ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

В сила от 25.05.2018 г.

Система за управление на личните данни

Администратор

„НИДА ЕС“ ООД

Интернет страница

http://hotelplaza.bg/

Отговорник по защита на данните

Мариана Палазова

Електронен адрес за връзка

contact@hotelplaza.bg

Телефон за връзка

+359 888 802 351

1. **ВЪВЕДЕНИЕ**

1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 (Общ регламент за защита на данните) замества Директивата 95/46/ЕО за защита на данните. Има пряко действие и действа успоредно с националното законодателство – Закона за защита на личните данни - в областта на защитата на личните данни. Неговата цел е да защитава „правата и свободите“ на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

2. Обхват, очертан от Общия регламент за защита на данните

Материален обхват *(член 2)* – регламентът се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (*например ръчно и на хартия*), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват *(член 3)* – правилата на Общия Регламент важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Регламентът се прилага и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

3. Понятия

„Лични данни" - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.

„Обработване" - означава всяка операция или съвкупност от операции, извършвана с

лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

„Администратор" - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

„Субект на данните“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.

„Съгласие на субекта на данните" - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

„Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

„Профилиране" - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

„Нарушение на сигурността на лични данни" - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

„Основно място на установяване“ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.

Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи. (Член 4 т.16) от ОРЗД)

„Получател" - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

1. **ДЕКЛАРАЦИЯ ОТНОСНО ПОЛИТИКАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**

1. Ръководството на „НИДА ЕС“ ООД (по-долу „организацията“ или „дружеството“) се ангажира да осигури съответствие със законодателството на ЕС и Република България

по отношение на обработването на личните данни и защитата на „правата и свободите“ на лицата, чиито лични данни предприятието събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

2. В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.

3. Регламент (ЕС) 2016/679 и тази политика се отнасят до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на клиенти, служители, доставчици и партньори и всякакви други лични данни, които организацията обработва от различни източници.

4. Отговорникът по защита на данните отговаря за преразглеждането на **„Регистъра на дейностите по обработване
“**
ежегодно в светлината на всякакви промени в дейностите на „НИДА ЕС“ ООД, както и всички допълнителни изисквания. Този регистър трябва да бъде на разположение по искане на надзорния орган.

5. Тази политика се прилага за всички служители, работници и заинтересованите страни на „НИДА ЕС“ ООД, както и по отношение на външните доставчици. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-кратък възможен срок на съответните държавни органи.

6. Партньори и трети лица, които работят с или за „НИДА ЕС“ ООД, както и които имат или могат да имат достъп до личните данни, ще се очаква да се запознаят, разбират и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от „НИДА ЕС“ ООД, без предварително да е сключила **Договор между Администратор и Обработващ**
, което налага на третата страна задължения, не по-малко обременяващи от тези, които „НИДА ЕС“ ООД е поело, и което дава право на дружеството да извършва проверки на спазването на наложените със споразумението задължения. Последното не се прилага, доколкото третите страни имат право на достъп съгласно разпоредба на нормативен акт.

1. **ЗАДЪЛЖЕНИЯ И РОЛИ ПО РЕГЛАМЕНТ (ЕС) 2016/679**

1. „НИДА ЕС“ ООД е Администратор на данни съгласно Регламент (ЕС) 2016/679.

2. Управителят на „НИДА ЕС“ ООД е отговорният орган по управление на системата за управление на лични данни, както и за разработване и насърчаване на добри практики в областта на обработване на информация в предприятието.

3. Отговорникът по защита на данните (по-долу ОЗД), с роля определена в Регламент (ЕС) 2016/679, е упълномощено и отговаря за управлението на личните данни в рамките на дружеството и за гарантирането на възможността за доказване на съответствието със законодателството за защита на данните и добрите практики. Тази отчетност на ОЗД включва периодичен преглед на документацията на системата за управление на лични данни съгласно изкисванията на РЕГЛАМЕНТ (ЕС) 2016/679 и управление на сигурността и риска по отношение на съответствието с политиката. Задачите и функциите на
ОЗД са определени в
Длъжностна характеристика на ОЗД
.

4. Отговорникът по защита на данните поема отговорността за съответствието на дейността на „НИДА ЕС“ ООД с тази политика на ежедневна основа. ОЗД е пряко отговорен да гарантира, че както като цяло организацията на „НИДА ЕС“ ООД, така и дейността на всеки член на ръководния състав, която се извършва в рамките на неговата област на отговорност, съответстват на изискванията на Регламент (ЕС) 2016/679.

5. ОЗД има специфични отговорности по отношение на **„Процедура за управление на исканията от субектите“** и
следва да бъде контактна точка за служителите на администратора, които искат разяснения по всеки аспект на спазването на защитата на данните.

6. Спазването на законодателството за защита на данните е отговорност на всички служители
на
„НИДА ЕС“ ООД
, които обработват лични данни.

7. **Политиката за провеждане на обучения** в „НИДА ЕС“ ООД определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите/работници
в дружеството.

1. **ПРИНЦИПИ ЗА ЗАЩИТА НА ДАННИТЕ**

Обработването на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на „НИДА ЕС“ ООД имат за цел да гарантират спазването на тези принципи.

