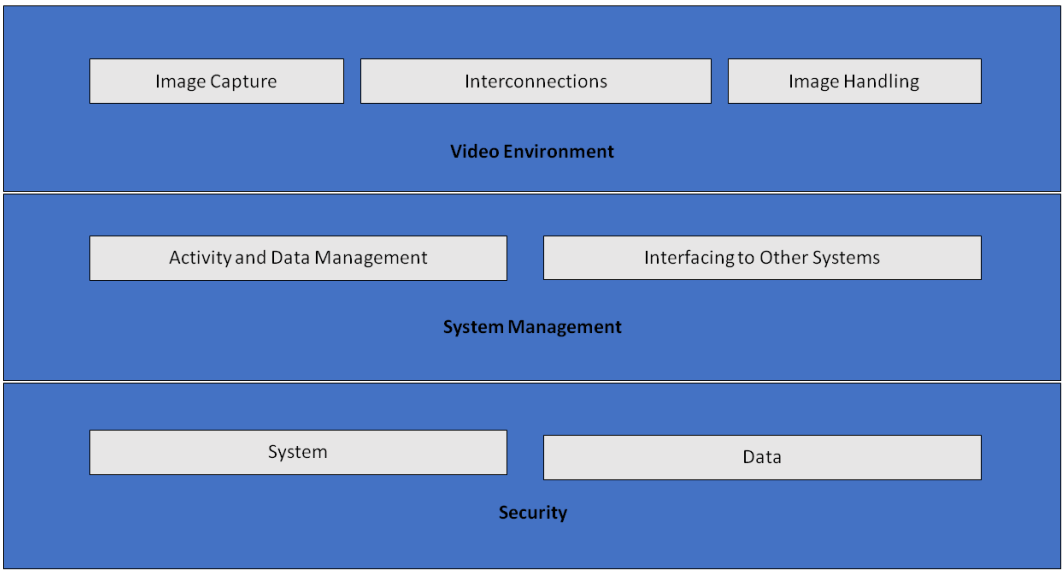

Image Capture	Snimanje snimke
Interconnections	Međusobno povezivanje
Image Handling	Upravljanje snimkom
Video Environment	Videookruženje
Activity and Data Management	Upravljanje aktivnostima i podatcima
Interfacing to Other Systems	Povezivanje s drugim sustavima
System Management	Upravljanje sustavom
System	Sustav
Data	Podatci
Security	Sigurnost

Slika 1. – Sustav videonadzora

9.2 Tehnička i integrirana zaštita podataka

126. Kao što je navedeno u članku 25. Opće uredbe o zaštiti podataka, voditelji obrade moraju početi s provedbom odgovarajućih tehničkih i organizacijskih mjera povezanih sa zaštitom podataka čim postave videonadzor – prije nego što počnu prikupljati i obrađivati videosnimke. Tim se načelima ističe potreba za ugrađenim tehnologijama za unapređenje zaštite privatnosti, zadanim postavkama koje smanjuju obradu podataka i osiguravanjem nužnih alata koji omogućuju najvišu moguću razinu zaštite osobnih podataka[22].

127. Voditelji obrade trebali bi uvesti mjere zaštite podataka i privatnosti ne samo u specifikacije dizajna tehnologije već i u organizacijske postupke. Kad je riječ o organizacijskim postupcima, voditelj obrade trebao bi donijeti odgovarajući okvir upravljanja te utvrditi i provoditi politike i postupke povezane s videonadzorom. Kad je riječ o tehničkim pitanjima, specifikacije i dizajn sustava trebali bi uključivati zahtjeve za obradu osobnih podataka u skladu s načelima iz članka 5. Opće uredbe o zaštiti podataka (zakonitost obrade, ograničavanje svrhe i podataka, smanjenje količine podataka integriranim načinom u smislu članka 25. stavka 2. Opće uredbe o zaštiti podataka, cjelovitost i povjerljivost, odgovornost

[22] WP 168, Mišljenje „The Future of Privacy" („Budućnost privatnosti"), zajednički doprinos Radne skupine iz članka 29. i Radne skupine za policiju i pravosuđe savjetovanju Europske komisije o pravnom okviru za temeljno pravo na zaštitu osobnih podataka (doneseno 1. prosinca 2009.).

itd.). U slučaju da voditelj obrade planira kupnju komercijalno upotrebljivog sustava videonadzora, te će zahtjeve morati navesti u specifikaciji za kupnju. Voditelj obrade mora osigurati usklađenost s tim zahtjevima na način da ih primijeni na sve sastavnice sustava i na sve podatke koje taj sustav obrađuje, tijekom čitavog životnog vijeka sustava.

