ПОЛИТИКА ЗА ПОВЕРИТЕЛНОСТ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В НСНИ

1. ВЪВЕДЕНИЕ

1.1. „Национално сдружение недвижими имоти" (наричано за кратко „*НСНИ“, „сдружението“ или „Администратора“*) е юридическо лице с нестопанска цел, регистрирано в Търговския регистър към Агенция по вписванията с ЕИК: 000682469 и седалище и адрес на управление: гр. София, бул. „Патриарх Евтимий“ № 36-А и Интернет страница https://www.nsni.bg/

1.2. НСНИ има за основна цел защитата и гарантирането на професионалните интереси и авторитета на неговите членове и на останалите граждани и лица при осъществяването на посреднически и други услуги при сделки с недвижими имоти. За постигането на тази цел НСНИ се стреми да въздейства върху пазара на недвижими имоти чрез създаване на високи професионални критерии за работа при осъществяването на посреднически и други услуги при сделки с недвижими имоти, да утвърждава етичния и професионален кодекс на членовете си. Чрез създадената Национална академия за недвижими имоти, представляваща център за професионално обучение към НСНИ, се организират обучения и курсове за повишаване квалификацията на членовете си и други лица и се предоставя възможност на заинтересуваните лица да придобият професионалната квалификация „Брокер на недвижими имоти“.

1.3. НСНИе Администратор на лични данни по смисъла на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-долу „ОРЗД“) и Закона за защита на личните данни (наричан по-долу „ЗЗЛД“).

1.4. С настоящата Политиката за поверителност и защита на личните данни (наричана по-долу за краткост „Политика“) НСНИ отчита неприкосновеността на личността и полага усилия за защита срещу неправомерно обработване на личните данни на физическите лица. В съответствие с българското законодателството, ОРЗД и добрите практики, НСНИ е взело необходимите технически и организационни мерки за защита на личните данни на физическите лица.

Запознаването с настоящата Политика преди използване на нашите услуги е наложително, тъй като предоставянето им е свързано със събиране на определени категории лични данни, необходими на НСНИ за пълноценното предоставяне на услугите.

2. ЦЕЛИ И ОБХВАТ НА ПОЛИТИКАТА

2.1. С настоящата Политиката за поверителност и защита на личните данни НСНИ цели да информира физическите лица относно:

2.1.1. целите и средствата на обработване на личните данни;

2.1.2. получателите или категориите получатели, на които могат да бъдат разкрити данните;

2.1.3. основанието за обработване на личните данни /задължителния или доброволния характер на предоставяне на данните/, както и последиците при отказ за предоставянето им;
2.1.4. информация за правото на достъп, за правото на коригиране и заличаване на събраните данни.

3. ТЕРМИНИ И ДЕФИНИЦИИ

3.1. „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;
3.2. „Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработването 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;
3.3. „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;
3.4. „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;
3.5. „Съвместни Администратори“ – когато двама или повече Администратори съвместно определят целите и средствата за обработване на лични данни, те са съвместни Администратори;
3.6. „Обработващ лични данни“ – физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на Администратора
3.7. „Регистър“ - означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

3.8. „Субект на данните“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.
3.9. „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;
3.10. „Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработването 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;
3.11. „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;
3.12. „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;
3.13. „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;
3.14. „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;
3.15. „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;
3.16. “Разкриващ лични данни” – страна по Договор, която предава на Получател лични данни на физически лица, които обработва.

4. ПРАВНО ОСНОВАНИЕ ЗА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ, ИЗТОЧНИЦИ НА ЛИЧНИ ДАННИ И СРОК, ЗА КОЙТО СЕ СЪХРАНЯВАТ СЪБРАНИТЕ ЛИЧНИ ДАННИ

4.1. НСНИ обработва лични данни на следните основания:

4.1.1. Въз основа на свободно, информирано и изрично съгласие на субекта на данните;

4.1.2. При наличие на законово задължение за обработване на данните;

4.1.3. При сключване или изпълнение на договор, както и за действия, предхождащи сключването на договор;

4.1.4. Когато това е необходимо за защита на жизненоважни интереси на физическото лице или легитимният интерес на Администратора, при положение че той не противоречи на законните интереси на физическото лице

4.2. НСНИ обработва лични данни, предоставени от служители, клиенти, възложители, доставчици, контрагенти и други физически лица, за които се отнасят данните във връзка с предоставяне на услуги от предмета на дейността си, както и за подготовка и сключване на договори.

