



**ПОЛИТИКА
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА „ЗД ЕВРОИНС“ АД**

ИНФОРМАЦИОННА КАРТА

Дата на приемане на документа:	30.01.2020 г.
Дата на влизане в сила:	30.01.2020 г.
Версия на документа:	2.2
В сила от:	10.12.2025 г.
Структура, издател на документа:	Отдел „Методология и бизнес процеси“
Срок на валидност на документа:	Безсрочен
Одобен от/на:	Управителен съвет/30.01.2020 г.
Изменен от/на:	Съвет на директорите/18.12.2020 г. Съвет на директорите/10.12.2025 г.

Съдържание:

ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ.....	3
ГЛАВА II. ПРЕДНАЗНАЧЕНИЕ И ВОДЕНЕ НА РЕГИСТРИТЕ	4
ГЛАВА III. ЛИЧНИ ДАННИ, СЪХРАНЯВАНИ В РЕГИСТРИТЕ	4
ГЛАВА IV. ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ	8
ГЛАВА V. ПРАВА НА СУБЕКТИТЕ НА ДАННИ И РЕД ЗА УПРАЖНЯВАНЕТО ИМ	10
ГЛАВА VI. ОТГОВОРНОСТ И КОНТРОЛ	11
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ.....	11

ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1.(1) „Застрахователно дружество Евроинс“ АД („ЗД Евроинс“ АД, Дружеството, Администратора) е юридическо лице със седалище и адрес на управление: гр. София 1592, р-н „Искър“, бул. „Христофор Колумб“ № 43 и основен предмет на дейност застраховане и застрахователни услуги.

(2) Дружеството е администратор на лични данни по смисъла на чл. 4(7) от 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, ОРЗД).

(3) Дружеството, като администратор на лични данни, се придържа, оповестява и предоставя информация на субектите на данни по смисъла на чл. 13 и чл. 14 от ОРЗД чрез Уведомление за поверителност във връзка с предоставянето на застрахователни услуги, Уведомление за поверителност за служителите и лица заети по гражданско правоотношение, Уведомление за поверителността относно личните данни, обработвани от „ЗД Евроинс“ АД, в качеството му на администратор на лични данни при подбор на персонала и Правила за предоставяне на информация за упражняване правата на субектите на лични данни.

(3) Дружеството като администратор на лични данни определя:

1. вида на обработваните данни, съобразно предвидените цели;
2. целта и средствата за обработване;
3. мерките за гарантиране на сигурността на личните данни, при спазване на изискванията на ОРЗД, Закона за защита на личните данни (ЗЗЛД) и други нормативни актове.

Чл.2.(1) Настоящата Политика за защита на личните данни на „ЗД Евроинс“ АД (Политиката) има за цел да регламентира:

1. воденето, поддържането и защитата на регистрите с лични данни (обработваните лични данни в Дружеството);
2. задълженията на лицата, оправомощени да обработват лични данни и тяхната отговорност;
3. необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване (неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до личните данни на трети лица, както и от всички други незаконни форми на обработване на лични данни).

(2) Политиката се прилага за лични данни, обработвани в Дружеството.

(3) Дружеството обработва лични данни при спазване на следните основни принципи (съгласно чл. 5 от ОРЗД):

1. законосъобразност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхранението;
6. цялостност и поверителност.

(4) Дружеството носи отговорност във всеки един момент да е в състояние да докаже спазването на принципите, свързани с обработване на лични данни (принцип на отчетност).

(5) Дружеството обработва лични данни самостоятелно, чрез писмено възлагане на обработващ лични данни или като съвместен администратор (съгласно чл. 26 от ОРЗД).

(6) Всяко лице, действащо под ръководството на Дружеството, което има достъп до личните данни, обработва тези данни само по указание на Администратора – чл. 29 от ОРЗД. Такива лица са:

1. служителите на „ЗД Евроинс“ АД, чиито служебни задължения или конкретно възложени задачи налагат обработване на лични данни. Тези лица са в структурата на Администратора;
2. други лица (напр. по граждански договор), които за изпълнение на задачите или дейностите, които са им възложени, имат достъп до лични данни. Тези лица са извън структурата на Администратора.

