ЕОЗЛП Пленарна седница, 09-10 јули 2019 година

Водич 3/2019 за обработка на лични податоци преку видео уреди

Верзија за јавно советување

Усвоен на 10 јули 2019 година

Табела на содржина

Европскиот одбор за заштита на личните податоци

Имајќи го предвид членот 70 (1д) од Регулативата 2016/679/ЕУ на Европскиот парламент и на Советот од 27 април 2016 година за заштита на физички лица во однос на обработката на личните податоци и слободното движење на таквите податоци и укинување на Директивата 95/46/ЕУ, (понатаму „ОРЗЛП“),

Имајќи го предвид Договорот за ЕЕА, особено Прилог XI и Протокол 37 од него, изменет со Одлуката на Заедничкиот комитет на ЕЕА бр. 154/2018 од 6 јули 2018 година,

Имајќи ги предвид членот 12 и членот 22 од неговиот Деловник за работа од 25 мај 2018 година, ревидиран на 23 ноември 2018 година,

ГИ УСВОИ СЛЕДНИТЕ НАСОКИ

1 ВОВЕД

1. Зголемената употреба на видео уреди има влијание врз однесувањето на граѓаните. Значителното спроведување на ваквите алатки во многу сфери од животот на физичките лица ќе изврши дополнителен притисок врз лицето за да спречи откривање на она што може да се сфати како аномалија. Всушност, овие технологии може да ги ограничат можностите за анонимно движење и анонимно користење на услуги и генерално да ја ограничат можноста да се биде незабележан. Импликациите врз заштитата на личните податоци се огромни.

2. Додека физичките лица може да се чувствуваат удобно со видео надзорот поставен за на пр. одредена безбедносна намена, мора да се преземат гаранции за да се избегне злоупотреба за тотално различни и - за субјектот на личните податоци - неочекувани цели (на пр. цел на маркетинг, надгледувања на продуктивноста на вработените итн.). Покрај тоа, сега многу алатки се применуваат за да се искористат снимените слики и да се претворат традиционалните камери во паметни камери. Количината на податоците собрани од видеото, во комбинација со овие алатки и техники, ги зголемуваат ризиците од секундарна употреба (без оглед дали се поврзани или не со намената првично доделена на системот) или дури и ризиците од злоупотреба. Општите принципи во ОРЗЛП (член 5), секогаш треба внимателно да се земат предвид кога се работи за видео надзор.

3. Системите за видео надзор на повеќе начини го менуваат начинот на кој професионалците од приватниот и јавниот сектор взаемно дејствуваат на приватни или јавни места со цел зајакнување на безбедноста, добивање на анализа на публиката, доставување на персонализирано рекламирање, итн. Видео надзорот се здоби со високи перформанси преку зголемената имплементација на интелигентните видео анализи. Овие техники можат да бидат повеќе нападни (на пр. комплексни биометриски технологии) или помалку нападни (на пр. едноставни алгоритми за броење). Општо, да се остане анонимен и да се зачува приватноста станува сè потешко. Прашањата за заштита на личните податоци покренати во секаква ситуација може да се разликуваат, како и правната анализа при употреба на некоја од овие технологии.

4. Покрај проблемите со приватноста, постојат и ризици поврзани со евентуални дефекти на овие уреди и пристрасностите што можат да ги предизвикаат. Истражувачите известуваат дека софтверот што се користи за идентификација, препознавање или анализи на лицето, различно се извршува врз основа на возраста, полот и етничката припадност на лицето што го идентификува. Алгоритмите ќе постапуваат врз основа на различни демографии, така што пристрасноста во препознавањето на лицето се заканува да ги засилат предрасудите на општеството. Затоа, контролорите на личните податоци мора исто така да обезбедат дека обработката на биометриските податоци што произлегува од видео надзорот подлежи на редовна проценка на нејзината релевантност и достатност на предвидените гаранции.

5. Видео надзорот не е вообичаена потреба кога има други средства за да се постигне основната цел. Инаку, ризикуваме промена во културните норми што доведува до прифаќање на недостаток на приватноста како општа почетна точка.

6. Овие насоки имаат за цел да дадат насочување за тоа како да се применува ОРЗЛП во однос на обработката на личните податоци преку видео уреди. Примерите не се исцрпни, општото расудување може да се примени за сите потенцијални области на употреба.

2 ОПСЕГ НА ПРИМЕНАТА [1]

2.1 Лични податоци

7. Систематското автоматско набљудување на одреден простор со оптички или аудио-визуелни средства, претежно за цели на заштита на имотот или за заштита на животот и здравјето на поединецот, стана значаен феномен во нашето време. Оваа активност овозможува собирање и задржување на слики или аудио-визуелни информации за сите лица кои влегуваат во набљудуваниот простор кои се идентификуваат врз основа на нивниот изглед или други специфични елементи. Идентитетот на овие лица може да се утврди врз основа на овие детали. Исто така, овозможува понатамошна обработка на личните податоци за присуството и однесувањето на лицата во дадениот простор. Потенцијалниот ризик од злоупотреба на овие лични податоци расте во однос на големината на набљудуваниот простор, како и со бројот на лица што го посетуваат просторот. Овој факт се одразува во Општата регулатива за заштита на личните податоци во член 35(3)(в) кој бара спроведување на проценка на влијанието врз заштитата на личните податоци во случај на систематско набљудување на јавно достапна површина во голем обем, како и во член 37(1)(б) кој бара од обработувачите да назначат офицер за заштита на личните податоци, доколку операцијата за обработка по својата природа повлекува редовно и систематско набљудување на субјектите на лични податоци.

[1] ЕОЗЛП забележува дека таму каде што тоа го дозволува ОРЗЛП, може да се применат одредени барања во националното законодавство.

8. Сепак, Регулативата не се применува за обработка на лични податоци што нема упатување на личност, на пр. ако индивидуата не може да се идентификува, директно или индиректно.

9.

Пример: ОРЗЛП не се применува за лажни камери (т.е. каква било камера која што не функционира како камера и со тоа не обработува лични податоци). *Сепак, во некои земји-членки тоа може да биде предмет на друго законодавство.*

Пример: Снимките од голема надморска височина спаѓаат во опсегот на ОРЗЛП доколку под околностите обработените податоци можат да бидат поврзани со одредено лице.

Пример: Видео камера е интегрирана во автомобил за помагање при паркирање. Ако камерата е конструирана или прилагодена на таков начин што не собира никакви информации во врска со физички лица (како што се регистарски таблички или информации што би можеле да ги идентификуваат минувачите), ОРЗЛП не се применува.

2.2 Примена на ЕУ Директива 2016/680 (Полициска директива)

10. Имено, обработката на личните податоци од надлежните органи со цел на спречување, испитување, откривање или гонење на кривични дела или извршување кривични казни, вклучително и заштита и спречување на закани по јавна безбедност, спаѓа во ЕУ Директивата 2016/680.

2.3 Исклучок на активности во домот

11. Согласно член 2(2)(в), обработката на лични податоци од страна на физичко лице при исклучително лични и домашни активности, која исто така може да вклучува и активност преку интернет, не е во рамките на опсегот на ОРЗЛП.[2]

12. Оваа одредба - т.н. исклучок на активности во домот - во контекст на видео надзор мора тесно да се толкува. Оттука, како што смета Европскиот суд на правдата (ЕСП), т.н. „исклучок на активности во домот“ мора *„да се толкува дека се однесува само на активности што се вршат во текот на приватниот или семејниот живот на физичките лица, што очигледно не е случај со обработка на лични податоци што се состои во објавување на интернет,*

[2] Види исто образложение 18.

така што тие податоци ќе бидат достапни за неопределен број на луѓе“.[3] Понатаму, ако системот за видео надзор, до степен до кој вклучува постојано снимање и чување на лични податоци и опфаќа *„дури и делумно, јавен простор и соодветно е насочен нанадвор од приватното опкружување на лицето што ги обработува податоците на тој начин, не може да се смета како активност која е чисто ’лична или домашна‘ активност за целите на вториот потстав од член 3(2) од Директивата 95/46“* [4].

13. Што се однесува до видео уредите што делуваат во просториите на приватно лице, тоа може да потпаѓа под исклучок на домашни активности. Тоа ќе зависи од неколку фактори, кои сите треба да се земат предвид со цел да се дојде до заклучок. Покрај горенаведените елементи утврдени со пресудите на ЕСП, корисникот на видео надзор во домот треба да разгледа дали има некаков личен однос со субјектот на личните податоци, дали размерот или зачестеноста на надзорот укажува на некаква професионална активност од неговата страна и на потенцијално негативното влијание на надзорот врз субјектите на лични податоци. Присуството на било кој од горенаведените елементи не значи дека обработката е надвор од опсегот на исклучок на активности во домот, туку потребна е целокупна проценка за тоа утврдување.

Пример: Еден турист прави видео снимки преку неговиот мобилен телефон и преку видео камера за да ги документира своите одмори. Тој ги прикажува снимките на пријателите и семејството, но не ги прави достапни за неопределен број на луѓе. Ова би потпаѓало под исклучок на активности во домот.

Пример: Планинска велосипедистка во сака да го сними своето спуштање со спортска камера. Таа се вози во оддалечена област и планира да ги користи снимките само за лична забава во домот. Ова би потпаѓало под исклучок на активности во домот.

Пример: Некој ја набљудува и снима сопствената градина. Имотот е ограден и само контролорот и неговото семејство редовно влегуваат во градината. Ова би потпаѓало под исклучок на активности во домот, под услов видео надзорот да не се проширува дури и делумно на јавен простор или соседната сопственост.

14.

[3] Европски суд на правдата, Пресуда во случај Ц-101/01, случајот *Bodil Lindqvist*, 6 ноември 2003 година, став 47.

[4] Европски суд на правдата, пресуда во случај Ц-212/13, *František Ryneš v Úřad pro ochranu osobních údajů,* 11 декември 2014 година, став 33.

3 ЗАКОНИТОСТ НА ОБРАБОТКАТА

15. Пред употреба, целите на обработката треба да бидат детално наведени (член 5(1)(б)). Видео надзорот може да послужи за многу цели, на пр. заштита на имот и други средства, прибирање докази за граѓански парници.[5] Овие цели за набљудување треба да бидат документирани во писмена форма (член 5(2)) и треба да бидат одредени за секоја надзорна камера што се користи. Камерите што се користат за истата цел од еден контролор можат да бидат документирани заедно, сè додека секоја камера што се употребува има документирана намена. Понатаму, субјектите на лични податоци мора да бидат информирани за целта(целите) на обработката во согласност со член 13 (*види дел 7, Транспарентност и обврски за информации*). Видео надзорот основан само на цел за „безбедност“ или „за ваша безбедност“ не е доволно одреден (член 5(1)(б)). Покрај тоа, тоа е спротивно на принципот дека личните податоци се обработуваат законски, праведно и на транспарентен начин во однос на субјектот на личните податоци (види член 5(1)(а)).

