

Прирачник

за заштита на личните податоци при
вршење видео надзор



Дирекција за заштита на
личните податоци



Подршка на Дирекцијата за заштита на личните
податоци

Проектот е финансиран од Европската унија



www.privacy.mk





Проектот е имплементиран Human Dynamics во соработка со :

IPS Institute

AlmavivA S.p.A.

Czech Office for Personal Data Protection OPDP

Privacy International

“This publication has been produced with the assistance of the European Union. The contents of this publication are sole responsibility of the Directorate for Personal Data Protection and can in no way be taken to reflect the views of the European Union.”

“Оваа публикација е изготвена со помош на Европска унија. Содржината на оваа публикација е единствена одговорност на Дирекцијата за заштита на личните податоци и на никаков начин не ги рефлектира гледиштата на Европската унија .”

“Ky publikim është përgaditur me ndihmën e Unionit Evropian. Përmbajtja e këtij publikimi është përgjegjësi vetëm e Drejtoria për Mbrojtjen e të Dhënave Personale dhe në asnjë mënyrë nuk reflekton opinionin e Unionit Evropian.”

За издавачот:

Димитар Ѓеорѓиевски

Издавач:

Дирекција за заштита на личните податоци

Печати :

МПЦ-ОА-Митрополија Скопска печатница "Синај"

Печатењето на публикацијата финансиски е поддржано од:

Проектот „Поддршка на Дирекцијата за заштита на личните податоци“ финансирано од Европската Унија

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738.071.1(497.7)"2012/2016"

Прирачник за заштита на личните податоци при вршење на видео надзор:
Дирекција за заштита на личните податоци, 2012. - 18 стр. :
табели ; 19 см

ISBN 978-608-4682-01-1

а) Заштита на лични податоци - Стратегија - Македонија - 2012-2016
COBISS.MK-ID 89777674

I. ВОВЕД	2
ЗА КОГО Е НАМЕНЕТ ОВОЈ ПРИРАЧНИК?	6
II. ДЕФИНИЦИИ	7
III. ОПШТИ ПРИНЦИПИ ЗА ОБРАБОТКА	8
<i>ПРАВО НА ГРАЃАНИТЕ ДА БИДАТ ИНФОРМИРАНИ</i>	<i>9</i>
<i>ПОДАТОЦИТЕ МОРА ДА БИДАТ ЦЕЛОСНИ, ТОЧНИ И АЖУРИРАНИ</i>	<i>10</i>
<i>ИНФОРМАЦИИ ВО СЛУЧАЈ НА ОТКРИВАЊЕ</i>	<i>10</i>
<i>САМО ОВЛАСТЕНИ ЛИЦА ИМААТ ПРАВО НА ПРИСТАП</i>	<i>11</i>
IV. ВРШЕЊЕ НА ВИДЕО НАДЗОР НА РАБОТНОТО МЕСТО	12
V. ОСТВАРУВАЊЕ НА ПРАВАТА НА СУБЈЕКТОТ (ГРАЃАНИНОТ)	13
VII. ДИРЕКЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ	15
<i>Како да поднесете барање за заштита на личните податоци?</i>	<i>16</i>

I. ВОВЕД

Овој прирачник ги поставува основните начела и дава насоки за ефикасна заштита на приватноста на граѓаните во однос на обработката на нивните личните податоци преку вршењето на видео надзор во согласност со Законот за заштита на личните податоци (понатаму: ЗЗЛП). Видео надзорот е дел од различни системи кои што следат неколку области на човековите активности – сообраќајот на патиштата, движењето на улиците, банките, болниците, контрола на вработените, контрола на безбедноста со цел спречување на грабежи и во многу други области и случаи. За време на овој мониторинг/следење голема е веројатноста дека ќе постои и обработка на лични податоци.

Која е целта на овој прирачник?

Целта на овој прирачник е да покаже дека видео надзорот е само еден дел од вршењето надзор врз општеството. Постојат и неколку други техники за следење и профилирање на поединците. Главниот интерес на органите за заштита на личните податоци е да се фокусираат на надзорот над поединците врз основа на системот со камери. Во модерното општество употребата на компјутерски - базираниот систем и комуникациски технологии дозволува пристап до приватни и забранети простори.



