

**ПОЛИТИКА НА ГЕНЕРАЛНИЯ СЕКРЕТАРИАТ НА
СЪВЕТА
ОТНОСНО ИЗПОЛЗВАНЕТО НА ВИДЕОСИСТЕМИ**

Съдържание

<u>1. Цел и обхват на политиката</u>	3.
<u>2. Съответствие с приложимите текстове за защита на данните</u>	3.
<u>3. Наблюдавани зони</u>	6.
<u>4. Събрани лични данни и цел на събирането</u>	7.
<u>5. Достъп до събраните лични данни</u>	9.
<u>6. Защита и гарантиране на личните данни</u>	11.
<u>7. Срок на запазване на данните</u>	12.
<u>8. Информация за обществеността</u>	12.
<u>9. Права на субектите на данни</u>	13.
<u>10. Средства за правна защита</u>	15.

Политика на генералния секретариат на Съвета относно използването на видеосистеми

1. Цел и обхват на политиката

С оглед на безопасността и сигурността на служителите, посетителите, сградите, имуществото и информацията и от логистични съображения, генералният секретариат на Съвета (ГСС) използва система за видеозащита в някои зони на своите сгради. В политиката относно използването на видеосистеми се описват видеосистемата на ГСС и предпазните мерки, предприети от ГСС за защита на личните данни, неприкосновеността на личния живот и други основни права и легитимни интереси на лицата, попадащи в обсега на камерите.

Политиката на ГСС относно използването на видеосистеми не се прилага за записите или излъчването на прояви за целите на политиката на Съвета или на Европейския съвет за медиите и комуникацията с обществеността. Следва да се отбележи също, че камерата, инсталирана в медицинската служба на ГСС (която не прави записи), е преминала отделна процедура за нотифициране.

2. Съответствие с приложимите текстове за защита на данните

2.1. ГСС използва видеосистемите си в съответствие с Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни¹ и с Решение 2004/644/ЕО на Съвета от 13 септември 2004 г. за приемане на правила за прилагането на Регламент (ЕО) № 45/2001². По този начин Съветът надлежно отчита препоръките, които се съдържат в Насоките относно видеонаблюдението (наричани по-нататък „Насоките“) от 17 март 2010 г.³, изготвени от Европейския надзорен орган по защита на данните.

¹ ОВ L 8, 12.1.2001 г., стр. 1.

² ОВ L 296, 21.9.2004 г., стр. 16.

³ https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

2.2. Използването на видеосистема е необходимо за доброто управление и функциониране на ГСС, по-конкретно за целите на контрола за сигурност и безопасност, както е посочено в точка 4.2 по-долу. Използването на видеосистема е нужно за подпомагане на по-широките политики в областта на сигурността, установени с Решение 2013/488/ЕС на Съвета от 23 септември 2013 г. относно правилата за сигурност за защита на класифицирана информация на ЕС⁴, и допринася за изпълнението на мандата на дирекцията за безопасност и сигурност, установен с Решение 181/10 на генералния секретар на Съвета относно задачите на службата за сигурност⁵.

2.3. Нотифициране относно степента на съответствие. Действащата видеосистема на ГСС е инсталирана след оценка на риска и проучване на различните възможни решения, като на 15 юни 2007 г. длъжностното лице за защита на данните в ГСС е нотифицирано за това в съответствие с член 25 от Регламент (ЕО) № 45/2001. На 20 юни 2007 г. системата е представена на Европейския надзорен орган по защита на данните (ЕНОЗД) за предварителна проверка ex-post. Тази предварителна проверка първо е преустановена и впоследствие приключена от ЕНОЗД до публикуването на насоките. След публикуването на насоките ГСС изготви политиката на ГСС относно използването на видеосистеми и досие за съответствие.

След приемането длъжностното лице за защита на данните ще уведоми ЕНОЗД за тази политика и за степента на съответствие.

2.4. Контакти с компетентния орган по защита на данните в държавата членка. Белгийският компетентен орган по защита на данните — *Commission de la Protection de la Vie Privée* („CPVP“) — е информиран относно използването на видеосистеми от ГСС.

⁴ ОВ L 274, 15.10.2013 г., стр. 1.

⁵ Може да се намери в сайта DOMUS, раздел „DGs & Teams - DG A - SSCIS - Safety and Security“.

2.5. Процес на вземане на решения. ГСС изготви тази политика, след като в консултация със съответните служби стигна до заключението, че използването на видеосистемата продължава да бъде необходимо за целите на безопасността и сигурността и съизмеримо с тях. ГСС се консултира с Комитета на персонала на ГСС и с длъжностното лице за защита на данните и взе предвид техните становища. Политиката беше одобрена от генералния секретар.

2.6. Прозрачност. Политиката относно използването на видеосистеми е достъпна на уебсайта на Съвета на адрес <http://www.consilium.europa.eu/bg/general-secretariat/corporate-policies/data-protection/> и на интранет сайта на ГСС в DOMUS, раздел „DGs & Teams - DG A - SSCIS - Safety and Security“.