4.3. НСНИ обработва и лични данни, които не са получени от физическото лице, за което се отнасят, а са предоставени от трето лице във връзка с конкретна услуга, като лицето, предоставило тези данни на НСНИ се задължава:

4.3.1. да предостави на третото лице данни за Администратора;

4.3.2. да уведоми третото лице за целите, категориите предоставени данни и категориите получатели на тези данни;

4.3.3. да предостави информация за правото на достъп и на коригиране на лични данни на лицето, за което се отнасят.

4.4. Лични данни се съхраняват за период, необходим съгласно целите, за които те са събрани или за срок, установен в нормативен акт.

4.5. При дадено съгласие от субекта на лични данни за директен маркетинг, личните данни се съхраняват докато същият не се отпише или поиска да бъде отписан.

5. СРЕДСТВА, ПРИНЦИПИ И ЦЕЛИ НА ОБРАБОТВАНЕТО

5.1. НСНИ обработва лични данни чрез съвкупност от действия, които могат да се извършват с автоматични или други неавтоматични средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространение, предоставяне, актуализиране или комбиниране, блокиране, заличаване и унищожаване.

5.2. НСНИ обработва личните данни самостоятелно или чрез възлагане на обработващи данните, като с писмен договор определя целите и обемът на задълженията, възложени от Администратора на обработващия данните, при наличие на релевантно правно основание, съгласно изискванията на ОРЗД/ЗЗЛД. Обработващи от името на НСНИ се явяват например служителите на Администратора, чиито права и задължения, във връзка с обработването на лични данни на физически лица са надлежно регламентирани във вътрешни актове на Администратора, както и в трудовите характеристики на съответните служители. Обработващи са и трети лица

извън структурата на Администратора, на които е възложено обработването на лични данни от името на Администратора.

5.3. Посочените действия по обработване се извършват при спазване на следните принципи:

5.3.1. Законосъобразност, добросъвестност и прозрачност на обработването на лични данни;

5.3.2. целесъобразност на обработването на лични данни;

5.3.3. пропорционалност на обработването на лични данни;

5.3.4. актуалност на обработваните лични данни;

5.4. Във връзка с изпълнение на нормативно установени задължения и преддоговорни, и договорни отношения, при осъществяване на своята дейност, НСНИ обработва лични данни на своите служители, клиенти и на трети лица, за следните цели:

5.4.1. администриране на трудовоправни отношения: лични данни на лица, кандидатстващи за работа и служители по повод съществуващо трудово правоотношение (обработването на данни е най-често вследствие на изпълнение на нормативно установени задължения на Администратора на лични данни, произтичащи от спецификата на изискванията на законодателството, регламентиращо дейността му, финансово-счетоводната дейност, пенсионна, здравна и социално-осигурителна дейност, дейността по управление на човешките ресурси, автоматичния обмен на информация в областта на данъчното облагане и други);

5.4.2. администриране на договорни отношения: лични данни на лица преди договор за услуга и настоящи клиенти (включително когато е дадено изрично съгласие или 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 искане на лицето).

6. КАТЕГОРИИ ОБРАБОТВАНИ ЛИЧНИ ДАННИ

6.1. Категории лични данни, които НСНИ обработва за осъществяване на своята дейност:

6.1.1. Свързани с физическата идентичност на физическите лица – име, ЕГН, паспортни данни, данни от шофьорска книжка, адрес, телефон, e-mail, и др.;

6.1.2. Свързани с икономическата идентичност – имотно и финансово състояние, участие и/или притежание на дялове, ценни книжа в дружества, наличие на публични задължения, данни, необходими за идентифициране за целите на данъчното законодателство на територията на юрисдикцията, където лицето е местно лице за данъчни цели, данъчен идентификационен номер, издаден от тази юрисдикция, функция на контролиращи лица и др.;

6.1.3. Свързани със социалната идентичност – образование, трудова дейност, гражданство, постоянно местопребиваване;

6.1.4. Свързани със семейната идентичност - семейно положение, родствени връзки и др.;

6.2. Лични данни, отнасящи се до здравословното състояние, се обработват само по отношение на служителите, във връзка с изпълнение на нормативно установени

задължения на НСНИ в областта на трудовото и осигурително законодателство, при спазване изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и/или на правен акт на Република България, уреждащ материята.

