УТВЪРЖДАВАМ:

.....

/Димитър Димитров – Изп.Директор/

ИНСТРУКЦИЯ
за мерките за защита на личните данни в „Неохим" АД - Димитровград

I. Общи положения

Предмет

Чл. 1. Тази инструкция урежда условията и реда за водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в „Неохим" АД - Димитровград.

Принципи при обработване на лични данни

Чл. 2. При обработването на лични данни в „Неохим"АД се спазват следните принципи:

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;
7. отчетност.

II. Администратор и регистри с лични данни

Индивидуализиране на администратора на лични данни

Чл. 3. (1) Администратор на лични данни е „Неохим"АД, със седалище и адрес на управление: гр.Димитровград, ул."Химкомбинатска". Адресът за кореспонденция и контакт е: гр.Димитровград, ул."Химкомбинатска"№3 , тел. 0391 65 200.

(2) Администраторът обработва лични данни във връзка с изпълнение на законови задължения, реализиране на лигитимен /законен/ интерес и за сключване на договори, като определя сам целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни, както и чрез възлагане на обработващ лични данни.

(4) Администраторът определя лице, което да отговаря за координиране и прилагане на мерките за защита на личните данни.

Условия за достъп до лични данни

Чл. 4. Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае" и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата

подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си /Приложение № 4/.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Чл. 5. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;
2. целите на обработването на личните данни и правното основание за обработването;
3. категориите лични данни, отнасящи се до съответното физическо лице;
4. получателите или категориите получатели, на които могат да бъдат разкрити данните;
5. срока за съхранение на личните данни;
6. информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните;
7. право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;
8. правото на жалба до надзорен орган – за Република България Комисията за защита на личните данни;
9. източника на данните;
10. съществуване на автоматизирано вземане на решения, включително профилиране.

(2) Алинея 1 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;
2. вписването или разкриването на данни са изрично предвидени в закон;
3. физическото лице, за което се отнасят данните, вече разполага с информацията по ал. 1;
4. е налице изрична забрана за това в закон.

Поддържани регистри на дейностите по обработване на лични данни

Чл. 6. В „Неохим"АД се обработват лични данни в следните регистри:

1. Регистър „Човешки ресурси" ;
2. Регистър „Служба Трудова медицина";
3. Регистър „Правен отдел";
4. Регистър „Клиенти";
5. Регистър „Доставчици";
6. Регистър „Видеонаблюдение";
7. Регистър „Деловодство".

III. Регистър „Човешки ресурси""

Общо описание на регистъра

Чл. 7. В регистъра се обработват лични данни на кандидати за работа и на служители, работници и изпълнители по граждански договори, договори за възлагане на управление /ДВУ/ с оглед:

1. индивидуализиране на трудови, граждански правоотношения и ДВУ;
2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд, Търговски закон,Закон за търговския регистър, Закон за насърчаване на заетостта.;
3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори или ДВУ;

г) за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови и служебни правоотношения, граждански договори и ДВУ.

Категории лични данни, обработвани в регистъра

Чл. 8. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес) телефон за връзка;

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография; при възникване на трудово правоотношение се събират данни за придобито образование, специалност, квалификация и правоспособност само за длъжности, които го изискват.

3. семейна идентичност: майки с деца до 18 годишна възраст предоставят информация за дата на раждане и трите имена на децата във връзка с чл.168 от КТ и чл.28, ал.3 от КТД;

4. икономическа идентичност: данни относно банкови сметки, трудови възнаграждения, начисления и удръжки;

5. лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

6. данни за здравословното състояние (медицинско свидетелство при постъпване на работа, периодични прегледи, преминавани с оглед характера на работата, изпълнявана по трудовото правоотношение и изискванията за безопасни условия на труд);

7. данни за членство в синдикални организации.

Технологично описание на регистъра

Чл. 9. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в „Неохим"АД. Данните се въвеждат директно в договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция .

(4) Данните в регистъра относно ведомости и заплати се съхраняват за срок от 50 години във връзка с нормативно установени срокове; документи за данъчно-осигурителен контрол – 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани; документи за отговорности, пълномощия и обмен на информация – 10 години; документи на кандидати за работа – до 3 месеца след приключване на подбора и назначаване на избрано лице; списъци с посетители – до една седмица след посещението; всички останали носители – 5 години.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни при поискване от съответните държавни или местни органи, институции или администрации в кръга на тяхната компетентност или по изрично писмено искане на субекта на лични данни и при условията на чл.14.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 10. (1) Данните от регистъра се обработват от служителите в отдел „Човешки ресурси", в чиито длъжностна характеристика е определено задължение за обработване на данните на служителите и при спазване на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при или по повод изпълнение на служебните им задължения.

Оценка на въздействието на Регистър Човешки ресурси"

Чл. 11. (1) Оценка на въздействието на Регистър „Човешки ресурси" се извършва в съответствие с критериите на Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 250, но не надхвърля 10 000;

2. в регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите и данни за членство в синдикални организации, данни във връзка с упражняване на родителски права върху деца, с оглед прилагане на изискванията на трудовото законодателство.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Човешки ресурси" е средно.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на „Регистър Човешки ресурси"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Човешки ресурси	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в Регистър „Човешки ресурси"

Чл. 12. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на лицата по чл. 10.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения с контролиран достъп само за лицата по чл.10.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра са оборудвани със заключване на вратите и осигурени пожарогасителни средства на етажа на сградата.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само в присъствието на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват електронно лични данни от регистъра, само в присъствието на служители по чл.10.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД, и настоящата Инструкция .

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Всички служители в отдела, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4.Споделяне на изисквания за критична информация между персонала/напр. идентификатори, пароли за достъп и т.н./

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Човешки ресурси" се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим"АД.

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае".

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в зоните с контролиран достъп.

5. Ръководителят на структурното звено „Човешки ресурси" е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Човешки ресурси", които са на хартиен носител, са определени в чл. 9, ал. 4 и във вътрешни правила за съхранение и работа в архив.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим"АД.

8. Архивирането на документи се възлага на експерт „Човешки ресурси" и специалист организиране, нормиране и отчитане на труда, при спазване на вътрешните правила за работа и архив и при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от служителите в този отдел само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра / например събирани за конкурси за свободни работни места/, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия. Унищожаването се извършва след писмено разрешение на Директор „УРЧР".

