УТВЪРЖДАВАМ,

АЛЕКСАНДР МАКАРЕВИЧ

УПРАВИТЕЛ НА НИС ПЕТРОЛ ЕООД:

.....

НИС ПЕТРОЛ ЕООД София Sofia NIS PETROL EOOD

Собственик: НИС ПЕТРОЛ ЕООД	Дата: 20.02.2020	Версия 2.0

НИС ПЕТРОЛ ЕООД

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

РЕГЛАМЕНТ 2016/679

Организация за обработване и защита на личните данни

Принципи. Правила. Изисквания. Мерки за защита

СЪДЪРЖАНИЕ

I. ОБЩИ ПОЛОЖЕНИЯ 2
II. ДЕФИНИЦИИ 2
III. ЦЕЛИ ЗА СЪБИРАНЕТО И ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ 2
IV. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ 3
V. ПРИЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ 4
VI. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ 5
VII. ОСНОВНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА 12
VIII. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ 14
IX. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ 14
X. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ 15

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) НИС ПЕТРОЛ ЕООД (НИС ПЕТРОЛ) е юридическо лице, което извършва дейности свързани с търговия на горива и петролни продукти.

(2) НИС ПЕТРОЛ е юридическо лице със седалище и адрес на управление в София, бул. Никола Й. Вапцаров 51А.

(3) НИС ПЕТРОЛ е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679

(4) Като администратор на лични данни, при обработването на лични данни НИС ПЕТРОЛ спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

(5) Като юридическо лице, възникнало по силата на закона, НИС ПЕТРОЛ осъществява дейностите, описани в Правилник за вътрешния трудов ред.

(6) НИС ПЕТРОЛ обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им в зависимост от изискванията, заложени в съответните закони, регламенти и нормативни актове. В този случай НИС ПЕТРОЛ действа като администратор на лични данни. В някои от тези случаи НИС ПЕТРОЛ работи с трети лица, явяващи се обработващи на личните данни, с които има подписани споразумения, съгласно изискванията на чл. 24 от Общия регламент.

(7) В случаите, в които НИС ПЕТРОЛ обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от НИС ПЕТРОЛ и трето лице, НИС ПЕТРОЛ има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

Чл. 2.(1) Настоящата Политика за защита на личните данни на НИС ПЕТРОЛ урежда организацията на обработване и защитата на лични данни на служителите, включително и на кандидатите за работа в НИС ПЕТРОЛ, на контрагентите и партньорите на НИС ПЕТРОЛ, както и на всички други групи физически лица, с които НИС ПЕТРОЛ влиза в отношения при осъществяването на дейността си. Неотменна част от настоящата Политика е Инструкция за техническите мерки за защита на личните данни, утвърдена от Управителя на НИС ПЕТРОЛ.

(2) В съответствие с изискванията на чл. 37, § 7 от Регламент (ЕС) 2016/679 в НИС ПЕТРОЛ със Заповед на Управителя е определено Длъжностно лице по защитата на обработваните лични данни.

II. ДЕФИНИЦИИ

Чл. 3.(1) „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 чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни“ 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, заличаване или унищожаване.

(3) „Регистър с лични данни" представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до който се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

III. ЦЕЛИ ЗА СЪБИРАНЕТО И ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл. 4. (1) Личните данни се събират за конкретни, точно определени от закона цели, приложимите нормативни актове и регламенти, прилагани от НИС ПЕТРОЛ. Личните данни се обработват законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(2) Ако конкретната цел или цели, за които се обработват лични данни от НИС ПЕТРОЛ, не изискват или вече не изискват идентифициране на субекта на данните, НИС ПЕТРОЛ не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

(3) Основанието за законосъобразност на обработването на личните данни от НИС ПЕТРОЛ, съгласно Член 6 от Регламента са:

а) субектът на данни е дал съгласие за обработването на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) 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.

В тези случай, НИС ПЕТРОЛ информира субектите на лични данни за всички аспекти по обработването на личните им данни, включително, но не само за правата им, съгласно изискванията на Общия регламент.

В случаите, когато НИС ПЕТРОЛ обработва лични данни на субектите на основание чл. 6 , параграф 1, буква а) от Общия регламент, НИС ПЕТРОЛ изисква предварителното съгласие на субектите и ги уведомява предварително за всички аспекти по обработването на личните им данни, включително, но не само за правата им, съгласно изискванията на Общия регламент.

IV. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 5. (1) Всеки, който предоставя личните си данни има следните права:

1. Да даде изрично съгласие или несъгласие за обработване на личните му данни;
2. Да получи информация за обработването на личните си данни;
3. Да получи достъп до съхраняваните му лични данни;
4. Да поиска неправилните, неточните или непълните лични данни да бъдат коригирани;
5. Да поиска личните данни да бъдат унищожени, когато вече не са необходими или ако обработването им е незаконно;
6. Да възрази срещу обработването на лични му данни на основания, свързани с конкретна ситуация;
7. Да поиска ограничаване на обработването на личните си данни в конкретни случаи;
8. Да получи личните си данни в пригоден за машинно четене формат и да ги изпраща на друг администратор („преносимост на данните“);
9. Да поиска решенията, основаващи се на автоматизирано обработване и са въз основа на личните данни на притежателя им и които значително засягат субекта, да бъдат направени от физически лица, а не само от компютри. Също така притежателят им има право в този случай да изрази личната си гледна точка и да оспори решението.

V. ПРИЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 6. (1) Принципите за защита на личните данни са:

1. ***Законосъобразност, добросъвестност и прозрачност*** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни.
2. ***Ограничение на целите*** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;
3. ***Свеждане на данните до минимум*** – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;
4. ***Точност*** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно унищожаване или коригиране на неточни данни, при отчитане на целите на обработването;
5. ***Ограничение на съхранението*** – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;
6. ***Цялостност и поверителност*** – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически и организационни мерки за обезпечеността на данните;

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

VI. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 7. НИС ПЕТРОЛ организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени и са в съответствие с определените нива на въздействие.

Чл. 8 (1) НИС ПЕТРОЛ прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на информационните системи и мрежи;
5. Криптографска защита.

Чл. 9 (1) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на задълженията на НИС ПЕТРОЛ и/или за срока, определен от нормативен акт.

(2) Събирането, обработването и съхраняването на лични данни в регистрите на НИС ПЕТРОЛ се извършва на хартиен, технически и/или електронен носител в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 10. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от НИС ПЕТРОЛ, подписват информирано съгласие по образец.

Чл. 11. (1) Право на достъп до регистрите с лични данни имат само определените за тази цел служители на НИС ПЕТРОЛ, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

(2) Определянето на служители по чл. 11, ал.1 се извършва на база длъжностна характеристика или чрез изрична заповед на Управителя на „НИС Петрол“ ЕООД или оправомощено от него лице.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни наказания по отношение на съответните служители.

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

Чл. 12. (1) Документите и преписките, по които работата е приключила, се съхраняват на хартия и електронен носител - сървър на НИС ПЕТРОЛ.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещенията по отдели в НИС ПЕТРОЛ, със срокове за съхранение, съобразени с действащото законодателство.

(3) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система

(4) Достъп до документи, съдържащи лични данни, имат единствено определените за тази цел лица, съобразно възложените им правомощия.

Чл. 13. (1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец.

Чл. 14. (1) Веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от НИС ПЕТРОЛ регистри. Проверките се извършват от комисия, определена от Управителя, която изготвя Доклад за резултата от проверката.

(2) Докладът по ал. 1 трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. Докладите се адресират до Длъжностното лице по защита на данните и до Управителя.

Чл. 15. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позвалява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 16. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, НИС ПЕТРОЛ може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

Чл. 17. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от НИС ПЕТРОЛ регистри, респ. след изтичане на определения срок за това, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящата Политика за защита на личните данни.

(2) В случаите, в които се налага унищожаване на носител на лични данни, НИС ПЕТРОЛ прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3) Унищожаване се осъществява от служители, упълномощени с изрична писмена заповед на Управителя и след уведомяване на Длъжностното лице по защита на данните.

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3.

Чл. 18. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство и/или с цел изпълнение на техни служебни задължения, след подаване на заявление за достъп до информация и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, НИС ПЕТРОЛ съобщава в 1-месечен срок от подаване на заявлението. При необходимост, този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на заявленията от определено лице. НИС ПЕТРОЛ информира субекта на данните за всяко удължаване в срок от един месец от получаване на заявлението, като посочва и причините за удължаването.

(3) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(4) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец съгласно, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(5) Третите страни получават достъп до лични данни, обработвани в НИС ПЕТРОЛ, при наличие на законово основание за обработването на лични данни (напр. НАП, НОИ и др.п.).

Чл. 19. ***Физическата защита*** в НИС ПЕТРОЛ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградата и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 20. (1). Основните ***организационни мерки за физическа защита*** в НИС ПЕТРОЛ включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,
3. определяне на организацията на физическия достъп;

(2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите

по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения*, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи.

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

(5) Зони с контролиран достъп са всички помещения на територията на НИС ПЕТРОЛ, в които се събират, обработват и съхраняват лични данни.

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

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения със заключващи се шкафове. Достъпът е ограничен и се предоставя само на служителите, на които той е необходим.

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

Чл. 21. (1). Основните ***технически мерки за физическа защита*** в НИС ПЕТРОЛ включват:

1. използване на сигнално-охранителна техника;
2. използване на ключалки и заключващи механизми;
3. шкафове, метални каси;
4. оборудване на помещенията с пожарогасителни средства.

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

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

(4) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложимата нормативна уредба.