6.3. НСНИ **не** обработва лични данни, които:

6.3.1. разкриват расов или етнически произход;

6.3.2. разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;

6.3.3. се отнасят до генетични и биометрични данни, които се обработват за целите единствено на идентифицирането на физическо лице;

6.3.4. се отнасят до сексуалния живот или сексуалната ориентация на физическото лице или до човешкия геном.

7. РЕГИСТРИ

7.1. НСНИ води следните регистри на дейностите по обработване на лични данни:

7.1.1. Подбор на персонал

7.1.2. Персонал

7.1.3. Клиенти

7.1.4. Контрагенти

7.1.5. Видеонаблюдение

8. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

8.1. **Право на информация, достъп до личните данни и преносимост на данните**

8.1.1. Субектът на данни има право на информация за целите на обработване на личните му данни, която му се предоставя при събиране на личните му данни и при последваща промяна на целите на обработването.

8.1.2. Субектът на данни има правото да изисква потвърждение дали се обработват негови лични данни и да получи информация относно вида лични данни, обработвани от НСНИ, които го засягат лично. Тази информация следва да бъде предоставена независимо от мястото, където личните данни се обработват. Субектът на данни може да отправи искане за достъп до лични данни към администратора, включително чрез отговорника за защита на личните данни на НСНИ.

8.1.3. Когато обработването на лични данни става по автоматичен начин, субектът на данните има и правото да получава отнасящите се до него лични данни, които той е предоставил на администратора, в структуриран, широко използван, пригоден за машинно четене и оперативно съвместим формат, и да ги предава на друг администратор. Това право се прилага, когато субектът на данни е предоставил личните данни въз основа на собственото си съгласие или обработването е необходимо поради договорно задължение. Правото не се прилага, когато обработването се базира на правно основание, различно от съгласие или договор. При упражняването на това право НСНИ съдейства на субекта като му предостави, по възможност, обработваните за него лични данни в желания от него формат, който трябва да бъде структуриран, в широко

използван и пригоден формат за машинно четене. Тази информация се предоставя на субекта съгласно приета от НСНИ процедура.

8.2. **Право на корекция**

8.2.1. Ако съхраняваните лични данни са некоректни или непълни, субектът на данни може да изиска те да бъдат коригирани.

8.2.2. Субектите на данни са отговорни за предоставянето на коректни лични данни на Администратора. В допълнение към това, субектът на данните следва да информира Администратора относно всякакви релевантни промени в личните му данни, като, но не само, промени в адреса или името на субекта.

8.3. **Ограничаване на обработването**

8.3.1. Във всеки момент от обработването на личните данни, субектът на данни може да поиска от Администратора да ограничи използването на личните му данни за част или всички цели на обработването, за което субектът е дал съгласие.

8.3.2. Субектът на данни има право да изиска от Администратора да ограничи обработването на данните му в следните случаи:

8.3.2.1. точността на личните данни се оспорва от субекта на данни, за срока, който е необходим да се извърши проверка на точността на личните данни

8.3.2.2. когато обработването е неправомерно, но субектът на данни не желае личните му данни да бъдат изтрити, а изисква вместо това да се ограничи използването им

8.3.2.3. когато Администратора не се нуждае повече от личните данни за целите на обработването, но субектът на данни ги изисква за установяването, упражняването или за защитата на правни претенции

8.3.2.4. субектът на данни е възразил срещу обработването и е в очакване на проверка от страна на Администратора дали законните му основания имат преимущество пред неговите интереси.

8.3.3. Когато обработването на данни е ограничено съгласно условията на т.8.3.2., такива данни се обработват, с изключение на съхранението им, само със съгласието на субекта на данни или в случай на необходимост от установяването, упражняването или защитата на правни претенции или за защитата на правата на други физически лица или поради важни основания от обществен интерес.

8.4. **Отказ на искане за информация, корекция или ограничаване на обработването на лични данни**

8.4.1. Ако искането за информация, корекция или ограничаването на обработването бъде отказано, субектът на данни ще бъде информиран относно причината за съответния отказ.

8.4.2. Отказът се прави във вида на подаденото искане от субекта и следва да бъде мотивиран.