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1.Всеки отговорен служител се регистрира на използвания персонален компютър с потребител и парола като се спазват правилата на изградената в дружеството активна директория /АД/.

2. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване, в които отговорните служители се идентифицират с личен профил /потребител с парола/ с определени съобразно задълженията му права и нива на достъп.

3. Данните се въвеждат в база данни и се съхраняват на сървър, разположен в помещение с контролиран достъп.

4. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, сървърна система и база данни.

5. Сървърът за съхранение на данни и персоналните компютри, от които се извършва обработката, се защитават от външни посегателства със софтуерни решения и хардуерни продукти.

6. Ръководителят на структурно звено „Информационни технологии" е отговорен за контрол на достъпа до автоматизираните информационни системи и мрежи.

7. За сървъра и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

8. За цялостта на базата данни се извършват автоматични и ръчни архиви, чиято цялост и наличност се проверява от отдел „Информационни технологии".

9. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим Протект"ЕООД - Димитровград;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

10. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

11. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

12.Унищожаване/заличаване/изтриване на носители се извършва по реда на Процедура за съхраняване и унищожаване на данните.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита, съгласно утвърдена процедура.

Действия за защита при аварии, произшествия и бедствия

Чл. 13. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Директор „УРЧР", като това се отразява в дневника по архивиране и възстановяване на данни.

(4) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(5) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 14. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР , Агенция по заетостта, Бюрата по труда, Инспекцията по труда, Съдилищата, Държавни съдебни изпълнители, Частни съдебни изпълнители, Агенция по вписванията – Търговски регистър или Имотен

регистър, Нотариуси, Централен регистър по особените залози, Национална здравноосигурителна каса, Органи на медицинска експертиза, РИОКОЗ).

(2) В качеството си на работодател, или респективно на платец на възнаграждения към физически лица, „Неохим"АД предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори и ДВУ или плащания, произтичащи от други отношения /като членствени – на акционери, съдружници, облигационери по изплащане на дивиденти, лихви или други/. Личните данни, който се предоставят, са три имена и единен граждански номер и идентификационни данни за декларирана от лицето лична банкова сметка се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица „Неохим"АД посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място, а когато услугата на пощенския оператор го изисква – и телефонен номер за връзка с получателя на пощенската /куриерската/ пратка.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 15. Администраторът на лични данни извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 16. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването. За прехвърлянето се съставят съответно приемо-предавателни протоколи.

IV. Регистър „Служба трудова медицина"

Общо описание на регистъра

Чл. 17. В регистъра се обработват лични данни на следните лица: лица с ръководни функции в „Неохим"АД; работници и служители в „Неохим"АД; физически лица, по силата на договори за обслужване от СТМ, и са необходими за осъществяване на законово задължение за администратора на лични данни за следните цели: Анализ на здравното състояние на работещите и връзката му с условията на труд.

Категории лични данни, обработвани в регистъра

Чл. 18. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: име , ЕГН, адрес, данни от лична карта;телефон, личен лекар;

2. чувствителни лични данни: здравни досиета, съдържащи медицински свидетелства и други данни за здравословното състояние на физическото лице – предварителен медицински преглед, резултати и заключения от задължителния периодичен медицински преглед, заключения на службата за пригодността на работещия да изпълнява даден вид

работа, експертни решения на ТЕЛК/НЕЛК, болнични листи /при трудоустрояване, ползване на отпуски за временна неработоспособност и майчинство и др./, епикризи, разпореждане на териториалното поделение на НОИ за приемане на злополука за трудова.

Технологично описание на регистъра

Чл. 19. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Здравните досиета се съхраняват за срок от 50 години във връзка с нормативно установени срокове /Наредба № 3 за условията и реда за осъществяване дейността на службите по трудова медицина/, всички останали носители – 5 години.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 20. (1) Данните от регистъра се обработват от служителите в „Служба Трудова медицина" при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Служба трудова медицина"

Чл. 21. (1) Оценка на въздействието на регистър „Служба трудова медицина" се извършва в съответствие с критериите на Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2 .в регистъра се съдържат специални категории лични данни, свързани със здравословното състояние на работниците и служителите, както и на други физически лица, по силата на сключени договори.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Служба трудова медицина" е средно.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Служба трудова медицина"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Служба трудова медицина	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в регистър „Служба трудова медицина"

Чл. 22. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на лицата по чл. 20.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с контролиран достъп само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с контролиран достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани с заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с контролиран достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на отговорни служители.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД, и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Служба трудова медицина“ се поддържа на хартиен и електронен носител (здравни досиета, чието съдържание съответства на нормативната уредба на Република България).

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим”АД.

3. Достъп до регистъра имат лицата по чл. 20 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващи се шкафове в зоните с ограничен достъп.

5. Ръководителят на Служба трудова медицина е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 19, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим”АД

8. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1.Всеки упълномощен служител се регистрира на използвания персонален компютър с потребител и парола като се спазват правилата на изградената в дружеството активна директория /АД/.

2. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване, в които упълномощените лица се идентифицират с личен профил /потребител с парола/ с определени съобразно задълженията му права и нива на достъп.

3. Данните се въвеждат в база данни и се съхраняват на сървър, разположен в помещение с контролиран достъп.

4. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, сървърна система и база данни.

5. Сървъра за съхранение на данни и персоналните компютри, от които се извършва обработката, се защитават от външни посегателства със софтуерни решения и хардуерни продукти.

6. Ръководителят на структурно звено „Информационни технологии" е отговорен за контрол на достъпа до автоматизираните информационни системи и мрежи.

7. За сървъра и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

8. За цялостта на базата данни се извършват автоматични и ръчни архиви, чиято цялост и наличност се проверява.

9. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим Протект"ЕООД - Димитровград;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

10. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

11. Сроковете за съхранение на данни от регистъра са описани в чл. 19, ал. 4.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита.

Действия за защита при аварии, произшествия и бедствия

Чл. 23. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Директор „УРЧР", като това се отразява в дневника по архивиране и възстановяване на данни.

(4) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(5) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 24. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, Органи за медицинска експертиза, РЗИ и т.н.).