ГЛАВА II. ПРЕДНАЗНАЧЕНИЕ И ВОДЕНЕ НА РЕГИСТРИТЕ

Чл.3.(1) Дружеството структурира, организира, поддържа и актуализира регистрите с лични данни, като самостоятелно определя целите и средствата за обработка на данните.

(2) Регистрите се поддържат в писмена форма и в електронен формат. Носителите на данни се съхраняват в определените за това помещения с регламентиран достъп.

Чл.4.(1) Хартиените носители на лични данни се съхраняват в папки (досиета) по начин позволяващ нарушение на целостта им или загуба на защитена от закона информация.

(2) Достъп до съответните досиета имат само оправомощени служители на Дружеството, съгласно длъжностните и функционални характеристики и преки разпореждания на представляващите „ЗД Евроинс“ АД. Възможността за предоставяне на друго лице на достъп до личните данни при обработката им е ограничена и изрично регламентирана в настоящата Политика, друг писмен документ на Дружеството или в нормативната уредба.

Чл.5.(1) Обработката на лични данни в електронен формат се извършва само в корпоративната мрежа, несвързана с обществената мрежа, като правата за достъп и обработка на лични данни в системите се определят и предоставят при съблюдаване на служебните ангажименти и при спазване на условията и реда съгласно Правилата за управление на достъпите. При работа с данните се използват софтуерни продукти за обработка на данните, които са адаптирани към специфичните нужди на Дружеството.

(2) Достъп до операционните системи, където се обработват лични данни, имат само оправомощените лица чрез потребител и парола за автентификация. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява чрез поддържане на защитни стени, антивирусни програми, обновяване на операционни системи, периодично архивиране на данните, периодична смяна на паролите, VPN, както и чрез поддържане на информацията на хартиен носител.

ГЛАВА III. ЛИЧНИ ДАННИ, СЪХРАНЯВАНИ В РЕГИСТРИТЕ

Чл.6.(1) В регистъра, относно човешките ресурси, се събират и съхраняват личните данни на кандидати за работа, лицата, заети по трудови или граждански правоотношения и свързани с тези лица, трети лица, когато такива данни се изискват за прилагане на законодателството (членове на семейства, лица, намиращи се в икономическа или друга нормативно регламентирана свързаност) във връзка с администриране на процесите, свързани със задълженията на Дружеството по трудовото, данъчно-осигурително законодателство и специалното законодателство, относимо към дейността, с цел:

1. подбор на персонала;
2. индивидуализиране на страните в трудовите и граждански правоотношения;
3. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закон за здравното осигуряване, Закон за данък върху доходите на физическите лица, Закона за счетоводството, Закона за задълженията и договорите, Кодекс за застраховането и други;
4. за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения – за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и други подобни), процедури във връзка с изискванията за квалификация и надеждност и процедури, свързани с изискванията към работодателите за осигуряване на здравословни и безопасни условия на труд и други;
5. кореспонденция с надзорен орган и други специфични за дейността регулации;
6. за установяване на връзка с лицето по телефон, за изпращане на кореспонденция на физически или електронен адрес, отнасяща се до администриране и изпълнение на трудови или граждански договори, по които субектът на данни е страна;
7. за водене на счетоводна отчетност, за възнагражденията на посочените по-горе лица по трудови и граждански договори;
8. други съгласно посоченото в Уведомлението за поверителност за служителите и лица заети по гражданско правоотношение и Уведомлението за поверителността относно личните данни, обработвани от „ЗД Евроинс“ АД, в качеството му на администратор на лични данни при подбор на персонала.

(2) Личните данни на служителите на Дружеството се подреждат в лични трудови досиета и се съхраняват в картотечен шкаф. Намират се в нарочно оборудвано помещение, предназначено за работа на оправомощения/те служител/ли, ангажиран с дейностите по управление на човешките ресурси.