8.5. **Право на изтриване („право да бъдеш забравен“)**

8.5.1. Субектът на данни има право да поиска от Администратора изтриване на свързаните с него лични данни, а Администраторът има задължението да ги изтрие без ненужно забавяне, ако:

8.5.1.1. данните вече не са необходими за първоначалната цел и не съществува

нова законосъобразна цел
8.5.1.2. законното основание за обработването е съгласие на субекта на данни и той оттегли това съгласие, и липсва друго правно основание за обработване
8.5.1.3. субектът на данни възразява срещу обработването на данни и липсва друго правно основание за обработване
8.5.1.4. личните данни са били обработвани незаконосъобразно
8.5.1.5. личните данни трябва да бъдат изтрити с цел спазване на правно задължение, произтичащо от законодателство, което се прилага спрямо Администратора
8.5.1.6. личните данни са събрани във връзка с предлагане на услуги на информационното общество на субект на данни – дете.
8.5.2. При упражняване на това право от страна на субекта на данни, Администраторът указва на субекта по какъв начин изтриването ще засегне отношенията между тях занапред.
8.5.3. Правото на изтриване на данните на субекта на данни не следва да се прилага от дружеството, доколкото обработването е необходимо:
8.5.3.1. за изпълнение от Администратора на правно задължение, предвидено в законодателството, което изисква обработване на данните
8.5.3.2. за установяването, упражняването или защитата на правни претенции на Администратора.

8.6. **Право на възражение**
8.6.1. Субектът на данни има право да възрази срещу обработването на лични данни, отнасящи се до него. Администраторът прекратява обработването на лични данни, освен ако не докаже, че съществува законово основание за продължаване на обработването.
8.6.2. Освен това, всеки субект на данни има право да възрази, ако личните му данни се ползват за рекламни цели (директен маркетинг) или за цели, свързани с проучване на пазара или общественото мнение. В този случай личните данни следва да бъдат блокирани и да не бъдат използвани за съответните цели.

8.7. **Оттегляне на съгласие за обработване на лични данни**
8.7.1. Субектът на лични данни има право да оттегли съгласието си за обработване на личните му данни по всяко време с отделно искане, отправено до Администратора.
8.7.2. Администраторът указва на субекта по какъв начин изтриването ще засегне отношенията между тях занапред.

8.8. **Искания и жалби. Средства за правна защита на субекта на данни.**
8.8.1. Субектът на данни има право да подава искания и жалби до Администратора, свързани с обработването на личните му данни., на които Администраторът реагира в съответствие с приета процедура.
8.8.2. За упражняване на тези свои права, Субектът се обръща към Администратора чрез искане в свободен текст или като използва приети от Администратора образци на заявления, отправено на имейл или чрез писмо, изпратено до гр. София, бул. „Патриарх

Евтимий“ № 36-А на което Администраторът отговаря в съответствие с приета процедура.

8.9. **Право да изрази съгласие за обработване на личните му данни**

8.9.1. За наличие на съгласие Администраторът приема само в случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие, без върху него да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, не е валидно основание за обработване на лични данни.

8.9.2. 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 следва да може да докаже, че е получено съгласие за дейностите по обработване.

8.9.3. В повечето случаи, съгласието за обработване на лични данни се получава от Администратора, като се използват стандартизирани документи за съгласие, например, когато нов клиент подписва договор или по време на набиране на нов персонал.

8.9.4. При обработване на лични данни на деца, Администраторът следва да получи разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години (освен ако държавата-членка не е предвидила по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

8.10. **Право на представителство**

8.10.1. Субектът на данни може да упълномощи друго лице да упражнява правата по т. 8.1. до т. 8.8. от настоящата политика.

8.10.2. Упълномощаването следва да бъде изрично и направено в писмена форма.

8.10.3. При всяко едно упражняване на правата на субекта на данни, пълномощникът е длъжен да представи копие от пълномощното си на Администратора или на обработващият лични данни от името на Администратора.

9. ОБЩИ ПРИНЦИПИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО И СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

9.1. **Допустимост на обработването на данните**

9.1.1. Обработването на лични данни е допустима единствено ако субектът на данните се е съгласил с това, ако е налице законово задължение за обработване на данните, при сключване или изпълнение на договор, когато е необходимо за защита на жизненоважни интереси на физическото лице или легитимният интерес на Администратора, при положение че той не противоречи на законните интереси на физическото лице. Допустимостта на обработването на личните данни е предпоставка за предаване на лични данни.