16. Во принцип, секоја правна основа според член 6(1) може да обезбеди правна основа за обработка на податоци од видео надзор. На пример, се применува член 6(1)(в), кога националното законодавство пропишува обврска за видео надзор.[6] Сепак, одредбите што најверојатно ќе се користат во пракса се:

- Член 6(1)(ѓ) (легитимен интерес).
- Член 6(1)(д) (неопходност за извршување на задача од јавен интерес или при вршење на службена дејност на надлежен орган)

Во прилично исклучителни случаи, членот 6(1)(а) (согласност) може да се користи како правна основа од контролорот.

3.1 Легитимен интерес, член 6(1)(ѓ)

17. Правната проценка на членот 6(1)(ѓ) треба да се основа на следните критериуми во согласност со образложението 47.

3.1.1 Постоење на легитимни интереси

18. Видео надзорот е законски доколку е неопходно да се исполни целта на легитимниот интерес спроведен од контролорот или трето лице, освен кога со такви интереси предност имаат интересите или основните права и слободи на субјектот на личните податоци (член 6(1)(ѓ)). Легитимните интереси што ги следи контролорот или третото лице можат да бидат правни[7], економски или нематеријални интереси.[8] Како и да е, контролорот треба да смета дека доколку субјектот на личните податоци има приговор против видео надзорот согласно член 21, контролорот може да продолжи со видео надзорот на тој субјект на лични податоци, ако докаже дека постојат *убедливи* легитимни интереси кои имаат предност пред интересите,

[5] Правилата за собирање на докази за граѓански парници варираат во секоја земја-членка.

[6] Овие насоки не ги анализираат или не влегуваат во детали за националното законодавство што може да се разликува помеѓу земјите-членки.

[7] Европски суд на правдата, пресуда во случајот C-13/16, случај *Rīgas satiksme*, 4 мај 2017 година

[8] види wp 217, Работна група 29.

правата и слободите на субјектот на личните податоци или за воспоставување, извршување или одбрана на правни барања.

19. Во случај на реална и опасна ситуација, целта да се заштити имотот од провалување, кражба или вандализам, може да претставува легитимен интерес за видео надзор.

20. Легитимниот интерес треба да биде вистински и мора да биде тековно прашање (т.е. не смее да биде измислен или шпекулативен)[9]. Треба да се случи вистинска опасна ситуација - како што се штети или сериозни инциденти во минатото - пред да започнете со видео надзорот. Имајќи го предвид принципот на одговорност, на контролорите ќе им биде препорачано да документираат релевантни инциденти (датум, начин, финансиска загуба) и сродни кривични пријави. Овие документирани инциденти можат да бидат силен доказ за постоење на легитимен интерес.

Пример: Сопственик на продавница сака да отвори нова продавница и сака да инсталира систем за видео надзор. Со претставување на статистички податоци тој може да покаже дека постои големо очекување на вандализам во околното соседство. Исто така, корисно е и искуството на соседните продавници. Не е нужно дека на контролорот мора да му се случи штета. Сепак, не е доволно да се претстави национална или општа статистика на криминалот без да се анализира предметната област или опасностите за оваа
21. специфична продавница.

22. Непосредните опасни ситуации можат да претставуваат легитимен интерес, како што се продавници што продаваат скапоцени производи (на пр. златарници), или области за кои е познато дека се типични места на злосторства за имотни престапи (на пр. бензински пумпи).

23. ОРЗЛП исто така јасно наведува дека јавните органи не можат да ја засноваат нивната обработка врз основа на легитимен интерес при извршување на нивните задачи, член 6 (1) реченица 2.

3.1.2 Неопходност на обработката

24. Личните податоци треба да бидат соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат („минимален обем на податоци“), видете во член 5(1)(в). Пред да се инсталира систем за видео надзор, контролорот треба секогаш критички да испита дали оваа мерка е прво најпогодна за постигнување на посакуваната цел, а второ дали е соодветна и неопходна за нејзините цели. Мерките за видео

[9] види wp 217, Работна група 29, стр. 24 секв.

надзор треба да бидат избрани само ако целта на обработката не може да се исполни разумно со други средства кои се помалку наметливи кон основните права и слободи на субјектот на личните податоци.

25. Со однос на ситуацијата кога контролорот сака да спречи кривични дела поврзани со имотот, наместо да инсталира систем за видео надзор, контролорот може да преземе и алтернативни безбедносни мерки, како што е оградување на имотот, воведување на редовни патроли на безбедносните лица, користење на вратари, обезбедување на подобро осветлување, инсталирање на безбедносни брави, заштитни прозорци и врати, или нанесување на слоеви на боја против цртање на графити или фолии на ѕидовите. Овие мерки можат да бидат ефективни против провалување, кражба и вандализам исто како и системите за видео надзор.

26. Пред да се управува со систем на камери, контролорот е должен да процени каде и кога се строго неопходни мерките за видео надзор. Обично системот за набљудување што работи ноќно време, како и надвор од редовното работно време, ќе ги задоволи потребите на контролорот за да спречи какви било опасности на неговиот имот.

27. Општо гледано, потребата да се користи видео надзор за заштита на просториите на контролорите завршува на границите на имотот[10]. Сепак, постојат случаи кога надзорот на имотот не е доволен за ефективна заштита. Во некои поединечни случаи можеби ќе биде потребно да се надмине видео надзорот кон непосредната околина на просториите. Во овој контекст, контролорот треба да преземе физички и технички средства, на пример блокирање или замаглување на неважните области.

Пример: Книжарница сака да ги заштити своите простории од оштетување. Во принцип, камерите треба да ги снимаат само просториите на книжарницата затоа што не е неопходно да се набљудуваат соседните простории или јавните места во околината на
28. просториите на книжарницата за таа намена.

29. Прашања во врска со неопходноста од обработка исто така се појавуваат во врска со начинот на зачувување на доказите. Во некои случаи, можеби е неопходно да се користат решенија од црна кутија кога снимките автоматски се бришат по одреден период на зачувување и се пристапува кон нив само во случај на инцидент. Во други ситуации можеби нема да биде неопходно воопшто да се снима видео материјал, туку наместо тоа посоодветно е да се користи набљудување во реално време. Одлуката помеѓу решенија од црни кутии и набљудување во реално време, исто така, треба да се основа на целта која се спроведува. Ако

[10] Ова исто така може да биде предмет на националното законодавство во некои земји членки.

на пример, целта на видео надзорот е зачувување на докази, методите за реално време обично не се соодветни. Понекогаш, набљудувањето во реално време може да биде повеќе наметливо од зачувување и автоматско бришење на материјал по ограничена временска рамка. Во овој контекст мора да се земе предвид принципот за минимален обем на податоци (член 5(1)(в)). Исто така, треба да се има предвид дека е можно контролорот да користи безбедносен персонал наместо видео надзор, кои се во можност веднаш да реагираат и да интервенираат.

3.1.3 Балансирање на интересите

30. Претпоставувајќи дека видео надзорот е неопходен за да се заштитат легитимните интереси на контролорот, системот за видео надзор може да се стави во функција само ако легитимните интереси на контролорот или на третото лице (на пр. заштита на сопственост или физички интегритет) не се надминати од интересите или основните права и слободи на субјектот на личните податоци. Контролорот треба да размисли 1) до кој степен набљудувањето влијае врз легитимните интереси, основните права и слободите на физичките лица и 2) ако тоа предизвикува прекршувања или негативни последици во однос на правата на субјектот на личните податоци. Всушност, балансирањето на интересите е задолжително. Основните права и слободи од една страна и легитимните интереси на контролорот, од друга страна, треба да бидат внимателно проценети и урамнотежени.

Пример: Приватна компанија за паркирање има документирано повторливи проблеми со кражби во паркирани автомобили. Областа за паркирање е отворен простор и лесно пристаплива од секого, но е јасно обележана со знаци и блокатори на патот што го опкружуваат просторот. Компанијата за паркирање има легитимен интерес (спречување на кражби во автомобилите на клиентите) да го следат просторот во текот на денот кога искусуваат проблеми. Субјектите на личните податоци се набљудуваат во ограничена временска рамка, тие не се во областа за рекреативни цели и исто така и во нивен интерес е да се спречат кражбите. Интересот на субјектите на личните податоци да не бидат набљудувани во овој случај е надминат од легитимниот интерес на контролорот.

Пример: Ресторан одлучува да инсталира видео камери во тоалетите за да ја контролира уредноста на санитарните јазли. Во овој случај, правата на субјектите на личните податоци јасно го надминуваат интересот на контролорот, затоа камерите не можат да бидат таму инсталирани.

31.

3.1.3.1 Донесување на одлуки од случај до случај

32. Бидејќи според регулативата балансирањето на интересите е задолжително, одлуките треба да се носат од случај до случај (види член 6(1)(ѓ)). Наведување на апстрактни ситуации или споредување на слични случаи едни со други не е доволно. Контролорот треба да ги оцени ризиците од наметнување во правата на субјектот на личните податоци; овде пресуден критериум е интензитетот на интервенцијата за правата и слободите на поединецот.

33. Интензитетот може, меѓу другото, да се дефинира според видот на собраните информации (содржина на информации), обемот (густина на информациите, просторен и географски степен), бројот на засегнатите субјекти на лични податоци, или како конкретен број или како дел од релевантната популацијата, предметната состојба, вистинските интереси на групата на

субјекти на лични податоци, алтернативните средства, како и според природата и обемот на проценка на личните податоци.

34. Важни фактори за балансирање може да бидат големината на областа која е под надзор и бројот на субјекти на лични податоци под надзор. Употребата на видео надзор во оддалечена област (т.е. за да гледате животински свет или да се заштити критична инфраструктура, како што е приватна радио антена) мора да се процени различно од видео надзорот во пешачка зона или трговски центар.

