Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДП „НАЦИОНАЛНА КОМПАНИЯ
ЖЕЛЕЗОПЪТНА ИНФРАСТРУКТУРА”

ISO 9001 BUREAU VERITAS Certification

бул. „Мария Луиза” №110, София 1233
тел.: (+359 2) 932 37 64
факс: (+359 2) 932 24 04
c.ivanova@rail-infra.bg.

ОДОБРЯВАМ:

ИНЖ. КРАСИМИР ПАПУКЧИЙСКИ
ГЕНЕРАЛЕН ДИРЕКТОР

ПОЛИТИКА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДП НКЖИ

Настоящата политика за защита на личните данни се издава във връзка с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. 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 (Общ регламент относно защитата на данните) (Регламента), Закона за защита на личните данни (ЗЗЛД) и всички приложими към дейността му нормативни актове по защита на личните данни. Тя касае защитата на личните данни в контекста на изпълнение на правомощията и законовите задължения, които се прилагат спрямо ДП НКЖИ като управител на железопътната инфраструктура в България.

1. ДАННИ ЗА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Държавно предприятие „Национална компания „Железопътна инфраструктура“ (ДП НКЖИ) е Администратор на лични данни по смисъла на Регламента и ЗЗЛД, наричано по-нататък „Администратор“.

ДП НКЖИ е основен управител на железопътната инфраструктура в Република България.

ДП НКЖИ управлява предоставеното и имущество - публична и частна държавна собственост. Имуществото - публична и частна държавна собственост, се предоставя от държавата за изпълнението на предмета й на дейност с решение на Министерския съвет.

Компанията организира, осъществява и отговаря за изпълнението на задължения по дългосрочен договор, сключен с Държавата, планира цялостната дейност за развитие на железопътната инфраструктура в съответствие с него.

Основният предмет на дейност на Компанията е: осигуряване на равнопоставени условия при използването на инфраструктурата от лицензирани превозвачи; извършване на дейности по развитието, ремонта, поддържането и експлоатацията на железопътната инфраструктура; развива транспортните връзки и сътрудничеството с другите жп администрации; управление на влаковата работа в железопътната инфраструктура при спазване на изискванията за безопасност, надеждност и сигурност; приемане и изпълнение

на всички заявки заявителите за получаване на капацитет от железопътната инфраструктура, във връзка с изпълнение на възложените им задължения за извършване на обществени превозни услуги; осъществяване на инвестиционна политика при развитието, модернизацията, поддържането и ремонта на железопътната инфраструктура за реализация на европейските критерии и стандарти и др.

Организационната структура на ДП НКЖИ се състои от: Централно управление; Поделение „Железен път и съоръжения“ и неговите регионални поделения – Железопътни секции в София, Пловдив, Горна Оряховица, Враца, Шумен, Бургас; Поделение „Управление движението на влаковете и капацитета“ с регионални поделения – Управление движението на влаковете и гаровата дейност в София, Пловдив и Горна Оряховица; Поделение „Електроразпределение“, с регионални поделения – Енергосекции в София, Пловдив и Горна Оряховица и Поделение „Сигнализация и телекомуникации“, с регионални поделения - Секции в София, Пловдив и Горна Оряховица.

Администраторът обработва лични данни на физически лица във връзка с трудовото им правоотношение, както и на лица, които се намират в договорни отношения с ДП НКЖИ, като определя сам целите и средствата за обработването им, при спазване на всички приложими нормативни актове по защита на личните данни.

Личните данни се обработват самостоятелно от Администратора или чрез определени от него служители в ДП НКЖИ.

Седалище и адрес на управление на Администратора: бул. „Княгиня Мария Луиза“ № 110, София, 1233, електронна поща: office@rail-infra.bg, тел. 02/932 6062.

2. ДАННИ ЗА КОНТАКТ С ДЛЪЖНОСТНОТО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

По всички въпроси, свързани с обработването на Вашите лични данни и с упражняването на права, можете да се обърнете към определеното от ДП НКЖИ длъжностно лице по защита на личните данни - Цветелина Рангелова Иванова, на длъжност „служител, сигурност на информацията“, по Ваш избор на някой от посочените данни за контакт: телефон: 02932 3764/0888134691, електронен адрес за кореспонденция: : c.ivanova@rail-infra.bg.