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 25. Администраторът на лични данни трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 26. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

V. Регистър „Правен"

Общо описание на регистъра

Чл. 27. В регистъра се обработват лични данни на следните лица: лица с ръководни функции в „Неохим"АД; работници и служители в „Неохим"АД; физически лица, контрагенти по договори с „Неохим"АД, и са необходими за осъществяване на законово задължение за администратора на лични данни и др. държавни органи, за изпълнение на договорни и трудови отношения, мандатни отношения, корпоративни отношения и такива, свързани или произтичащи от акционерно участие в „Неохим"АД за издаване на пълномощни за целите на дружеството, за постигане на законово определени цели , изпълнение на законови задължения на администратора и осъществяване на лигитимния му интерес.

Категории лични данни, обработвани в регистъра

Чл. 28. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: име , ЕГН, адрес, данни от лична карта;телефон, електронна поща, служебни данни за контакт.

2. чувствителни лични данни: свидетелства за съдимост /данни относно наличие на осъждане на лицето, квалификация на престъплението, изтърпяване на наказанието/, синдикална принадлежност, присъединяване към колективен трудов договор.

Технологично описание на регистъра

Чл. 29. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен носител и на сървър.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Личните данни, съдържащи се в договори, се съхраняват за срок от 10 години след прекратяване действието на договора, съгласно Основна процедура ОП 01 Управление на документирана информация в „Неохим"АД, , отговорите на запорните съобщения – до 5

години от датата на издаване на кореспонденцията, копията от издадените през годината пълномощни се съхраняват до 5 години от датата на издаване /нотариално заверяване/ на пълномощните; всички еднократни молби, становища, справки и др. документи се съхраняват до 5 години от датата на издаване на документите.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт. Данни от регистъра могат да бъдат предоставяни с оглед изпълнение на законови задължения на дружеството – администратор за вписване на обстоятелства с правно значение в съответните регистри или за прилагане на предвиден в действащото законодателство разрешителен, лицензионен, уведомителен или друг административно-правен режим.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 30. (1) Данните от регистъра се обработват от служителите в отдел „Правен" при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Правен"

Чл. 31. (1) Оценка на въздействието на регистър „Правен" се извършва в съответствие с критериите на Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2 .в регистъра се съдържат специални категории лични данни, свързани със членство в синдикални организации и наличие на осъждания за извършени престъпления.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Правен" е средно.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Правен"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Правен	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в регистър „Правен"

Чл. 32. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на лицата по чл. 30.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с контролиран достъп само за отговорни лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен

само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на отговорни служители.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД, и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Правен“ се поддържа на хартиен носител.

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим”АД.

3. Достъп до регистъра имат лицата по чл. 30 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с контролиран достъп.

5. Ръководителят на отдел „Правен” е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 29, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим”АД

8. Личните данни могат да бъдат размножавани и разпространявани от отговорните служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1.Всеки упълномощен служител се регистрира на използвания персонален компютър с потребител и парола като се спазват правилата на изградената в дружеството активна директория /АД/.

2. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване, в които упълномощените лица се идентифицират с личен профил /потребител с парола/ с определени съобразно задълженията му права и нива на достъп.

3. Данните се въвеждат в база данни и се съхраняват на сървър, разположен в помещение с ограничен или контролиран достъп.

4. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, сървърна система и база данни.

5. Сървъра за съхранение на данни и персоналните компютри, от които се извършва обработката, се защитават от външни посегателства със софтуерни решения и хардуерни продукти.

6. Ръководителят на структурно звено „Информационни технологии" е отговорен за контрол до автоматизираните информационни системи и мрежи.

7. За сървъра и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

8. За цялостта на базата данни се извършват автоматични и ръчни архиви, чиято цялост и наличност се проверява.

9. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим Протект"ЕООД - Димитровград;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

10. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

11. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита.

Действия за защита при аварии, произшествия и бедствия

Чл. 33. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Директор „УРЧР", като това се отразява в дневника по архивиране и възстановяване на данни.

(4) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(5) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 34. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП-Публичен изпълнител, МВР, Инспекцията по труда,Съдилища, Държавни съдебни изпълнители, Частни съдебни изпълнители, Агенция по вписванията – Търговски регистър или Имотен регистър, Нотариуси, Централен регистър по особените залози, Органи за медицинска експертиза, РИОКОЗ, други Агенции и други държавни органи, ведомства и администрации, министерства и регионалните им структури, общини и общински администрации.).

Данни от регистъра могат да бъдат предоставяни и с оглед изпълнение на законови задължения на дружеството – администратор за вписване на обстоятелства с правно значение

в съответните регистри или за прилагане на предвиден в действащото законодателство разрешителен, лицензионен, уведомителен или друг административно-правен режим.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 35. Администраторът на лични данни трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 36. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

VI. Регистър „Клиенти"

Общо описание на регистъра

Чл. 37. В регистъра се обработват лични данни на клиенти на дружеството, както и на шофьори на транспортни фирми, които са наети от клиентите и са необходими за изпълнение на договорни отношения /Закон за задълженията и договорите/, и за осъществяване на лигитимния интерес на администратора.

Категории лични данни, обработвани в регистъра

Чл. 38. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: име , ЕГН ; данни от лична карта; телефон.

Технологично описание на регистъра

Чл. 39. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Личните данни, съдържащи се в договори, заявления и декларации, се съхраняват за срок от 5 години съгласно Основна процедура ОП 01 Управление на документирана информация в „Неохим"АД или до отпадане необходимостта от съхраняването им.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 40. (1) Данните от регистъра се обработват от служителите в отдел „Продажби" и/или отдел „Правен" при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае". Електронен достъп до личните данни имат: Ръководител ИО и програмист софтуерни приложения, Търговски директор,

Ръководител отдел „Продажби", Зам. Ръководител отдел „Продажби", Експерт отдел „Продажби".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Клиенти"

Чл. 41. (1) Оценка на въздействието на регистър „Клиенти" се извършва в съответствие с критериите Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2 .в регистъра не се съдържат специални категории лични данни.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Клиенти" е ниско.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Клиенти"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Клиенти	ниско	ниско	ниско	ниско

Технически и организационни мерки за защита на личните данни в регистър „Клиенти"

Чл. 42. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на лицата по чл. 40 .

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в кабинет с контролиран достъп само за лицата по чл.40.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства, разположени в коридорите на сградата.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на отговорните служители.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Клиенти“ се поддържа на хартиен и електронен носител .

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим”АД.