Пример: Ако е инсталирана камера во автомобил (на пр. со цел собирање на докази во случај на несреќа), важно е да се обезбедите дека оваа камера постојано не го снима сообраќајот, како и лица кои се наоѓаат во близина на патот. Во спротивно, интересот за видео снимки како доказ во повеќе теоретски случај на сообраќајна несреќа, не може да го оправда ова сериозно мешање во правата на субјектот на личните податоци.[11]

3.1.3.2 Разумни очекувања на субјектите на лични податоци

35. Според образложението 47, постоењето на легитимен интерес изискува внимателна проценка. Тука треба да бидат вклучени разумните очекувања на субјектот на личните податоци во тоа време и во контекст на обработката на неговите лични податоци. Што се однесува до систематското набљудување, односот помеѓу субјектот на личните податоци и контролорот може значително да варира и може да влијае врз тоа што е разумно очекувано од субјектот на личните податоци. Толкувањето на концептот на разумни очекувања не треба да се заснова само на предметните субјективни очекувања. Наместо тоа, одлучувачки критериум треба да биде ако објективно трето лице може разумно да очекува и заклучи дека ќе биде предмет на набљудување во оваа конкретна ситуација.

36. На пример, работникот на неговото работно место во повеќето случаи веројатно нема очекува да биде набљудуван од неговиот работодавец.[12] Покрај тоа, не треба да се очекува да се врши набљудување во нечија приватна градина, во места на живеење или во простории за преглед и третман. Во истата насока, не е разумно да се очекува набљудување во санитарни објекти или сауни – набљудување на вакви простории се смета како интензивен упад во правата на субјектот на личните податоци. Разумните очекувања на субјектите на лични податоци се дека

[11] Дури и ако под некои околности може теоретски да се идентификува правна основа за делови од таков надзор, контролорот сепак ќе треба да ги почитува општите принципи (чл. 5 од ОРЗЛП) и обврските за транспарентност за правилно информирање на субјектот на личните податоци (чл. 13 од ОРЗЛП).

[12] Види исто: Работна група 29, Мислење 2/2017 за обработка на лични податоци на работа, WP249, усвоено на 8 јуни 2017 година.

нема да се изврши видео надзор во такви простории. Од друга страна, клиентот на некоја банка може да очекува дека тој/таа се набљудува во банката или од банкоматот.

37. Субјектите на личните податоци исто така може да очекуваат да бидат ослободени од набљудување на јавни места, особено ако тие јавни места обично се користат за опоравување, регенерација и активности за слободно време, како и во простории каде што поединците остануваат и/или комуницираат, како што се места за седење, маси во ресторани, паркови, кина и сали за вежбање. Овде, легитимните интереси или права и слободи на субјектот на личните податоци честопати ќе ги надминат легитимните интереси на контролорот.

38.

> Пример: Субјектите на лични податоци очекуваат да не бидат набљудувани во тоалети. На пример, видео надзорот за да се спречат несреќи не е пропорционален.

39. Знаците што го информираат субјектот за видео надзорот немаат важност при утврдување на тоа што субјектот на лични податоци објективно може да очекува.

3.2 Неопходност за извршување на задача од јавен интерес или при вршење на службена надлежност доделена на контролорот, член 6(1)(д)

40. Личните податоци може да се обработуваат преку видео надзор според член 6(1)(д) доколку е неопходно да се изврши задача од јавен интерес или при вршење на службена надлежност.[13] Можно е извршувањето на службена надлежност да не дозволува ваква обработка, но други законски основи како што се „здравје и безбедност“ за заштита на вработените, посетителите и вработените може да обезбедат ограничен опсег на обработка, притоа сè уште да се земаат предвид обврските на ОРЗЛП и правата на субјектите на личните податоци.

41. Земјите членки можат да задржат или воведат одредени национални законодавства за видео надзор за да ја прилагодат примената на правилата на ОРЗЛП со утврдување на поточни конкретни барања за обработка сè додека тоа е во согласност со принципите утврдени со ОРЗЛП (на пр. ограничување на чување, пропорционалност).

3.3 Согласност, член 6(1)(а)

42. Согласноста треба да е слободно дадена, конкретна, информирана и недвосмислена, како што е опишано во насоките за согласност.[14]

[13] Основата за наведената обработка е утврдена со законодавството на Унијата или законодавството на земјата членка» и «е неопходна за извршување на задача од јавен интерес или при вршење на службена надлежност доделена на контролорот (член 6(3)).

[14] Покрај тоа, Работната група 29 (РГ 29) донесе „Насоки за согласност според Регулативата 2016/679“ (WP 259 rev. 01) што треба да се земат предвид.

43. Во однос на систематското набљудување, согласноста на субјектот на личните податоци може да служи како правна основа во согласност со член 7 (види образложение 43) само во исклучителни случаи. Во природата на надзорот е оваа технологија да набљудува во исто време непознат број на луѓе. Контролорот тешко ќе може да докаже дека субјектот на личните податоци дал согласност пред обработката на неговите/нејзините лични податоци (член 7(1)). Под претпоставка дека субјектот на лични податоци ја повлекува својата согласност, ќе му биде тешко на контролорот да докаже дека личните податоци веќе не се обработуваат (член 7 (3)).

Пример: Спортистите можат да бараат снимање за време на индивидуалните вежби со цел да ги анализираат нивните техники и перформанси. Од друга страна, кога спортски клуб презема иницијатива да следи цел тим за истата цел, согласноста честопати нема да важи, бидејќи поединечни спортисти може да се чувствуваат под притисок да дадат согласност, така што нивното одбивање на согласност нема да влијае негативно врз соиграчите.

44.

45. Доколку контролорот сака да се потпре на согласноста, негова должност е да се погрижи дека секој субјект на лични податоци што влегува во просторот кој е под видео надзор, ја дал неговата/нејзината согласност. Оваа согласност треба да ги исполнува условите од член 7. Влегување во означена набљудувана просторија (на пример, луѓето се поканети да поминат низ одреден ходник или порта за да влезат во набљудуваната просторија), не претставува изјава или јасно потврден чин потребен за согласност, освен ако не ги исполнува критериумите од член 4 и 7 како што е опишано во насоките за согласност.[15]

46. Со оглед на нерамнотежата на моќта меѓу работодавците и вработените, во повеќето случаи работодавците не треба да се потпираат врз согласност при обработка на лични податоци, бидејќи најверојатно нема да биде слободно дадена. Во овој контекст треба да бидат земени предвид насоките за согласност.

47. Правото на земјите членки или колективните договори, вклучително и „работните договори“, можат да предвидат конкретни правила за обработка на личните податоци на вработените во контекст за вработување (види член 88).

4 ОТКРИВАЊЕ НА ВИДЕО СНИМКИ НА ТРЕТО ЛИЦЕ

48. Во принцип, општите одредби на ОРЗЛП се применуваат за откривање на видео записи на трето лице.

[15] Додатно на тоа, Работната група 29 (РГ 29) донесе „Насоки за согласност според Регулативата 2016/679“ (WP 259) што треба да се земе предвид.

4.1 Општо откривање на видео снимки на трето лице

49. Откривањето е дефинирано во член 4(2) како пренос (на пр. индивидуална комуникација), објавување (на пр. објавување преку интернет) или на друг начин ставање на располагање. Трето лице е дефинирано во член 4(10). Онаму каде се прави откривање на трети земји или меѓународни организации, исто така се применуваат посебните одредби на член 44 и сл.

50. Секое откривање на лични податоци е посебен вид на обработка на лични податоци за кои контролорот треба да има правна основа во член 6.

> Пример: Контролорот кој сака да постави снимка на интернет, треба да има правна основа за таа обработка, на пример преку добивање на согласност од субјектот на личните податоци согласно член 6(1)(а).

51.

52. Преносот на видео снимки на трето лице со цел различна од онаа за која што се собрани личните податоците е возможно според правилата на член 6(4).

> Пример: Инсталиран е видео надзор на рампа (на паркинг) со цел откривање на штети. Се појавува штета и снимките се пренесуваат на адвокат за да започне предмет. Во овој случај, целта за снимање е иста како онаа за пренесување.
>
> Пример: Инсталиран е видео надзор на рампа (на паркинг) со цел откривање на штети. Снимката е објавена на интернет од прости забавни причини. Во овој случај, целта е променета и не е компатибилна со почетната намена. Поради тоа ќе биде проблематично да се идентификува правна основа за таа обработка (објавување).

53.

54. Примател/трето лице ќе мора да направи своја правна анализа, особено да ја идентификува правната основа според член 6 за неговата обработка (на пр. примање на материјалот).

4.2 Откривање на видео снимки до агенциите за спроведување на законот

55. Откривањето на видео снимки до агенциите за спроведување на законот е исто така независен процес, кој изискува посебна оправданост за контролорот.

56. Според член 6(1)(в), обработката е законска доколку е неопходна за исполнување на правна обврска на која е подложен контролорот. Иако важечкиот полициски закон е материја под единствена контрола на земјите членки, најверојатно постојат општи правила со кои се уредува преносот на докази до агенциите за спроведување на законот во секоја земја членка. Обработката на контролорот за предавање на личните податоците е регулирана со ОРЗЛП. Доколку националното законодавство бара контролорот да соработува со агенциите за спроведување на законот (т.е. истрага), правната основа за предавање на личните податоците е правна обврска согласно член 6(1)(в).

57. Ограничувањето на целта во член 6(4) во тој случај честопати не е проблематично, бидејќи откривањето експлицитно се враќа на законот на земјите членки. Разгледување на посебните барања за промена на целта во смисла на потсавки а - е поради тоа не е потребно.

58. Пример: Сопственик на продавница снима на нејзиниот влез. Снима лице како краде паричник на друго лице. Полицијата бара од контролорот да го предаде материјалот за да помогне во нивната истрага. Во тој случај, сопственикот на продавницата ќе ја искористи правната основа според член 6(1)(в) (правна обврска) прочитана во врска со релевантниот национален закон за обработка на преносот.

Пример: Во продавница е инсталирана камера од безбедносни причини. Сопственикот на продавницата верува дека снимил нешто сомнително во неговите снимки и решил материјалот да го испрати во полиција (без никакво навестување дека е во тек истрага од некој вид). Во овој случај, сопственикот на продавницата треба да процени дали се исполнети условите под член 6(1)(ѓ), во повеќето случаи.

59. Обработката на личните податоци од самите агенции за спроведување на законот не ја следи ОРЗЛП (види член 2(2)(г)), туку наместо тоа ја следи Полициската директива (ЕУ2016/680).

5 ОБРАБОТКА НА ПОСЕБНИ КАТЕГОРИИ НА ЛИЧНИ ПОДАТОЦИ

60. Системите за видео надзор обично собираат огромни количини на лични податоци што можат да откријат податоци со голема мера на лична природа, па дури и посебни категории на лични податоци. Всушност, навидум незначајните податоци првично собрани преку видео може да се

користат за да се заклучат други информации за да се постигне различна цел (на пр. да се мапираат навиките на поединецот). Сепак, видео надзорот не се смета секогаш за обработка на посебни категории на лични податоци.

