"ПРИСТАНИЩЕ ВАРНА" ЕАД

УТВЪРДИЛ:
ИЗП. ДИРЕКТОР.....
(П. Сеферов)

Дата: 17.05.2018 г.

ИНСТРУКЦИЯ

за обработване и защита на личните данни на физическите лица в „Пристанище Варна" ЕАД

I. Правно основание

Чл. 1. Настоящата Инструкция се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни (ЗЗЛД), чл. 19, ал. 2 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и във връзка с прилагането на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година.

II. Цели на Инструкцията

Чл. 2. (1) Инструкцията се приема с цел да регламентира:

1. Създаване на организация и вътрешен ред при обработване на лични данни на физическите лица в "Пристанище Варна" ЕАД.
2. Задълженията на служителите, обработващи лични данни в дружеството.
3. Осигуряване на адекватни технически и организационни мерки, за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.
4. Осигуряване на достъп на лицата до личните им данни - практическо упражняване на права от субектите на данните.
5. Актуализация на лични данни.
6. Информираност на субектите на данните и прозрачност на обработването.

(2) Инструкцията се утвърждава, допълва, изменя и отменя от Изпълнителния директор на „Пристанище Варна" ЕАД.

III. Изисквания

Чл. 3. Изисквания към съдържанието на Инструкцията съгласно чл. 20 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и Регламент (ЕС) 2016/679:

1. Индивидуализиране на администратора на лични данни.
2. Общо описание на поддържаните регистри – категории лични данни и основание за обработване.
3. Технологично описание на поддържаните регистри – носители на данни, технология на обработване, срок за съхранение и предоставени услуги.
4. Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.
5. Оценка на въздействие и определяне на съответно ниво на защита.
6. Описание на предприетите технически и организационни мерки.

7. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.).

8. Предоставяне на лични данни на трети лица – основание, цел, категории лични данни.

9. Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им;

10. Определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни.

11. Информацията по ал. 2-10 се описва за всеки един от поддържаните регистри.

12. Разширени изисквания по Регламент (ЕС) 2016/679.

IV. Обхват

Чл. 4. Инструкцията е задължителна за служителите, обработващи лични данни в „Пристанище Варна" ЕАД.

Чл. 5. Оправомощените лица трябва да се запознаят със съдържанието на тази Инструкция, удостоверено с техния подпис.

V. Обработване на лични данни на физическите лица

Чл. 6. Администратор на лични данни е „Пристанище Варна" ЕАД.

Чл. 7. (1) Обработващи лични данни от името на администратора са Изпълнителния Директор, а под негово ръководство са Административния Директор, Финансовия директор и Ръководителите на отдел „Правен", отдел „Финансово счетоводна отчетност" (ФСО), отдел „Човешки ресурси и административно обслужване" (ЧРиАО), отдел „Организация на труда, работна заплата и прогнозиране и анализ" (ОТРЗиПА), отдел „Маркетинг", отдел „Търговски, обществени поръчки и европрограми" (ТОПЕ) и на „Фирмена сигурност".

(2) Според функционалните си задължения, други длъжностни лица, имащи право да обработват лични данни са:

- Старши юрисконсулт и Технически организатор – отдел „Правен";
- Счетоводител, отговорен/ оперативен; Касиер, счетоводство – отдел ФСО;
- Старши инспектор и инспектор – отдел ЧриАО;
- Икономист организация на труда и Отчетник, начисляване на трудови възнаграждения – отдел ОТРЗиПА;
- Специалист договаряне пристанищни услуги и тарифна политика – отдел „Маркетинг";
- Икономист, обществени поръчки, Специалист и Старши специалист – отдел ТОПЕ;
- Оператори за контрол на достъпа – отдел „Фирмена сигурност";

Чл. 8. В дружеството има следните регистри: **„Персонал"**, **„Клиенти и доставчици"**, **„Обществени поръчки"** и **„Сигурност"**.

Чл. 9. Регистър „Персонал"

(1) Общо описание на поддържаните регистри - категории лични данни и основание за обработване в Регистър „Персонал".

1. Регистърът съдържа личните данни на служителите и работниците по трудови договори и изпълнители по граждански договори в „Пристанище Варна" ЕАД в изпълнение

на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив и др. Обработваните данни за съответните лица служат за служебни цели, свързани с трудовите и граждански правоотношения и необходими за изготвяне на всякакви документи в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни); за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори; за водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица по трудови и граждански договори.

2. В регистърът се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, адрес, телефон, месторождение, паспортни данни на лицето.

