ФИЛКАБ АД
ул. Коматевско шосе 92
4004 Пловдив, България
Т +359 32 277 171
Ф +359 32 671 133
office@filkab.com
www.filkab.com

ПОЛИТИКА НА „ФИЛКАБ“ АД ОТНОСНО ИЗПОЛЗВАНЕТО НА ВИДЕОНАБЛЮДЕНИЕ

1. Цел и обхват на политиката

С оглед на безопасността и сигурността на служителите, посетителите, сградата на Организацията, имуществото и обработваните лични данни, **„ФИЛКАБ“ АД** (за краткост „Организацията“) използва система за видеонаблюдение в някои зони на своите сгради. В политиката относно използването на видеонаблюдение се описват видео системата на Организацията и предпазните мерки, предприети за защита на личните данни, неприкосновеността на личния живот и други основни права и легитимни интереси на лицата, попадащи в обсега на камерите.

Тази политика определя процедурите, които трябва да се следват при обработването на лични данни. Процедурите и принципите, изложени тук, трябва да бъдат спазвани по всяко време от организацията, нейните служители, изпълнители или други страни, които работят от нейно име.

Настоящата политика е неразделна част от общите Политики по защита на личните данни на **„ФИЛКАБ“ АД.**

2. Съответствие с приложимите текстове за защита на данните

2.1. Организацията използва видео системите си в съответствие с Регламент (ЕС) № 2016/679 на Европейския парламент, както и националното законодателство на Република България.

2.2. Във връзка с използването на видео системите, Организацията е провела оценка на законния интерес, оценка на риска, както и балансиращ тест, за да определи степента на засягане личната неприкосновеност на посетителите, служителите и клиентите/посетителите на Организацията във връзка със запазването на своя законен интерес.

2.3. **Процес на вземане на решения** Организацията изготви тази политика, след като извърши и консултация с представител на служителите и стигна до заключението, че използването на видеонаблюдението е необходимо за целите на безопасността и сигурността и са съизмерими с тях.

2.4. **Прозрачност** Политиката, относно използването на видео системи, е достъпна в сградата на Организацията.

2.5. **Периодичен преглед** На всеки две години **„ФИЛКАБ“ АД** ще прави периодичен преглед на спазването на изискванията за защита на данните и оценка, като първият преглед трябва да се извърши най-късно до 31 декември 2020 г. В рамките на периодичния преглед Организацията ще преценява, наред с останалото:

- дали системата продължава да служи на заявената цел,
- дали са налични адекватни алтернативи и
- дали тази политика все още е в съответствие с Регламент № 2016/679.

2.6. **Защита на неприкосновеността на личния живот**

С цел да се засили защитата на неприкосновеността на личния живот, Организацията е предвидила, при нужда:

- размиване на изображението или заглушаване (за получаване на частично или напълно неразпознаваемо изображение),

- ограничаване на периода на съхранение на записите в съответствие с изискванията за сигурност (вж. точка 7 по-долу), както и
- стриктно управление на правата на операторите, що се отнася до достъпа до вътрешната система за видеонаблюдение („CCTV“).

3. Наблюдавани зони

Камери са монтирани на различни места в сградата на Организацията, включително:

- Общи части на помещения в административни сгради;
- Производствени сгради, вкл. периметъра им;
- Локални складове, вкл. периметъра им
- Магазинна мрежа.

Местоположението на камерите се преразглежда внимателно, за да се гарантира, че зони, които не са от значение за преследваните цели, са обхванати в минимална степен. Наблюдението извън територията на сградата е сведено до минимум.

Не се извършва наблюдение в зони, които са свързани със завишени очаквания за неприкосновеност, като стаите за почивка и санитарните помещения на Организацията. По изключение, при надлежно обосновани нужди, свързани със сигурността, камери могат да се инсталират и в такива зони, като във всички случаи това се прави след оценка на въздействието и след уведомяване на длъжностното лице за защита на данните и искане на разрешение от КЗЛД. В тези случаи в помещенията се поставя специално съобщение, което е ясно видимо.

По изключение, при надлежно обосновани и доказуеми нужди, свързани със сигурността, могат да се използват скрити камери, когато е необходимо за предотвратяването, разследването, разкриването и съдебното преследване на престъпни деяния. Използването на скрити камери е предмет на предварително одобрение от КЗЛД и на системно уведомяване на длъжностното лице за защита на данните. Използването на скрити камери е винаги съразмерно с тежестта на предполагаемото престъпно деяние.