9.1.2. Съгласието следва да бъде декларирано в писмена форма или въз основа на други законово допустими средства, а субектът на данните трябва да бъде уведомен предварително относно целта на обработването и възможността за предаване на лични данни на трети страни. Върху предоставянето на съгласие се поставя акцент, когато се включва в други декларации, така че да бъде ясно за субекта на данните.

9.2. **Предвидена цел**

9.2.1. Лични данни могат да бъдат събирани единствено за изчерпателно изброените цели и не могат да бъдат обработвани за цели, различни от предвидените.

9.2.2. Целта на събиране и обработване на данните трябва да бъде съобразена от Администратора при допълнително обработване и съхраняване на такива данни.

9.2.3. Промени в целта са допустими единствено със съгласието на субекта на данните или ако това е разрешено от местното законодателство на съответната държава, от която са получени личните данни.

9.3. **Икономия на данните**

9.3.1. Обработването на лични данни трябва да бъде необходимо за предвидената цел.

9.3.2. Наличните възможности за анонимизация или въвеждане на псевдонимизация за личните данни трябва да се използват на ранен етап, доколкото това е възможно и рентабилно за предвидената защитна цел.

9.4. **Качество на данните**

9.4.1. Личните данни трябва да бъдат фактически верни и, доколкото е необходимо, актуални.

9.4.2. Администраторът предприема подходящи и разумни мерки за коригиране или изтриване на неправилните или непълни данни.

9.5. **Сигурност на данните**

9.5.1. Администраторът на данните въвежда подходящи технически и организационни мерки, за да осигури необходимата сигурност на данните.

9.5.2. Тези мерки се отнасят в частност до компютрите (сървъри и работни места), мрежите и комуникационните връзки и приложения, като те са инкорпорирани в системата за управление на ИТ сигурността, чрез подходящи мерки за защита на тези данни от изтриване по погрешка, неоторизирано изтриване или изгубване (информация в тази връзка е представена в Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).

9.6. **Поверителност на обработването на данните**

9.6.1. Единствено оторизиран персонал, който се е ангажирал да спазва изискванията за поверителност на данните, има право да участва в обработването на лични данни.

9.6.2. На служителите е забранено да използват такива данни за лични цели или да ги предоставят на неоторизирани дружества и трети страни. Неоторизирани в този контекст означава и използването на лични данни от служители, които не се нуждаят от достъп до такива данни, за да изпълняват служебните си отговорности.

9.6.3. Задължението за поверителност продължава да действа и след прекратяване на трудовите/гражданските/служебните правоотношения с Администратора.

10. МЕРКИ ЗА СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ

10.1. НСНИ осигурява сигурността на личните данни съгласно принципите, заложени в ОРЗД/ ЗЗЛД като взема подходящи и достатъчни технически и организационни мерки, за да осигури защита на данните от загуба, кражба, злоупотреба, както и от неоторизиран достъп, разкриване, промяна или унищожаване.

10.2. **Технически мерки за защита на личните данни**

10.2.1. За осигуряване на достатъчна защита на обработваните лични данни, НСНИ използва технически мерки като, но не само, защита от вируси, защитна стена, опция за криптиране/ шифроване и други.

10.2.2. Администраторът определя защитени зони за съхраняване на физическите носители на лични данни, достъпът до които се определя съгласно процедурни правила.

10.2.3. Администраторът въвежда следните мерки за ограничаване на достъпа до физическите носители на данни – (например поставени ключалки с високо ниво на защита на вратите на офиса на Администратора, както и на вратите, осигуряваща достъп до сградата, в която се намира офиса; заключване на шкафовете, в които се намират хартиени носители на данни).

10.3. **Организационни мерки за защита на личните данни**

10.3.1. НСНИ приема вътрешни правила, с които се определят нивата на чувствителност на обработваните лични данни (информация), въз основа на които се създават отделни категории лични данни, които биват обработвани за конкретни цели. Отделните категории лични данни се обособяват в регистри с лични данни. С вътрешните правила се определя както редът за достъп до тези регистри, така и лицата, които имат право да ги достъпват, респективно обработват съхранените в тях лични данни.

10.3.2. Администраторът приема процедурни правила, определящи мерките и реда за физически достъп и защита на личните данни, които са задължителни за всички служители, които извършват обработване на лични данни

10.3.3. Всички лични данни следва да са достъпни само за тези служители/ обработващи лични данни, в чиито задължения е включено обработването на конкретните данни, а достъпът се осъществява само в съответствие с приетите вътрешни правила за контрол на достъпа.

