

УТВЪРДИЛ:

ДИРЕКТОР НА НСД

(НИКОЛАЙ ИВАНОВ)

ИНСТРУКЦИЯ

**за мерките и средствата за защита на личните данни,
събрани, обработвани, съхранявани и предоставяни от Националния студентски
дом**

Раздел първи

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящата Инструкция урежда организацията и вътрешния ред на Националния студентски дом, наричан по-нататък за краткост "НСД", като администратор на лични данни, както и нивото на технически и организационни мерки при обработване на лични данни и допустимия вид защита.

Чл.2. Инструкцията е изготвена в съответствие с разпоредбите на Закона за защита на личните данни (ЗЗЛД) и Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (Наредба № 1) и цели защита на интересите на контрагентите - физически лица и физическите лица, представляващи юридическите, както и на служителите на НСД от незаконосъобразно и недобросъвестно обработване на личните им данни.

Чл.3. За целите на настоящата Инструкция понятията по-долу имат следното значение:

1. „**Лични данни**” са всяка информация, отнасяща се до контрагентите (физически лица и физическите лица, представляващи юридическите) на НСД, както и тази, свързана с неговите служители, които са идентифицирани или чрез която същите могат да бъдат идентифицирани пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

2. **„Обработване на лични данни”** е всяко действие или съвкупност от действия, които НСД извършва по отношение на личните данни с автоматични или неавтоматични средства (събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване и др.).

3. **„Администратор на лични данни”** е НСД, което самостоятелно или чрез възлагане на друго лице обработва лични данни.

4. **„Специфични признаци”** са признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето.

5. **„Регистър на лични данни”** е структурирана съвкупност от лични данни, достъпна по определени критерии съобразно вътрешните документи на НСД, която може да бъде централизирана и децентрализирана и е разпределена на функционален принцип.

6. **„Съгласие на физическо лице”** е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява те да бъдат обработвани.

7. **„Контрагент“** - физическо лице или физическо лице представител на юридическо лице, което влиза в преговорни или договорни отношения с НСД, във връзка с изпълнението на публични услуги или друго взаимодействие, свързано с предмета на дейност на НСД.

Чл.4.(1) НСД обработва само законно събрани лични данни, необходими за конкретни, ясно определени и законни цели. Личните данни, които НСД събира и обработва следва да бъдат точни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстващи на целите, за които се обработват.

(2) НСД поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

(3) НСД спазва принципа за забрана на обработване на специални категории данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход; разкриване на политически, религиозни или философски убеждения; членство в политически партии или организации; сдружения с религиозни, философски, политически или синдикални цели; лични данни, които се отнасят до здравето, сексуалния живот или до човешкия геном).

Чл.5.(1) Контрагентът - притежател на личните данни - изразява свободно своето съгласие относно обработването на отнасящи се за него лични данни.

(2) Контрагентът има право по всяко време на обработването да поиска блокиране или унищожаване (изтриване) на събрани за него лични данни, в случаите, когато оспорва тяхната точност или обработването им е незаконосъобразно.

(3) В случаите, когато данните не са получени от контрагента, НСД го информира за целите и правното основание на обработването, за категориите предоставени данни и техния източник, за получателите, на които ще бъдат предоставени, както и за правото му на достъп до неговите лични данни.

Чл. 6. Като администратор на лични данни НСД поддържа личните данни във вид, който позволява идентифициране на физическите лица.

Чл.7. Обработването на личните данни се извършва, когато:

1. Това е необходимо за изпълнение на нормативно установено задължение.

2. Физическото лице, за което се отнасят данните, е дало своето изрично съгласие. Контрагентите (физически лица или физическите лица, представители на юридическите) и служителите на НСД, се идентифицират посредством официален документ за самоличност (лична карта). Документът за самоличност може да бъде копиран само след предварително съгласие на контрагента, който удостоверява съгласието си с надпис на копието „Съгласен/а съм с копирането” и се подписва върху него. Оригиналът се връща на клиента, а копието се съхранява в архива на НСД за срок от 5 години.

3. Обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане.

Чл.8. Всички служители на НСД при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни с клиенти на НСД, в т. ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения.

Чл.9. НСД поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.

Раздел втори

ОПИСАНИЕ НА РЕГИСТРИТЕ

Чл.10. НСД поддържа следните регистри:

(1) Лични данни на служителите на трудов и граждански договор на НСД, които се събират, обработват и съхраняват в Регистри „Персонал”;

(2) „Видеонаблюдение”;

(3) „Деловодство и контрагенти”

Чл.11. Служителите на НСД нямат право да разгласяват или предоставят индивидуални данни от регистрите.