61. Пример: Видео снимките на кои се гледа субјектот на лични податоци како носи очила или користи инвалидска количка, не се сметаат за посебни категории на лични податоци.

62. Меѓутоа, ако видео снимката е обработена за да се извлече посебни категории на лични податоци, се применува член 9.

63. Пример: Политички мислења би можеле, на пример, да се извлечат од слики што покажуваат субјекти на лични податоци што можат да се идентификуваат, како учествуваат во некој настан, вклучуваат штрајк и др. Ова би спаѓало во член 9.

Пример: Болница што инсталира видео камера за да ја следи здравствената состојба на пациентот, ќе се смета за обработка на посебни категории на лични податоци (член 9).

64. Општо, како принцип, секогаш кога се инсталира систем за видео надзор треба внимателно да се внимава на принципот за минимален обем на податоците. Оттука, дури и во случаи кога не се применува членот 9(1), контролорот на личните податоци треба секогаш да се обиде да го минимизира ризикот од правење на снимки кои откриваат други чувствителни податоци (надвор од член 9), без оглед на целта.

Пример: Видео надзорот кој опфаќа некоја црква не спаѓа во член 9. Сепак, контролорот треба да спроведе особено внимателна проценка согласно член 6(1)(ѓ), земајќи ја предвид природата на личните податоци, како и ризикот од опфаќање на други чувствителни податоци (надвор од член 9) при проценка на интересите на субјектот на личните податоци.

65.

66. Ако се користи систем за видео надзор со цел да се обработуваат посебни категории на лични податоци, контролорот на личните податоци мора да идентификува исклучок за обработка на посебни категории на лични податоци според член 9 (т.е. исклучок од општото правило дека не треба да се обработуваат посебни категории на лични податоци) и правна основа според член 6.

67. На пример, членот 9(2)(в) (обработката е неопходна за да се заштитат виталните интереси на субјектот на личните податоци или на друго физичко лице, кога субјектот на лични податоци е физички или правно неспособен да дава согласност) би можел - во теорија и во исклучителна ситуација – да биде употребен, но контролорот на лични податоци треба да го оправда како апсолутна неопходност да ги заштити виталните интереси на некое лице и да докаже дека ова лице „*е физички или правно неспособно да даде согласност*“. Додатно на тоа, контролорот на лични податоци нема да може да го користи системот за која било друга причина.

68.

Пример: Болницата набљудува пациент од медицински причини. Субјектот на лични податоци е донесен во несвест со брза помош во болницата. Во овој случај, може да се примени член 9(2)(в).

69. Важно е да се напомене овде дека секој исклучок наведен во член 9 веројатно нема да биде употреблив за да се оправда обработката на посебните категории на лични податоци преку видео надзор. Поконкретно, контролорите на лични податоци кои ги обработуваат тие податоци во контекст на видео надзор не можат да се потпираат на член 9(2)(д), кој овозможува обработка која се однесува на лични податоци што се јасно објавени од субјектот на личните податоци. Самиот акт на влегување во опсегот на видео камерата не значи дека субјектот на лични податоци има намера да ги објави во јавност посебните категории на лични податоци што се однесуваат на него или неа.

70. Понатаму, обработката на посебни категории на лични податоци бара зголемена и континуирана претпазливост кон одредени обврски; на пример, високо ниво на безбедноста и проценка на влијанието врз заштитата на личните податоците, доколку е потребно.

71. Пример: Работодавачот не смее да ги користи снимките за видео надзор што покажуваат штрајк со цел да ги идентификува штрајкувачите.

5.1 Општи разгледувања при обработка на биометриски податоци

72. Употребата на биометриски податоци, а особено препознавање на лице предизвикува зголемени ризици за правата на субјектите на лични податоци. Од клучно значење е прибегнувањето кон таквите технологии да биде со почитување на принципите на законитост, неопходност, пропорционалност и минимален обем на податоци, како што е утврдено во

ОРЗЛП. Со оглед на тоа што употребата на овие технологии може да се сфати како особено ефикасна, контролорите пред сè треба да го проценат влијанието врз основните права и слободи и да земат предвид помалку наметливи средства за да ја постигнат својата легитимна цел на обработката.

73. Да се квалификуваат како биометриски податоци, како што е дефинирано во ОРЗЛП, обработката на сирови податоци, како што се физичките, физиолошките или карактеристики на однесувањето на физичкото лице, мора да подразбира мерење на овие карактеристики. Бидејќи биометриските податоци се резултат на ваквите мерења, ОРЗЛП во својот член 4.14 наведува дека „*се лични податоци добиени како резултат на посебна техничка обработка во однос на физичките, физиолошките или карактеристики на однесувањето на физичко лице*“. Видео снимка од физичко лице не може сама по себе да се смета како биометриски податок според член 9, доколку не е посебно технички обработена со цел да се придонесе за идентификација на физичко лице.[16]

74. За да може да се смета како обработка на посебни категории на лични податоци (член 9), се бара биометриските податоци да бидат обработени „со цел на единствено идентификување на физичко лице”.

75. Да се сумира, во однос на член 4.14 и 9, мора да се земат предвид три критериуми:

- **Природа на личните податоци:** податоци што се однесуваат на физички, физиолошки или карактеристики на однесување на физичко лице,
- **Средства и начин на обработка**: податоци „како резултат на посебна техничка обработка“,
- **Цел на обработка:** податоците мора да се користат со цел на единствено идентификување на физичко лице.

76. Употребата на видео надзор, вклучително и функционалност на биометриското препознавање, инсталирана од приватни субјекти за свои цели (на пр. маркетинг, статистика, па дури и безбедност) во повеќето случаи ќе бара изречна согласност од сите субјекти на лични податоци (член 9(2)(а)), сепак, може да се примени и друг соодветен исклучок од член 9.

[16] Образложението 51 ја поддржува оваа анализа, изјавувајќи дека „*обработката на слики не треба систематски да се смета за обработка на посебните категории на лични податоци, бидејќи сликите се опфатени со дефиницијата за биометриски податоци само кога се обработуваат преку посебни технички средства кои овозможуваат единствена идентификација или проверка на автентичноста на физичко лице*“.

77. Пример: За подобрување на својата услуга, приватна компанија ги заменува точките за проверка на идентификација на патниците во рамките на аеродромот (оставање на багажот, качување на авионот) со системи за видео надзор кои користат техники за препознавање на лицето за да го проверат идентитетот на патниците што избрале да се согласат на таква постапка. Бидејќи обработката спаѓа во член 9, патниците, кои претходно ќе дадат изречна и информирана согласност, ќе треба да се пријават себеси, на пример, на автоматски терминал со цел да го создадат и да го регистрираат нивниот образец на лицето поврзан со нивната карта за влез во авионот и идентитет. Точките за проверка со препознавање на лицето треба да бидат јасно одвоени, на пр. системот мора да биде инсталиран во рамки на оградена платформа, така што биометриските обрасци на лицата што не се согласуваат да бидат сликани нема да бидат опфатени. Само патниците, кои претходно дале согласност и продолжиле со нивното пријавување, ќе ја користат ограденатa платформа опремена со биометрискиот систем.

Пример: Контролорот управува со пристапот до неговата зграда користејќи метод за препознавање на лицето. Луѓето можат да го користат овој начин на пристап само доколку претходно изречно дале информирана согласност (согласно член 9(2)(а)). Меѓутоа, со цел да се обезбеди дека никој кој претходно не ја дал својата согласност не е сликан, методот за препознавање на лицето треба да го активира самиот субјект на лични податоци, на пример со притискање на копче. За да се обезбеди законитоста на обработката, контролорот секогаш мора да понуди алтернативен начин за пристап до зградата, без биометриска обработка, како што се пропусници или клучеви.

78. Во овој вид на случаи, кога се создаваат биометриски обрасци, контролорите обезбедуваат дека откако ќе се добие резултат од совпаѓање или не совпаѓање, сите преодни обрасци направени во летот (со изречна и информирана согласност од субјектот на личните податоци) со цел да се споредат со оние создадени од субјектите на лични податоци за време на пријавувањето, веднаш и безбедно се бришат. Обрасците создадени за пријавувањето треба да се задржат само за реализација на целта на обработката и не треба да се чуваат или архивираат.

79. Меѓутоа, кога целта на обработката е, на пример, да се разликува една категорија на луѓе од друга, а не единствена идентификација на некое лице, обработката не спаѓа во член 9.

80. Пример: Сопственик на продавница би сакал да го прилагоди своето рекламирање засновано врз пол и возраст на клиентите што се опфатени со системот за видео надзор. Доколку тој систем не создава биометриски обрасци со цел единствено да ги идентификува лицата, туку само да ги открие тие физички карактеристики а, следствено на тоа, само да ја класифицира личноста, тогаш обработката не спаѓа во член 9.

81. Сепак, член 9 се применува ако контролорот чува биометриски податоци (најчесто преку обрасци што се создадени со вадење на клучни карактеристики од сировата форма на биометриските податоци (на пр. мерења на лице од слика)) со цел единствено да се

идентификува личност. Доколку контролорот сака да следи субјект на лични податоци како повторно влегува во просторија или влегува во друга просторија (на пример, со цел спроведување на прилагодено рекламирање), тогаш целта е единствено да се идентификува физичко лице, што значи дека операцијата од почеток спаѓа под член 9. Ова може да биде случај ако контролорот чува направени обрасци за да обезбеди дополнително прилагодено рекламирање на неколку билборди на различни локации во продавницата. Бидејќи системот користи физички карактеристики за да открие одредени лица кои се враќаат во опсегот на камерата (како посетители на трговски центар) и да ги следат, тоа би претставувало метод на биометриска идентификација бидејќи е насочен кон препознавање преку употреба на одредена техничка обработка.

Пример: Сопственик на продавница има инсталирано систем за препознавање на лицето во рамките на својата продавница со цел да го прилагоди своето рекламирање кон поединци. Контролорот на личните податоци треба да добие изречна и информирана согласност од сите субјекти на лични податоци пред да го користи овој биометриски систем и да достави прилагодена реклама. Системот ќе биде незаконски ако ги снима посетителите или минувачите кои не се согласиле за создавање на нивен биометриски образец, дури и ако нивниот образец е избришан во најкусиот можен рок. Всушност, овие привремени обрасци претставуваат биометриски податоци обработени со цел
82. единствено идентификување на лице кое можеби не сака да добие насочено рекламирање.