(3) Достъп до информацията от кадровите досиета, съхранявана с автоматизирани средства има оправомощен/и служител/и по ал. 2, изречение второ, чрез парола за отваряне на тези файлове. Възможността за предоставяне на друго лице на достъп до личните данни при обработката им е ограничена и изрично регламентирана в настоящата Политика и относимите вътрешни правила на Дружеството, доколкото не произтича от действащото законодателство.

(4) В регистъра се обработват следните категории и видове данни:

1. Идентификационна информация (физическа идентичност) – три имена, ЕГН, номер на лична карта, дата и място на издаване, месторождение.

2. Контактна информация/информация за местоположение – телефони за връзка, имейл адрес, постоянен/настоящ адрес или адрес за кореспонденция.

3. Икономическа идентичност – данни за банкова сметка за превод на възнаграждение, данни за имущественото състояние и икономическа свързаност, съгласно Кодекса за застраховането (КЗ).

4. Социална идентичност – образование и трудов стаж, документ за придобито образование, квалификация и правоспособност, когато такива се изискват за длъжността, за която лицето кандидатства и др., документи за трудова дейност и професионална биография, документи, удостоверяващи роднински връзки и семейно положение (акт за брак, акт за раждане на дете, декларации за наличие на свързаност), данни, свързани с присъди и нарушения – свидетелство за съдимост, когато се изисква за заемане на длъжността, декларации за квалификация и надеждност.

5. Специални категории лични данни (здравна идентичност) – данни за здравословното състояние на лицето, съдържащи се в медицинско свидетелство за започване на работа, експертизи от органите на медицинската експертиза във връзка с предоставянето на документи за временна неработоспособност и трайно намалена работоспособност, данни за вероизповедание, различно от православно, когато са декларирани от лицето за ползване на правата по чл. 173 от Кодекса на труда.

(5) Данните за този регистър се набират при постъпване/възлагане на работа по трудово или гражданско правоотношение на дадено лице в изпълнение на нормативно задължение – разпоредбите на Кодекса на труда, Кодекса за социално осигуряване, Закон за здравното осигуряване, Закон за данък върху доходите на физическите лица, Закона за счетоводството, Закон за задълженията и договорите, Кодекс за застраховането и други по един от следните начини:

1. Устно интервю с лицето (при постъпване или в процеса на работа).

2. На хартиен носител – писмени документи – молби, заявления за постъпване/извършване на работа по трудово или гражданско правоотношение и приложените документи, за изменение или прекратяване на тези отношения, по текущи въпроси в процеса на работа, подадени от лицето.

3. От външни източници (от съдебни, финансови, осигурителни, данъчни и други институции в изпълнение на нормативни изисквания).

4. Във всички случаи когато е необходимо на основание нормативно задължение, лицата, чиито данни задължително подлежат на обработка в регистъра, подават необходимите лични данни на Администратора, съответно на оправомощения служител.

(6) Служителят от отдел „Човешките ресурси“ е задължен да предостави на субекта на данни информацията по член 13 от ОРЗД по образец не по-късно от момента на получаване на данните от него.

(7) При определени случаи ограничен достъп до лични данни от този регистър могат да имат: членовете на Съвета на директорите (СД) на „ЗД Евроинс“ АД, главен счетоводител, както и лицата, осъществяващи технически счетоводни операции при изготвяне на разплащателни документи, свързани с преводи на възнагражденията по банков път, както и други служители на Дружеството, на които им е необходимо да обработват лични данни с оглед изпълнение на задълженията им съгласно длъжностната им характеристика, например, но не само, юрисконсулти.

(8) Оправомощеният служител по ал. 2, изречение второ, осигурява достъп до съхраняваната от него информация при спазване изискванията на настоящата Политика, а за неуредените случаи след писмено разпореждане на представляващ Дружеството.

(9) Личните данни, събирани при подбор на персонал, се обработват и съхраняват съгласно Уведомлението за поверителността относно личните данни, обработвани от „ЗД Евроинс“ АД, в качеството му на администратор на лични данни при подбор на персонала.