3. Достъп до регистъра имат лицата по чл. 40 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Ръководителят на отдел „Продажби” е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 39, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим”АД.

8. Личните данни могат да бъдат размножавани и разпространявани от отговорните служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Ръководителят на отдел „Информационни технологии” е отговорен за управлението на автоматизираните информационни системи и мрежи. Само лицата посочени в чл. 40 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

6. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм.

7. Контролът по използването на тези носители се осъществява от Ръководителя на отдел „Информационни технологии”.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим протект"ЕООД – Димитровград.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 39, ал. 4.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита, съгласно утвърдена процедура.

Действия за защита при аварии, произшествия и бедствия

Чл. 43. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(4) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 44. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение .

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 45. Администраторът на лични данни трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 46. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

VII. Регистър „Доставчици"

Общо описание на регистъра

Чл. 47. В регистъра се обработват лични данни на доставчици на дружеството, както и на шофьори на транспортни фирми, които са наети от доставчиците и са необходими за изпълнение на договорни отношения /Закон за задълженията и договорите/, и за осъществяване на лигитимния интерес на администратора.

Категории лични данни, обработвани в регистъра

Чл. 48. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: име , ЕГН ; телефон, данни от лична карта.

Технологично описание на регистъра

Чл. 49. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Личните данни, съдържащи се в договори, декларации и др. документи, се съхраняват за срок от 5 години съгласно Основна процедура ОП 01 Управление на документирана информация в „Неохим"АД или до отпадане необходимостта от съхраняването им.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 50. (1) Данните от регистъра се обработват от служителите в отдел „Продажби" и/или отдел „Правен" и отдел „МТСРСО" при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Доставчици"

Чл. 51. (1) Оценка на въздействието на регистър „Доставчици" се извършва в съответствие с критериите на Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2 .в регистъра не се съдържат специални категории лични данни.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Доставчици" е ниско.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Доставчици"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Доставчици	ниско	ниско	ниско	ниско

Технически и организационни мерки за защита на личните данни в регистър „Доставчици"

Чл. 52. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 50 лица.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в кабинет с ограничен достъп само за лицата по чл.50.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с контролиран достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани със заключване на вратите и пожарогасителни средства на етажа на сградата.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на отговорните служители.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Доставчици" се поддържа на хартиен и електронен носител .

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим"АД.

3. Достъп до регистъра имат лицата по чл. 50 в съответствие с принципа „Необходимост да се знае".

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Ръководителят на отдел „Продажби" и отдел „МТСРСО" са отговорни за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 49, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим"АД.

8. Личните данни могат да бъдат размножавани и разпространявани от отговорни служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки отговорен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Ръководителят на отдел „Информационни технологии" е отговорен за управлението на автоматизирани информационни системи и мрежи. Само лицата посочени в чл. 50 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

6. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм.

7. Контролът по използването на тези носители се осъществява от Ръководителя на отдел „Информационни технологии".

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим протект"ЕООД – Димитровград.

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 49, ал. 4.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита, съгласно утвърдена процедура .

Действия за защита при аварии, произшествия и бедствия

Чл. 53. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(4) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 54. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение .

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 55. Администраторът на лични данни трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 56. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

VIII. Регистър „Видеонаблюдение"

Общо описание на регистъра

Чл. 57. В регистъра се обработват лични данни на следните категории субекти на лични данни: работници и служители на дружеството, бивши работници и служители, стажанти, практиканти, посетители, работници на фирми, страни по договори с „Неохим"АД и са необходими за осъществяване на законния интерес на администратора – спазване на трудовата дисциплина, защита от незаконни посегателства, предотвратяване на загуба на интелектуална и материална собственост. Обработването на лични данни се извършва съвместно с „Неохим Протект"ЕООД – Димитровград.

Категории лични данни, обработвани в регистъра

Чл. 58. В регистъра се обработват следните категории лични данни:

1. Чувствителни лични данни – физическа идентичност – видеообраз, включително разпознаване на лица.

Технологично описание на регистъра

Чл. 59. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на електронен носител.

(3) Данните в регистъра се събират посредством технически средства за видеозапис.

(4) Личните данни се съхраняват на паметта на DVR устройства за срок не повече от 2 месеца, освен в случаите на съдебен спор или търговска рекламация. В тези случаи личните данни се съхраняват за срока на възникналата необходимост на DVD носител.

(5) Администраторът на лични данни предоставя достъп, справки, и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт; ако е настъпило събитие, в т.ч. трудова злополука, или зловредно действие на трети лица или на служители на дружеството – администратор (като например нахлуване с взлом, кражба, грабеж, палеж, увреждане на частно или обществено имущество, хулигански прояви и др. Подобни) и е необходимо предоставянето на данни от регистър „Видеонаблюдение" за изясняване и установяване на случая с оглед защитата на легитимните интереси на администратора или на на защитата на обществения интерес; при поискване от органите на МВР или други оправомощени разследващи органи.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 60. (1) Данните от регистъра се обработват от: Директор УРЧР, Ръководител отдел, „Експерт УЧР", Началник цех, Заместника началник цех" Инженер химически процеси", „Апаратчик химични процеси", „Главен ревизор", „Финансов ревизор", „Инженер телекомуникации", Системен администратор, Директор производство, Регистратор към „Неохим Протект" ЕООД, Охранител Диспечер към „Неохим Протект" ЕООД и Управител към „Неохим Протект" ЕООД при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Видеонаблюдение"

Чл. 61. (1) Оценка на въздействието на регистър „Видеонаблюдение" се извършва в съответствие с Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2. в регистъра се съдържат специални категории лични данни – физическа идентичност - видеообраз.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Видеонаблюдение" е средно.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Видеонаблюдение"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Видеонаблюдение	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в регистър „Видеонаблюдение"

Чл. 62. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 60 лица.

2. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в комуникационни шкафове с ограничен достъп.

3. Физическият достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица нямат достъп до помещенията, в които се обработват лични данни от регистъра.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД, и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

4. Ръководителят на отдел „Информационни технологии"към „Неохим"АД и Управителят на „Неохим Протект"ЕООД са отговорни за контрол на достъпа до регистъра.

5. Сроковете за съхранение на лични данни от регистъра, са определени в чл. 59, ал. 4.

6. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи .

10. След изтичане на срока от 2 месеца личните данни от регистъра се унищожават автоматично, а в останалите случаи се унищожават с протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване, които са инсталирани само на персоналните компютри, които се водят на упълномощените служители.