83. ЕОЗЛП забележува дека некои биометриски системи се инсталирани во неконтролирана средина[17], што значи дека системот подразбира снимање на лицата на кој било поединец што минува во опсегот на камерата при летот, вклучително и лица кои не се согласиле на биометрискиот уред, а со тоа создавање на биометриски обрасци. Овие обрасци се споредуваат со оние создадени од субјектите на лични податоци кои дале претходна согласност за време на процесот на пријавување (т.е. корисник на биометриски уред) со цел за контролорот на личните податоци да препознае дали лицето е корисник на биометриски уред или не. Во овој случај, системот често е креиран да ги дискриминира лицата што сака да ги препознае од база на податоци на оние коишто не се пријавени. Бидејќи целта е единствено идентификување на физички лица, исклучок според член 9(2) на ОРЗЛП е сè уште потребен за секој што е опфатен од камерата.

[17] Тоа значи дека биометрискиот уред се наоѓа на простор отворен за јавноста и е во состојба да работи на секој што поминува, наспроти биометриските системи во контролирани средини што можат да се користат само со одобрување на учество на лицето.

Пример: Хотелот користи видео надзор за автоматски да го предупреди менаџерот на хотелот дека многу важно лице пристигнало откако ќе се препознае лицето на гостинот. Овие ВИП лица претходно дале изречна согласност за употреба на препознавање на лицето пред да бидат евидентирани во базата на податоци основана за таа цел. Овие системи за обработка на биометриски податоци би биле незаконски, освен ако сите други гости кои се набљудувани (со цел да се идентификуваат ВИП лицата) не се согласиле на обработката според член 9(2)(а) ОРЗЛП.

Пример: Контролор инсталира систем за видео надзор со препознавање на лицето на влез на концертна сала со која управува. Контролорот мора да постави јасно раздвоени влезови; еден со биометриски систем и еден без (каде што наместо препознавање на лицето, на пример, се скенира билет). Влезовите опремени со биометриски уреди, мора да бидат инсталирани и достапни на начин што ќе го спречи системот да опфати биометриски обрасци на гледачи што не дале согласност.

84.

85. Конечно, кога се бара согласност според член 9 од ОРЗЛП, контролорот на личните податоци не го условува пристапот до неговите услуги до прифаќањето на биометриската обработка. Со други зборови и особено кога биометриската обработка се користи за проверка на автентичноста на физичкото лице, контролорот на личните податоци мора да понуди алтернативно решение кое не вклучува биометриска обработка - без ограничувања или дополнителни трошоци за субјектот на личните податоци. Ова алтернативно решение е исто така потребно за лицата кои не ги исполнуваат ограничувањата на биометрискиот уред (невозможно запишување или читање на биометриските податоци, состојба на инвалидитет што го отежнува користењето, итн.) а во очекување на недостапност на биометрискиот уред (т.е. како дефект на уредот), мора да се примени „резервно решение“ за да се обезбеди континуитет на предложената услуга, која сепак е ограничена на употреба во исклучителна ситуација.

5.2 Предложени мерки за намалување на ризиците при обработка на биометриски податоци

86. Во согласност со принципот на минимален обем на податоците, контролорите на личните податоци мора да обезбедат дека податоците извлечени од дигитална слика за да се изгради образец нема да бидат претерани и ќе ги содржат само потребните информации за одредена цел, со што ќе се избегне можна понатамошна обработка. Треба да се преземат мерки за да се гарантира дека обрасците не можат да се пренесат преку биометриските системи.

87. Идентификацијата и автентикацијата/верификацијата веројатно ќе бараат зачувување на образецот за употреба во подоцнежна споредба. Контролорот на личните податоци мора да ја земе предвид најсоодветната локација за зачувување на податоците. Во контролирана средина (ограничени ходници или контролни пунктови), обрасците се чуваат на поединечен уред што го чува корисникот и под негова/нејзина единствена контрола (во паметен телефон или лична карта) или - кога е потребно за конкретни цели и во присуство на објективни потреби - зачувани во централизирана база на податоци во криптирана форма со клуч/тајна единствено во рацете на лицето за да се спречи неовластен пристап до образецот или локацијата за чување на податоците. Доколку контролорот на личните податоци не може да избегне пристап до обрасците, тој мора да преземе соодветни чекори за да ја обезбеди безбедноста на зачуваните

лични податоци. Ова може да вклучува криптирање на образецот со помош на криптографски алгоритам.

88. Во секој случај, контролорот ги презема сите неопходни мерки на претпазливост за да ја зачува достапноста, интегритетот и доверливоста на обработените лични податоци. За таа цел, контролорот особено треба да ги преземе следниве мерки: да ги подели податоците на категории за време на преносот и чувањето, да ги чува биометриските обрасци и сирови податоци или податоци за идентитет на одделни бази на податоци, да ги криптира биометриските податоци, особено биометриските обрасци и да дефинира политика за криптирање и управување со клучевите, да интегрира организациска и техничка мерка за откривање измама, да поврзе код за интегритет со податоците (на пример потпис или криптографска хеш функција) и да забрани каков било надворешен пристап до биометриските податоци.

89. Покрај тоа, контролорите на лични податоци треба да продолжат со бришење на сирови податоци (слики на лица, говорни сигнали, одот, итн.) и да обезбедат ефективност на ова бришење. Навистина, сè додека биометриските обрасци произлегуваат од ваквите податоци, може да се земе предвид дека составувањето на базите на податоци може да претставува еднаква, па дури и поголема закана (затоа што не е секогаш лесно да се прочита биометриски образец без знаење за тоа како бил програмиран, додека пак сировите податоци секогаш ќе бидат составни елементи на било кој образец). Во случај контролорот на личните податоците да има потреба да ги чува таквите податоци, мора да се истражи методот за „додавање на врева“ (како што е воден печат), што ќе го оневозможи креирањето на образецот. Контролорот исто така мора да ги избрише биометриските податоци и обрасците во случај на неовластен пристап до терминалот за читање-споредба или серверот за чување и да го избрише секој податок што не е корисен за понатамошна обработка на крајот на животот на биометрискиот уред.

6 ПРАВА НА СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

90. Поради карактерот на обработката на личните податоци при користење на видео надзор, некои права на субјектот на лични податоци под ОРЗЛП нудат дополнително разјаснување. Меѓутоа, ова поглавје не е исцрпно, сите права според ОРЗЛП се применуваат за обработка на лични податоци преку видео надзор.

6.1 Право на пристап

91. Субјектот на личните податоци има право да добие потврда од контролорот дали се обработуваат или не неговите/нејзините лични податоци. За видео надзор, ова значи дека ако не се чуваат податоци или се пренесуваат на кој било начин, тогаш откако ќе помине моментот на набљудување во реално време, контролорот може само да ги даде информациите дека веќе не се обработуваат никакви лични податоци (покрај општите обврски за информации според член 13, видете *дел 7 - Обврски за транспарентност и информации*). Доколку сепак податоците сè уште се обработуваат во моментот на барањето (т.е. ако податоците се зачувани или континуирано се обработуваат на кој било друг начин), субјектот на личните податоците треба да добие пристап и информации во согласност со член 15.

92. Сепак, постојат голем број ограничувања што можат во некои случаи да се однесуваат во однос на правото на пристап.

- Членот 15(4) од ОРЗЛП, неповолно влијае врз правата на другите

93. Со оглед на тоа дека, неопределен број на субјекти на лични податоци може да биде снимен во иста секвенца на видео надзорот, прикажување на снимката тогаш ќе предизвика дополнителна обработка на лични податоци на други субјекти на лични податоци. Доколку субјектот на личните податоци сака да добие копија од материјалот (член 15(3)), тоа може неповолно да влијае врз правата и слободите на другите субјекти на лични податоци во материјалот. За да се спречи таа последица, контролорот треба да земе предвид дека поради наметливата природа на видео снимките контролорот не треба во некои случаи да дели видео снимки во кои што може да се идентификуваат други субјекти на лични податоци. Заштитата на правата на трети лица, од друга страна, не треба да се користи како изговор за да се спречат легитимни побарувања за пристап од страна на поединци, контролорот наместо тоа треба да спроведе технички мерки за исполнување на барањето за пристап (на пример, со уредување на слики како што е маскирање или криптирање).

- Член 11(2) од ОРЗЛП, контролорот не е во состојба да го идентификува субјектот на личните податоци

94. Доколку видео снимката не може да се пребарува за лични податоци, (т.е. контролорот веројатно ќе треба да помине низ голема количина на зачувани материјали за да го пронајде предметниот субјект на личните податоци) контролорот може да не е во можност да го идентификува субјектот на личните податоци.

95. Од тие причини субјектот на личните податоци треба (покрај тоа што се идентификувал себе си вклучително со документ за идентификација или лично) во своето барање до контролорот, да наведе кога - во разумна временска рамка во однос на количината на снимените субјекти на лични податоци - тој или таа влегол во набљудуваната област. Контролорот треба претходно да го извести субјектот на личните податоци за тоа кои информации се потребни за контролорот да го исполни барањето. Ако контролорот е во можност да докаже дека не е во состојба да го идентификува субјектот на личните податоци, контролорот мора соодветно да го информира субјектот на личните податоци, доколку е тоа можно.

Пример: Доколку субјект на лични податоци бара копија од неговите/нејзините лични податоци обработени преку видео надзор на влезот на трговски центар со 30 000 посетители на ден, субјектот на личните податоци треба да наведе кога тој или таа ја поминале контролираната област во временска рамка од приближно два часа. Ако контролорот сè уште го обработува материјалот, треба да се обезбеди копија на видео снимките. Доколку други субјекти на лични податоци можат да се идентификуваат во истиот материјал, тогаш тој дел од материјалот треба да биде анонимизиран (на пример со замаглување на копијата или на нејзините делови) пред да му се предаде копијата на субјектот на лични податоци што го поднел барањето.

96. Пример: Доколку контролорот автоматски ги брише сите снимки на пример во рок од 2 дена, субјектот на личните податоци може да добие пристап само до таа информација [дека материјалот е избришан] ако барањето е претставено на контролорот после тие 2 дена.

- Член 12 од ОРЗЛП, прекумерни барања

97. Во случај на прекумерно или очигледно неосновано барање од субјект на лични податоци, контролорот може да наплати разумна сума во согласност со член 12(5)(а) од ОРЗЛП, или да одбие да постапи по барањето (член 12(5)(б)) од ОРЗЛП. Контролорот треба да биде во можност да го докаже прекумерниот или очигледно неоснованиот карактер на барањето.