2.7. Периодичен преглед. На всеки две години ГСС ще прави периодичен преглед на спазването на изискванията за защита на данните и оценка. В рамките на периодичния преглед ГСС 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 № 45/2001.

2.8. Защита на неприкосновеността на личния живот. С цел да се засили защитата на неприкосновеността на личния живот, ГСС е предвидил:

- размиване на изображението (за получаване на частично или напълно неразпознаваемо изображение според случая),
- 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 сградите Justus Lipsius, LEX и „Европа“, в детските ясли на Съвета, както и в сградите в Neder-Over-Heembeek, включително: на централния вход; при турникетите, отварящи се с електронни карти; на аварийните изходи; на входа на паркингите; в заседателните зали; в защитените помещения; по коридорите; и около сградите, за да се защити външният периметър.

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 сградите на територията на Белгия е сведено до минимум и компетентните национални органи са информирани.

Не се извършва наблюдение в зони, които са свързани със завишени очаквания за неприкосновеност, като офиси или спортни зали. 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. 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 страна на директора на дирекцията за сигурност и безопасност и на системно уведомяване на длъжностното лице за защита на данните в рамките на официално разследване за целите на сигурността, възложено от генералния секретар. Използването на скрити камери е винаги съразмерно с тежестта на предполагаемото престъпно деяние и се извършва в съответствие с член 20 от Регламент (ЕО) № 45/2001. 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.** Видеосистемата 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.

ГСС не използва високотехнологични или интелигентни технологии за видеозащита, но системите за видеозащита в сградите, посочени в точка 3 от политиката, са свързани.

4.2. Цел на използването на видеосистемата. ГСС използва видеосистемата си единствено за целите на сигурността и безопасността. Видеосистемата способства да се гарантира сигурността на сградите на ГСС, безопасността на служителите и посетителите, както и на имуществото и информацията, които се намират или се съхраняват в помещенията.

Когато е необходимо, видеосистемата допълва другите системи за физическа сигурност като системите за контрол на достъпа и системите за контрол срещу физическо проникване. Тя е част от мерките за подпомагане на по-широките политики в областта на сигурността, установени с Решението на Съвета относно правилата за сигурност за защита на класифицирана информация на ЕС, и допринася за предотвратяването, възпирането и при необходимост разследването на неразрешен физически достъп, включително неразрешен достъп до обезопасени помещения и защитени зали, информационна инфраструктура или оперативна информация.

4.3. 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. Разследванията се провеждат винаги в рамките на конкретен мандат от генералния секретар или органа по назначаването, според случая.

4.4. Ad hoc използване на видеосистеми. При надлежно обоснована, свързана със сигурността нужда от ad hoc видеозащита, тя може да се осигури, като операциите се планират предварително, изготвя се оценка на въздействието и се информира длъжностното лице за защита на данните.

4.5. Уебкамери. ГСС не използва уебкамери за видеозащита.

4.6. Специални категории данни. Видеосистемата на ГСС няма за цел да прихваща (напр. чрез увеличаване на образа или целево насочване) или да обработва по друг начин (напр. индексирание, профилиране) изображения, които разкриват т.нар. „специални категории данни“ по смисъла на точка 6.7 от Насоките.

5. Достъп до събраните лични данни

5.1. Достъпът до видеозаписите и до заснемания в момента материал е ограничен до малко на брой, точно определени лица на базата на принципа „необходимост да се знае“.

5.2. Достъпът до записите и/или до техническата архитектура на видеосистемата е ограничен до малко на брой, точно определени лица на базата на принципа „необходимост да се знае“. ГСС уточнява целта и обхвата на правата им на достъп. По-конкретно, ГСС 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.

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, ще бъдат организирани 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. Всички случаи на прехвърляне и разкриване извън дирекцията за безопасност и сигурност се документират и подлежат на строга оценка на необходимостта от такова прехвърляне и съвместимостта на целите на прехвърлянето с първоначалната, свързана със сигурността цел на обработката. Службите за вътрешен одит на ГСС и длъжностното лице на Съвета за защита на данните могат да преглеждат регистъра на запазената информация и прехвърлянията.

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 местната или националната полиция, признати съдебни органи, органите на ЕС за борба с измамите (напр. OLAF) и службите за сигурност на другите европейски институции или заинтересовани международни организации.

Не се удовлетворяват искания за извличане на данни (data mining)⁶.

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 Извличане на данни (data mining): процес на екстраполиране на модели от съществуващи бази данни.

6. Защита и гарантиране на личните данни

С цел да се защити сигурността на видеосистемите, 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 контролора, 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 ГСС 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.

Политика на ГСС във връзка с използването на видеосистеми е изготвена в съответствие с раздел 9 от Насоките на ЕНОЗД.