2. Достъпът до персоналните компютри е чрез потребител и парола от изградената Активна директория.

3. За достъп до софтуера всеки упълномощен потребител има профил /потребителско име и парола/.

4. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

5.Ръководителят на отдел „Информационни технологии" е отговорен за управлението на регистъра. Само лицата посочени в чл. 60 имат достъп до регистъра.

6. За всички устройства и комуникационни средства, от които зависи правилното поддържане на регистъра, са осигурени непрекъсваеми токозахранващи устройства (UPS).

7.Всички DVD носители, на които при нужда се записват лични данни в резултат на възникнала необходимост се предават и съхраняват в огнеупорна каса със заключващ механизъм.

8. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

9.Достъпът до локалната мрежа се ограничава чрез хардуерно устройство – защитна стена.

Действия за защита при аварии, произшествия и бедствия

Чл. 63. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

Чл. 64. Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 65. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение .

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 66. (1) След изтичане на двумесечния срок за съхранение , данните се изтриват автоматично, а в случаите на съдебен спор или търговска рекламация, от комисия с протокол.

IX. Регистър „Деловодство"

Общо описание на регистъра

Чл. 67. В регистъра се обработват лични данни на следните лица:; работници и служители в „Неохим"АД; кандидати за работа и физически лица, контрагенти по договори с „Неохим"АД, и са необходими за осъществяване на законово задължение за администратора на лични данни, за изпълнение на договорни и трудови отношения, за постигане на законово определени цели , изпълнение на законови задължения на администратора и осъществяване на лигитимния му интерес.

Категории лични данни, обработвани в регистъра

Чл. 68. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: име , ЕГН, адрес, данни от лична карта; телефон, международен паспорт.

2. чувствителни лични данни: данни относно здравния статус на физически лица.

Технологично описание на регистъра

Чл. 69. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и на електронен носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Личните данни се съхраняват за срок от 5 години . След изтичане времето за съхранение, личните данни се унищожават физически, чрез изтриване и унищожаване на хартиените екземпляри.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 70. (1) Данните от регистъра се обработват от завеждащ административна служба и упълномощените със заповед лица при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Деловодство"

Чл. 71. (1) Оценка на въздействието на регистър „Деловодство" се извършва в съответствие с критериите на Общия регламент за защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;

2 .в регистъра се съдържат специални категории лични данни, свързани със здравния статус на физически лица.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Деловодство" е средно.

(3) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Оценка на нивото на въздействие на регистър „Деловодство"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Деловодство	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в регистър „Деловодство"

Чл. 72. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на лицата по чл. 70.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с ограничен достъп само за отговорни лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани с заключване на вратите и пожарогасителни средства, разположени на етажа на сградата.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на отговорни служители.

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават с Общия регламент за защита на личните данни,ЗЗЛД и настоящата Инструкция.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора.

3. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и

по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Деловодство" се поддържа на хартиен и електронен носител.

2. Обработването на личните данни се извършва в рамките на работното време на „Неохим"АД.

3. Достъп до регистъра имат лицата по чл. 70 в съответствие с принципа „Необходимост да се знае".

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Завеждащ административна служба е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 69, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в „Неохим"АД

8. Личните данни могат да бъдат размножавани и разпространявани от отговорните служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

9. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

10. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Изпълнителния директор комисия.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1.Всеки отговорен служител се регистрира на използвания персонален компютър с потребител и парола като се спазват правилата на изградената в дружеството активна директория /АД/.

2. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване, в които упълномощените лица се идентифицират с личен профил /потребител с парола/ с определени съобразно задълженията му права и нива на достъп.

3. Данните се въвеждат в база данни и се съхраняват на сървър, разположен в помещение с ограничен или контролиран достъп.

4. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, сървърна система и база данни.

5. Сървъра за съхранение на данни и персоналните компютри, от които се извършва обработката, се защитават от външни посегателства със софтуерни решения и хардуерни продукти.

6. Ръководителят на структурно звено „Информационни технологии" е отговорен за контрол на достъпа до автоматизираните информационни системи и мрежи.

7. За сървъра и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

8. За цялостта на базата данни се извършват автоматични и ръчни архиви, чиято цялост и наличност се проверява.

9. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от „Неохим Протект"ЕООД - Димитровград;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

10. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

11. Сроковете за съхранение на данни от регистъра са описани в чл.69, ал. 4.

(5) Предаване на данни от регистъра по електронен път или на преносими технически носители се осъществява чрез използване на съвременни технологии за защита.

Действия за защита при аварии, произшествия и бедствия

Чл. 73. (1) При възникване и установяване на инцидент, веднага да се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, длъжностното лице по защита на данните вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Директор „УРЧР", като това се отразява в дневника по архивиране и възстановяване на данни.

(4) При установяване нарушение на сигурността на личните данни, длъжностното лице по защита на данните уведомява КЗЛД за нарушението без забавяне и когато е осъществимо – не по-късно от 72 часа след като е разбрал за него.

(5) Длъжностното лице по защита на данните уведомява субекта на данни за нарушението без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице.

Предоставяне на лични данни на трети лица

Чл. 74. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Публичен изпълнител, Агенции и други държавни органи, ведомства и администрации, министерства и регионалните им структури, Държавен съдебен изпълнител, съдилища, общини и общински администрации, МВР, Посолства).

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 75. Администраторът на лични данни трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 76. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Ако събраните лични данни на субектите ще се използват за цел, различна от тази, за която са събрани, администраторът следва да предостави на субекта на данни допълнителна писмена информация за целите на предоставянето на лични данни, съгласно примерен образец /Приложение № 3 – Уведомление до частен съдебен изпълнител/.

§2. Да се предостави на официалния сайт на „Неохим"АД обобщена, кратка и разбираема информация относно:

идентифициране на дружеството – наименование и данни за контакт, вкл. с Длъжностното лице по защита на данните;

-какви категории лични данни се събират и за какви цели се обработват;

-категориите получатели на лични данни извън дружеството, както и дали ще се предават данни в трети страни извън ЕС;

-срока за съхранение на данните;

-конкретни права на субектите на данни / право на достъп, коригиране или изтриване на лични данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните/ и реда за упражняването им;

-правото на жалба до КЗЛД и до съда;

-дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени;

-извършва ли се видеонаблюдение на територията на дружеството.