Чл.7.(1) В регистъра, относно клиентите на Дружеството – ползватели на застрахователни услуги и посредници, се набират и съхраняват лични данни на контрагенти, посредници и ползватели на застрахователни услуги, с оглед:

1. целите на застраховането – дейност по осигуряване на застрахователно покритие на рискове по силата на договор, изразяващо се в набиране и разходване на средства, предназначени за изплащане на обезщетения и други парични суми при настъпване на събития или сбъждане на условия, предвидени в договор или в закон, както и в пряко свързаните с това дейности, включително:

- а) оценка на застрахователния риск/тарифиране;
 - б) определяне на застрахователната премия;
 - в) установяване на настъпило застрахователно събитие;
 - г) определяне размера на причинените вреди;
 - д) прехвърляне на всички или на част от застрахователните рискове, покрити от застраховател, на презастраховател или на друг застраховател;
 - е) други.
2. индивидуализиране на лицата за съответния вид застраховка;
3. изпълнение на нормативните изисквания по Кодекса за застраховането и други;
4. за всички дейности, свързани с изготвяне на всякакви документи и справки за лицата (удостоверения, сертификати, уверения, и други подобни);
5. за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на съответния договор;
6. други съгласно посоченото в Уведомление за поверителност във връзка с предоставянето на застрахователни услуги.

(2) Служителите, които са пряко ангажирани с дейностите по сключване и администриране на застрахователни и посреднически договори, са задължени да предоставят на разположение на субектите на данни информацията по чл. 13 и чл. 14 от ОРЗД под формата на утвърденото и публикувано на официалната интернет страница на Дружеството Уведомление за поверителност във връзка с предоставянето на застрахователни услуги.

(3) Хартиените носители на лични данни се съхраняват в джобове за документи, папки, класьори, шкафове, метални каси и други подобни инструменти за организиране, подредба и съхранение на документация. В служебните помещения, в които се обработват данните, като части от сгради или отделни крила на етажи, физическият достъп е контролиран, предназначен за работа на оправомощените служители на Дружеството, които имат задължение да обработват носителите на лични данни и друга защитена от закона информация, съгласно длъжностната си характеристика.

(4) При водене на регистъра на електронен носител, личните данни се въвеждат и обработват в корпоративните мрежи и софтуерни програми с контрол на достъпа.

(5) В регистъра се поддържат следните видове данни:

1. Идентификационна информация (физическа идентичност) – три имена, ЕГН, данни от документ за самоличност.
2. Контактна информация/информация за местоположение – електронна поща, адрес и телефон.
3. Икономическа идентичност – номер на банкова сметка, данни за имотно състояние (притежавано имущество, като данни за МПС, имот) история на плащанията.
4. Социална идентичност – трудов стаж, професионален опит, професия, възнаграждение.
5. Специални категории лични данни (здравна идентичност) – информация относно здравното състояние на ползвателите на застрахователни услуги (диагноза, епикризи, други медицински документи за извършени прегледи, изследвания или други интервенции).

(6) Личните данни в регистъра по чл. 7 се набират при сключване на съответния вид договор, предявяване на претенция/регистрация на щета, жалба и т.н., от физическите лица, за които се отнасят данните (застрахованите лица, респ. застраховащи и/или увредените лица респ. техните пълномощници), държавни органи и трети лица, съгласно КЗ и от публични регистри.

Чл.8.(1) В регистъра, относно деловодството и архива на Дружеството се набират и съхраняват лични данни за различни категории физически лица – ползватели на застрахователни услуги, посредници доставчици, законни представители и пълномощници, включително данни, предоставени във връзка с установяването и упражняване на правни претенции пред съдебни и извънсъдебни инстанции, и данни обработвани посредством запитвания на регулаторни и надзорни органи. Също така сигнали по Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (личните данни на сигнализиращите, подпомагащите ги и свързаните с тях лица, вкл. и на засегнатите лица, които попадат в обхвата на Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения).