За да упражните Вашите права, свързани с тази обработка на данни, можете да подадете искане по някой от посочените начини, като:

- изпратите искане за упражняване на права на хартиен носител на адрес: бул. „Мария Луиза” №110, София 1233

- подадете лично искане за упражняване на права на адрес: бул. „Мария Луиза” №110, София 1233

- изпратите искане за упражняване на права на електронна поща: office@rail-infra.bg, c.ivanova@rail-infra.bg.

3. РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ОТ 27 АПРИЛ 2016

Регламентът се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни.

Защитата на физическите лица във връзка с обработването на лични данни е основно право. Член 8, параграф 1 от Хартата на основните права на Европейския съюз („Хартата“) и член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС) предвиждат, че всеки има право на защита на личните му данни.

Обработването на лични данни следва да е предназначено да служи на човечеството. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано

във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност.

Като администратор на лични данни, ДП НКЖИ прилага принципите за обработване на лични данни и чрез настоящото съобщение предоставя информация и условия за упражняването на правата на субектите на данни съгласно чл. 13 и чл. 14 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. 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 (Общ регламент относно защитата на данните), наричан по-нататък Общ регламент.

Принципите и правилата на Общия регламент се прилагат по отношение на цялата информация, съдържаща лични данни, която се обработва във връзка с осъществяването на функциите на ДП НКЖИ. Информацията може да се съдържа както в документи на хартиен носител, така и в електронни документи, без значение дали са подписани с квалифициран електронен подпис или не.

4. ОПРЕДЕЛЕНИЯ

- ***„Лични данни“*** са 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;

- ***„Администратор“*** - 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;

- ***„Обработване“*** е 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;

- ***„Обработващ лични данни“*** - физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

- ***„Получател“*** - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

5. ПРИНЦИПИ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

При обработването на лични данни Администраторът спазва следните принципи:

- ***Законосъобразност, добросъвестност и прозрачност*** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

- ***Ограничение на целите*** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

- ***Свеждане на данните до минимум*** - Личните данни трябва да бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;

- ***Точност*** - Личните данни трябва да бъдат точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички мерки, за да се гарантира

своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

- ***Ограничение на съхранението*** - Личните данни се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в Регламента с цел да бъдат гарантирани правата и свободите на субекта на данните;

- ***Цялостност и поверителност*** - Личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;

- ***Отчетност –*** Администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

6. ПРАВА НА СУБЕКТА НА ДАННИ

Администраторът отчита, спазва и създава условия за упражняването на следните права на субекта на данни:

1. право да бъде информиран;
2. право на достъп;
3. право на коригиране;
4. право на изтриване/заличаване (или още „правото да бъдеш забравен“);
5. право на ограничаване на обработката;
6. правото на преносимост на данни (право на пряко прехвърляне на личните данни от един Администратор към друг);
7. правото на възражение;
8. права по отношение на автоматизираното вземане на решения и профилиране;
9. право на оттегляне на съгласие;
10. право на жалба до надзорен орган.

7. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Обработването на лични данни на физически лица в ДП НКЖИ е допустимо само в случаите, когато е налице поне едно от условията, а именно:

- Обработването е необходимо за спазването на законово задължение, което се прилага спрямо Администратора;
- Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- Обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
- Обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора;
- Субектът на данните е дал съгласие за обработване на личните му данни за една

или повече конкретни цели, като **попълва** ***Декларация - съгласие за обработване на лични данни от субекта на лични данни по образец- Приложение № 1 към настоящата политика.***

В ДП НКЖИ се обработват лични данни само за конкретни и законни цели, произтичащи от Закона за железопътния транспорт, Закон за държавната собственост и Правилника за прилагане на Закона за държавната собственост, Закон за устройство на територията, Правилника за устройството и дейността на ДП НКЖИ, Кодекса на труда, Закона за счетоводството, Закона за противодействие на корупцията и за отнемане на незаконно придобито имущество, Закон за здравословни и безопасни условия на труд, Правилника за реда за упражняване правата на държавата в търговските дружества с държавно участие в капитала, Търговския закон, Закона за обществените поръчки, Правилника за прилагане на Закона за обществените поръчки, Закона за управление на средствата от Европейските структурни и инвестиционни фондове, Наредбата за удостоверенията за електронен подпис в администрациите и други законови и подзаконови нормативни актове.