10.3.4. Всички служители на Администратора са отговорни за гарантирането на сигурността при съхранението на данните, които обработват, както и за това, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети лица, освен ако Администраторът не е предоставил такива права на тези трети лица въз основата на писмен договор или клауза за поверителност.

10.3.5. Администраторът въвежда политика на „чистото бюро“, с която всички служители, които обработват лични данни се запознават и прилагат. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни за неоторизирани лица и не могат да бъдат изваждани от определените защитени помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа по обработване на лични данни, те следва да бъдат архивирани по съответния ред, а ако липсва основание за тяхното архивиране, следва да бъдат унищожени в съответствие със създадена за това процедура.

10.3.6. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с приетата от Администратора процедура. Записите на хартиен носител, чиито срок за обработване е изтекъл, следва да бъдат нарязани (шредирани) и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на неизползвани персонални

компютри трябва да бъдат изтрити или дисковете унищожени, съгласно въведените процедури.

10.3.7. Обработването на лични данни извън обектите на Администратора се осъществява съгласно съответните процедурни правила и е допустимо с изрично писмено съгласие на прекия ръководител на обработващия лични данни или на Администратора.

10.3.8. Администраторът с вътрешен акт определя реда за контрол на отделянето на лични данни. Тези правила съдържат мерки, които да гарантират, че данните, събирани за различни цели, могат да се обработват отделно от оторизираните служители/ лица.

10.3.9. Във връзка с мерките, гарантиращи защитата на личната информация срещу случайно унищожаване или загуба, Администраторът определя процедури за възстановяване на наличността на лични данни след физически или технически инцидент. С оглед изпълнение на тези задължения, Администраторът осигурява необходимите технически средства като, но не само, сървъри, компютърна мрежа, облачно пространство.

10.4. **Отговорник по защита на данните**

10.4.1. НСНИ определя Отговорник по защита на личните данни (ОЗЛД). Отговорникът е служител на Администратора. Ролята на това лице е да следи за спазването на настоящата Политика в предприятието на Администратора и да гарантира възможността за доказване на съответствието на обработването на лични данни в съответствие със законодателството за защита на личните данни.

10.4.2. ОЗЛД разработва и внедрява изискванията за защита на личните данни съгласно разпоредбите на настоящата Политика. ОЗЛД извършва управление на сигурността и риска по отношение на съответствието с настоящата Политика.

10.4.3. ОЗЛД отговаря за администриране и обработване на исканията и жалбите, отправени от субекта на данни към Администратора. ОЗЛД дава необходимите разяснения на служителите на Администратора по повод спазване защитата на личните данни.

10.4.4. ОЗЛД периодично изготвя и представя отчети на Администратора във връзка с прилагане на настоящата Политика, нормативните разпоредби, уреждащи защитата на лични данни, както и за съответствието на осигурената защита на личните данни в предприятието с нормативните изисквания в тази област.

11. СЪХРАНЯВАНЕ, УНИЩОЖАВАНЕ И ИНВЕНТАРИЗАЦИЯ НА ЛИЧНИ ДАННИ

11.1. **Съхраняване**

11.1.1. НСНИ не съхранява лични данни във вид, който позволява идентифицирането на субектите за период, по-дълъг от необходимия за осъществяване на обработването, за което е дадено съгласието на субекта на лични данни и с оглед на целите, за които са били събрани. Съхраняване на лични данни за по-дълъг период е допустимо и без изричното съгласие на субекта на данни, ако е предвидено в нормативен акт на вътрешното законодателство или на правото на Европейския съюз

11.1.2. Администраторът може да съхранява данни за по-дълъг период от необходимия за извършване на обработването, за което е дадено съгласие и в случаите, когато личните данни ще бъдат обработвани за целите на архивиране в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните

11.1.3. Периодът за съхраняване на всяка категория лични данни, обособена в отделен регистър, се определя в приета от Администратора процедура. В тази процедура са посочени критериите, използвани за определяне на периода на съхранение, включително всякакви законови задължения вменени на Администратора по отношение съхранение на данните.

11.1.4. Процедурата за съхранение и унищожаване на данните, както и правилата за унищожаване на информацията върху физически носители се прилагат във всички случаи.