6.2 Право на бришење и право на приговор

6.2.1 Право на бришење („право да се биде заборавен“)

98. Доколку контролорот продолжи да обработува лични податоци преку набљудување во реално време (на пр. чување), субјектот на личните податоци може да побара бришење на личните податоци според член 17, ОРЗЛП.

99. На барање, контролорот е должен да ги избрише личните податоци без непотребно одложување, доколку се применува една од околностите наведени во член 17 (1), ОРЗЛП (а не се применува ниту еден исклучок наведен во член 17(3) од ОРЗЛП). Ова ја вклучува обврската да се избришат личните податоци кога веќе не се потребни за целта за која првично биле зачувани, или кога обработката е незаконска (видете исто така дел 8 за рокови на чување и обврска за бришење). Понатаму, во зависност од правната основа на обработката, личните податоци треба да се избришат:

- *за согласност* секогаш кога ќе се повлече согласноста (и нема друга правна основа за обработка)

- за легитимен интерес:

- секогаш кога субјектот на лични податоци остварува право на приговор (види *дел 6.2.2*) и не постојат преовладувачки неспорни легитимни основи за обработка, или
- во случај на директен маркетинг (вклучително и профилирање) секогаш кога субјектот на личните податоци има приговор на обработката.

100. Доколку контролорот ја објави видео снимката (на пр. јавен пренос или семрежно емитување 'streaming' преку интернет), треба да се преземат разумни чекори за да се информираат другите контролори (кои сега ги обработуваат личните податоци за кои станува збор) за барањето согласно член 17(2) ОРЗЛП. Разумните чекори треба да вклучуваат технички мерки, земајќи ја предвид достапната технологија и трошоците за имплементација. До можниот степен, контролорот треба да го извести - по бришење на личните податоци - секој на кого претходно му ги дале личните податоци, во согласност со член 19, ОРЗЛП.

101. Покрај обврската на контролорот да ги избрише личните податоци по барање на субјектот на личните податоци, контролорот е должен според општите принципи на ОРЗЛП да ги ограничи зачуваните лични податоци *(види дел 8)*.

102. За видео надзор вреди да се забележи дека на пр. со замаглување на сликата без ретроактивна можност за враќање на личните податоци што претходно биле содржани во сликата, личните податоци да се сметаат за избришани во согласност со ОРЗЛП.

Пример: Продавница има проблеми со вандализам особено во однос на нејзината надворешност и затоа користи видео надзор надвор од нејзиниот влез во директна врска со sидовите. Минувач бара да му се избришат неговите лични податоци во тој момент. Контролорот е должен да одговори на барањето без непотребно одложување и најдоцна во рок од еден месец. Бидејќи, засегнатите снимки повеќе не ја исполнуваат целта за која првично биле зачувани (не се случил вандализам во времето кога субјектот на личните податоците поминал), во моментот на барањето не постои легитимен интерес за чување на податоците што би ги надминале интересите на субјектот на личните податоци. Контролорот треба да ги избрише личните податоци.

103.

6.2.2 Право на приговор

104. За видео надзор врз основа на *легитимен интерес* (член 6(1)(ѓ) ОРЗЛП) или за потребата при вршење на *задача од јавен интерес* (член 6(1)(д) ОРЗЛП) субјектот на лични податоци има право - во секое време - на приговор, врз основа на поврзаност со неговата или нејзината посебна состојба, на обработката во согласност со член 21, ОРЗЛП. Освен ако контролорот не

покаже неспорни легитимни основи што ги надминуваат правата и интересите на субјектот на личните податоци, обработката на личните податоци на лицето што приговорило тогаш мора да престане. Контролорот треба да биде должен да одговори на барањата на субјектот на личните податоци без непотребно одложување и најдоцна во рок од еден месец.

105. Во контекст на видео надзор, овој приговор може да се даде или пред влегувањето, за време на, или по напуштањето на набљудуваната област. Во пракса, ова значи дека освен ако контролорот има неспорни легитимни основи, набљудувањето на областа каде што може да се идентификуваат физичките лица е законско само ако

(1) контролорот е во состојба веднаш да ја спречи камерата да обработува лични податоци кога тоа се бара, или

(2) областа на набљудување е ограничена на таков начин, така што контролорот може да обезбеди одобрение од субјектот на личните податоци пред да влезе во областа и тоа не е област каде што субјектот на лични податоци како граѓанин има право на пристап.

106. При користење на видео надзор за целите на директен маркетинг, субјектот на личните податоци има право на приговор на обработката на основа на дискреција, бидејќи правото на приговор е апсолутно во тој контекст (член 21(2) и (3) ОРЗЛП).

Пример: Една компанија доживува тешкотии со нарушувања на безбедноста на нивниот јавен влез и користи видео надзор заради легитимен интерес, со цел да ги фати тие што незаконски влегуваат. Посетителот се спротивставува на обработката на неговите или нејзините лични податоци преку системот за видео надзор врз основа на поврзаност со неговата или нејзината особена состојба. Компанијата сепак во овој случај го отфрла барањето со образложение дека снимките се потребни заради тековна внатрешна истрага, а со тоа имаат неспорни легитимни основи да продолжат со обработката на личните податоци.

107.

7 Обврски за транспарентност и информации[18]

108. Веќе долго време во суштината на европскиот закон за заштита на личните податоците е дека субјектите на личните податоци треба да бидат свесни за фактот дека видео надзорот е во функција. Тие треба да бидат детално информирани за местата кои се снимаат.[19] Според ОРЗЛП, општата обврска за транспарентност и информации се поставени во член 12, ОРЗЛП и

[18] Може да се применат конкретни барања во националното законодавство.

[19] Работна група 29, Мислење 4/2004 за обработка на лични податоци преку видео надзор (ВП89).

сл. Во „Насоките за транспарентност согласно Регулативата 2016/679 (WP260)“ на Работната група 29, кои беа одобрени од ЕОЗЛП на 25.05.2018 година, се предвидуваат дополнителни детали. Во согласност со ВП260 параграф 26, членот 13 од ОРЗЛП е тој што се применува доколку личните податоци се собрани „од субјект на лични податоци преку набљудување (на пр. користејќи уреди за автоматско снимање на податоци или софтвер за снимање на податоци, како што се камери)“.

109. Со оглед на обемот на информации, што е потребно да се достават до субјектот на личните податоци, контролорите на личните податоци може да проследат со слоевит пристап, доколку се одлучат да користат комбинација на методи за да обезбедат транспарентност (ВП260, пара. 35; ВП89, стр. 22). Во однос на видео надзорот, најважните информации треба да бидат прикажани на самиот знак за предупредување (првиот слој), додека понатамошните задолжителни детали може да бидат обезбедени со други средства (втор слој).

7.1 Информации за првиот слој (знак за предупредување)

110. Првиот слој се однесува на почетниот начин на кој контролорот прво доаѓа во допир со субјектот на личните податоци. Во оваа фаза, контролорите можат да користат знак за предупредување што ги прикажува релевантните информации. Прикажаните информации можат да бидат дадени во комбинација со икона со цел да се даде, на лесно видлив, разбирлив и јасно читлив начин, целисходен преглед на наменетата обработка (член 12(7) ОРЗЛП). Форматот на информациите треба да се прилагоди на индивидуалната локација (ВП89 стр. 22).

7.1.1 Поставување на знакот за предупредување

111. Информациите треба да се постават на разумно растојание од набљудуваните места (ВП 89, стр. 22) на таков начин што субјектот на лични податоци може лесно да ги препознае околностите на надзорот пред да влезе во набљудуваната област (приближно на ниво на окото). Не е неопходно да се прецизира точната локација на опремата за надзор сè додека нема сомнеж за тоа кои области се предмет на набљудување и контекстот на надзорот треба да се разјасни недвосмислено (ВП 89, стр. 22). Субјектот на личните податоци мора да биде во можност да процени која област е снимана од камера, така што тој или таа можат да го одбегнат надзорот или да го прилагодат своето однесување доколку е потребно.

7.1.2 Содржина на прв слој

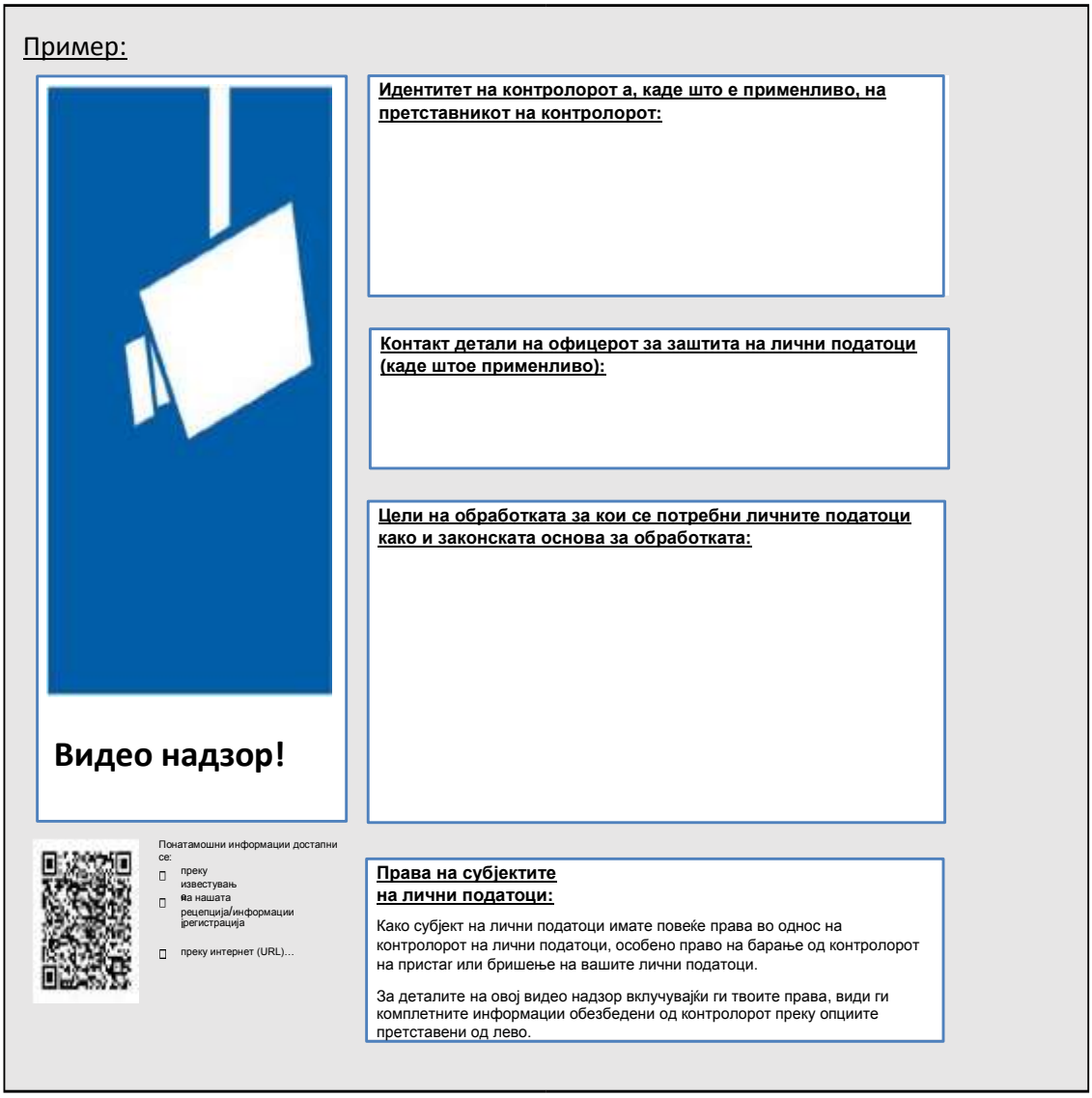
112. Информациите од првиот слој (знакот за предупредување) генерално треба да ги пренесат најважните информации, на пр. детали за целите на обработката, идентитетот на контролорот и постоењето на правата на субјектот на личните податоци, заедно со информации за најголемите влијанија од обработката.[20] Ова може да вклучува, на пример, легитимни интереси од страна на контролорот (или трето лице) и детали за контакт на офицерот за заштита на податоците (доколку е применливо). Исто така, треба да упатува кон подеталниот втор слој на информации и каде и како да ги пронајдеме.