- медицински данни: здравен статус, данни за физиологичното, психическо и психологическо състояние на физическото лице при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи.

- социална идентичност: притежавано образование, допълнителна квалификация, трудова дейност и професионална биография.

- семейна идентичност: наличие на брак, развод, брой членове на семейството, в това число деца до 18 години.

- други: гражданско-правен статус на лицата, необходими за длъжностите свързани с материална отговорност, свидетелство за съдимост.

(2) Технологично описание на Регистър „Персонал":

1. Носители на данни, технология на обработване.

По този критерий попада начина на съхранение и невъзможността неоторизирани лица да манипулират личните данни на Регистъра. Данните са на хартиен и технически носител:

- На хартиен носител личните данни се съхраняват в папки, подредени в шкаф, който се заключва. Обработката на тези данни е от назначено за обработването длъжностно лице. Това става в специално помещение, което също се заключва;

- На технически носител личните данни се въвеждат в твърд диск на сървър от локалната мрежа. Сървърът е в изолирано помещение с контрол на достъпа. Влизането в операционната система става чрез парола, известна само на оторизираното длъжностно лице. Защитата на техническите данни от неправомерен достъп, повреждане, изгубване или унищожава се осигурява чрез система от мерки: определяне на роли и отговорности (администратор, ползвател), идентификация и автентификация, лицензирани програмни продукти, антивирусни програми, контроли на сесията, копия/резервни копия за възстановяване, процедури за унищожаване/заличаване/изтриване на носители и чрез поддържане на информацията на хартиен носител.

2. Срока на съхранение на личните данни в Регистър „Персонал".

Срока на съхранение на личните данни е съгласно чл. 12 и чл. 42 от Закона за Счетоводството и Закона за Държавния архив е за период, както следва:

- ведомости за заплати – 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;

- счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции – 10 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;

- документи за данъчен контрол – до 5 г. след изтичане на давностния срок за погасяване на публичното задължение, което удостоверяват тези документи;

- документи за финансов одит – до извършване на следващ вътрешен одит и одит на Сметната палата;

- всички останали носители на счетоводна информация – три години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;

- лични досиета – 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят.

3. Предоставени услуги.

По този регистър се предоставя достъп до договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни.

(3) Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.

1. В Регистър "Персонал" правомерен достъп до кадровите досиета на персонала, при спазване принципа „Необходимо да се знае" имат служителите от отдел ЧР и АО и ФСО, както и други лица, пряко ангажирани с оформяне и проверка законосъобразността на документите – Изпълнителен директор, Ръководител, отдел „Правен" и Ръководител, отдел „ОТРЗиПА".

Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

2. Възможността за предоставяне на други лица на достъп до личните данни е ограничена и изрично регламентирана в чл. 7, ал. 7 от Инструкцията.

(4) Оценка на въздействие и определяне на съответно ниво на защита.

1. Общия брой на физическите лица, на които се обработват личните данни в Регистър „Персонал" е по-малко от 10000.

Оценка на нивото на въздействие на Регистър „Персонал"

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Регистър „Персонал"	**СРЕДНО**	**СРЕДНО**	**СРЕДНО**	**СРЕДНО**

2. За да се оцени въздействието, Администраторът отчита критериите за поверителност, цялостност и наличност. 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.

3. Администраторът отчита категориите на обработваните лични данни по „Специфични признаци", които се отнасят до физическата, физиологичната (медицински данни), социалната, семейната идентичност и други на група физически лица, чийто брой надхвърля 2, но е по-малък от 10000.

4. Минималното ниво на технически и организационни мерки, които следва да се осигури за Регистър „Персонал" при **СРЕДНО НИВО НА ВЪЗДЕЙСТВИЕ** е **СРЕДНО НИВО НА ЗАЩИТА**.

(5) Описание на предприетите технически и организационни мерки.

1. Физическа защита. Организационни и технически мерки.

На територията на дружеството помещенията, където се обработват лични данни от Регистър „Персонал", са общо 11 (единадесет):

- в Пристанище Варна-Изток са 3 (три) помещения на отдел ЧРиАО и 1 (едно) за архив на документи;

- в Пристанище Варна-Запад са 1 (едно) помещение на отдел ЧРиАО и 1 (едно) за архив на документи;

- в Пристанище Варна-Изток са 3 (три) помещения на отдел ФСО и 1 (едно) за архив на документи;

- в Пристанище Варна-Запад са 2 (две) помещения на отдел ФСО и 1 (едно) за архив на документи.