Чл. 22. (1). Основните ***мерки за персонална защита*** на личните данни, приложими в НИС ПЕТРОЛ, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящата Политика за защита на личните данни, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни;
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от НИС ПЕТРОЛ;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.) между персонала и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Чл. 23. (1). Основните ***мерки за документална защита*** на личните данни, са:

1. *Определяне на регистрите, които ще се съхраняват на електронен носител при координаторите по отдели* - на електронен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изискванията на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на НИС ПЕТРОЛ, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на НИС ПЕТРОЛ, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. *Регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";
4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение, на които са изтекли и не са необходими за нормалното функциониране на НИС ПЕТРОЛ или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае", за да изпълняват техните задължения;

2. *Правила за размножаване и разпространение*, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или изискване на държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни наказания и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл. 24. (1) ***Защитата на информационните системи/базите с данни и/или мрежи*** в НИС ПЕТРОЛ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на ***информационните системи/базите с данни*** и/или мрежи, обработващи лични данни в НИС ПЕТРОЛ, включват:

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на НИС ПЕТРОЛ. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае";
2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;
3. Управление на *външни връзки и/или свързаност*, включващи от своя страна:

- Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка", които се намират под контрола и администрацията на НИС ПЕТРОЛ. Като *външни мрежи* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на НИС ПЕТРОЛ.

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

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

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

4. *Защитата от зловреден софтуер* включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от определени от Управителя лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на отдел "ИТ" на НИС ПЕТРОЛ.

- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Управителя лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

- активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от Управителя лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на НИС ПЕТРОЛ.

- Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

- Отговорност за архивиране има лицето, обработващо личните данни.

- Срокът на архивиране следва да е съобразен с действащото законодателство.

- Съхраняването на архива е в отделно помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

6. Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)

7. *Персоналната защита на данните* е част от цялостната охрана на НИС ПЕТРОЛ.

8. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на НИС ПЕТРОЛ.

9. Данните, които вече не са необходими за целите на НИС ПЕТРОЛ и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. *Организация на телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на НИС ПЕТРОЛ:

- Отдалечен достъп до вътрешни мрежи на НИС ПЕТРОЛ не е предвиден. По изключение, и след изричното разрешение от ръководството на НИС ПЕТРОЛ, може да се разреши подобен достъп на изрично определени лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

- На персонала на НИС ПЕТРОЛ може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до елекронните ригистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка на Управителя на НИС ПЕТРОЛ. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на Управителя на НИС ПЕТРОЛ, както и в случаите на заплаха за сигурността на данните.

- Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмено разрешение от Управителя.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на НИС ПЕТРОЛ, включват:

- Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на НИС ПЕТРОЛ от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на НИС ПЕТРОЛ, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър.

3. Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура, както и подходяща пожарогасителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл. 25. (1) По отношение на личните данни се прилагат и мерки, свързани с ***криптографска защита на данните*** чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

VII. ОСНОВНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 26. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към

системата. При приключване на работното време служителите изключват или заключват локалния си компютър.

(2) НИС ПЕТРОЛ прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност, като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от НИС ПЕТРОЛ период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) Системите, обработващи и/или съхраняващи лични данни включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, неизключване/незаключване на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Ръководството на икономическа сигурност и Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 27. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 28. (1) В НИС ПЕТРОЛ се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от системния администратор. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 29. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят този КЕП на трети лица, респ. да споделят своя PIN с трети лица.

VIII. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 30. (1) Всеки отдел работещ с лични данни поддържа регистъра с лични данни. Длъжностното лице по защита на данните поддържа общ регистър, в който са упоменати всички регистри по места.

(2) Поддържани регистри в НИС Петрол:

1. *Регистър „Икономическа сигурност“;*
2. *Регистър „Юридически“;*
3. *Регистър „Развитие и строителство“;*
4. *Регистър „Търговия на едро“;*
5. *Регистър „Логистика“;*
6. *Регистър „Търговия на дребно“;*
7. *Регистър „Финанси“;*
8. *Регистър „Персонал“;*
9. *Регистър „Поръчки“;*
10. *Регистър „Информационни технологии“;*
11. *Регистър „Безопасност на труда и околна среда“;*

(3) Данните в регистрите по ал.(1) се поддържат в съответствие с правното основание за обработка.

Чл. 31. За обработване на данните от регистрите по чл. 30, НИС ПЕТРОЛ води Регистър на дейностите по обработка.

IX. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 32. (1) Длъжностното лице по защита на данните се определя от Управителя на дружеството.

(2) Длъжностното лице по защита на данните има следните правомощия и длъжностни задължения:

1. Следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;
2. Осъществява контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящата Политика за защита на личните данни;
3. Поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
4. Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;
5. Води регистър на дейностите по обработване на лични данни в НИС ПЕТРОЛ.

Чл. 33. Служителите на НИС ПЕТРОЛ са длъжни:

1. Всички служители на НИС ПЕТРОЛ са длъжни да се запознаят с настоящата Политика за защита на личните данни и да я спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

2. Да обработват лични данни законосъобразно и добросъвестно;
3. Да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
4. Да актуализират при необходимост регистрите на личните данни;
5. Да унищожават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
6. Да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват, респ. не по-дълъг от законово определения.

Чл. 34. (1) За неспазването на разпоредбите на настоящата Политика за защита на личните данни служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за НИС ПЕТРОЛ или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

X. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 35.(1) За всички неуредени в настоящата Политика за защита на личните данни въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

(2) Образците на документите, съставяни при и по повод обработката на лични данни са разписани в пакета от процедурите по защита на личните данни на НИС ПЕТРОЛ.