1. **Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно** .

Законосъобразно – да се идентифицира законна основа, преди да може да се обработват лични данни. Законната основа често е посочвана като „основания за обработване“, например „законово задължение“, „съгласие на субекта“ или „изпълнение на договор“.

Добросъвестно - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са

получени директно от субектите на данни или от други източници. Регламент (ЕС) 2016/679 определя изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхванатата от изискването за „прозрачност“.

Прозрачно – Регламентът включва правила относно предоставяне на поверителна информация на субектите на данни. Известията за поверителност следва да са подробни и конкретни, разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език. Правилата за уведомяване на субекта на данни от
„НИДА ЕС“ ООД
са определени в
Процедура за прозрачност при обработката на лични данни
.
Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора, данните за контакт на администратора и на представителя на администратора;
- контактите на ОЗД;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат да се събират само за конкретни, изрично указани и законни цели.

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, официално обявени в **Регистъра на дейностите по обработване на данни** на „НИДА ЕС“ ООД. **Процедурата за прозрачност при обработката на лични данни** определя съответните правила.

3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел. (принцип на минимално необходимото **)**

- ОЗД е отговорно да осигури, че „НИДА ЕС“ ООД не събира информация, която не е необходимо за целта, за която тя е получена.

- Доколкото е приложимо в дейността на дружеството (например при обработване на лични данни на основание „съгласие“), всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват **Съгласие за обработване на лични данни** и да бъдат одобрени от ОЗД.

- Отговорникът по защита на данните следва да гарантира, че всички способи за събиране на данни се преглеждат периодично, за да се осигури, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни.

4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

- Данните, които се съхраняват от администратора на данни, трябва да бъдат прегледани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите когато има вероятност да не са точни.
- Отговорникът за защита на данните е отговорен да гарантира, че целият персонал е обучен в значението на събирането на точни данни и поддържането им.
- Също така, задължение на субекта на данните е да декларира, че данните, които предава за съхраняване в „НИДА ЕС“ ООД са точни и актуални. Попълването на формуляр от субекта на данни, предназначени за администратора, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване (когато е приложимо).

- От служителите/работниците трябва да се изисква да уведомяват „НИДА ЕС“ ООД за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни.

- Отговорникът по защита на данните носи отговорност да се гарантира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени, както и други относими фактори.

- Най-малко на годишна база Отговорникът по защита на данните преглежда сроковете на съхранение на всички записи с лични данни, обработвани от „НИДА ЕС“ ООД
, като се позовава на инвентаризацията на данните и идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

- Отговорникът по защита на данните е отговорен за съответствие с искания за корекция на данни в рамките на един месец съгласно
Процедура за управление на исканията от субектите
. Този срок може да бъде удължен с още два месеца за сложни заявки. Ако „НИДА ЕС“ ООД
реши да не се съобрази с искането, Отговорникът по защита на данните трябва да отговори на субекта на данните, за да обясни мотивите си и да го информира за правото му да подаде жалба пред надзорния орган (Комисия за защита на личните данни), и да потърси правна защита.

- Отговорникът за защита на данните е отговорен за вземане на подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни. Той следва да ги информира, че информацията е неточна или остаряла и да не се използва за вземане на решения относно лицата. ОЗД следва да информира съответните страни и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5. Личните данни трябва да се съхраняват в такава форма, че субектът на данните може да бъде идентифициран само толкова дълго, колкото е необходимо за целите на обработването.

- Когато личните данни се запазват след датата на обработването, те ще бъдат съх ранявани по подходящ начин
,
за да се защити по най-добър начин самоличността на субекта на данните в случай на нарушение на данните.

- Лични данни се пазят в съответствие с **Процедурата за съхраняване и унищожаване на данните** и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания в споменатата процедура ред.

- Отговорникът за защита на данните специално трябва да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в **Процедурата за съхраняване и унищожаване на данните** и трябва да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност. При определянето на това доколко уместно е обработването, Отговорникът по защита на данните трябва да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или клиенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите. При оценяването на подходящи технически мерки, Отговорникът по защита на данните ще разгледа следното:

- Ограничаване на достъпа до помещения, в които се съхраняват лични данни;
- Заключване на хартиени документи с лични данни в метални шкафове;
- Осигуряване с пожароизвестителни и пожарогасителни системи;
- Осигуряване със сигнално-охранителна техника;
- Защита с пароли на компютри;
- Автоматично заключване на бездействащи работни станции;
- Антивирусен софтуер и защитни стени;
- Правата за достъп основани на роли;
- Защитата на устройства, които напускат помещенията на дружеството като лаптопи или други;
- Сигурност на мрежите;
- Сигурност на служебните пощи;

При оценяването на подходящите организационни мерки Отговорникът за защита на

данните взима предвид следното:

- Нивата на подходящо обучение в „НИДА ЕС“ ООД;
- Мерките, които отчитат надеждността на служителите;
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до записи на хартиен или електронен носител;
- Контрол върху спазването на политиката „чисти бюра и чисти екрани“;
- Контрол върху спазването на правилата относно сложността на паролите;
- Редовно създаване на резервни копия на записите с лични данни.