113. Покрај тоа, знакот треба да ја содржи и секоја информација која што може да го изненади субјектот на личните податоци (РГ260, стр. 38). На пример, тоа може да биде пренесување на трети страни, особено ако се наоѓаат надвор од ЕУ и периодот на чување. Доколку оваа информација не е наведена, субјектот на личните податоци мора да биде во можност да верува дека постои само набљудување во живо (без никакво снимање на податоци или пренесување на трети страни).

[20] Види ВП260, параграф. 38

114.

Пример:



7.2 Информации од втор слој

115. Информациите од вториот слој мора исто така да бидат овозможени на место кое е лесно достапно за субјектот на лични податоци, на пример како комплетен информативен лист достапен на централна локација (на пр. биро за информации, рецепција или каса) или прикажан на лесно достапен постер. Како што споменавме погоре, знакот за предупредување од првиот слој треба јасно да упатува кон информациите за вториот слој. Покрај тоа, најдобро е ако информациите од првиот слој упатуваат кон дигитален извор (на пр. QR-код или адреса на веб-страница) на вториот слој. Сепак, информациите исто така треба да бидат лесно достапни и не-дигитално. Во секој случај, мора да биде можно да се пристапи до информациите од вториот слој без да се влезе во набљудуваната област. Ова може да се постигне на пример со врска (линк) или кое било друго соодветно средство како телефонски број што може да се повика. Мора да ги содржи сите други информации што се задолжителни според член 13, ОРЗЛП.

116. Покрај овие опции, а во исто време и да ги направи поделотворни, ЕОЗЛП промовира употреба на технолошки средства за обезбедување на информации за субјектите на лични податоци. Ова може да вклучува на пример; гео-локализирање на камерите и вклучување на информации во

апликации за мапи или веб-страници за да можат физичките лица, од една страна, лесно да ги идентификуваат и прецизираат видео изворите поврзани со остварувањето на нивните права, а од друга страна, да добијат подетални информации за операцијата за обработка.

117. Пример: Сопственик на дуќан врши набљудување на неговата продавница. За да се усогласи со член 13, доволно е да постави знак за предупредување на лесно видлива точка на влезот од неговата продавница, кој ги содржи информации од првиот слој. Покрај тоа, тој треба да обезбеди информативен лист што содржи информации од вториот слој на касата или која било друга централна и лесно достапна локација во неговата продавница.

8 Рокови на чување и обврска за бришење

118. Личните податоци не можат да се чуваат подолго од она што е потребно за целите за кои се обработуваат личните податоци (член 5(1)(в) и (д) од ОРЗЛП). Во некои земји-членки, може да има конкретни одредби за рокови на чување во однос на видео надзорот, во согласност со член 6(2) од ОРЗЛП.

119. Без оглед дали е неопходно личните податоци да се чуваат или не, тоа треба да биде контролирано во тесна временска рамка. Генерално, легитимни цели за видео надзор најчесто се заштита на имот или зачувување на докази. Вообичаено штетите што се случиле можат да се препознаат во рок од еден или два дена. Имајќи ги предвид принципите на член 5(1)(в) и (д) од ОРЗЛП, имено минимален обем на податоци и ограничување на чувањето, личните податоци треба во повеќето случаи (на пр. за цел на откривање на вандализам) да бидат избришани, идеално автоматски, после неколку дена. Колку е подолг рокот на чување (особено ако е подолг од 72 часа), мора да се обезбедат повеќе аргументи за легитимноста на целта и за потребата од чување. Доколку контролорот користи видео надзор не само за набљудување на неговите простории, туку има намера и да ги чува податоците, контролорот мора да увери дека чувањето е всушност неопходно за да се постигне целта. Доколку е така, рокот на чување треба да биде јасно дефиниран и поединечно да се постави за секоја одредена намена. Одговорност на контролорот е да го дефинира рокот на задржување во согласност со принципите на неопходност и пропорционалност и да прикаже усогласеност со одредбите на ОРЗЛП.

Пример: Сопственик на мала продавница вообичаено ќе примети каков било вандализам уште истиот ден. Како последица на тоа, доволен е редовен рок на чување од 24 часа. Затворените викенди или празници, сепак, може да бидат причини за подолг рок на чување. Доколку се открие штета, можеби ќе треба да ги чува и видео снимките на подолг период со цел да преземе правно дејство против сторителот.

120.

9 ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

121. Како што е наведено во член 32(1) од ОРЗЛП, обработката на личните податоци преку видео надзор не само што мора да биде законски дозволена, туку контролорите и обработувачите треба, исто така, да обезбедат соодветно ниво на безбедност. Имплементираните **организациски и технички мерки** мора да бидат **пропорционални на ризиците за правата и слободите на физичките лица**, како резултат на случајно или незаконско уништување, загуба, промена, неовластено откривање или пристап до податоци од видео надзор. Според член 24 и 25 од ОРЗЛП, контролорите треба, исто така, да спроведат технички и организациски мерки со цел да ги заштитат сите принципи за заштита на личните податоци при обработката и да воспостават средства за субјектите на лични податоци да ги остварат своите права, како што е дефинирано во членовите 15 – 22 од ОРЗЛП. Контролорите на лични податоци треба да усвојат внатрешна рамка и политики што ја обезбедуваат оваа имплементација и во моментот на утврдување на средствата за обработка и во моментот на самата обработка, вклучително и извршувањето на проценките на влијанието врз заштитата на податоците кога е тоа потребно.

9.1 Преглед на системот за видео надзор

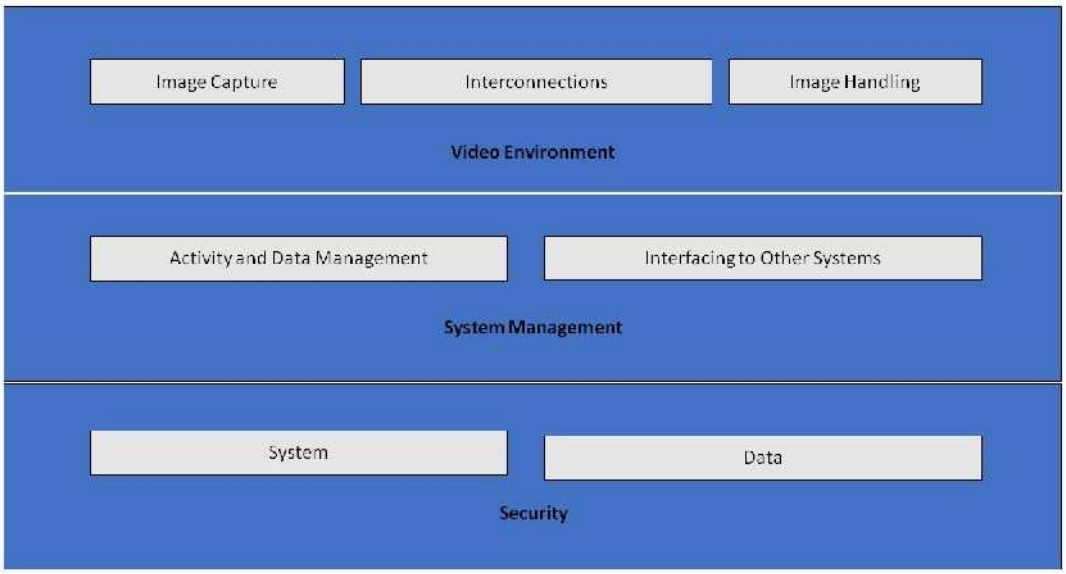
Системот за видео надзор – СВН (VSS)[21] се состои од аналогни и дигитални уреди, како и софтвер со цел за снимање на слики од сцена, ракување со слики и нивно прикажување на оператор. Неговите компоненти се групирани во следниве категории:

- Видео опкружување: снимање на слики, интерконекции и ракување со слики
    - целта на снимање на слика е создавање на слика од реалниот свет во таков формат што може да се користи од останатиот дел од системот
    - интерконекциите го опишуваат целиот пренос на податоци во рамките на видео опкружувањето, т.е. врски и комуникации. Примери за врски се кабли, дигитални мрежи и безжични преноси. Комуникациите ги опишуваат сите сигнали за видео и за контролни податоци, кои можат да бидат дигитални или аналогни
    - ракувањето со слики вклучува анализа, чување и презентација на слика или низа слики
- Од гледна точка на управување со системот, СВЗ ги има следниве логички функции:
    - управување со податоци и управување со активности, што вклучува ракување со командите на операторот и активности генерирани од системот (процедури за тревога, оператори за тревога)
    - интерфејси со други системи може да вклучуваат поврзување со друга безбедност (контрола на пристап, аларм за пожар) и не-безбедносни системи (системи за управување со згради, автоматско препознавање на регистарски таблички)

[21] ОРЗЛП не дава дефиниција за тоа, технички опис може да се најде на пример во EN 62676-1-1:2014 Системи за видео надзор за употреба во безбедносни апликации - Дел 1-1: Услови за видео систем.