Всеки случай на използване на скрити камери се документира подробно, като се включва:

- ясно определена цел, която не може да се постигне посредством алтернативен начин на разследване, който да нарушава неприкосновеността на личния живот в по-малка степен;
- оценка на въздействието във връзка със зоната в обхвата на скритите видеокамери и засегнатите лица;
- строго ограничен период от време;
- строго ограничени местоположения;
- строго ограничаване на ползватели и ясно определяне на тяхната самоличност;
- изтриване на записите веднага след като станат ненужни за целите на разследването.

4. Събрани лични данни и цел на събирането

4.1. Видео системата е конвенционална и предимно статична система. Записват се дигитални образи и има сензори за движение. Записва се конкретно движение,

уловено от камерите в наблюдаваните зони, заедно с часа, датата и мястото. Всички камери работят непрекъснато. По целесъобразност качеството на образа да позволява да бъдат идентифицирани лицата в обсега на камерата. Почти всички камери са стационарни и много малко от тях могат да се използват от операторите за увеличаване на образа в конкретна ситуация от съображения за сигурност. Обучени за целта оператори трябва да спазват настройките по отношение на защитата на личния живот и правата за достъп.

4.2. Цел и правно основание на използването на видеонаблюдението

Организацията използва Видеонаблюдението си единствено за целите на:

- сигурността и безопасността;
- защита на активите на Организацията;
- оптимизиране бизнес процеси;
- предпазване на служителите;

Когато е необходимо, видеонаблюдението допълва другите системи за физическа сигурност като системите за контрол на достъпа и системите за контрол срещу физическо проникване.

Ограничаване на целите - Системата не се използва за никакви други цели като наблюдение на работата на служителите или на останалия персонал или проследяване на присъствието. Системата се използва като инструмент за разследване или за доказателство в рамките на вътрешни разследвания или дисциплинарни процедури, изключително за целите на разследване на инцидент, свързан с физическата сигурност, или в извънредни случаи в рамките на наказателно разследване.

Правното основание за извършването на видеонаблюдението е законен интерес на Организацията, вкл. в качеството й на Работодател.

4.3. Специални категории данни Видео системата на Организацията няма за цел да прихваща (напр. чрез увеличаване на образа или целево насочване) или да обработва по друг начин (напр. индексиране, профилиране) изображения, които разкриват т.нар. „специални категории данни“.

5. Достъп до събраните лични данни

5.1. Достъпът до видеозаписите е ограничен до малко на брой, точно определени лица на базата на принципа „необходимост да се знае“. В своята вътрешна организация Организацията определя кой има право: да гледа излъчването от камерите в реално време; да гледа записите; да копира, да сваля, да изтрива или да променя даден запис. Организацията предвижда възможност в прегледа на материалите да участват и представители на служителите.

5.2. Всички служители, които имат права на достъп, включително охранителите, наети от външен подизпълнител, преминават базисно обучение по защита на данните. Обучение се провежда за всички новопостъпили служители, а периодични семинари по въпроси, свързани със спазване на правилата за защита на данните, ще бъдат организирани най-малко на всеки две години за всички служители с права на достъп.

5.3. След обучението всеки служител подписва декларация за поверителност. Такава декларация се подписва и от всички външни подизпълнители и техния персонал.

5.4. На ръководството и на служителите, работещи в сферата на човешките ресурси, не се предоставя достъп, освен в рамките на дисциплинарни процедури, които са пряко следствие от инцидент, свързан с физическата сигурност, и съгласно мандат

от органа по назначаването.
Ако е необходимо за целите на разследването или наказателното преследване на престъпно деяние, достъп може да се предостави на органите на реда.
Всяко нарушение на сигурността по отношение на камерите се завежда в регистъра на разследванията и своевременно се съобщава на длъжностното лице за защита на данните.

6. Защита и гарантиране на личните данни

С цел да се защити сигурността на видео системите, включително на личните данни, са взети следните технически и организационни мерки:

- Сървърите, на които се съхраняват записите, се намират в обезопасени помещения, защитени чрез мерки за физическа сигурност; мрежови защитни стени защитават логическия периметър на информационната инфраструктура; главните компютърни системи, които съхраняват данните, са с допълнителна защита за сигурност.
- Административните мерки включват задължението да се извърши индивидуална проверка за надеждност на всички наети подизпълнители, които имат достъп до системата (включително на персонала за поддръжка на оборудването и системите).
- Всички служители (външни и вътрешни) подписват споразумения за неразкриване на информация и поверителност.
- Правата на достъп за потребителите се предоставят единствено за ресурсите, които са абсолютно необходими за изпълнение на задълженията им.
- Единствено системният администратор, специално назначен за тази цел от контрольора, може да предоставя, променя или отнема правата на достъп на служителите. Всяко предоставяне, промяна или отнемане на права за достъп се извършва съобразно строги критерии.
- Във всеки един момент Организацията поддържа актуализиран списък на всички лица с достъп до системата и описва в детайли правата им на достъп;
- Длъжностното лице за защита на данните се консултира преди придобиването или инсталирането на нова система за видеозащита.