9.3 Konkretni primjeri relevantnih mjera

128. Većina mjera koje se mogu primjenjivati radi osiguravanja sigurnosti sustava videonadzora, posebno u slučajevima u kojima se upotrebljava digitalna oprema i softver, neće se razlikovati od mjera koje se upotrebljavaju u drugim informacijskim sustavima. Međutim, neovisno o tome koje se rješenje odabere, voditelj obrade mora na odgovarajući način zaštititi sve sastavnice sustava videonadzora i podatke u svim fazama, tj. tijekom pohrane (podatci u mirovanju), prijenosa (podatci u prijenosu) i obrade (podatci u uporabi). Kako bi to ostvarili, voditelji obrade i izvršitelji obrade moraju kombinirati organizacijske i tehničke mjere.

129. Pri odabiru tehničkih rješenja, voditelj obrade trebao bi uzeti u obzir tehnologije kojima se pogoduje zaštiti privatnosti i zbog toga što one jačaju sigurnost. Primjeri takvih tehnologija jesu sustavi kojima se omogućuje maskiranje ili premetanje dijelova slike koji nisu relevantni za nadzor, ili brisanje trećih osoba ako se videosnimke dostavljanju ispitanicima.[23] S druge strane, odabrana rješenja ne bi trebala omogućiti funkcije koje nisu nužne (npr. neograničena mogućnost kretanja kamere, mogućnost zumiranja, radioprijenos, analiza i audiosnimke). Funkcije koje su omogućene, ali nisu nužne, moraju se isključiti.

130. O toj je temi moguće pronaći mnogo literature, uključujući međunarodne norme i tehničke specifikacije u području fizičke sigurnosti multimedijskih sustava[24] i sigurnosti općih informacijskih sustava[25]. Stoga ovaj odjeljak pruža samo općenit pregled te teme.

9.3.1 Organizacijske mjere

131. Osim eventualno potrebne procjene učinka na zaštitu podataka (vidjeti *odjeljak 10.*), voditelji bi obrade pri izradi politika i postupaka povezanih s videonadzorom trebali razmotriti pitanja navedena u nastavku:

- tko je odgovoran za upravljanje i rukovođenje sustavom videonadzora
- svrha i opseg projekta videonadzora
- primjerena i zabranjena uporaba (gdje i u kojim je slučajevima dopušteno odnosno nije dopušteno postavljanje videonadzora; npr. uporaba skrivenih kamera i snimanje audiosnimki uz videosnimke)[26]
- mjere koje se odnose na transparentnost iz *odjeljka 7. (Obveze u pogledu transparentnosti i dostavljanja informacija)*
- kako se snima videosnimka i vrijeme njezina trajanja, uključujući arhivsko pohranjivanje videosnimki povezanih sa sigurnosnim incidentima
- tko mora proći odgovarajuće osposobljavanje i u kojim slučajevima
- tko ima pristup videosnimkama i u koju svrhu

[23] U nekim slučajevima primjena takvih tehnologija čak može biti obvezna radi usklađivanja s člankom 5. stavkom 1. točkom (c). One u svakom slučaju mogu poslužiti kao primjeri najbolje prakse.

[24] IEC TS 62045 – Sigurnost multimedijskih sustava – Smjernica za zaštitu privatnosti opreme i sustava koji su u uporabi i koji su izvan uporabe.

[25] ISO/IEC 27000 – Serija normi povezanih sa sustavima upravljanja sigurnošću informacija.

[26] To može ovisiti o nacionalnom zakonodavstvu i sektorskim propisima.

- operativni postupci (npr. tko se služi videonadzorom, gdje je postavljen videonadzor, kako postupiti u slučaju povrede podataka)
- koje postupke vanjske strane moraju slijediti kako bi uspješno podnijele zahtjev za videosnimku te postupci za odbijanje i prihvaćanje takvih zahtjeva
- postupci za nabavu, postavljanje i održavanje sustava videonadzora
- upravljanje incidentima i postupci oporavka.

9.3.2 Tehničke mjere

132. **Sigurnost sustava** odnosi se na **fizičku sigurnost** svih sastavnica sustava i na cjelovitost sustava, tj. **zaštitu od namjernog i nenamjernog ometanja normalnog rada sustava i otpornost na takva ometanja** te **kontrolu pristupa**. Sigurnost podataka odnosi se na **povjerljivost** (podatci su dostupni samo osobama s odobrenim pristupom), **cjelovitost** (sprečavanje gubitka podataka ili manipulacije podatcima) i **dostupnost** (podatcima se može pristupiti prema potrebi).

133. **Fizička sigurnost** ključan je dio zaštite podataka i prva linija obrane jer se njome sustav videonadzora štiti od krađe, vandalizma, prirodnih katastrofa, katastrofa uzrokovanih ljudskim djelovanjem i slučajnog oštećenja (npr. visoki električni napon, ekstremne temperature i prolivena kava). Kad je riječ o analognim sustavima, fizička sigurnost ima glavnu ulogu u njihovoj zaštiti.