Всеки субект на данни ще бъде информиран (уведомен) за целите, за които се обработват личните му данни в срок до един календарен месец след събирането, в случай че данните са получени от трета страна. В случай, че данните се използват за връзка със субекта на данните, същият се уведомява най-късно при осъществяване на първия контакт с него.

Всеки субект на данни има право на достъп до личните си данни, обработвани и съхранявани в ДП НКЖИ, след подаване на ***писмено заявление по образец – Приложение № 2 към настоящата политика.***

Субектът на данни получава отговор на заявлението ***с уведомление по образец – Приложение № 3 към настоящата политика.***

Лицата, определени да обработват лични данни в определен информационен масив, нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения, за което преди обработването, задължително подписват Декларация за поверителност, която се съхранява в личното досие на всеки служител.

В случаите, когато се обработват лични данни на дете, във връзка с ползване на отпуски по Кодекса на труда и Наредбата за работното време, почивките и отпуските за отглеждане на дете и с оглед спазване на изискването за специална защита на личните данни на деца, родителят задължително подписва Декларация за съгласие за обработване на лични данни на дете.

8. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Физическата защита на личните данни в ДП НКЖИ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Основните организационни мерки за физическа защита включват:

1. определяне на помещенията, в които се обработват лични данни;

2. определяне на помещенията, в които се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;

3. определяне на организацията на физическия достъп.

Като помещения, в които се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и

контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния масив с лични данни. Когато в тези помещения имат достъп и външни лица, в тях се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

Организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Зони с контролиран достъп са всички помещения на територията на ДП НКЖИ, в които се събират, обработват и съхраняват лични данни.

Използваните технически средства за физическа защита на личните данни са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на служебните им задължения.

Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Основните технически мерки за физическа защита включват:

- Използване на сигнално-охранителна техника;
- Използване на ключалки и заключващи механизми;
- Използване на шкафове и метални каси;
- Използване на помещения, които са оборудвани с пожароизвестителни и пожарогасителни средства.

Документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично определените лица (по силата на служебните им задължения или със заповед на Администратора).

Оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица, заключваеми шкафове и пожарогасителни средства.

Пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Основните мерки за персонална защита на личните данни са:

- Задължение на служителите е да се запознаят с нормативната уредба в областта на защитата на лични данни и

- Запознаване и осъзнаване за опасностите за личните данни, обработвани от ДП НКЖИ;

- Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п.) между служителите и всякакви други лица, които са неоторизирани;

- Деклариране на съгласие за поемане на задължение за неразпространение на личните данни, чрез попълване на декларация за поверителност.

Основните мерки за документална защита на личните данни, са:

- Определяне на масивите, които ще се поддържат на хартиен носител - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на ДП НКЖИ, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;

- Определяне на условията за обработване на лични данни - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на предприятието, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

- Регламентиране на достъпа до масивите с лични данни – достъпът до масивите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;

- Определяне на срокове за съхранение - личните данни се съхраняват не по-дълго отколкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.

- Процедури за унищожаване - документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на предприятието или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

Защитата на автоматизираните информационни системи и/или мрежи в ДП НКЖИ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

- Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на ДП НКЖИ. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае”;

- Управление на масивите, съобразено с ограничаване на достъпа до съответния масив единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;

- Управление на външни връзки и/или свързване, включващо от своя страна:

• Дефиниране на обхвата на вътрешните мрежи: като вътрешни мрежи се разглеждат всички локални мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на ДП НКЖИ. Като външни мрежи се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на ДП НКЖИ.

• Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално оторизирани за това лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае“. Минималното изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

• Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

• Контрол на достъпа до вътрешната мрежа: отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат необходимите мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на ДП НКЖИ, включително и чрез използване на защитни стени и други адекватни мерки и инструменти.