7. Срок на запазване на данните

А) Записите от видеонаблюдението се запазват за срок от 30 дни. След изтичането на този срок изображенията се заличават в същата последователност, в която са записани в системата.
При инцидент, свързан със сигурността, съответният запис може да бъде запазен за по-дълъг от обичайния срок, колкото е необходимо за по-нататъшното разследване на инцидента. Запазването е строго документирано и необходимостта от запазване се преразглежда периодично.

8. Информация за обществеността

Организацията прилага множество мерки за информираност, които обхваща следното:

- подробно съобщение с информация за използването на видеонаблюдение е поставено на всеки от входовете на сградите и търговските обекти на Организацията,
- на място в сградите се поставят съобщения с пиктограми, за да се укаже, че се

извършва наблюдение, и за сведение как да се получи допълнителна информация,

- политиката относно използването на видеонаблюдение може да се открие във всеки наш офис, като там може да се получи по-подробна информация за практиките на Организацията в областта на видеонаблюдението.

Съобщението, което Организацията поставя на място, е поместено в **Приложение № 1** към настоящата Политика.

9. Права на субектите на данни

Субектите на данни имат право на достъп до касаещите ги лични данни, съхранявани от Организацията, както и право да коригират и допълват такива данни. Всички искания за достъп, коригиране, блокиране и/или заличаване на лични данни в резултат от използването на камери следва да се изпращат на хартия в офисите на дружеството, по телефон и на електронен адрес, а именно: гр. Пловдив, ул. Коматевско шосе № 92, ел. поща: office@filkab.com, телефон 032/277 171

Отговорен служител на Организацията изпраща на подателя потвърждение за получаване в рамките на 10 работни дни след получаване на искането. По възможност ДЛЗД изпраща конкретен отговор във връзка с искането в рамките на до 30 календарни дни. Когато това е невъзможно, подателят се уведомява относно следващите стъпки и причините за забавянето. Дори в най-сложните случаи, най-късно в рамките на три месеца искането трябва да се удовлетвори или да се предостави окончателен мотивиран отговор, с който се отхвърля на искането.

С цел защита на данните, Организацията може да поиска от подателите категорично да удостоверят самоличността си (напр. като представят документ за самоличност), както и да уточнят датата, времето, мястото и обстоятелствата, при които са били заснети от камерите или записани по телефона. Подателите трябва също да представят своя актуална снимка, която да позволи на охранителния персонал да ги разпознае върху разглежданите записи.

При нередности или очевидна злоупотреба от страна на субекта на данните при упражняване на правата му, Организацията може да откаже достъп.

10. Средства за правна защита

Всеки субект на данните има право да подаде жалба пред надзорния орган - Комисия за защита на личните данни, София 1592, бул. „Проф. Цветан Лазаров” № 2 или www.cpdp.bg, ако смята, че правата му са били нарушени в резултат на обработването на касаещите го личните данни от Организацията.

ФИЛКАБ АД
ул. Коматевско шосе 92
4004 Пловдив, България
Т +359 32 277 171
Ф +359 32 671 133
office@filkab.com
www.filkab.com

Приложение № 1
(Примерно уведомление за видеонаблюдение

	**ОБЕКТЪТ Е ПОД ПОСТОЯННО ВИДЕОНАБЛЮДЕНИЕ** **Администратор на личните данни:** „ФИЛКАБ“ АД с ЕИК 115328801, със седалище и адрес на управление: гр. Пловдив 4004, район р-н Южен, ул. „Коматевско шосе“ № 92 **Цели на обработването:** Охрана на лица, материални и интелектуални активи; Защита на живота и здравето; Превенция и разкриване на престъпления; Установяване на обстоятелства; Повишаване на качеството на предлаганите услуги. **Основание:** Законен интерес на администратора. **Срок за съхранение:** До 30 дни от момента на записа. **Получатели:** Служители на дружеството и органи на реда. Администраторът осигурява всички права, предвидени в законодателството на субектите на данни. За повече информация: www.filkab.com