(2) Данните в регистъра по чл. 8, ал. 1 се събират и обработват с цел извършване на управление на деловодство и архивно съхранение на хартиени документи при съблюдаване на вътрешните правила, процедури, инструкции и указания на Дружеството.

(3) Архивирането и съхранението на документи се извършва съгласно Правилник за архивна дейност, Указания за прилагане на номенклатура на делата и Номенклатурата на делата със срокове за съхранение.

(4) В регистъра по чл. 8, ал. 1 се обработват следните категории лични данни:

1. Идентификационна информация (физическа идентичност) – имена, ЕГН/ЛНЧ, данни по документи за самоличност.
2. Контактна информация/информация за местоположение – електронна поща, адрес и телефон.
3. Други данни - предоставени по преценка на физическото лице, автор на инициращия документ, депозиран в деловодната система на Дружеството.

Чл.9.(1) Дружеството може да обработва лични данни изцяло или частично с автоматични средства в регистри с лични данни за цели, произтичащи от легитимните интереси на Администратора или трето лице (като видеонаблюдение, карти за достъп и други) в контекста на:

1. управление на физическа сигурност;
2. охрана на имущество;
3. контрол на достъпа;
4. наблюдение на служителите за целите на изпълнението на служебните задължения и използването на ресурси и информация;
5. сигурност на информационните технологии;
6. мрежова сигурност;
7. подобряване обслужването на клиентите.

(2) В Дружеството се обработват лични данни на наети по трудово и друго правоотношение и на трети лица:

1. преминаващи през охраняем периметър;
2. обаждащи се на телефонната централа на „ЗД Евроинс“ АД;
3. посещаващи сградите/офисите на Дружеството;
4. достъпващи на легитимно основание информационни ресурси или използващи ресурси, за които се използват системи за охрана и наблюдение.

(3) Обработването се осъществява чрез карти за достъп, системи за видеонаблюдение, GPS-системи на служебните автомобили и мониторинг на служебните информационни ресурси.

(4) Данните се събират в хода на прилагането на съответните технически и организационни мерки за защита с оглед предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения и системи, в които се обработват лични данни във връзка с дейността на „ЗД Евроинс“ АД.

(5) В регистъра по чл. 9 се обработват следните категории лични данни:

1. Идентификационна информация (физическа идентичност) – имена на служителя, номер на служебна карта, служебен електронен адрес, позиция, логове, снимка или видео, включващо

попадащите в обхвата лица, запис на телефонни разговори, провеждани при обаждане от и на телефонна централа на Дружеството.

2. Информация за местоположение – географска локация;

3. Онлайн идентификатори – пароли, потребителско име, IP адрес на използвано устройство, данни за устройство при използване на VPN.

ГЛАВА IV. ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.10.(1) Служителите в Дружеството се запознават още с постъпването си на работа, а в последствие и периодично, но не по-рядко от веднъж годишно, с изискванията на действащото законодателство, регулиращо защитата на личните данни, както и с настоящата Политика.

(2) Служителите на Дружеството, на които, поради естеството на извършваната работа и/или заеманата длъжност е възложено да обработват лични данни, са длъжни в своите действия да съблюдават спазването на законодателството, регулиращо защитата на личните данни. За неспазване на това свое задължение те носят отговорност съгласно българското законодателство.

Чл.11.(1) Дружеството определя или назначава длъжностно лице по защита на данните (ДЛЗД), за което уведомява по надлежния ред надзорния орган за защита на личните данни и субектите на данни. Контакт с това лице се осъществява чрез имейл адреса dpo@euroins.com или office@euroins.com.

(2) Функции на ДЛЗД:

1. Участва по подходящ начин и своевременно при решаването на всички въпроси, свързани със защитата на личните данни, включително, но не само, когато се вземат решения, имащи отражения върху обработването и защитата на данните (приемане и изменение на нови вътрешни политики, правила и процедури, въвеждане на нови програмни и бизнес продукти), както и когато се установи нарушение на сигурността на данните или друг инцидент.