Чл.12. За защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване НСД организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Раздел трети

ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ - НОСИТЕЛИ НА ДАННИ, ТЕХНОЛОГИЯ НА ОБРАБОТВАНЕ, СРОК ЗА СЪХРАНЕНИЕ И ПРЕДОСТАВЕНИ УСЛУГИ

Чл. 13. (1) НСД събира и обработва лични данни автоматизирано и неавтоматизирано /хартиен носител/.

Чл.14. (1) В регистър „Персонал” се съхраняват следните видове лични данни:

1. физическа идентичност – имена, ЕГН, адрес, телефон, данни за личната карта;
2. образование – документ за придобито образование, квалификация правоспособност;
3. трудова дейност – съгласно приложените документи за трудов стаж и професионална биография;
4. медицински данни – карта за предварителен медицински преглед за постъпване на работа, документи от ТЕЛК и други (ако има такива, изискуеми от действащото законодателство във връзка с трудовите правоотношения);
- 5 свидетелство за съдимост, когато се изисква;
6. формуляри по образец;
7. имотно състояние и конфликти на интереси, съобразно действащото законодателство.

(2) Данните в регистъра на хартиен носител се събират, обработват и съхраняват от сътрудника АОЧРДА на НСД. Данните в регистъра на хартиен и технически носител се обработват и съхраняват от счетоводителя на НСД.

(4) Личните данни в регистър “Персонал” се набират при подаване на документи за постъпване на работа, и се актуализират периодично при необходимост.

Чл.15. (1) Регистър „Видеонаблюдение” се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите към входовете на сградата на НСД и помещенията с определен статут. Записите с видеообрази се съхраняват на отделен персонален компютър, монтиран в помещението на физическата охрана.

(2) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на НСД. На входовете на сградата са поставени предупредителни табели, че обектът се намира под постоянно видеонаблюдение. Данните от този регистър се съхраняват 30 дни.

(3) Физическата защита на личните данни се осъществява от денонощна физическа охрана.

Чл.16. (1) Регистър „Деловодство и контрагенти” съдържа следните лични данни за физически лица и за физически лица представляващи юридически лица: три имена и длъжност.

(2) Данните в регистъра не се предоставят на трети лица.

(3) Физическата защита на личните данни от регистъра е организирана, като данните се обработват и съхраняват в заключващи се помещения и строг контрол на достъпа до тях.

Чл. 17. НСД предприема следните мерки за защита на личните данни:

(1) програмно-технически – надеждна и защитена идентификация и автентификация на изпращача и на получателя на информацията и осигуряване конфиденциалност и интегритет на пренасяната информация

(2) физически – система от мерки по защита на сградата, помещенията и съоръженията, в които се създават, обработват и съхраняват лични данни и контрола върху достъпа до тях;

(3) организационни и административни – регламентирани с правила и заповеди на директора на НСД;

(4) нормативни, предвидени в законови и подзаконови нормативни актове.

Чл.18. (1) Сроковете за съхранение са съобразно описанията в част 2 от съответния регистър, както следва:

1. за Регистър „Персонал” - 50 години;

2. за Регистър „Видеонаблюдение” – 30 дни;

3. за Регистър „Деловодство и контрагенти” – според номенклатурата на делата;

(2) Служителите на НСД са задължени да спазват технологията за безопасно поддържане и съхранение, обновяване, заличаване, унищожаване и т.н на лични данни.

Раздел четвърти

ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ

Чл. 19. (1) Лице по защита на личните данни (Data Protection Officer) в НСД е директорът на НСД.

(2) Лицето по защита на информацията има следните правомощия:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, като чрез регистрация на всички извършени действия с регистрите в компютърната среда.
8. определя ред за съхраняване и унищожаване на информационни носители;
9. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др. ;
10. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл.20. (1) Съветът по защита на информацията осъществява цялостната политика на НСД по защитата на информацията. Съветът организира, координира, анализира и контролира дейностите свързани със създаването, получаването, обработването, съхраняването и архивирането на информация, представляваща държавна или служебна тайна, както и условията и реда за предоставяне на достъпа до тях в съответствие с българската и европейската нормативна уредба.

(2) Функциите на Съвет по защита на информацията се изпълняват от Експертната комисия на НСД, която е постоянно действащ съвещателен орган към директора на НСД.

