РЕПУБЛИКА БЪЛГАРИЯ
ВЪРХОВЕН
КАСАЦИОНЕН
СЪД

*УТВЪРЖДАВАМ:*_____

ГАЛИНА ЗАХАРОВА
ПРЕДСЕДАТЕЛ НА
ВЪРХОВНИЯ КАСАЦИОНЕН СЪД
(заповед:..808./.30...08..2023г.)

ИНСТРУКЦИЯ ЗА ПРИЛАГАНЕ НА ПОДХОДЯЩИ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ВЪВ ВЪРХОВНИЯ КАСАЦИОНЕН СЪД

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата инструкция определя подходящи технически и организационни мерки за защита на личните данни и правилата за тяхното прилагане при обработване на лични данни от Върховния касационен съд.

Чл. 2. Инструкцията има за цел да гарантира правата и свободите на физическите лица във връзка с обработване на личните им данни и съответствието на обработването на лични данни с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), Закона за защита на личните данни и други нормативни изисквания във връзка с обработването на лични данни.

Чл. 3. Прилаганите технически и организационни мерки са задължителни за всички служители във Върховния касационен съд, както и за всички други лица, които изпълняват задачи или договори, възложени от или изпълнявани във Върховния касационен съд, при които се обработват лични данни.

Чл. 4. Подходящите технически и организационни мерки за защита на личните данни се определят въз основа на анализ на риска, извършен въз основа на следните фактори:

1. естеството, обхвата, контекста и целите на обработването;
2. рисковете с различна вероятност и тежест за правата и свободите на физическите лица;
3. достиженията на техническия прогрес;
4. разходите за прилагане.

Чл. 5. Прилаганите технически и организационни мерки се разпределят в следните видове защита:

1. мерки за персонална защита;
2. мерки за физическа защита;
3. мерки за документална защита;

4. мерки за защита на автоматизирани информационни системи и криптографска защита.

Чл. 6. Прилаганите технически и организационни мерки се преценяват периодично веднъж на две години с оглед ефективността им да гарантират постоянна поверителност, цялостност, наличност и устойчивост на системите и дейностите по обработване на лични данни, като подлежат на редовно изпитване и оценка на ефективността.

II. МЕРКИ ЗА ПЕРСОНАЛНА ЗАЩИТА

Чл. 7. Персоналната защита на личните данни включва следните организационни мерки:

1. определяне на отговорниците за достъп до регистрите с лични данни;

2. спазване на принципа „необходимост да се знае“ от всяко лице, което има достъп до лични данни под ръководството на администратора;

3. обработване на лични данни само по указание на администратора, освен ако обработването не се изисква от задължение, произтичащо от правото на Европейския съюз и от българското законодателство;

4. периодично обучение на служителите на администратора, които обработват лични данни, включително тренировки за действия при инциденти, свързани със защитата на личните данни и познаване на процедура за действия при нарушения на сигурността на личните данни.

Чл. 8. Служителите на Върховния касационен съд имат оторизиран достъп само до тези регистри с лични данни, които са необходими за изпълняване на техните задължения или конкретно възложени задачи.

Чл. 9. (1) Обучението в областта на защитата на личните данни на служителите от Върховния касационен съд се организира от длъжностното лице по защита на данните, от Националния институт на правосъдието или друга обучаваща организация.

(2) Обучение се провежда задължително при постъпване на работа, по указание на надзорен орган или при констатиране на необходимост от такова, поради промени в правната уредба, практиката по нейното прилагане или друга необходимост.

(3) Проведените обучения в областта на защитата на личните данни се документират с цел спазване на принципа за отчетност.

III. МЕРКИ ЗА ФИЗИЧЕСКА ЗАЩИТА

Чл. 10. Организационните мерки за физическа защита включват:

1. определяне на зоните с контролиран достъп, в които се съхраняват лични данни, както следва: ползваните от съдиите и съдебните служители помещения в Съдебната палата, отредени за дейността на Върховния касационен съд;

2. физически достъп до зоните с контролиран достъп да се осигурява само на оторизирани служители, като се предотвратява нерегламентиран достъп до лични данни.

3. определяне на екип за реагиране при нарушения на сигурността на личните данни, който включва служители, определени със заповед на административния ръководител – председател на съда.

Чл. 11. Техническите мерки за физическа защита включват:

1. ключалки на помещения, в които се съхраняват лични данни, които се заключват, ако в тях няма отговорен служител;

2. шкафове за съхранение на лични данни, които се заключват, ако в съответното помещение няма отговорен служител;

3. устройства за контрол на физическия достъп;

4. охрана на сградата, ползвана от администратора, осъществявана с физическа охрана при влизане в сградата и с видеонаблюдение в коридорите на сградата;

5. пожароизвестителна система;

6. видеонаблюдение към адвокатска стая, архив и РКИ, в които се съхраняват делата или страните се запознават с тях .