Нивото на вршење на надзор над јавните простори/површини се зголеми нагло во последните 20 години, но и понатаму нивото продолжува да се зголемува. Дигитално вршење на видео надзор значи дека системот овозможува да се соберат податоци за поединецот и да се пренесат на било кое место за натамошна обработка. Модерните системи за вршење на надзор користат мрежни и дигитални камери – камерата е поврзана на интернет, компјутер, телекомуникациска опрема, RFID, систем за препознавање на ликови и слично. Овој пример покажува дека е неопходно да се информира пошироката јавност за можностите на модерните системи за надзор како и за ризиците кон приватноста на граѓаните.

Камера инсталирана на зграда

Заштита на приватноста и личните податоци значи заштита на правото на поединецот да врши контрола за начинот како се собираат, користат, чуваат или пренесуваат неговите лични податоци. Заштита на приватноста, исто така, подразбира и информациска безбедност – заштита на тајноста, интегритетот и достапноста на личните податоци. За да се смета за безбеден во однос на приватноста, системот за идентификација мора да биде дизајниран да ги задоволи двата параметри.

Видео надзорот често се користи за различни цели во денешното општество. Многу често за целта на вршењето видео надзор се наведува јавната и индивидуалната безбедност, борбата против криминалот, превенцијата на кражби итн. Но, некогаш наведената цел и вистинската причина за вршење на видео надзор се различни, видео надзорот се користи единствено за следење на поединци, надзор над приватните активности на поединецот, вршење мониторинг на ефикасноста на работата на вработените итн. Многу често наведената цел/причина не се исполнува и целта на вршење на видео надзорот е различна од онаа за која е известен органот за заштита на личните податоци.

Еден од најголемите проблеми при инсталација на систем за вршење на видео надзор е тоа дека **поединците/** граѓаните не се известени за воведувањето на системот или пак за целта поради која се воведува. Како и да е, сите предност на видео надзорот наметнуваат нови проблеми на кои треба да им се обрати внимание – пр. кој е контролорот кој ги собира личните податоци, кој е одговорен за точноста и безбедноста на податоците кога во системот имаат пристап и други субјекти, кои се ризиците кои се наметнуваат врз приватниот живот на поединците итн.



Видео надзор на сообраќајот



Видео надзорот врши мониторинг на движењето околу станбените објекти

Правна позадина

Секој кој има намера да инсталира систем за вршење на видео надзор мора да биде свесен дека начинот на вршење на видео надзор е регулиран со одредбите на ЗЗЛП (членовите 9-а, 9-б и 9-в се однесуваат за вршење на видео надзор).

Институцијата која врши видео надзор е обврзана да истакне Известување за вршење на видео надзорот. Известувањето мора да биде јасно, видливо и истакнато на начин што овозможува секој поединец да биде запознаен дека на одредениот простор или објект се врши видео надзор.

Со цел да се изврши унификација на образецот на Известувањето, Дирекцијата за заштита на личните податоци (ДЗЛП) изработи образец кој ги исполнува законските барања во поглед на информациите кој истиот треба да ги содржи. Целта на ова решение е да се развие пракса на користење на унифицирано Известување за вршење на видео надзор кое ќе биде лесно препознатливо за сите граѓани .



Видео надзор може да се врши единствено на простор кој е неопходен за исполнување на целта поради која се врши видео надзор.

На пр. доколку целта за вршење на видео надзор е единствено за контрола на влезот и излезот од службените и деловните простории, тогаш е дозволено поставување на камери и снимање единствено на влезовите и излезите на објектот. Поставување на камери во внатрешноста на целиот објект врз основа на оваа цел не е дозволено.

Снимките кои се направени преку вршењето на видео надзорот може да се чуваат до исполнување на целта заради кој е поставен видео надзорот, но не повеќе од 30 дена, освен ако со друг закон не е предвиден подолг рок.

На пр. доколку се врши видео надзор за цел на заштита на сопственоста и имотот, снимките од видео надзорот се чуваат 30 дена и потоа истите се уништуваат. Но, во случај кога настанала некаква штета врз сопственоста или е извршено некое противправно дело врз имотот. во тој случај снимките од видео надзорот може да се чуваат и подолго од 30 дена се до исполнување на целта, односно откривање на сторителот на штетата или извршителот на противправното дејствие врз сопственоста.