9. ИНФОРМАЦИОННИ МАСИВИ

За обработване на личните данни, ДП НКЖИ поддържа в Регистъра на хартиен и/или технически (електронен) формат, следните самостоятелни информационни масиви:

- Информационен масив „Човешки ресурси”;

- Информационен масив „Единна информационна система за документооборот в ДП НКЖИ”;

- Информационен масив „Възнаграждения и документи за осигурителен доход”;

- Информационен масив „Професионално обучение в Център за професионална квалификация /ЦПК/ на ДП НКЖИ”;

- Информационен масив „Декларации по чл. 35 от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество на членовете на Управителния съвет и на директорите на поделения на ДП НКЖИ”;

- Информационен масив „Пълномощни“;

- Информационен масив „Достъп до обществена информация“

- Информационен масив „Електронен подпис“;

- Информационен масив „Данни на физически лица по договори от обществени поръчки“;

- Информационен масив „Лични данни за резервация на самолетни билети“;

- Информационен масив „Инспекция Здраве и безопасност при работа“;

- Информационен масив „Трудова медицина“;

- Информационен масив „Удостоверения за квалификационна група по безопасност при работа в електрически уредби и мрежи“;

- Информационен масив „Удостоверение за работа с устройствата на осигурителната техника на началник гари и влакови диспечери“;

- Информационен масив „Регистър на издадените допълнителни удостоверения“;

- Информационен масив „Отсрочване на запасни и техника - запас”;

- Информационен масив „Пропуски за преминаване на държавната граница с Република Сърбия”;

- Информационен масив „Открити листа за преминаване на границата с Република Турция”;

- Информационен масив „Разрешения за работа в стратегически зони”;

- Информационен масив „Данни на физически лица по подробни устройствени планове и отчуждаване на имоти за инфаструктурни обекти на ДП НКЖИ”;

- Информационен масив „Информационна система ИСУН 2020“;

- Информационен масив „Управление на държавната собственост и кадастър“

- Информационен масив „Видеонаблюдение“;

- Информационен масив „Архив“.

10. КАТЕГОРИИ ЛИЧНИ ДАННИ, КОИТО СЕ ОБРАБОТВАТ ОТ ДП НКЖИ

В информационните масиви се обработват следните категории лични данни:

1. физическа идентичност: имена и данни от лична карта (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение), снимка, телефони за връзка и др.;

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и служебна/трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице;

4. икономическа идентичност: размер на възнаграждението/осигурителния доход, лични банкови сметки; данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др. в изпълнение на ЗПКОНПИ;

5. лични данни относно гражданско-правния статус на лицата.

6. специални (чувствителни) категории лични данни:

- свързани със здравословното състояние на работниците и служителите с оглед прилагане на изискванията на трудовото законодателство, ЗЗБУТ и други подобни – медицинско свидетелство при назначаване на работа, експертни решения от ТЕЛК/НЕЛК, ТОЛЕК/ТЦЛЕК, заключения от периодични медицински и психологически прегледи, преминавани с оглед спазване изискванията за безопасни условия на труд;

- свързани със здравословното състояние на работниците и служителите с оглед прилагане на Социалната програма към КТД за подпомагане на работници и служители изпаднали в затруднение;

- свързани с ползване на лични данни на членовете на семейството на работниците и служителите във връзка с ползване на отпуски по Кодекса на труда и Наредбата за

работното време, почивките и отпуските за отглеждане на дете и за издаване на безплатни билети за пътуване по железопътния транспорт.

7. други данни: свидетелство за съдимост при кандидатстване за работа, както и данни, чието обработване е необходимо за изпълнение на правата и задълженията на ДП НКЖИ като работодател.

11. НАРУШЕНИЕ НА СИГУРНОСТТА НА ДАННИТЕ. СРЕДСТВА ЗА ПРАВНА ЗАЩИТА

За всяко установено нарушение на сигурността на личните данни – умишлено изтичане на лични данни; неправомерно предоставяне на трети страни или изтриване, случайно унищожаване или загуба; увреждане на целостта на данните и всяко друго действие, което е вероятно да доведе до риск за правата и свободите на субектите на данни (например: финансови загуби, нарушаване на поверителността, дискриминация, вреди, причинени на репутацията или други значителни социални или икономически щети), Длъжностното лице по защита на личните данни информира незабавно Комисията за защита на лични данни за нарушението, не по-късно от 72 часа, след като е узнало за него, освен ако Длъжностното лице не е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът съобщава на субекта на данните за нарушението на сигурността на личните данни.