11.2. **Унищожаване**

11.2.1. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране на подходящо ниво на сигурност и приетата от Администратора процедура.

11.2.2. Спазването на процедурата е задължително с оглед гарантиране защитата срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане на данните, като се прилагат подходящи технически или организационни мерки.

11.3. **Инвентаризация и оценка на риска**

11.3.1. Администраторът извършва инвентаризация на данните и оценка на риска като част от своя подход за справяне с възможните рискове при обработване на събираните лични данни.

11.3.2. При инвентаризацията на данните и при тяхното обработване се извършва оценка на риска на личните данни, чиято методология и елементи са уредени с приета от Дружеството процедура. Определянето на рисковете съгласно тази методология се прилага и по отношение на обработването, предприето от други лица / организации от името на Администратора..

11.3.3. Когато се установи, че вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии, и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване, Администраторът извършва Оценка за въздействието върху защитата на личните данни съгласно приетата от Дружеството процедура за оценка на въздействието във връзка със защитата на данните и по заложената в същата процедура Методология за извършване на оценка на въздействието върху защитата на личните данни.

11.3.4. Когато в Оценка на въздействието върху защитата на личните данни е установено/указано, че операциите по обработването водят до висок риск, който Администраторът не може да ограничи с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди обработването се осъществява консултация с надзорния орган (КЗЛД).

11.3.5. ОЗЛД, прави периодичен преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ с оглед всякакви промени в дейностите на Администратора.

12. ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

12.1. Администраторът на лични данни има право да разкрие обработваните лични данни само на следните изчерпателно изброени категории лица:

12.1.1. физически лица, за които се отнасят данните

12.1.2. лица, за които правото на достъп е предвидено в нормативен акт или

12.1.3. лица, за които правото произтича по силата на договор.

12.2. С цел предоставяне на услуги, Администраторът разкрива информация /необходими лични данни/ за изпълнението на поето договорно задължение към субекта на лични данни. Администраторът предоставя лични данни на трети страни, които предоставят услуги от негово име въз основа на изрична писмена инструкция/ писмен договор. Тези трети страни нямат право да използват или разкриват данните извън целите, за които са им предоставени, освен когато това е необходимо за извършване на услуги от името на Администратора или за съобразяване със законови изисквания. Целите за обработване на предоставените лични данни са изрично определени в писмената инструкция/ писмения договор, въз основа на който данните са предоставени на третото лице. Третите лица (обработващи на лични данни) са задължени да осигурят необходимите технически и организационни мерки за защита на личните данни, предоставяни от Администратора или по-големи;

12.3. Администраторът разкрива получените лични данни на негови филиали, франчайзополучатели, дилъри и съвместни партньори въз основа на изрична писмена инструкция или писмен договор. Тези лица могат да използват информацията за целите, описани в настоящата Политика за защита на личните данни. При предоставено изрично съгласие от субекта на лични данни, последните могат да бъдат споделени с трети страни въз основа на писмен договор, за техни собствени цели, като например предлагане на продукти и услуги, които могат да представляват интерес за субекта на данни;

12.4. Администраторът разкрива лични данни на компетентни органи/ лица с оглед организиране защитата на законните си права и интереси при иницииране на заповедни, арбитражни, охранителни, искови и други производства;

12.5. Администраторът разкрива лични данни за субекти, чиито лични данни обработва, когато е задължен за това по закон, подзаконов нормативен акт, международен договор или акт на правото на Европейския съюз, или във връзка със съдебна процедура, в отговор на искане от държавни органи, (например правоприлагащи или разследващи органи), или при съмнение за сериозно и незаконосъобразно засягане законните права и интереси на субектите на правото.

13. ОБУЧЕНИЕ

13.1. Като има предвид уредбата на защитата на личните данни на физически лица и засилените мерки за защита на личните данни, въведени с ОРЗД/ ЗЗЛД, НСНИ отчита необходимостта от провеждане на първоначално и последващо обучение на своя

персонал, в задълженията на който е включено обработването на лични данни на физически лица от името на Администратора.

13.2. Първоначалното и последващите обучения имат за цел да информират служителите относно установените правила и процедури за спазването на настоящата Политика и приложимата нормативна уредба в сферата на защита на личните данни, както и други въпроси, свързани със защитата на личните данни и неприкосновеността на личния живот.