Видео надзорот може да се врши во службените и деловните простории ако е неопходно за:

- ➔ заштита на животот и здравјето на луѓето
- ➔ заштита на сопственоста
- ➔ заштита на животот и здравјето на вработените поради природата на работата или
- ➔ обезбедување контрола над влегувањето и излегувањето од службените и деловните простории.

Институцијата е должна да ги извести вработените за вршењето на видео надзор во службените и деловните простории.

ЗАБРАНЕТО Е да се врши видео надзор во гардероби, соблекувални, тоалети, лифтови и други слични простории.

За вршење на видео надзор во едностанбени и повеќестанбени објекти задолжително е потребна писмена изјава за согласност од сите сопственици, односно закупци на становите. Тоа значи дека доколку живеете во повеќестанбена зграда и еден од вашите соседи не се согласи за вршење на видео надзорот, тогаш истиот не е дозволен. Во секој случај снимањето на влезовите на индивидуалните станови е забрането.

За кого е наменет овој прирачник?

Овој прирачник е наменет за контролорите и обработувачите на збирки на лични податоци¹ и било кои компании, институции и организации кои имаат инсталирано видео надзор и преку тоа вршат обработка на лични податоци. Меѓутоа, исто така, граѓаните и пошироката јавност кои се субјекти на видео надзорот имаат право да бидат информирани за техничките и правните услови за видео надзорот можат да најдат бројни информации кои се однесуваат на исполнување на нивните права утврдени со ЗЗЛП. Се надеваме дека овој прирачник ќе биде корисен и за офицерите за заштита на личните податоци².



Примена на прирачникот

Овој прирачник може да се применува за секој систем на видео надзор кој се користи од страна на јавните или приватните правни лица со кој се врши снимање на физички лица и снимките се зачувуваат со користење на технологија на снимање. Овој прирачник не се применува на:

- видео-телефонски разговори на видео-конференции;
- правење слики за артистички и новинарски цели (на пр. снимање на филм, емитување на важни настани итн.);
- снимање или емитување на настани како конференции, семинари, состаноци, документирање на обуки и тренинзи и слични активности.

Под опсегот на овој прирачник исто така, спаѓа и користењето на други електронски уреди или системи, фиксни или мобилни, ако имаат можност да прават записи/слики (на пример преносливи видео-камери, фотоапарати, веб камери, инфрацрвени камери итн.)



¹ Дефиницијата за контролор и обработувач на збирка на лични податоци е дадена во член 2 ставови 5 и 6 од ЗЗЛП

² Види член 26-а од ЗЗЛП

Како е дефиниран видео надзорот?

Видео надзорот се дефинира како вршење на мониторинг на одреден простор, настан, активност или личност преку електронски уред или систем за визуелен мониторинг. Технологијата за системите на видео надзор се однесува на камери кои ги монтираат или снимаат активностите на поединците, вклучувајќи но, не лимитирано на: видео камери, CCTV (систем за видео надзор со затворено коло на телевизиски камери) дигитални камери итн. Овие уреди можат да се користат за да се направат записи, вклучувајќи видеоленти, фотографии или дигитални слики. Видео надзорот може да се користи од страна на јавните власти на јавни простори за спречување на кривични дела како и од приватните лица за различни причини.

III. ОПШТИ ПРИНЦИПИ ЗА ПРАВИЧНА ОБРАБОТКА

Кои се основните права на граѓаните?

Мора се потенцира дека системите за вршење на видео надзор се справуваат со лични податоци на поединци, и други човекови права, вклучувајќи го правото на приватност кои треба да бидат земени во предвид. Поради тоа, сите начела за заштита на личните податоци ќе се применуваат за овие системи. Видео надзорот на јавните места исто така, го ограничува слободното движење на поединците. Правото на слободно движење е утврдено со Дополнителен протокол на Европската конвенција за човекови права. Оваа слобода не се однесува само на правото на слободно движење во физички простори туку и на правото постојно движење без да се биде следен. Заштита на приватноста исто така вклучува и безбедност на податоците – заштита на доверливоста, интегритетот и достапноста на личните податоци.