2. Действа като лице за контакт с надзорния орган и субектите на данни, като последните могат да се обръщат към ДЛЗД по всички въпроси, свързани с обработването на техните лични данни и с упражняването на правата им, съгласно ОРЗД.

3. Информира и съветва Администратора и служителите, които извършват обработване на лични данни за техните задължения по спазване на законодателството за защита на данните, вътрешните правила на Дружеството, участва в дейностите по повишаване на осведомеността на персонала, включително в организирането и провеждане на обучения по теми, свързани с обработването и защитата на сигурността на данните.

4. Наблюдава спазването на законодателството и вътрешните правила на Дружеството за защита на данните, като събира информация за определяне на дейностите по обработване, анализира и проверява изпълнението им и отправя препоръки към Администратора.

5. Изразява становище относно необходимостта да се извърши оценка на въздействието върху защитата на данните (ОВЗД) за определен вид обработване, каква методика да се използва за извършването ѝ, какви гаранции да се приложат, за да се намалят рисковете за правата и интересите на субектите на данни, дали ОВЗД е направена правилно и дали заключенията водят до необходимост от предварителна консултация с надзорния орган.

6. Води Регистър на дейностите по обработване съгласно чл. 30 от ОРЗД, Оперативен регистър на искания за упражняване на права и Регистър на нарушенията на сигурността на данните.

7. Други дейности съгласно длъжностната му характеристика.

(3) ДЛЗД е независимо и Администраторът му осигурява техническа, организационна, обучителна, финансова и всяка друга помощ, както и достъп до съответните регистри и операции, доколкото е необходимо във връзка с изпълнение на задълженията му.

(4) ДЛЗД спазва конфиденциалност и поверителност при изпълнението на своите задачи, произтичащи от настоящата Политика и приложимото законодателство.

Чл.12. В Регистъра на дейностите по обработване съгласно чл. 30 от ОРЗД се описва обработката на лични данни в регистрите с данни на Дружеството.

Чл.13.(1) Личните данни в поддържаните регистри се съхраняват и защитават от случайно или незаконно унищожаване, от случайна загуба, неправомерен достъп, изменение или

разпространение, както и от други незаконосъобразни форми на обработване чрез система от технически и организационни мерки.

(1) Защитата на личните данни е:

1. физическа;
2. персонална;
3. документална;
4. защита на автоматизирани информационни системи и/или мрежи;
5. криптографска защита.

(3) Мерките за защита на личните данни се съобразяват със съвременните достижения на технически прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработване, както и с рисковете с различна вероятност и тежест за правата и свободите на физическите лица, включително когато е целесъобразно, се прилагат мерките съгласно чл. 32 от ОРЗД.

(4) Техническите и организационните мерки, които Дружеството прилага за отделните регистри и дейности по обработване се вписват в Регистъра на дейностите по обработване съгласно чл. 30 от ОРЗД. Мерките се актуализират и подлежат на периодичен преглед при промени в целите, средствата или основанията за обработване, както и по предложение на звената (отделите/дирекциите), участващи в процесите по обработване на лични данни, препоръки от одити и проверки или по предложение на ДЛЗД.

(5) Мерките за физическа защита включват правила, процедури и разпореждания на СД на Дружеството за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни като: контролиран режим на влизане, движение и излизане от работните помещения; съхранение на ключове от помещения, каси, шкафове и други съоръжения, служещи за съхраняване на информация, която съдържа лични данни, пожарогасителни системи, регламентиран режим на посещенията и други.

(6) Персоналната защита включва система от организационни мерки, осигуряваща подходящо ниво на познаване на нормативната уредба в областта на защита на личните данни, задължения за неразгласяване на критична информация между персонала и извън Дружеството, провеждане на обучения, тренировки на служителите за реакции при кризи, включително събития, които застрашават сигурността на данните.

(7) Документалната защита е система от организационни мерки, които се изразяват в регламентиране с политики, процедури и правила на дейностите, свързани с обработка на лични данни както и поддържането на регистри на дейностите, Оперативен регистър на искания за упражняване на права, процедури за съхраняване, достъп и унищожаване на носители на данни, определяне на срокове на съхранение.