§3. Да се създаде служебна електронна поща, която да се използва само при кандидатстване за работа. На всяко получено съобщение от кандидат за работа да се изпраща автоматичен отговор с данните на администратора и информация, че личните данни на лицето ще бъдат използвани само за целите на подбор на персонал и срока, за който ще бъдат съхранявани.

§4. Неразделна част от настоящата инструкция са: Приложение № 1 Процедура за приемане, разглеждане и отговаряне на искания от физически лица за упражняване на правата им; Приложение № 2 Процедура за действие в случай на нарушение на сигурността на личните данни; Приложение № 3 Примерен образец за уведомление на ЧСИ и Приложение № 4 Декларация за поверителност.

§5. Инструкцията се приема на основание чл. 23, ал. 4 от Закона за защита на личните данни, чл. 19, т. 2 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни .

Дата:23.05.2018 г.
Гр.Димитровград

Съгласувано със:

Стефан Димитров
Директор „УРЧР"

Калинка Койнарска
Директор ДСТОРПО

Андон Димитров
Директор дирекция „Продажби"

Светла Вълчева
Ръководител СТМ

Дияна Димитрова
Ръководител отдел „ЧР"

Борислав Точаров
Ръководител отдел „ИТ"

Павлина Бълварова
Завеждащ адм.служба

Катя Господинова
Главен юрисконсулт

Изготвили:
Петя Дичева
Юрисконсулт

Златка Драгиева
Ръководител отдел" Reach и стандартизация"

ПРОЦЕДУРА ЗА ПРИЕМАНЕ, РАЗГЛЕЖДАНЕ И ОТГОВАРЯНЕ НА ИСКАНИЯ ОТ ФИЗИЧЕСКИ ЛИЦА ЗА УПРАЖНЯВАНЕ НА ПРАВАТА ИМ

1. ПРЕДМЕТ И ЦЕЛ НА ПРОЦЕДУРАТА

Настоящата процедура регламентира приемането, разглеждането и отговарянето на искания на физически лица за упражняване на правото им.

Цел на процедурата е да осигури упражняване на правата на физическите лица във връзка с Общ регламент за защита на данните – Регламент (ЕС) 2016 / 679

2. ОБХВАТ И ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща дейностите, които се извършват при искания на субектите на данни за упражняване на правата им по Регламента (ЕС) 2016 / 679. Отговорник за управление на процеса е длъжностното лице по защита на личните данни.

3. УСЛОВИЯ ЗА УПРАЖНЯВАНЕ НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ ВЪВ ВРЪЗКА С ОБЩ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ДАННИТЕ – РЕГЛАМЕНТ (ЕС) 2016 / 679 И СРОКОВЕ ЗА ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ

„Неохим“ АД съдейства за упражняването на правата на субектите на данни и не отказва да предприеме действия по тях, освен ако докаже, че не е в състояние да идентифицира субекта на данните.

Когато „Неохим“ АД има основателни опасения във връзка със самоличността на субекта на данни, който подава искане за упражняване на права, администратора на данни може да поиска предоставяне на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

„Неохим“ АД предоставя на субекта на данни информация относно действията, предприети във връзка с искане за упражняване на правата, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането.

При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Дружеството информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето.

Когато „Неохим“ АД не предприеме действия по искането на субекта на данни, той уведомява субекта на данни без забавяне и най късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.

Когато субекта на данни с електронни средства, по възможност информацията му се предоставя с електронни средства, освен ако субекта на данни не е поискал друго.

„Неохим“ АД предоставя възможност за подаване на искания за упражняване на правата на субектите по електронен път особено, когато личните данни се обработват електронно.

4. ПРАВА ОТ СУБЕКТИТЕ НА ДАННИ

Субектите на данни имат:

- ***право на достъп*** до личните им данни, свързани с тях, които се обработват от „Неохим АД

- ***право на коригиране или допълване*** на неточни или непълни лични данни

- право на изтриване / *"право да бъдеш забравен"* / на лични данни, които се обработват незаконосъобразно или с отпаднало правно основание / изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани и др. /

- ***право на ограничаване на обработването*** – при наличие на правен спор между дружеството и физическото лице до неговото решаване и / или за установяването, упражняването или защитата на правни претенции

- ***право на преносимост на данните*** – ако се обработват по автоматизиран начин на основание съгласие или договор. За целта данните се предават в структуриран, широко използвн и пригоден за машинно четене формат. Ако е технически осъществимо, прехвърлянето на данни може да стане пряко от „Неохим" АД към друг администратор. Дружеството пренася данни, предоставени лично от субекта на данни, както и лични данни, генерирани и събрани от неговата дейност

- ***право на възражение*** – субектите на данни имат право по всяко време и на основания, свързани с конкретната ситуация на лицето, при условие, че не съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субектите на данни, или съдебен процес

- ***право да не бъде обект на изцяло автоматизирано решение, включващо профилиране***, което поражда правни последствия за субекта на данните или го засяга в значителна степен

5. ПРАКТИЧЕСКО УПРАЖНЯВАНЕ НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ

Когато субектите на данни желаят да ползват от правата си посочени в т. 4 попълват заявление по утвърден образец за осъществяване на правата си в деловодството на дружеството или по електронен път, чрез сайта на дружеството. Работниците и служители, които трябва да минат през портала на дружеството, за да подадат заявлението си в деловодството уведомяват прекия си ръководител, който е длъжен да им издаде служебна бележка за преминаване през главен портал. След като бъдат заведени в с входящ номер заявленията се предоставят на Изпълнителен Директор, който след запознаване с исканията им ги препраща на длъжностното лице по защита на личните данни. Длъжностното лице в зависимост от подаденото заявление за упражняване на права извършва следното

При подаване на заявление за разрешаване на достъп до обработваните лични данни на субектите на данни длъжностното лице в срока по т. 3 събира информация обработват ли се лични данни свързани със субекта на данните и го уведомява за следното:

- целите на обработването

- съответните категории лични данни

- получателите или категориите получатели, пред които а или ще бъдат разкрити личните данни

- срока, за който ще се съхраняват личните данни, а ако това е невъзможно критериите, използвани за определяне на този срок

- съществуване на право да се изиска от „Неохим" АД коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване

- правото на жалба до надзорен орган

- когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник

- съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4 от ОРЗД, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните

- когато личните данни се предават на трета държава или на международна организация, субектът на данните се информира относно подходящите гаранции по член 46 от ОРЗД във връзка с предаването

- „Неохим" АД предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, дружеството може да наложи разумна такса въз основа на административните разходи. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго

При искане за коригиране или допълване на лични данни, лицето подава заявление за корекция или допълване на личните му данни. В заявлението се описва точно кои данни лицето желае да бъдат коригирани или допълнени като се посочват основанията за това. Длъжностното лице по защита на личните данни в срока по т. 3 проверява верността на личните данни на субекта. В случай, че се установи неточност на личните му данни длъжностното лице предприема необходимите мерки те да се коригират или допълнят.