Контролорите и обработувачите мора да ги решат следните прашања пред поставување на системот за видео надзор:

- ⇒ Дали видео надзорот е очигледно неопходен за исполнување на одредена цел или намера?
- ⇒ Дали е веројатно да бидат ефективни во исполнување на целта или намерата?
- ⇒ Дали постои алтернативен метод за исполнување на целта? (некој помалку „интрузивен“ за приватноста)
- ⇒ Дали деградацијата на приватноста е во баланс со добиениот бенефит?

При користењето на системите за видео надзор како технологијата за обработка на лични податоци, неопходно е да се утврдат правни, етички или други правила за заштита на податоците од неовластен пристап, изменување, објавување или било каков друг вид на неовластена обработка.



Центар за набљудување на уличен видео надзор

Принцип на правична обработка – што значи?

Собирањето и обработка на лични податоци преку вршење на видео надзор треба да биде правично и законито. Само личните податоци кои се неопходни за исполнување на целта за која системот е креиран треба да бидат собрани и зачувани на медиум за чување на системот. Системите кои користат видео надзор треба да бидат транспарентен кон субјектите на лични податоци (граѓаните) чии лични податоци се чуваат и обработуваат.

- ⇒ Видео надзорот треба да биде поставен за решавање на реални, итни и значителни проблеми.
- ⇒ Видео надзорот треба да биде „скроен“ за да ги минимизира влијанието врз приватноста.
- ⇒ Видео надзорот треба да се гледа како вонреден чекор кој треба да биде земен во предвид доколку не постои алтернатива која е помалку интрузивна врз приватноста.
- ⇒ Преобемни и неопходни „мешања“ врз приватноста треба да бидат обесхрабрувани.
- ⇒ Влијанието на предложениот видео надзор врз приватноста треба да биде оценет пред да биде истиот воведен.
- ⇒ Правото на поединците да имаат пристап до нивните лични податоци треба да биде почитувано
- ⇒ Локацијата на камерата треба да биде избрана така што ќе го минимизира покривањето/гледањето на просторот кој не е релевантен за наменетата цел.
- ⇒ Системот на видео надзор треба да е предмет на независна ревизија и евалуација
- ⇒ Јавноста има право да биде информирана за поставувањето на видео надзор.
- ⇒ Јавна консултација мора да претходат на секоја одлука за воведување на видео надзор.
- ⇒ Видео надзорот треба да биде во согласност со важечките закони.

Принципот на правичност и законитост бара:

Право на граѓаните да бидат информирани

Во случаи каде што личните податоци се собираат и чуваат на систем за видео надзор, граѓаните треба да бидат информирани за целта на обработката (вршењето на видео надзор), идентитетот на контролорот, категориите на лични податоци кои се обработуваат (кои лични податоци се снимаат) како и кои се корисниците или категориите на корисници на зачуваните податоци. Зависно од ситуацијата и други информации треба да им бидат дадени на граѓаните каде што е неопходно да се гарантира правичната обработка на лични податоци.

Граѓаните можат во секое време да бараат од контролорот да ги информира за обемот или категориите на лични податоци кои се однесуваат за него, за целта и начините на вршењето на видео надзор. (види членови 10, 11 и 12 од ЗЗЛП)

Информациите на граѓанинот треба да му бидат дадени во разбирлива форма, користејќи разбирлив и едноставен јазик, особено кога некоја обработка се однесува на малолетни лица.

Граѓаните треба секогаш да бидат известени дека влегуваат во простор кој е под видео надзор; ова исто важи и за јавни настани (пр. концерти, спортски натпревари итн.) За таа цел ДЗЛП смета дека истиот едноставен образец со „минимум“ на информации – каде што е наведен називот на контролор и контакт за добивање на информации – може да се искористи како што е опишано во ЗЗЛП (член 9-а). Овој модел на известување очигледно може да се прилагоди кон специфични ситуации. Доколку се монтирани повеќе камери и просторот над кој се врши видео надзор е особено голем, неколку известувања треба да бидат истакнати.

Податоците мора да бидат целосни, точни и ажурирани

Принципот на прецизност значи дека личните податоци собрани и обработени преку системот на видео надзор треба да бидат точни и кога е потребно ажурирани. Не е дозволен личните податоци кои се снимени со видео надзорот да бидат менувани пред нивната понатамошна обработка. Личните податоци (снимките) кои се неточни, нецелосни или неажурирани имајќи ја предвид целта заради која се собрани или обработени треба да се избришат или коригираат. Кај системите за видео надзор, податоците кои се веќе снимени и зачувани на меморија за складирање ќе се сметаат за ажурирани дури и ако се собрани во некое минато време. Не е дозволено никаква манипулација која резултира со модификација на податоците.