(8) Дружеството прилага система от технически и организационни мерки при обработка на данни чрез информационни системи с цел защита от незаконни форми на обработване на лични данни, която гарантира ясно разпределение на роли и отговорности, идентификация и автентификация, контроли на сесията и на отдалечените достъпи, защита от вируси, поддържане на резервни копия за възстановяване. Прилагането на мерките за защита се осигурява чрез Политиката за информационна сигурност и система от процедури и правила за управление на достъп до информационните системи, промени, конфигурация на антивирусната система и други. Служителите от дирекция „Информационни технологии и дигитализация“ извършват текущ анализ за способността на мрежата и информационните системи да издържат на високо равнище на случайни събития, неправомерни или злонамерени действия, които биха могли да окажат съществено влияние върху целостта, наличността и поверителността на обработваните, съхраняваните и предаваните данни в Дружеството и при необходимост предлага промени, съобразени с нивата на риск.

(9) Криптографска защита представлява система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне. Основните мерки на криптографската защита са:

1. стандартните криптографски възможности на операционните системи;
2. стандартните криптографски възможности на системите за управление на бази данни;
3. стандартните криптографски възможности на комуникационното оборудване;
4. системи за разпределение и управление на криптографските ключове;

5. нормативно определените системи за електронен подпис.

Чл.14.(1) ОВЗД е процес, който цели да опише обработването на лични данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, като ги оцени и определи мерки за справяне с тези рискове.

(2) Извършването на ОВЗД е задължително за операция или съвкупност от операции, при които съществува вероятност обработването да породи висок риск за правата и свободите на физическите лица, както и за операции, които са включени в списък на надзорния орган по член 35(4) от ОРЗД. Администраторът обосновава и документира причините, поради които взема решение дали да извърши ОВЗД, включително изисква становище от ДЛЗД. Когато обработването се извършва изцяло или отчасти от обработващ лични данни, същият подпомага Администратора при извършването на ОВЗД в съответствие с изискванията на ОРЗД, като се отчита естеството на обработване и информацията, до която е осигурен достъп. Ролята и отговорностите на обработващия лични данни по отношение ОВЗД се определят в сключения договор.

(3) Звената (отделите/дирекциите), които отговарят за процесите по обработване на лични данни, определят целите и средствата за обработка и/или оценка на риска, както и ДЛЗД, могат да предлагат да бъде извършена ОВЗД. Те предоставят необходимата информация за ОВЗД и участват в процеса по документиране и валидирането ѝ.

(4) При извършване на ОВЗД се използва подходяща методология, чието съдържание се съобразява с оповестените насоки, препоръки и най-добри практики на компетентните органи по защита на данните (надзорен орган и Европейски комитет по защита на данните, съответно Работна група за защита на лицата при обработване на лични данни по член 29).

Чл.15.(1) Лични данни се съхраняват до постигане на целите, за които са събрани и съобразно сроковете, определени за съхранение на съответния носител.

(2) Съхранение и унищожаване на носители на лични данни се извършва съгласно утвърдените в Дружеството Правилник за архивна дейност; Номенклатура на делата със срокове за съхранението им; Процедура за предаване на документи в архива; Процедура за унищожаване на документи.

ГЛАВА V. ПРАВА НА СУБЕКТИТЕ НА ДАННИ И РЕД ЗА УПРАЖНЯВАНЕТО ИМ

Чл.16.(1) Субектите на лични данни могат да упражнят правата си по чл. 15 – 22 от ОРЗД, като подадат писмено заявление до Администратора. Заявлението може да бъде подадено:

1. по електронен път, подписано с усъвършенстван електронен подпис, основан на квалифицирано удостоверение за електронни подписи, или квалифициран електронен подпис, съгласно посоченото в Правила за предоставяне на информация за упражняване правата на субектите на лични данни;
2. на място в офис на „ЗД Евроинс“ АД от субекта на данни. При условие че искането се подаде от упълномощен представител, оригиналното пълномощно се представя за сверка;
3. по пощата на адреса на Централно управление на Дружеството (гр. София, бул. „Христофор Колумб“ № 43);
4. и е безплатно.