134. **Sigurnost sustava i podataka**, tj. zaštita od namjernog i nenamjernog ometanja normalnog rada može uključivati sljedeće:

- zaštitu čitave infrastrukture sustava videonadzora (uključujući kamere na daljinsko upravljanje, kablove i napajanje) od fizičkog interveniranja i krađe
- zaštitu prijenosa snimki s pomoću komunikacijskih kanala zaštićenih od presretanja
- enkripciju podataka
- primjenu hardverskih i softverskih rješenja kao što su vatrozidovi, antivirusni sustavi ili sustavi za otkrivanje neovlaštenog upada za zaštitu od kiberincidenata
- otkrivanje neispravnosti komponenata, softvera ili međusobnog povezivanja
- sredstva za ponovnu uspostavu dostupnosti sustava i pristupa sustavu u slučaju fizičkog ili tehničkog incidenta.

135. **Kontrolom pristupa** osigurava se da sustavu i podatcima mogu pristupiti samo ovlaštene osobe, dok su drugi u tome spriječeni. Mjere kojima se podupire kontrola fizičkog i logičkog pristupa navode se u nastavku:

- osiguravanje da svi prostori pod videonadzorom i sva mjesta na kojima se pohranjuju videosnimke budu zaštićeni od neovlaštenog pristupa trećih strana
- postavljanje zaslona (posebno ako se nalaze u otvorenim prostorima, kao što je recepcija) na način da pogled na njih imaju samo ovlašteni operatori
- utvrđivanje i provedba postupaka za dodjelu, promjenu i ukidanje fizičkog i logičkog pristupa
- primjena metoda i sredstava za autentifikaciju i ovlašćivanje korisnika, uključujući npr. dužinu lozinke i učestalost njezine izmjene
- bilježenje i redovito preispitivanje aktivnosti koje obavlja korisnik (povezane sa sustavom i podatcima)
- kontinuirano praćenje i otkrivanje neispravnosti u pogledu pristupa i rješavanje utvrđenih nedostataka u najkraćem mogućem roku.

10 PROCJENA UČINKA NA ZAŠTITU PODATAKA

136. U skladu s člankom 35. stavkom 1. Opće uredbe o zaštiti podataka, voditelji obrade dužni su provoditi procjene učinka na zaštitu podataka ako je vjerojatno da će neka vrsta obrade podataka prouzročiti visok rizik za prava i slobode pojedinaca. U članku 35. stavku 3. točki (c) Opće uredbe o zaštiti podataka propisuje se da su voditelji obrade dužni provoditi procjene učinka na zaštitu podataka ako obrada čini sustavno praćenje javno dostupnog područja u velikoj mjeri. Nadalje, u skladu s člankom 35. stavkom 3. točkom (b) Opće uredbe o zaštiti podataka, procjena učinka na zaštitu podataka nužna je i ako voditelj obrade namjerava opsežno obrađivati posebne kategorije podataka.

137. U Smjernicama o procjeni učinka na zaštitu podataka[27] pružaju se dodatni savjeti i detaljniji primjeri koji su relevantni za videonadzor (npr. povezani s „upotreb[om] sustava nadzornih kamera za praćenje ponašanja vozača na autocestama"). U članku 35. stavku 4. Opće uredbe o zaštiti podataka zahtijeva se da svako nadzorno tijelo objavi popis vrsta postupaka obrade koje u predmetnoj zemlji podliježu obveznim procjenama učinka na zaštitu podataka. Ti se popisi obično mogu pronaći na internetskim stranicama tih nadzornih tijela. Uzimajući u obzir uobičajene svrhe videonadzora (zaštita osoba i imovine, otkrivanje, sprečavanje i nadzor kaznenih djela, prikupljanje dokaza i biometrijska identifikacija osumnjičenika), razumno je pretpostaviti da će u mnogim slučajevima videonadzora biti potrebno provesti procjenu učinka na zaštitu podataka. Voditelji obrade stoga bi trebali pažljivo pregledati te dokumente kako bi utvrdili je li takva procjena potrebna te je prema potrebi provesti. Na rezultatima provedene procjene učinka na zaštitu podataka trebao bi se temeljiti odabir voditelja obrade u pogledu mjera za zaštitu podataka koje će poduzeti.

138. Važno je napomenuti i da ako rezultati procjene učinka na zaštitu podataka upućuju na to da bi obrada dovela do visokog rizika unatoč sigurnosnim mjerama koje planira provesti voditelj obrade, tada će prije obrade biti potrebno savjetovati se s relevantnim nadzornim tijelom. Pojedinosti o prethodnom savjetovanju mogu se pronaći u članku 36.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

[27] WP 248 rev. 01, Smjernice o procjeni učinka na zaštitu podataka te utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679, koje je potvrdio Europski odbor za zaštitu podataka.