13.3. Чрез обученията на работниците и служителите се цели постигане на тяхната осведоменост относно вече наличните или нововъзникнали изисквания относно защитата на личните данни, както и предприетите от Администратора мерки в съответствие с тях.

14. ЗАДЪЛЖЕНИЯ И РОЛИ

14.1. Отговорникът по защита на данните следи за правилното разпределение на отговорностите на служителите във връзка със защитата на данните съобразно правилата и процедурите на Администратора за обработване на личните данни.

14.2. Отговорникът по защита на данните следва да гарантира, че всички служители, които имат текущи задължения, свързани с лични данни и операции по обработване, както и тези с постоянен/редовен достъп до лични данни, показват съответствие с изискванията за защита на личните данни.

14.3. Служителите трябва да могат да докажат компетентност в разбирането си относно изискванията за съответствие с нормативните изисквания, и как те се прилагат в организацията на Администратора.

14.4. Отговорникът по защита на данните носи отговорност, тези служители да актуализират своите познания и да бъдат информирани за всички въпроси, свързани с личните данни съгласно кръга на техните професионални задължения като организира текущи обучения при промяна в нормативната уредба на защитата на личните данни или при промяна в предмета на дейност на Администратора, както и при въвеждане на нови процедури/ мерки за защита на личните данни от Администратора.

14.5. Администраторът насърчава мерки за обучение и повишаване на осведомеността като предоставя необходимите ресурси и материална база за това.

14.6. Отговорникът по защита на данните запознава и информира служителите относно значението на защитата на данните в изпълнението на преките им задължения, и в съответствие с ролята им в организацията.

14.7. Отговорникът по защита на данните носи отговорност да се увери, че служителите разбират как и защо се прилагат правилата и процедурите в организацията на Администратора за обработването на личните данни, за което съставя съответните отчети/ протоколи.

14.8. Отговорникът по защита на данните разработва програми за обучение и информиране както за целият личен състав, така и за всяка конкретна роля в организацията, която има отношение към обработването на лични данни.

14.9. Отговорникът по защита на данните създава система за периодична проверка на осведомеността, както и за актуализиране на знанията на служителите във връзка с настъпили промени в изискванията по защита на данните.

14.10. Служителите получават конкретно обучение за обработване на лични данни, свързани с техните постоянни трудови роли и отговорности и в съответствие с правилата и процедурите, приети от Администратора.
14.11. Служителите получават конкретно обучение по всички изисквания и процедури за защита на информацията, приложими към защитата на данните и обработването на данни в рамките на техните ежедневни трудови роли и отговорности, включително докладване на нарушения на лични данни.
14.12. Служителите получават обучение относно постъпилите за разглеждане на искания и жалби от субекти на данните, свързани със защитата на личните данни и обработването на лични данни, съгласно правилата и процедурите на Администратора.
14.13. Отговорникът по защита на данните организира обучения за всички отговорни лица и служители.
14.14. Отговорникът по защита на данните документира всяко проведено обучение като за целта изготвя списък/протокол с присъствалите на съответните обучения, извършени в подходящо време според дейността на Администратора.
14.15. Първоначално обучение на служителите се провежда при привеждане в действие на настоящата политика, както и при постъпване на работа на нови служители, чиито трудови задължения включват обработване на лични данни.
14.16. Последващи обучения се провеждат периодично (не по-рядко от веднъж на 6 месеца) или при промяна в нормативната уредба на защитата наличните данни/ промяна в предмета на дейност на Администратора по отношение обработване на лични данни или при въвеждане на нови мерки/ процедури за защита.

15. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

15.1. Настоящата Политика е приета с Протокол № 4 от 26.04.2018 г. на Управителния съвет на НСНИ и влиза в сила от същата дата.;
15.2. Субектите на лични данни могат да се запознаят с настоящата политика в офиса на Дружеството, находящ се в гр. София, бул. „Патриарх Евтимий“ № 36-А, както и на сайта на Дружеството https://www.nsni.bg/ ;
15.3. Отговорник по защита на личните данни при НСНИ е:
15.3.1. име:Анастасия Велева
~~15.3.2. ……~~
~~15.3.3.~~15.3.2. адрес: гр. София, бул. „Патриарх Евтимий“ № 36-А
~~15.3.4.~~15.3.3. имейл адрес: veleva@nsni.bg