ТРАКИЙСКИ УНИВЕРСИТЕТ
СТАРА ЗАГОРА

ПОЛИТИКА НА ТРАКИЙСКИ УНИВЕРСИТЕТ С БУЛСТАТ 123024538 ОТНОСНО ИЗПОЛЗВАНЕТО НА ВИДЕОНАБЛЮДЕНИЕ

Утвърдил:

доц. д-р Добри Ярков
Ректор на Тракийски университет

1. Цел и обхват на политиката

С оглед на безопасността и сигурността на студентите, служителите, посетителите и опазване имуществото, **ТРАКИЙСКИ УНИВЕРСИТЕТ** (за краткост „Организацията“) използва система за видеонаблюдение в някои зони на своите сгради и прилежащите им територии. В политиката, относно използването на видеонаблюдение, е описана 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 се следват при обработването на лични данни. Процедурите и принципите, изложени тук, се спазват 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 **ТРАКИЙСКИ УНИВЕРСИТЕТ.**

2. Съответствие с приложимите текстове за защита на личните данни

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

- Закон за частната охранителна дейност.
- НАРЕДБА № 8121з-1225 от 27 септември 2017 г. за видовете обекти по чл. 23, ал. 1 от Закона за противодействие на тероризма, чиито собственици и ползватели разработват и прилагат мерки за противодействие на тероризма, минималните изисквания към тези мерки и реда за упражняване на контрол.
- Решение на Министерски съвет № 669 от 02.11.2017 г., съгласно национален план за мерки за борба с тероризма.
- На основание Уведомително писмо от МВР 824500-850-17.01.2018 г., съгласно чл.: 66, ал. 1 и ал. 2 от Закона за МВР ДВ. бр. 24 от 31.03.2015 г.
- На основание Уведомително писмо от МВР 824500-19203-24.11.2015 г., съгласно чл.: 66, ал. 1 и ал. 2 от Закона за МВР ДВ. бр. 24 от 31.03.2015 г.

2.2. Във връзка с използването на видео системите за наблюдение, Организацията проведе 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 представители на служителите и стигна до заключението, че използването на видеонаблюдението е необходимо за целите на безопасността и сигурността и е съизмеримо 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 **ТРАКИЙСКИ УНИВЕРСИТЕТ** прави периодичен преглед на спазването на изискванията за защита на данните и оценка. В рамките на периодичния преглед Организацията 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 предвижда, 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).
- стриктно управление на правата на операторите, що се отнася до достъпа до вътрешната система за видеонаблюдение.

3. Наблюдавани зони

Камери са монтирани на различни места в сградата на Организацията и прилежащите им територии, включително:

- Общи части на помещения в административните сгради;
- Всички входно-изходни точки на сградите /главен вход, второстепенни входове/.
- Входно-изходните зони за паркиране и достъп на автомобили.

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 Организацията 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.

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 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 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 на работните процеси;
- предпазване на студентите и 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 Тракийски университет определи 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, а именно:

- Служители от отдел охранителна дейност,
- Служител от отдел ЦИКО.

5.2. Организацията предвижда възможност, в прегледа на материалите, да участват и представители на служителите.

5.3. 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, се организират най-малко на всеки две години за всички служители с права на достъп.

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

5.5. 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 регистър 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. С цел избягване на всяка възможност за неоторизиран достъп е изградена самостоятелна независима видео мрежа. Видео мрежата не е свързана по никакъв начин с други локални и интернет мрежи.
- 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 до системата за видеонаблюдение.

7. Срок на запазване на данните

Съгласно ЗАКОН ЗА ЧАСТНАТА ОХРАНИТЕЛНА ДЕЙНОСТ в сила от 31.03.2018 г. Обн. ДВ. бр.10 от 30 Януари 2018 г., изм. ДВ. бр.27 от 27 Март 2018 г., изм. ДВ. бр.92 от 6 Ноември 2018 г., доп. ДВ.

бр.13 от 12 Февруари 2019 г., изм. ДВ. бр.17 от 26 Февруари 2019 г.:
Чл. 56. (1) При извършване на дейност по чл. 5, ал. 1 изпълнителите на частна охранителна дейност:
(4) Записите от техническите средства за видеонаблюдение се съхраняват в регистър "Видеонаблюдение" два месеца след изготвянето им. Унищожаването им се удостоверява от ръководителя на охранителната дейност.

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, поставено на всеки от входовете на сградите и обектите 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 е публикувана в сайта на университета на: http://www.uni-sz.bg/lichni-danni.

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 Организацията, по телефон и на електронен адрес, а именно: dpo@uni-sz.bg. Отговорен служител на Организацията /ДЛЗД/ 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.

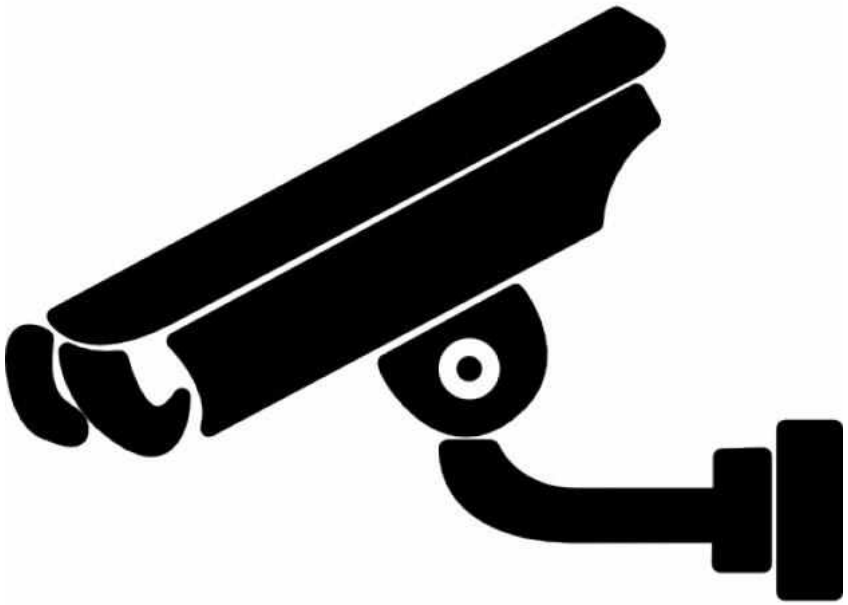
С цел защита на данните, Организацията може да поиска от подателите категорично да удостоверят самоличността си (напр. като представят документ за самоличност), както и да уточнят датата, времето, мястото и обстоятелствата, при които са били заснети от камерите. Подателите трябва също да представят своя 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.

Приложение № 1
Уведомление за видеонаблюдение



ОБЕКТЪТ Е ПОД ПОСТОЯННО ВИДЕОНАБЛЮДЕНИЕ!!!

Администратор на личните данни:
Тракийски университет
БУЛСТАТ: 123024538
седалище и адрес на управление: гр. Стара Загора, Студентски град.

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 - Закон за частната охранителна дейност, Наредба № 8121з-1225.

Срок за съхранение: Съгласно ЗАКОН ЗА ЧАСТНАТА ОХРАНИТЕЛНА ДЕЙНОСТ чл. 56. ал. 4: два месеца от момента на записа.

Получатели: Служители на Тракийски университет и органи на реда.

За повече информация: http://www.uni-sz.bg/lichni-danni