Тези контроли са избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват.

7. Спазване на принципа на отчетност

Принципът на отчетност изисква администраторът да докаже, че спазва останалите принципите в ОРЗД. „НИДА ЕС“ ООД ще доказва спазването на принципите за защита на данните чрез прилагане на настоящата политика за защита на данните, процедурите и другите документи от системата за управление на личните данни, чрез внедряване на подходящи технически и организационни мерки и спазване на вече внедрените такива, както и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране.

1. **ПРАВА НА СУБЕКТИТЕ НА ДАННИ**

1. Всеки субект на данни има следните права по отношение на обработването на данни, както и на данните, които се записват за него/нея:

- Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;
- Да поиска копие от своите лични данни от администратора;
- Да иска от администратора коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг;
- Да се обърне с жалба до надзорен орган, ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
- Да поиска да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие.

2. „НИДА ЕС“ ООД осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е регламентирано в **Процедурата за управление на исканията от субектите**. Цитираната процедура също така описва как „НИДА ЕС“ ООД ще гарантира, че отговорът на искането на субекта на данни отговаря на изискванията на Общия регламент за защита на данните.

- Субектите на данни имат право да подават жалби до „НИДА ЕС“ ООД, свързани с обработването на личните им данни. Обработването на искане от субекта на данни и обжалването от страна на субекта на данни, относно начина на обработване на жалбите следва да се провеждат в съответствие с **Процедура за начините на комуникация при жалби и искания от субекта на данни**
.

1. **СЪГЛАСИЕ**

В дейността на „НИДА ЕС“ ООД най-голям обем от лични данни се обработва на законосъобразните основания (съгласно чл. 6 ОРЗД) - „Изпълнение на законово задължение“ и „Изпълнение на договорни отношения“. В редки случаи (например при поискване от страна на клиентите на дружеството да получават маркетингови съобщения и оферти) основанието би следвало да бъде „съгласие от субекта на данни“. Дружеството приема следните правила във връзка с възможни хипотези, при които ще се обработват лични данни на основание „съгласие на субекта“:

1. Под „съгласие“ „НИДА ЕС“ ООД ще разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.

2. „НИДА ЕС“ ООД разбира под „съгласие“ само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване.

4. За специални категории данни трябва да се получи изрично писмено съгласие на субектите на данни, освен ако не съществува алтернативно законно основание за

обработване.

1. **СИГУРНОСТ НА ДАННИТЕ**

1. Всички служители/работници са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които „НИДА ЕС“ ООД държи, както и че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако „НИДА ЕС“ ООД не е дало такива права на тази трета страна, като са сключили **Договор между Администратор и Обработващ**.

2. Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените вътрешни правила за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- във физическа среда - в самостоятелни стаи с контролиран достъп и/или в заключени шкафове;
- в компютърна среда – защита с парола в съответствие с вътрешните изисквания, посочени в организационните и технически мерки за контролиране на достъпа до информация; или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

3. Създадена е организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители/работници на „НИДА ЕС“ ООД. От всички служители/работници се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат съхранени или унищожени в съответствие със създадена за това **Процедура за съхраняване и унищожаване на данни.**

5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с **Процедурата за съхраняване и унищожаване на данните**
. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като „поверителни отпадъци“. Данните върху твърдите дискове на персонални компютри трябва да бъдат изтрити съгласно
Процедурата за съхраняване и унищожаване на данни.

6. Обработването на лични данни „извън офиса“ представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

1. **РАЗКРИВАНЕ НА ДАННИ**

1. „НИДА ЕС“ ООД трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители/работници трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от организацията. Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на лични данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Отговорникът за защита на данните.

1. **СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ**

1. „НИДА ЕС“ ООД не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

2 Периодът на съхранение за всяка категория на лични данни е посочен в **Графика за събиране и унищожение на категориите данни**
.

3. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

1. **ТРАНСФЕР НА ДАННИ**

Всеки износ на лични данни от рамките на ЕС към страни извън ЕС (посочени в Общия регламент като „трети страни“) е незаконен, освен ако няма подходящо „ниво на защита на основните права на субектите на данни“. „НИДА ЕС“ ООД не осъществява трансфер на лични данни към други държави, включително такива извън ЕС.

1. ИНВЕНТАРИЗАЦИЯ НА ДАННИТЕ

1. „НИДА ЕС“ ООД е направило първоначална инвентаризация на данните в **Регистъра на дейностите по обработване**
като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламент (ЕС) 2016/679. При инвентаризацията на данните в „НИДА ЕС“ ООД са напълно установени:

- процесите, които използват лични данни;
- източниците на лични данни;
- категориите субекти на данни;
- описание на категориите лични данни и елементите на всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването;

- получателите или категориите получатели на личните данни;

- основните системи и места за съхранение;
- липсата на лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

2. Отговорникът по защита на данните прави **ежегоден** преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в
Регистъра на дейностите по обработване
в светлината на всякакви промени в дейностите на „НИДА ЕС“ ООД.