При нарушаване на правата му, субектът на лични данни разполага със средствата за правна защита и може да търси отговорност за причинените му вреди по реда на ЗЗЛД.

12. ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА СИСТЕМА ЗА ДОКЛАДВАНЕ НА НАРУШЕНИЯ

При възникване и установяване на инцидент относно личните данни всеки служител е длъжен незабавно да информира Длъжностното лице по защита на личните данни и служителя/ите, определен/и да обработва/т лични данни в съответния информационен масив.

Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

За инцидентите се води отделен регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада, последствията от инцидента и мерките, които са предприети за отстраняването им.

Във всеки конкретен случай Администраторът извършва вътрешно разследване с цел да се установи риска за субектите в резултат на конкретното нарушение.

При извършване на вътрешното разследване се изискват обяснения от лицата, отговорни за обработване на личните данни в съответния информационен масив или информационни масиви, ако нарушението засяга повече от един.

При извършване на вътрешното разследване всяко от лицата, отговорни за обработването на лични данни, представя на ДЛЗЛД становище и съответните доказателства.

За резултатите от разследването на инцидента и предприетите мерки ДЛЗЛД уведомява с доклад генералния директор, в качеството му на Администратор.

При трансгранична обработка на лични данни, нарушението може да засегне субектите на данни в повече от една държава-членка. В този случай Администраторът следва да уведоми надзорния орган на територията на своята собствена държава-членка.

13. ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ НА ТРЕТИ ЛИЦА И ТРЕТИ СТРАНИ

ДП НКЖИ, като Администратор не предоставя лични данни на трети лица, освен в предвидените в закон или описаните в тази Политика случаи.

При предоставяне на данни от ДП НКЖИ на трети лица или страна/и, Администратори, които обработват лични данни, същите предоставят *Декларация за поверителност по образец – приложение № 4 към настоящата политика*.

Данни от Регистъра на ДП НКЖИ могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР, ДАНС, МРРБ, МФ, Министерски съвет, МТИТС, ИАЖА, Комисията за противодействие на корупцията и за отнемане на незаконно придобито имущество,съдебни органи и др.).

14. СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ

ДП НКЖИ съхранява личните данни в нормативно установените срокове за постигане на целите, за които са били събрани.

Информацията се обработва при спазване на принципите за защита на личните данни и се предприемат нужните мерки за недопускането и предотвратяване на нарушение в сигурността на тази информация. За защита на данните са предприети множество мерки за физическа, персонална, документална защита и защита на информационните системи.

При съхраняването на документи, подадени в компанията се съобразяваме със сроковете, предвидени в действащото законодателство и приложимите подзаконови нормативни актове, изискванията за водене на учрежденския архив, отчитат се и сроковете, в които могат да бъдат предявени правни претенции.

След изтичането на срока за съхранението им носителите на информация (хартиени и електронни), които не подлежат на предаване в Националния архивен фонд, се унищожават.

15. ПРАВО НА ЖАЛБА ДО КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ИЛИ ДО СЪДА

Ако считате, че обработката на лични данни в ДП НКЖИ е незаконосъобразна или нарушава правата Ви, може да подадете жалба до Комисията за защита на личните данни с адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2, електронен адрес: https://www.cpdp.bg/ или до Административен съд София – град.

16. ПРОМЕНИ В ПОЛИТИКАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.

ДП НКЖИ си запазва правото да извършва промени в Политиката за защита на личните данни.

Настоящата политика влиза в сила, считано от 01.08.2019 г.

ПРИЛОЖЕНИЯ:

1. Приложение № 1 - Декларация - съгласие за обработване на лични данни от субекта на лични данни по образец- към настоящата политика.

2. Приложение № 2 – Заявление за достъп до лични данни.

3. Приложение № 3 – Уведомление до субекта на данни.

4. Приложение № 4 - Декларация за поверителност.