(3) Съвета по защита на информацията извършва и докладва на директора на НСД ежегодна оценка на въздействието на върху защитата на личните данни, която включва:

1. системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
2. оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
3. оценка на рисковете за правата и свободите на субектите на данни, мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица;
4. оценка на спазване и прилагане на принципа за отчетност на всички операции с лични данни, която включва и детайлна оценка на поддържането и воденето на регистрите.

Чл.21. Директорът на НСД, сътрудникът АОЧРДА на НСД и счетоводителят на НСД са длъжностните лица, които са оторизирани да обработват лични данни. Същите поддържат регистри за обработването на данните, които се подреждат по хронологичен ред.

Чл. 22. Служителите на НСД са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

Чл.23. (1) За неспазването на разпоредбите на настоящата инструкция служителите на НСД носят отговорност по Закона за защита на личните данни и Кодекса на труда.

(2) Ако в резултат на действията на съответен служител на НСД по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Чл.24. Програмно техническите средства за защита на личните данни се внедряват и използват съгласувано със Съвета по защита на информацията.

Чл.25. (1) Право на достъп до данните в регистър „Персонал” имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане изразено писмено;
2. Директорът на НСД - при изпълнение на правомощията му;
3. Обработващите и операторите на лични данни – сътрудникът АОЧРДА на НСД и счетоводителят на НСД;
4. Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

(2) Данните от регистъра не се предават на трети лица.

(3) Защитата на помещенията, в които се съхраняват личните данни се постига с контролиран достъп с допълнителна метална решетка и видеонаблюдение.

(4) Длъжностните лица, събиращи и обработващи лични данни в регистър „Персонал“ имат следните права и задължения:

1. да използват личните данни при спазване разпоредбите на Кодекса на труда, Закона за държавния служител /при възникване на трудови и служебни правоотношения/.
2. да използват личните данни при изпълнение на задълженията по Закона за здравното осигуряване /ЗЗО/.
3. да не изнасят и съхраняват личните данни извън специално определените за целта места, регламентирани с режим на специален достъп;
4. да не използват личните данни по нерегламентиран начин /фалшифициране и друг вид злоупотреба/.

(6) Данните от регистъра не могат да бъдат предавани по електронен път.

(7) Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

Чл. 26. (1) Право на достъп до данните в регистър „Видеонаблюдение” имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
2. Директорът на НСД - при изпълнение на правомощията му;
3. Длъжностното лице - дежурен охранител, което поддържа регистър „Видеонаблюдение“.

4. Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основаниято, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

5. Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

(2) Данните от регистъра не могат да бъдат предавани по електронен път.

(3) Длъжностното лице, което поддържа регистър „Видеонаблюдение“ трябва да следи за изправността на ползваната апаратура.

(4) Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

Чл.27. (1) Право на достъп до данните в регистър „Деловодство и контрагенти“ имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

2. Директорът на НСД - при изпълнение на правомощията му;

3. Обработващите и операторите на лични данни – сътрудникът АОЧРДА на НСД и счетоводителят на НСД;

(2) Данните от регистъра не се предават на трети лица.

Раздел пети

ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ОПРЕДЕЛЯНЕ НА СЪОТВЕТНО НИВО НА ЗАЩИТА

Чл.28. Оценка на въздействие е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

Чл.29. Нива на защита:

(1) За Регистър „Персонал“ се определя степен на защита – „средно ниво“;

(2) За Регистър „Видеонаблюдение“ се определя степен на защита – „ниско ниво“;

(1) Регистър „Деловодство и контрагенти“ е определена степен на защита - „ниско ниво“.

Раздел шести

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл.30. НСД е предприел мерки за защита, както технически така и организационни, а именно:

1. личните данни се съхраняват в шкафове със заключващи се устройства;
2. работата и съхранение при работата с компютърни системи е подсигурана с анти вирусни програми, пароли за достъп;
3. разполага с електронен подпис.

Раздел седми

ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

Чл.31. НСД предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независимо от НСД – предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

Раздел осми

СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл.32. Лични данни на физическите и юридическите лица се съхраняват до изтичане на периода, предвиден съгласно номенклатурата на делата със сроковете за тяхното съхранение в НСД г.

Чл.33. След изтичането на периода по предходния член личните данни на физическите и юридическите лица се унищожават физически, чрез претопяване за което надеждно се изготвят актови протоколи за унищожаване.