Информации во случај на откривање

Во прилог на основните информации, во случаи кога постои намера податоци да бидат доставувани до трети страни, контролорите мора да ги информираат граѓаните за:

- секој корисник или вид на корисник на кого му се откриваат податоците како и целта податоци која истите се дадени на користење;
- нивното право да се противат на откривањето заради специфични цели.

Кога се креира систем на видео надзор, граѓаните треба да бидат соодветно известени како системот работи и кои се нивните права.



Целта за вршење на видео надзор мора да биде специфицирана

Пред одлуката да се воведи нов систем за вршење на видео надзор институцијата/компанијата мора прво да ја утврди целта на системот за видео надзор, за кој треба да се осигура дека е законска. Специфицирањето на целта на видео надзорот може да и помогне на институцијата/компанијата да се усогласи ЗЗЛП, оцени успешноста на системот и да им објасни на работниците и јавноста зошто надзорот е потребен. Институцијата/компанијата мора да се обезбеди дека зачуваните податоци (видео снимки) нема да бидат подоцна користени за непредвидени цели или откриени на непредвидени корисници. Мора да се потенцира дека некомпатибилна цел не ги вклучува само новите цели кои не се поврзани со иницијалната цел, туку и сите цели кои не би биле разумно очекувани од поединците (субјектите на лични податоци) кои се под видео надзор (пр. кога целта поради кој е поставен видео надзорот е безбедност, и истата им е известена на вработените, зачуваните снимки не смеат да се користат за да се врши оценка колку добро вработените ја вршат својата работа или да во даден ден дошле навремено или не на работа).

Многу често видео надзорот се поставува за „безбедносни причини“. Во таквите случаи институцијата/компанијата треба внимателно да ги евалуира ризиците, а не едноставно да наведе дека целта е „да се набљудуваат некои аномалии внатре во безбедниот простор (пр. зграда) или „за справување со безбедносни инциденти“.

Контролорот (операторот на системот) не треба да има само генерална идеја за што сака да го употреби видео надзорот, туку мора да има детален концепт за употребата на системот. Исто така, контролорот треба да има и детална претстава за безбедносните инциденти кои се очекува да се случат на просторот кој е под видео надзор.

Само овластени лица имаат право на пристап

Само лицата со овластување добиено од контролорот или обработувачот, вклучително и самиот обработувач, може да имаат право на пристап до зачуваната меморија каде што се снимаат податоците од видео надзорот. Овие лица:

- мора да бидат запознаени со принципите за заштита на личните податоци пред пристапот до личните податоци (видео снимките);
- можат да вршат пристап до видео записите само во согласност со насоките и упатствата добиени контролорот, ако поинаку не е регулирано, и
- ќе ги чуваат личните податоци како доверливи, како и мерките кои се превземаат за нивна заштита.

Контролорот и обработувачот се должни да чуваат евиденција за лицата кои имаат пристап до зачуваните снимки, која содржи: име и презиме, дата на издавање на овластувањето, рок на траење на овластувањето, обемот на овластување како и начинот на пристап до видео записите.

Овластеното лице исто така придонесува за исполнување на начелата за заштита на личните податоци во согласност со ЗЗЛП.

Правото на пристап до зачуваните снимки и понатамошната употреба на личните податоци од тие снимки е доста чувствително прашање. Препорачливо е пристапот до зачуваните снимки секогаш да биде реализирана од страна на две овластени лица истовремено. Пристапот од само едно лице не треба да биде дозволено.

IV. ВРШЕЊЕ НА ВИДЕО НАДЗОР НА РАБОТНОТО МЕСТО

Неколку специфични прашања покренува вршењето на видео надзор над вработените. Мора да се земе во предвид дека вработените имаат легитимни очекувања дека можат да си ја зачуваат приватноста во својот приватен живот но и дека имаат право на одреден степен на приватност на работното место.