В същите помещения се разполагат елементите на комуникационно-информационните системи за обработване на лични данни. Сървърът, към който се свързват всички работни компютри от локалната мрежа на Регистъра се намира в изолирано помещение с ограничен достъп.

Създадена е организация на физическия достъп – до помещенията се допускат назначените да обработват лични данни служители.

Външни лица се допускат до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

В административните сгради се влиза с пропуск и придружител през физическа охрана и под видеонаблюдение. Помещенията на отдел ЧРиАО, намиращи се в Пристанище Варна-Изток на границата на охраняемия периметър, са със мерки за защита: физическа охрана, метална входна врата, СОТ и видеонаблюдение.

Шкафовете за съхранение на хартиените носители на данни в Регистъра се заключват, а помещенията са оборудвани с пожарогасителни средства.

2. Персонална защита.

Обработващите лични данни по този Регистър се запознават със Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, Регламент (ЕС) 2016/679 и настоящата Инструкция, в касаещия ги обем.

Лицата, обработващи лични данни, подписват декларация Образец № 4– съгласие за поемане на задължение за неразпространение на лични данни.

Голяма част от персонала преминава обучение по защита на личните данни.

Създадена е политика за несподеляне на критична информация между персонала чрез персонализиране на работната среда.

3. Документална защита.

Регистър „Персонал" се поддържа на хартиен носител с достъп само от упълномощените лица, определени в чл. 9, ал. 3.

Обработката се извършва в работно време.

Сроковете за съхранение са определени в чл. 9, ал. 2, т. 2.

Личните данни се размножават и разпространяват от назначените служители, само при необходимост за изпълнение на служебни задължения или ако са изискани по надлежния ред.

Унищожаването на документи с изтекъл срок на съхранение се извършва от назначена със заповед на Изпълнителния директор комисия.

4. Защита на автоматизирани информационни системи и/или мрежи.

Програмните продукти чрез които се обработват личните данни по регистъра са:

- програма ОМЕКС 2000 в отдел ЧРиАО;
- програми TERES в отдел ФСО.

Програмите се свързват с MSSQL сървър, намиращ се на физически сървър в помещение с контролиран достъп.

Пристанище Варна-Запад има VPN криптирана връзка с Пристанище Варна-Изток. Физическия сървър за личните данни се намира в административната зона на сигурност, в

изолирано помещение със строго контролиран и ограничен достъп, оборудвано с метална врата, климатик и СОТ.

Оправомощените лица са с персонален достъп с потребителско име и парола до операционната система на работните компютри и отделно за програмните продукти ОМЕКС 2000 и TERES.

Сроковете за съхранение на личните данни са дефинирани за целия Регистър в чл. 9, ал. 2, т. 2.

Унищожаване/заличаване/изтриване на носители се осъществява съгласно създадените процедури.

Компютрите са в работните помещения в зоната на сигурност на охраняемия периметър.

Реализацията на технически мерки се осъществява, като:

- потребителите се идентифицират с име и парола и се автентифицират с електронен подпис за НАП и НОИ;
- управление на регистрите от тип клиент-сървър-база данни;
- външните връзки и свързване между Пристанище Варна-Изток и Пристанище Варна-Запад са през криптирана връзка VPN;
- софтуерната и хардуерната среда периодично и при необходимост се обслужва за вируси, нежелани програми и замърсяване от отдел „Информационни технологии" (ИТ). Ползва се UPS на сървъра;
- забранява се ползването на лични технически носители на информация (флаш памет, телефон, външен диск и др.), инсталиране на нелицензирани програми;
- ползването на Интернет на компютри с достъп до сървъра, където се обработват личните данни, да става само с криптирана връзка;
- личните данни се архивират на технически носител, периодично на всеки 90 дни от обработващия лични данни или от служител в отдел ИТ с цел запазване на информацията за съответните лица в актуален вид. Същото се извършва на външен диск, достъп до който има само обработващият лични данни;
- по разписание се правят резервни копия за възстановяване;
- обработването на лични данни става само в работно време от назначеното длъжностно лице.

(6) Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.).

При възникване и установяване на инцидент, се действа съгласно утвърдена Процедура в случай на нарушение на сигурността на личните данни

Веднага се докладва на лицето, отговорно за защита на личните данни. 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, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(7) Предоставяне на лични данни на трети лица – основание, цел, категории лични данни.