При искане за изтриване на лични данни субекта на данни подава заявление в деловодството на дружеството или по електронен път. В заявлението се посочват личните данни, които лицето желае да бъдат изтрити. Длъжностното лице по защита на личните данни в сроковете по т. 3 предприема необходимите мерки личните данни на лицето да бъдат изтрити, когато е приложимо някое от посочените по долу основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин

- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните съгласно член 6, параграф 1, буква а) от ОРЗД или член 9, параграф 2, буква а) от ОРЗД, и няма друго правно основание за обработването

- субектът на данните възразява срещу обработването съгласно член 21, параграф 1 и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно член 21, параграф 2 от ОРЗД

- личните данни са били обработвани незаконосъобразно

- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора

- личните данни са били събрани във връзка с предлагането на услуги на информационното общество по член 8, параграф 1 от ОРЗД

Когато „Неохим" АД е направил личните данни обществено достояние преди субекта на данни да поиска те да бъдат изтрити администратора на лични данни предприема технически мерки, за да уведоми в сроковете по т. 3 администраторите, на които личните данни на субекта са предоставени, че субектът на данни е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

Изтриване на свързани със субекта лични данни не се прилага, когато обработването е необходимо:

- за упражняване на правото на свобода на изразяването и правото на информация

- за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора

- по причини от обществен интерес в областта на общественото здраве в съответствие с член 9, параграф 2, букви з) и и) от ОРЗД, както и член 9, параграф 3 от ОРЗД

- за установяването, упражняването или защитата на правни претенции

При искане за ограничаване на обработването на лични данни лицето подава заявление, в което посочва личните данни обработването, на които желае да бъде ограничено. Длъжностното лице по защита на данните в сроковете по т. 3 се запознава с искането, и ако е налице едно от долупосочените условия предприема необходимите технически и организационни мерки за ограничаване на обработването:

- точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на личните данни

- обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им

- администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции

- субектът на данните е възразил срещу обработването съгласно член 21, параграф 1 от ОРЗД в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните

При ограничаване на обработването в горепосочените случаи тези данни се обработват от „Неохим" АД с изключение на тяхното съхранение само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице или поради важни основания от обществен интерес за Съюза или държава членка.

Когато субект на данните е изискал ограничаване на обработването съгласно горепосочените условия, администраторът го информира преди отмяната на ограничаването на обработването.

„Неохим" АД уведомява за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

При искане от субекта на данни за получаване на личните му данни, които е предоставил в структуриран, широко използван и пригоден за машинно четене формат или желае „Неохим" АД да прехвърли тези данни на друг администратор попълва заявление, в което посочва кои данни желае да получи и / или прехвърли. Длъжностното лице по защита на данните в сроковете по т. 3 проверява дали:

- обработването е основано на съгласие в съответствие с член 6, параграф 1, буква а) от ОРЗД или член 9, параграф 2, буква а) от ОРЗД или на договорно задължение съгласно член 6, параграф 1, буква б) от ОРЗД; и

- обработването се извършва по автоматизиран начин

При изпълнение на горепосочените 2 условия длъжностното лице за защита на данните организира предоставянето на лицето на личните му данни в широко използван и пригоден за машинно четене формат. При искане от субекта личните му данни да бъдат прехвърлени на друг администратор, отдел „Информационни технологии" дав становище технически осъществимо ли е това. В случай, че е технически осъществимо данните на субекта се прехвърлят без забавяне в сроковете по т. 3.

При възражение от субекта на данни за обработване на данните му, което се основава на:

- обработването за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора

- обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете

той подава заявление, в което посочва срещу кои лични данни има възражение да бъдат обработвани от „Неохим“ АД. Длъжностното лице по защита на личните данни в сроковете по т. 3 предприема мерки за прекратяване на обработването на лични данни, освен ако не се докаже, че съществуват законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

Когато субекта на данни иска да упражни правото си да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен подава заявление. Длъжностното лице по защита на данните проверява дали решението:

- е необходимо за сключването или изпълнението на договор между субекта на данни и администратора
- е разрешено от правото на Съюза или правото на държава членка, което се прилага спрямо администратора, и в което се предвиждат също подходящи мерки за защита на правата и свободите, и легитимните интереси на субекта на данните

В случай, че едно от горепосочените две условия е изпълнено администратора не предприема никакви мерки. В противен случай в сроковете по т. 3 длъжностното лице по защита на личните данни предприема мерки субекта да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен.

6. ИЗПОЛЗВАНА ТЕРМИНОЛОГИЯ

- ***„Лични данни“*** означава 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 с 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 и социална идентичност на това лице
- ***„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
- ***„Ограничаване на обработването"*** означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще
- ***„Профилиране"*** означава 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
- **„Администратор"** означава 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 Съюза 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

- ***„Получател"*** означава 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
- **„Съгласие на субекта на данните"** означава 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

ПРОЦЕДУРА ЗА ДЕЙСТВИЕ В СЛУЧАЙ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

1. ПРЕДМЕТ И ЦЕЛ НА ПРОЦЕДУРАТА

Настоящата процедура регламентира план за действие в случай на нарушение на сигурността на личните данни.

Цел на процедурата е да осигури подготвеността и способността за подходяща, адекватна и навременна реакция в случай на нарушение на сигурността на личните данни.

2. ОБХВАТ И ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща дейностите, които се извършват при нарушение на сигурността на личните данни. Процедурата е задължителна за прилагане за всички длъжностни лица обработващи лични данни под ръководството на администратора. Отговорник за управление на процеса е длъжностното лице по защита на личните данни.