- Безбедноста на СВН се состои од доверливост на системот и податоците, интегритетот и достапноста
    - безбедноста на системот вклучува физичка безбедност на сите компоненти на системот и контролата на пристапот до СВН
    - безбедност на податоците вклучува спречување на загуба или манипулација со податоците

122.



Фигура 1- систем за видео надзор

9.2 Техничка и интегрирана заштита на личните податоци

123. Како што е наведено во член 25 од ОРЗЛП, контролорите треба да спроведат соодветни технички и организациски мерки за заштита на личните податоци веднаш штом почнат да планираат за видео надзор, пред да започнат со собирање и обработка на видео снимки. Овие принципи ја нагласуваат потребата за вградени технологии за подобрување на приватноста, стандардни поставки што ја минимизираат обработката на личните податоци и обезбедувањето на потребните алатки кои овозможуваат најголема можна заштита на личните податоци[22].

124. Контролорите треба да вградуваат заштитни мерки за заштита на личните податоци и приватноста не само во спецификациите за дизајнот на технологијата, туку и во организациските практики. Кога станува збор за организациските практики, контролорот треба да донесе соодветна рамка за управување, да воспоставува и спроведува политики и процедури поврзани со видео надзор. Од техничка гледна точка, спецификацијата и дизајнот на системот треба да содржи барања за обработка на лични податоци во согласност со принципите наведени во член 5 од ОРЗЛП (законитост на обработката, цел и ограничување на

[22] Мислење на ВП 168 за „Иднината на приватноста“, заеднички придонес на Работната група 29 за заштита на личните податоци и Работната група за полиција и правда на Консултацијата на Европската комисија за правната рамка за основното право на заштита на личните податоци (донесено на 01 декември 2009 година), https://ec.europa.eu/justice/Article29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

податоците, минимален обем на податоците како правило во смисла на член 25(2) од ОРЗЛП, интегритет и доверливост, одговорност итн.). Доколку контролорот планира да набави комерцијален систем за видео надзор, контролорот треба да ги вклучи овие барања во спецификацијата за набавка. Контролорот треба да обезбеди усогласеност со овие барања на начин со кој што ќе ги примени на сите компоненти на системот и на сите податоци обработени од него, во текот на целиот животен циклус.

9.3 Конкретни примери на релевантни мерки

125. Повеќето мерки што можат да се користат за обезбедување на видео надзор, особено кога се користи дигитална опрема и софтвер, нема да се разликуваат од оние што се користат во другите ИТ системи. Сепак, без оглед на избраното решение, контролорот мора соодветно да ги заштити сите компоненти на системот за видео надзор и личните податоци во сите фази, т.е. за време на чувањето (податоци во мирување), преносот (податоци во пренос) и обработката (податоци во употреба). За ова, неопходно е контролорите и обработувачите да комбинираат организациски и технички мерки.

126. При изборот на технички решенија, контролорот треба да земе предвид технологии кои се во прилог на приватноста, бидејќи тие, исто така, ја зајакнуваат безбедноста. Примери на такви технологии се системи кои овозможуваат маскирање или замаглување на области кои не се релевантни за надзор, или отстранување на слики од трети лица, при давање на видео снимките на субјекти на лични податоци.[23] Од друга страна, избраните решенија не треба да предвидуваат функции што не се потребни (на пр., неограничено движење на камерите, можност за зумирање, радио пренесување, анализи и аудио снимки). Функциите што се обезбедени, но не и неопходни, мора да бидат деактивирани.

127. Постои обемна литература на оваа тема, вклучувајќи ги меѓународните стандарди и техничките спецификации за физичката безбедност на мултимедијалните системи[24] и безбедноста на општите ИТ системи[25]. Затоа, овој дел дава само преглед на високо ниво на оваа тема.

9.3.1 Организациски мерки

128. Освен од потребата за потенцијална ПВЗЛП (види дел 10), контролорите треба да ги земат предвид следниве теми кога креираат свои политики и процедури за видео надзор:

- Кој е одговорен за управување и работење на системот за видео надзор
- Цел и опсег на проектот за видео надзор
- Соодветна и забранета употреба (каде и кога е дозволен видео надзор и каде и кога не е; на пр. употреба на скриени камери и аудио покрај видео снимањето [26])
- Мерки за транспарентност, како што е наведено во делот 7 (Обврски за транспарентност и информации)

[23] Употребата на таквите технологии може да биде дури и задолжителна во некои случаи заради усогласување со член 5(1)(в). Во секој случај, тие можат да послужат како примери за најдобри практики.

[24] IEC TS 62045 — Мултимедијална безбедност - Насока за заштита на приватноста на опрема и системи во и надвор од употреба

[25] ISO/IEC 27000 — Серија на системи за управување со безбедност на информации

[26] Ова може да зависи од националните закони и секторските прописи

- Како се снима видеото и за кое времетраење, вклучително и архивско чување на видео записи поврзани со безбедносни инциденти
- Кој мора да помине соодветна обука и кога
- Кој има пристап до видео записи и за какви цели
- Оперативни постапки (на пр. од кого и од каде се следи видео надзорот, што да се прави во случај на инцидент со нарушување на безбедноста на личните податоци)
- Кои постапки треба да ги следат надворешните страни за да побараат видео записи и постапки за негирање или потврдување на такви барања
- Постапки за набавка, инсталација и одржување на СВН
- Постапки за управување со инциденти и за опоравување.

9.3.2 Технички мерки

129. **Безбедност на системот** значи **физичка безбедност** на сите компоненти на системот, интегритет на системот, т.е. **заштита и отпорност од намерно и ненамерно мешање во нејзините нормални операции** и **контрола на пристап**. Безбедност на личните податоци значи **доверливост** (податоците се достапни само за оние на кои им е дозволен пристап), **интегритет** (спречување на губење на податоци или манипулација) и **достапност** (до податоците може да се пристапи кога тоа се бара).

130. **Физичката безбедност** е значаен дел од заштитата на личните податоци и првата линија на одбрана, затоа што ја штити опремата на СВН од кражби, вандализам, природна непогода, вештачки катастрофи и случајно оштетување (на пр., од електрични бранови, екстремни температури и истурено кафе). Во случај на аналогни системи, физичката безбедност ја игра главната улога во нивната заштита.

131. **Безбедност на системот и на податоците**, т.е. заштита од намерно и ненамерно мешање во нејзините нормални операции може да вклучуваат:

- Заштита на целата инфраструктура на СВН (вклучително и далечински камери, каблирање и напојување на струја) од физичко нарушување и кражба
- Заштита на пренесување на снимки со комуникациски канали заштитени од пресретнување
- Криптирање на лични податоци
- Употреба на хардверски и софтверски решенија, како што се „заштитни ѕидови“, антивируси или системи за откривање на упад против кибер напади
- Откривање на дефекти на компонентите, софтверот и интерконекциите
- Средства за враќање на достапноста и пристапот до системот во случај на физички или технички инцидент.

Контрола на пристап гарантира дека само овластени лица можат да пристапат до системот и личните податоци, додека останатите се спречени да го прават тоа. Мерките што ја поддржуваат физичката и логичката контрола на пристап вклучуваат:

- Осигурување дека сите простории каде што се врши надгледување на видео надзорот и се чуваат видео снимки се обезбедени од незаштитен пристап од трети лица
- Позиционирање на мониторите на таков начин (особено кога се во отворени области, како биро за прием), така што само овластените оператори можат да ги видат
- Постапките за доделување, промена и одземање на физички и логичен пристап се дефинирани и спроведени.
- Имплементирани се методи и средства за автентикација на корисниците и за овластување, вклучително на пр. должината на лозинките и фреквенција на промената.
- Активностите што ги извршува корисникот (како на системот, така и на податоците) се евидентираат и редовно се прегледуваат.
- Следењето и откривањето на дефектите на пристапот се врши континуирано и идентификуваните слабости се решаваат што е можно поскоро.

10 ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

132. Според член 35(1) од ОРЗЛП контролорите се должни да спроведат проценки на влијанието врз заштитата на личните податоци (ПВЗЛП) кога вид на обработка на личните податоци може да резултира со голем ризик врз правата и слободите на физичките лица. Членот 35(3)(в) од ОРЗЛП наложува дека контролорите треба да вршат проценки на влијанието врз заштитата на личните податоци, доколку обработката претставува систематско набљудување на јавно достапно подрачје во голем обем. Покрај тоа, според член 35(3)(б) од ОРЗЛП, проценка на влијанието врз заштитата на податоците е исто така потребна кога контролорот има намера да обработува посебни категории на лични податоци во голем обем.

133. Насоките за проценка на влијанието врз заштитата на личните податоци[27] дава понатамошни совети и подетални примери релевантни за видео надзор (на пр., во врска со „употреба на систем на камери за набљудување на однесувањето при возење на автопатите“). Членот 35(4) од ОРЗЛП бара секој надзорен орган да објави список на видот на операциите на обработка што се предмет на задолжителна ПВЗЛП во рамките на нивната земја. Овие списоци обично се наоѓаат на веб-страниците на органите. Со оглед на вообичаените цели на видео надзор (заштита на луѓе и имот, откривање, спречување и контрола на прекршоци, собирање докази и биометриска идентификација на осомничени), разумно е да се претпостави дека за многу случаи на видео надзор ќе биде потребна ПВЗЛП. Затоа, контролорите на лични податоци треба внимателно да се консултираат со овие документи за да утврдат дали е потребна таква

[27] Насоки за проценка на влијанието врз заштитата на личните податоци (ПВЗЛП) и утврдување дали обработката е „веројатно да резултира со висок ризик“ за целите на Регулативата 2016/679, wp248rev.01, http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236

проценка и доколку е потребно да се спроведе. Исходот од извршената ПВЗЛП треба да го одреди изборот на контролорот за спроведените мерки за заштита на личние податоци.

134. Исто така, важно е да се напомене дека ако резултатите од ПВЗЛП посочат дека обработката би резултирала со големи ризици и покрај безбедносните мерки што се планирани од контролорот, тогаш ќе биде неопходно да се консултира со релевантниот надзорен орган пред обработката. Детали за претходните консултации може да се најдат во член 36.

За Европскиот одбор за заштита на личните податоци

Претседателот

(Андреа Јелинек)