7. Срок на запазване на данните

Изображенията се запазват за срок от 30 дни. След изтичането на този срок изображенията се заличават в същата последователност, в която са влезли 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. Службите за вътрешен одит на ГСС и длъжностното лице на Съвета за защита на данните могат да преглеждат регистъра на запазената информация и прехвърлянията.

8. Информация за обществеността

8.1. Многопластов подход. ГСС прилага многопластов подход, който обхваща следното:

- подробно съобщение с информация за използването на видеосистеми е поставено на всеки от входовете на сградите на ГСС, включително на входовете на паркингите,
- 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 видеосистеми е публикувана на уебсайта на ГСС и на интранет сайта, като там може да се получи по-подробна информация за практиките на ГСС в областта на видеонаблюдението.

Брошури с информация са на разположение на различните рецепции в сградите на Съвета и при поискване от дирекцията за безопасност и сигурност. При запитване може да се предостави допълнителна информация.

Съобщения се поставят в близост до следните наблюдавани зони, например: до централния вход, асансьорите в паркингите и входовете на паркингите.

8.2. Специфично индивидуално съобщение. Независимо от правилата, приложими към разследванията, лицата, които са били заснети от камерите (например от охраната в рамките на разследване за целите на сигурността), получават индивидуално съобщение, стига да е изпълнено поне едно от следните условия:

- тяхната самоличност е отбелязана в някое от досиетата/записите,
- видеозаписът се използва срещу съответното лице, пази се за по-дълъг от обичайния срок или се прехвърля извън дирекцията за безопасност и сигурност, или
- самоличността на лицето е разкрита на някого извън дирекцията за безопасност и сигурност.

Изпращането на съобщението може да се забави, ако това е необходимо за предотвратяването, разследването, разкриването и съдебното преследване на престъпни деяния, както е предвидено в член 20 от Регламент (ЕО) № 45/2001.

Във всички такива случаи се прави консултация с длъжностното лице на Съвета за защита на данните, за да се гарантира спазването на правата на засегнатите лица, освен при провеждането на разследвания.

9. Права на субектите на данни

Субектите на данни имат право на достъп до касаещите ги лични данни, съхранявани от ГСС, 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 до директора на дирекцията за безопасност и сигурност в Съвета на Европейския съюз на адрес: Rue de la Loi 175, 1048 Brussels, с копие до длъжностното лице за защита на данните.

Директорът на дирекцията за безопасност и сигурност изпраща на подателя потвърждение за получаване в рамките на 5 работни дни след получаване на искането. По възможност директорът на дирекцията за безопасност и сигурност изпраща конкретен отговор във връзка с искането в рамките на 15 календарни дни. Когато това е невъзможно, подателят се уведомява относно следващите стъпки и причините за забавянето в рамките на 15 дни. 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 искането. Директорът на дирекцията за безопасност и сигурност прави всичко възможно да отговори по-рано, особено ако подателят обоснове спешния характер на искането.

При конкретно искане може да се организира разглеждане на снимките. В такива случаи подателите трябва категорично да удостоверяят самоличността си (напр. като представят документ за самоличност при разглеждането на снимките), 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 снимки.

При нередности или очевидна злоупотреба от страна на субекта на данните при упражняване на правата му, дирекцията за безопасност и сигурност може да се консултира с длъжностното лице за защита на данните относно искането и/или да пренасочи субекта на данните към длъжностното лице за защита на данните, което да вземе решение относно допустимостта на искането и съответните последващи действия.

Искане за преглеждане на запис може да бъде отхвърлено, когато изключение по член 20, параграф 1 от Регламент (ЕО) № 45/2001 се прилага в конкретен случай, например за защита на разследването на престъпно деяние. Може да възникне необходимост от налагане на ограничение, за да се защитят правата и свободите на други лица, които например присъстват на снимките и не е възможно да се получи тяхното съгласие за разкриване на касаещи ги лични данни или да се обработят снимките, за да се компенсира липсата на съгласие.

10. Средства за правна защита

Всеки субект на данните има право да подаде жалба пред Европейския надзорен орган по защита на данните (edps@edps.europa.eu), ако смята, че правата му по Регламент (ЕО) № 45/2001 са били нарушени в резултат на обработването на касаещите го личните данни от ГСС. Препоръчва се, преди да подадат жалба, засегнатите лица да се опитат да получат удовлетворение, като се обърнат към:

- директора на дирекцията за безопасност и сигурност (чрез центъра за сигурност, който отговаря без прекъсване на тел. 02 281 8909), Съвет на Европейския съюз, Rue de la Loi 175, 1048 Brussels, или video.protection@consilium.europa.eu, и/или
- длъжностното лице на ГСС за защита на данните, Съвет на Европейския съюз, Rue de la Loi 175, 1048 Brussels.

Служителите могат да се обръщат и към органа по назначаването съгласно член 90 от Правилника за длъжностните лица.