Во контекст на бројни пресуди на Европскиот суд за човекови права, можеме да речеме дека поединците не ја оставаат својата приватност и заштита на личните податоци секое утро на вратите од своите домови кога одат на работното место. Граѓаните имаат легитимни очекувања на одреден степен на приватност на работното место. Работните односи се значаен дел од нивната комуникација со други луѓе на работното место. Меѓутоа, ова право мора да биде балансирано со други легитимни права и интереси на работодавецот, особено со правото да го води својот бизнис ефикасно до одредена мерка, и над се, правото да се заштити себеси од одговорноста или штетата која може да ја нанесат постапките на вработените. Овие права и интереси можат да постават легитимна основа која може да ги оправда соодветните мерки за лимитирање на приватноста на работниците. Генерално може да се каже дека правата за вршење на надзор на работодавецот завршуваат таму каде што почнуваат уставните (фундаментални) права на работниците.



Ако работодавецот има намера да врши видео надзор во работните простории, мора да биде јасен во однос на целите и дека системот за видео надзор е оправдан со реална корист која ќе биде добиена од истиот. Вработените секогаш треба да бидат свесни за целите за вршење на надзорот, за поставеноста на камерите, за пристапот до снимките. Причините за вршење на видео надзорот треба да бидат јасно дефинирани и придобивки да бидат прикажани. Доколку постојат други мерки кои предизвикуваат помало нарушување на приватноста на субјектот (работникот), тие мерки треба да бидат превземени наместо видео надзорот.

Работодавецот треба да ги има во предвид основните начела за заштита на личните податоци кои треба да бидат исполнети при воведувањето на видео надзорот.

V. ОСТВАРУВАЊЕ НА ПРАВАТА НА СУБЈЕКТОТ (ГРАЃАНИНОТ)

Во демократските општества, граѓаните (субјектите на лични податоци) имаат право да го остваруваат своето право на слободно движење без притоа да се подложни на прекумерно психолошки условување во однос на нивното движење и однесување како и да не бидат предмет на детален надзор како што е следењето на нивното движење и/или активирање на „аларми“ базирани на софтвери кои автоматски го „детектираат“ наводното сомнително однесување на поединците без никаква човечка интервенција – за сметка на непропорционалната примена на видео надзорот од некои органи во бројни јавни и/или јавно достапни простори.

Правата на граѓаните се дефинирани во ЗЗЛП, вклучувајќи го правото за противење за обработка на лични податоци за специфични цели, противење на преносот на личните податоци до трето лице, пристапување и изменување на податоците кои не се точни, да се бара бришење или блокирање на податоците за кои не постои законска основа за обработка, противење за обработка на податоците за различни цели од онаа за која биле собрани. За исполнување на овие права во прва инстанца одговорен е контролорот или одговорното лице кај контролорот.

Одговорното лице/официрот за заштита на личните податоци мора да имплементира процедури кои ќе им овозможат на граѓаните да ги исполнат своите права кои се утврдени во законот на едноставен, брз и ефикасен начин, кој не предизвикува непотребно одложување или трошок, како и остварување придобивка за одговорното лице.

Доколку одговорното лице/официрот за заштита на личните податоци утврди дека согласно закон остварувањето на правата на граѓаните не е оправдано, треба да ги информира граѓаните за причините кои довеле до тоа решение.

VI. НЕКОЛКУ ПРАКТИЧНИ ПРАШАЊА

Во согласност со вообичаената пракса во ЕУ како и препораките на Европскиот Супервизор за заштита на личните податоци (EDPS), ДЗЛП исто така дава совети за некои практични прашања кога станува збор за поставување на видео надзор. Основниот принцип кој треба да го почитува секој вршител на видео надзор е минимизирањето на влијанието врз приватноста и другите фундаментални права и правна интереси на оние кои се под видео надзорот. Соодветноста на секое решение треба да се потврди и преоцени од оваа гледна точка.

Поставеност на камерите

Еден од клучните аспекти на видео надзорот е поставување на камерите и нивните технички параметри. Камерата треба да биде така поставена што ќе го минимизира вршењето на видео надзор на просторот кој е нерелевантен за исполнување на целта/ите. На пример, кога камерата е поставена со цел да се врши надзор над влезот на зградата, треба да се обезбеди дека камерата не го снима и соседниот просторот или соседните згради. Друг пример е – кога камерата е поставена во внатрешни простории истата смее да биде насочена и да снима простори кои се релевантни за обезбедувањето заштита на пример, но не и околните простории кои се сметаат за приватни (тоалети, кујни, соби за одмор, соблекувални итн.)