(2) Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Администраторът може да наложи разумна такса или да откаже да предприеме действия по искането.

Чл.17.(1) Заявлението за упражняване на права на лични данни следва да съдържа следната информация:

1. Идентификация на лицето – пълното име и допълнителни данни за идентификация като ЕГН, или ЛНЧ, или друг аналогичен идентификатор, или номер на полица, или клиентски номер.
2. Точно и конкретно описание на искането.
3. Предпочитана форма за предоставяне (изпращане) на информацията.
4. Подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) Заявлението се регистрира в общия входящ регистър на Дружеството и в Оперативен регистър на искания за упражняване на права на субектите на данни, поддържан от ДЛЗД.

Чл.18. Достъп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или неговия пълномощник;
4. предоставяне на копие от исканата информация.

Чл.19.(1) При постъпване на искане от субект на данни по чл. 16, заявлението се предоставя на ДЛЗД за разглеждане и изготвяне на мотивиран проект на решение.

(2) Звената, в които се обработват лични данни, оказват съдействие в хода на разглеждане на заявлението, като предоставят достъп до носители на данни и съдействие, когато Администраторът следва да предприеме конкретни действия във връзка с упражняването на правата на субекта на данни.

(2) Срокът за разглеждане на заявлението и произнасяне по него е един месец от получаване на искането. Този срок може да бъде удължен с още два месеца, като се вземе предвид сложността и броя на исканията. Администраторът информира субекта на данни за всяко такова удължаване на срока в срок от един месец от получаване на искането, като посочва и причините за забавянето.

(3) Решението се съобщава писмено на заявителя, получава се лично срещу подпис или по пощата с обратна разписка. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е посочил друго.

(4) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне на достъп може да се обжалва от лицето пред посочения в писмото орган и в рамките на посочения срок.

Чл.20. Дружеството оповестява реда и условията за упражняване на правата на субектите на данни, съгласно ОРЗД на официалната си страница в интернет в Правила за предоставяне на информация за упражняване правата на субектите на лични данни.

ГЛАВА VI. ОТГОВОРНОСТ И КОНТРОЛ

Чл.21.(1) Текущ контрол за спазване на настоящата Политика се осъществява от ръководителите на съответните звена от структурата на Дружеството (дирекции/отдели).

(2) Последващ контрол на спазването на изискванията за законосъобразно и добросъвестно обработване на лични данни се осъществява от специализирана служба „Вътрешен контрол“.

(3) ДЛЗД не по-малко от веднъж годишно информира СД с доклад за дейността си, включително относно броя и вида на подадените искания за упражняване на правата на субектите на данни, участието в процедури по съгласуване на документи, ОВЗД, нарушения на сигурността на личните данни и при необходимост предлага конкретни мерки във връзка със спазването на приложимото законодателство за защита на личните данни.

(4) СД периодично, но не по-малко от веднъж годишно, извършва преглед на настоящата политика и относимите вътрешни документи, които въвеждат правила, политики и принципи за законосъобразна и добросъвестна обработка на лични данни, като при необходимост ги актуализира.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. За целите на настоящата Политика използваните понятия имат значението дадено им от ОРЗД и ЗЗЛД.

§2. Настоящата политика подлежи на оповестяване и достъп до всички служители на Дружеството чрез споделен ресурс във вътрешната корпоративна мрежа за сведение и изпълнение.

§3. Настоящата Политика е приета от Управителния съвет (УС) на „ЗД Евроинс“ АД на 30.01.2020 г., влиза в сила от същата дата и отменя Инstrukция за условията и начините на събиране, обработване, съхраняване и защита на лични данни, приета с решение на УС на Дружеството от 15.08.2017 г. Политиката е изменена с решение на СД на Дружеството от 18.12.2020 г. и промените са в сила от същата дата, изменена е с решение на СД от 10.12.2025 г. и промените влизат от същата дата.