IV. МЕРКИ ЗА ДОКУМЕНТАЛНА ЗАЩИТА

Чл. 12. Мерките за документална защита на личните данни се отнасят до регистрите с лични данни, обработвани на хартиен носител, като включват:

1. определяне на регистрите с лични данни, които се обработват на хартиен носител, както следва: регистър „Граждански дела“, регистър „Търговски дела“, регистър „Наказателни дела“, регистър „Човешки ресурси“, регистър „Контрагенти“;

2. осигуряване на достъп до личните данни в съответния регистър от лицето, отговорно за достъпа до данните в регистъра, включително под формата на справки, извлечения, копия от документи и други подобни;

3. спазване на сроковете за съхранение на личните данни;

4. своевременно предприемане на действия по унищожаване на лични данни след изтичане на срока за съхранение и преценка за изпълнението на целите на обработването на лични данни;

5. документиране на унищожаването на лични данни;

6. извършване на проверки и контрол за спазване на установените мерки.

V. МЕРКИ ЗА ЗАЩИТА НА АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ И КРИПТОГРАФСКА ЗАЩИТА

Чл. 13. Администраторът осигурява контролиран достъп на служителите при обработване на лични данни във връзка с:

1. техническите и програмно-информационните ресурси, използвани при обработката и защитата на личните данни;

2. информационните носители и извършваните действия по тяхното регистриране, преместване, подреждане, копиране, преобразуване и друг вид обработка;

3. личните данни в регистрите, както и контрол на лицата, извършващи действия по обработване на личните данни съгласно предоставените им права;

4. разполагането, поддържането и преместването на техническите ресурси, използвани за обработка на личните данни.

Чл. 14. Архивното копие и процедурите за възстановяване на данни се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните.

Чл. 15. Защитата на автоматизираните информационни системи включва тяхното администриране, при отчитане на следните изисквания:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

2. администраторските профили са персонални;

3. администраторските профили се използват само за административни цели;

4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

6. данните за автентикацията на администраторските акаунти:

а) са различни за всяка система;

б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;

в) се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран служител;

7. поддържане на списък на администраторските профили за автоматизираните информационни системи и техните компоненти;

8. годишен преглед на администраторските профили с цел удостоверяване на актуалността им;

9. задължителна смяна на пароли периодично (най-малко веднъж годишно), при прекратяване на договорните отношения със служители или трети страни, на които те са били известни и при констатиране на нарушения на сигурността на личните данни.

Чл. 16. Забранява се ползването на компютърните и информационните системи на Върховния касационен съд в следните случаи:

1. ползване на информационните ресурси за извършване на нерегламентирана дейност;

2. използване на ресурсите за подпомагане дейността на външни организации, техните продукти, услуги или бизнес практика, с цел облага;

3. електронна поща не може да се ползва за комерсиални лични цели, политически цели, религиозни цели или за подпомагане на дейност, която не е свързана с дейността на съда;

4. подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от служители на съда трябва да са лично подписани и да са до точно определен брой адресати;

5. сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти и без нужния лиценз, ако се изисква такъв;

6. копиране на лицензираните компютърни програми на съда с цел лична употреба;

7. споделяне на пароли или възпроизвеждането им по друг нерегламентиран начин.

Чл. 17. Когато дадена информационна система или продукт изискват парола, се спазват най-малко следните мерки:

1. служителите променят първоначалната парола (обикновено генерирана от програмния продукт), като създават своя индивидуална при първото влизане в съответната информационна система;

2. паролите трябва да са с не по-малко от 7 знака;

3. паролите трябва лесно да се помнят, за да не се налага да бъдат записвани на хартия;

4. паролите не трябва да са лесни за отгатване от колегите;

5. паролите не се споделят с колеги или други познати и не се възпроизвеждат по нерегламентиран начин;

6. при необходимост паролите се променят;

7. при три неуспешни опита за влизане в дадена програма достъпът може да бъде блокиран;

8. при периодична промяна на паролата не трябва да се използват вече използвани пароли;

9. системите не трябва да позволяват един и същи потребител да се включи в няколко компютъра едновременно с една и съща парола.

Чл. 18. В случай, че забравят своята парола, служителите трябва незабавно да уведомят системните администратори за генериране на нова парола.

Чл. 19. Свалянето от Интернет на аудио или видео файлове за лични цели, както и посещението и сваляне на материали от уеб сайтове, които могат да компрометират сигурността на информационните системи на дружеството, е забранено.

Чл. 20. Служителите във Върховния касационен съд нямат право да вземат програмните продукти с цел инсталирането им на домашни компютри и преносими устройства, с изключение на помагала и софтуери за онлайн обучение.

Чл. 21. При напускане на Върховния касационен съд служителите нямат право да копират или изтриват/унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Чл. 22. По отношение на автоматизираното обработване на лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване, се прилагат мерките по чл. 66 от Закона за защита на личните данни, установени от администратора на съответната система.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Инструкцията е приета на основание чл. 24, пар. 1 и 2 и чл. 29 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните) и чл. 66 от Закона за защита на личните данни.