Број на камери



Бројот на камерите кои го сочинуваат системот на видео надзор зависи од големината на просторот на кој се врши видео надзор, големината на објектите, нивото на причината за безбедност и неколку други фактори. Препорачливо е да се инсталираат ист вид на камери кои се соодветни на системот за видео надзор. Кога бројот на поставени видео камери е непропорционален во однос на целта тогаш ризикот за веројатноста на влијанието врз приватноста и другите фундаментални права се зголемува. Препорачливо е да се лимитира бројот на камери онолку колку што се доволни за да се исполни целта на видео надзорот. Бројот, поставеноста и видот на камерите треба да се вклучат во Правилникот за вршење на видео надзор на контролорот.

Време на вршење на видео надзорот

Времето кога камерите од видео системот се поставени да снимаат, треба да биде поставено на начин да го минимизира вршењето надзор за времето кое не е релевантно за исполнување на целта/ите. На пример, ако целта на видео надзорот е безбедноста, кога е можно, времето на вршење на видео надзор треба да биде поставено кога постои поголема веројатност за појавување на проблемите за безбедноста. Снимањето само после работното време или за време на викенди може да биде доволно за исполнување на целта.



Резолуција и квалитет на сликата

Резолуцијата и квалитетот на сликата мора да биде соодветна на целта заради кој е поставен видео надзорот. Различните цели бараат различен квалитет на снимките. На пример, кога идентификацијата на поединците е клучниот очекуван резултат, тогаш параметрите на резолуцијата на камерите, подесувањата (сетирањата) на дигиталниот систем, локацијата, растојанието, светлоста и некои други фактори треба да бидат земени во предвид така што резултатот на квалитетот на сликата да биде доволен за идентификација. Од друга страна пак, ако идентификацијата на поединците не е примарната цел на системот за видео надзор, тогаш параметрите на резолуцијата на камерата треба да бидат поставени така што снимките не би содржеле препознатливи слики од ликовите на поединците.

VII. Дирекција за заштита на личните податоци

Во најширока смисла, Дирекцијата за заштита на личните податоци е одговорна за правилно спроведување на Законот за заштита на личните податоци. Ова значи дека Дирекцијата се грижи за заштита на личните податоци на граѓаните и ги штити нивните права



Оваа улога Дирекцијата ја врши преку:

- постапување по барање на граѓаните за утврдување на повреда на правото на заштита на нивните податоци преку инспекција;
- спроведување на инспекција по службена должност да се провери дали прописите за заштита на податоците се спроведуваат правилно

Сепак, треба да се напомени дека Дирекцијата нема само репресивна улога - да ги решава проблемите кога ќе се појават. Наместо тоа, улогата на Дирекцијата е да ги запознае граѓаните од поблиску со нивните права. Оваа улога, Дирекцијата ја практикува, а овие прирачници се наменети за подобрување на знаењата(познавањата) на граѓаните за нивните права за заштита на личните податоци.

Како да поднесете барање за заштита на личните податоци?

Тоа е многу лесно и едноставно. Секогаш кога некој верува дека нејзиното/неговото право на заштита на личните податоци е повредено и има некои факти или докази за повреда преку вршење на видео надзор, истите можат да ги достават до Дирекцијата за заштита на личните податоци преку:

- * Барање за утврдување на повреда на правото на заштита на личните податоци или
- * Иницијатива до Дирекцијата за вршење на инспекција (надзор) над вршењето на видео надзор од страна на контролорот.

Со цел да се олеснат овие постапки, Дирекцијата има донесено обрасци за Барање и Иницијативата за вршење на инспекција, кои се објавувани на веб страницата на Дирекцијата ([www.privacy.mk/prijavi zloupotreba](http://www.privacy.mk/prijavi_zloupotreba)).

По пополнување на потребните информации во Барањето или Иницијативата за вршење на инспекциски надзор истите можат лесно да се поднесат на е-меил адресата contact@dzlp.mk, contact@privacy.mk или по пошта . Целата постапка е во детали објаснета на веб - страницата на Дирекцијата [www.privacy.mk/prijavi zloupotreba](http://www.privacy.mk/prijavi_zloupotreba)).