3. НАРУШЕНИЕ НА СИГУРНОСТТА

3.1. Определяне нарушението на сигурността на личните данни и броя на засегналите лица.

Нарушение на сигурността на личните данни е такова нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, наразрешено разкриване или достъп до лични данни, които се съхраняват предават или обработват по друг начин. За да има нарушение на сигурността на личните данни трябва да се е е стигнало до реално събитие, състоящо се в случайното или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни. Потенциалният риск от възникване на такова събитие, доколкото не е реализиран, не съставлява нарушение на сигурността.

4. УВЕДОМЯВАНЕ НА НАДЗОРНИЯ ОРГАН В СЛУЧАЙ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

В случай, че длъжностните лица обработващи лични данни под ръководството на администратора засекат нарушение в сигурността на данни незабавно уведомяват прекия си ръководител, който веднага уведомява длъжностното лице по защита на данните, чрез доклад. В доклада се описва вида на нарушението, евентуалния брой засегнати лица и приблизителното количество на засегнатите записи на лични данни. Длъжностното лице по защита на данните в срок до 24 часа прави преценка нарушението съставлява ли нарушение на сигурността на данни по смисъла на Регламента и на следващо място дали съществува вероятност това нарушение да доведе до риск за правата и свободите на засегнатите субекти и уведомява за това администратора. Длъжностното лице по защита на данните уведомява администратора за евентуалните последици от нарушението на сигурността на личните данни и му предлага мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици. В случай, че съществува вероятност нарушението да породи риск за правата и свободите на физическите лица администратора без нужно забавяне, и когато това е

осъществимо – не по късно от 72 часа след като е разбрал за него, чрез длъжностното лице по защита на данните уведомява за нарушението на сигурността на личните данни надзорния орган

Уведомлението към надзорния орган за нарушение на сигурността на данните съдържа:

- описание на естеството на нарушение на сигурността на личните данни, включително, ако е възможно категориите и приблизителния брой на засегнатите субекти на данни и приблизителното количество на засегнатите записи на лични данни
- името и координатите за връзка с длъжностното лице по защита на данните или друга точка за контакт, от която може да се получи повече информация
- описание на евентуалните последици от нарушението на сигурността на личните данни
- описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици
- когато уведомлението не е подадено в срок до 72 часа след като администратора е разбрал за него се посочват причините за забавянето

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията се подава поетапно без по – нататъшно ненужно забавяне.

Длъжностното лице по защита на данните документира всяко нарушение на сигурността на личните данни, включително фактите свързани с нарушението на сигурността на лични данни, последиците от него и предприетите действия за справяне с него.

5. СЪОБЩАВАНЕ НА ЗАСЕГНАТИТЕ СУБЕКТИ НА ДАННИ ЗА НАРУШАВАНЕ СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица администратора информира засегнатите субекти на данни за нарушение на сигурността на личните данни. В тези случаи администратора, без ненужно забавяне най късно до 72 часа от откриването му, съобщава на субектите на данните за нарушението на сигурността на личните данни. В съобщението до субектите на данните на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочва:

- името и координатите за връзка с длъжностното лице по защита на данните или друга точка за контакт, от която може да се получи повече информация
- описание на евентуалните последици от нарушението на сигурността на личните данни
- описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици

Горепосоченото съобщение до субектите на данни не се прави, ако някое следните условия е изпълнено:

- предприети са подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по специално мерките, които правят данните неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране
- администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност вече да се материализира високият риск за правата и свободите на субектите на данни
- уведомяването би довело до непропорционални усилия. В такъв случай се прави публично съобщение.

6. ИЗПОЛЗВАНА ТЕРМИНОЛОГИЯ

- „Лични данни“ означава 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 с 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 и социална идентичност на това лице
- „Нарушение на сигурността на лични данни“ означава 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

Дата: 23.05.2018г.

Вариант 1

Приложение № 3

УВЕДОМЛЕНИЕ

До г-н/г-жа ……., на длъжност …….. в „Неохим"АД – Димитровград

Г-н/г-жо …….,

Уведомяваме Ви, че във връзка със законово задължение на „Неохим"АД, в качеството си на трето лице в изпълнително производство /на основание чл. 508, ал.2 от ГПК/ и по повод постъпило разпореждане на Частен съдебен изпълнител по изп. дело № …….., предоставихме информация на ЧСИ …….. относно преведеното Ви трудово възнаграждение по банковата Ви сметка.

Директор
„Управление и развитие на човешките ресурси":……
Стефан Димитров Димитров

Връчено на работника на дата:…….подпис:…….(работник/служител)

Връчител:

……
(име, фамилия, длъжност, подпис)

Съгласувано с:

……
Експерт „Управление на човешките ресурси"

Изготвил:

……
Юрисконсулт

Дата: 23.05.2018г.

Вариант 1

Приложение № 4

Към Инструкция за МЗЛД

на „Неохим”АД

Д Е К Л А Р А Ц И Я

Подписаният/та……ЕГН……

(име, презиме и фамилия)

на длъжност……..……..**в**……..……

……..……

(структурно звено)

……..

На основание Инструкция за мерките за защита на личните данни в „Неохим”АД, в сила от 23.05.2018г.

Декларирам, че доброволно предоставям всички посочени по-горе мои лични данни с цел валидно декларираме и документиране на волеизявленията ми, дадени с настоящата декларация, а именно:

Д Е К Л А Р И Р А М, ЧЕ :

1. Ще пазя в тайна личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения, няма да ги разпространявам и няма да ги използвам за други цели освен за прякото изпълнение на служебните ми задължения.
2. Запознат/а/ съм с нормативната уредба, политиката и ръководствата в областта на защита на личните данни, както и със съдържанието на Инструкция за мерките за защита на личните данни в „Неохим”АД, в сила от 23.05.2018г.
3. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни нося дисциплинарна отговорност по Кодекса на труда, административно-наказателна отговорност по Закона за защита на личните данни и наказателна отговорност, ако деянието осъществява състава на чл. 284 и /или на чл. 319д от Наказателния кодекс.
4. Уведомен/а съм, че настоящата Декларация ще се приложи към трудовото ми досие и копие от същата ще се предостави и съхранява и при лицето, отговорно за защита на личните данни в „Неохим”АД.

Дата:…… **ДЕКЛАРАТОР:**……..

гр…….. *(подпис)*