FAQs – Често поставувани

прашања

1. Зошто податоците од видео надзорот потпаѓаат под правниот режим за заштита на личните податоци?

Мораме да ја земеме во предвид дефиницијата за лични податоци дадена во Директивата (95/46/ЕК) и Законот за заштита на личните податоци. Во истите личните податоци се дефинирани како „секоја информација која се однесува за идентификувано физичко лице или физичко лице кое може да се идентификува („субјект на лични податоци“); лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет“.

Ова во пракса значи дека податоците (сликите/снимките) собрани при вршењето на видео надзорот се со иста суштина – преку нив може да се идентификуваат поединците (директно или индиректно). Логична последица би била дека таквите податоци (добиеени од вршење на видео надзор) мора да бидат соодветно заштитени во согласност со правниот режим за заштита на личните податоци.

2. Дали само постојаното вршење на видео надзор спаѓа под опсегот на правните обврски утврдени во закон?

Не, правните обврски се применуваат и важат и тогаш кога видео надзорот се користи на ad hoc основа.

3. Како да се одбере соодветна леќа на камерата?

Леќите на камерите кои се користат во системот за вршење на видео надзор мора да бидат соодветни на изјавената цел. Ако е потребна камера за надзор на склад, и потребно е да се види колку што е можно повеќе, би требало да се користи леќа од 2.8 mm – 4 mm (широк агол). Меѓутоа, доколку е потребно да надгледува лимитиран простор (како влезна врата, поглед од блиску на предмет итн.) треба да се користи 8mm леќа. Соодветните камери за видео надзорот зависат од неколку параметри, леќата на камерата да се прилагоди во согласност со целта заради која се користи.

4. Што е CCTV (систем за видео надзор со затворено коло на телевизиски камери)?

CCTV се однесува на видлив или таен видео систем наменет само за ограничен број на гледачи. Во CCTV снимките можат да се гледаат или снимаат, но не и да се емитуваат. Првично е развиен за безбедносни цели во банките и казината; меѓутоа денеска е развиен до степен каде што е едноставен и евтин за да се користи во Системи за безбедност на домот и за секојдневен надзор. Поконкретно, CCTV е систем за телевизиски пренос во кој претходно снимени сигнали и снимки направени во живо се праќаат преку затворен круг до ограничени и однапред определени групи на приматели, обично како кодирани радио сигнали кои се декодираат во моментот на прием. CCTV се јавува во различни форми и има широк спектар на апликации од подобрување на сликите за делумно слепите до пренос односно пренесување на емисии од принципот „плати па гледај“. Иако кабловската телевизија е технички еден вид на форма на CCTV, овој термин се користи за да се опишат системи со поспецифични апликации отколку стандардното емитување или кабловска телевизија.

5. Што значи „далечинско“ вршење на надзор?

Можноста да се врши надзор на домот или деловните простории од различни „далечни“ локации се нарекува „Можност за далечинско вршење на видео надзор“. Со овие системи може да се врши „далечински“ надзор на одредена локација преку интернет.

6. Од што се состојат основните системи за вршење на видео надзор?

Основниот систем се состои од надворешни или внатрешни камери во боја кои се поврзани до централен дигитален видео рекордер (DVR) лоциран на местото на вршење на видео надзорот. Рекордерот може да чува податоци со денови, недели или месеци зависно од опциите. Самите камери можат да имаат можност да снимаат преку ден или преку ноќ. Камерите можат да бидат „фиксни“ насочени кон однапред определен простор или „подвижни“ – автоматски да патролираат голем простор преку pan-tilt-zoom карактеристики кои се дефинирани од корисникот. Снимките можат да се гледаат внатрешно преку монитор, компјутер и/или повеќето кабелски телевизии или сателитски уреди. Надворешно, во системот за видео надзор може да се пристапи од секаде во светото преку интернет. Некои системи даваат можност да се гледаат и преку паметните телефони (iPhone, Blackberry, итн.)

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

www.privacy.mk

Email: info@dzlp.mk; info@privacy.mk; contact@dzlp.mk и contact@privacy.mk

Тел: ++ 389 (2) 3230 635

Факс: ++ 389 3230 635