1. Кадровото досие на лицето не се изнася извън сградата на администратора. Никое длъжностно или трето лице няма право на достъп до кадровите досиета на персонала на "Пристанище Варна" ЕАД, освен ако същото е изисквано по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). Достъпът на тези органи до личните данни на лицата е правомерен.

2. Надлежен е начинът, при който съответният съдебен орган е изискал кадрово досие или данни, съдържащи се в него, писмено с изрично искане, отправено до Изпълнителния директор на дружеството. В подобни случаи на органите на съдебна власт се предоставя копие от съдържащите се в кадровото досие документи, заверени с подпис на Ръководителя на съответния отдел и печат на дружеството, освен ако няма изрично искане от съда да бъдат предоставени оригиналите. За идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира заинтересованото лице, но не и да препятства работата на органите на съдебна власт.

3. Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на дружеството.

4. Правомерен е и достъпът на ревизиращите държавни органи и назначени от съда вещи лица, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала.

5. Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица.

6. При внедряване на нов програмен продукт за обработване на лични данни следва да се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

7. За неизпълнение на задълженията, вменени на съответните длъжностни лица по тази инструкция и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган - предвиденото наказание в Закона за защита на личните данни и Регламент (ЕС) 2016/679. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

8. „Пристанище Варна" ЕАД не предоставя лични данни на други държави по този регистър.

(8) Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

Сроковете са веднъж на две години или когато възникне основание за това.

(9) Определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни.

(1) След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни по този Регистър, данните трябва да се:

1. унищожат, или

2. прехвърлят на друг администратор, като предварително се уведоми за това комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни Регистърът се съхранява само в предвидените в закон случаи.

(3) В случаите, когато след постигане целта на обработване „Пристанище Варна" ЕАД иска да съхрани обработените лични данни като анонимни данни за исторически, научни или статистически цели, се уведомява за това комисията.

(4) Комисията за защита на личните данни може да забрани съхраняването за целите по ал.3, ако „Пристанище Варна" ЕАД не осигури достатъчната защита на обработените данни като анонимни данни.

(5) Решението на комисията по ал. 4 подлежи на обжалване пред съответния административен съд. Решението на административния съд не подлежи на обжалване. В случаите на отхвърляне на жалбата срещу решението на комисията, тогава „Пристанище Варна" ЕАД трябва да унищожи личните данни по Регистъра.

Чл. 10. Регистър „Клиенти и доставчици"

(1) Общо описание на поддържаните регистри - категории лични данни и основание за обработване в Регистър „Клиенти и доставчици".

1. В Регистър „Клиенти и доставчици" се обработват данни на контрагентите на „Пристанище Варна" ЕАД и/или техни упълномощени представители по време на дейността им по изпълнение на сключените договори и индивидуализиране на облигационно-правните правоотношения, в изпълнение на нормативните изисквания на Закона за счетоводството Търговския закон, Закона на задълженията и договорите и др. Обработваните данни за съответните лица са за служебни цели, свързани с облигациоонноправните отношения за изготвяне на договори, допълнителни споразумения и др., за установяване на връзки с лицата по телефон, за изпращане на кореспонденция.

2. В регистърът се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, адрес, месторождение, телефони за връзка и др.
- трудова дейност: месторабота и заемана длъжност, професионален опит.
- социално-икономическа идентичност: текущо финансово състояние, участие в сдружения.

(2) Технологично описание на поддържаните регистри.

1. Носители на данни, технология на обработване.

По този критерий попада начина на съхранение и невъзможността неоторизирани лица да манипулират личните данни на Регистъра. Данните са на хартиен и технически носител:

- На хартиен носител личните данни се съхраняват в папки за всеки клиент или доставчик. Данните се подреждат в специален шкаф, в помещение с ограничен достъп.
- На технически носител личните данни се въвеждат на твърд диск в мрежа. Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само от страна на обработващия лични данни. Местонахождението на компютъра е в помещение за самостоятелна работа на служителите, обработващи лични данни по регистъра. Достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият чрез известна само на него парола, за отваряне на тези файлове. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни

програми, периодично архивиране на данните, както и чрез поддържане на информацията на хартиен носител.

2. Срока на съхранение на личните данни в Регистър „Клиенти и доставчици".

Срока на съхранение на личните данни в Регистър „Клиенти и доставчици", съгласно чл. 12 и чл. 42 от Закона за счетоводството е за период, както следва:

- договори и протоколи за изпълнение на поръчките (документи за данъчен контрол) - до 5 г. след изтичане на давностния срок за погасяване на публичното задължение, което удостоверяват тези документи;
- документи за финансов одит - до извършване на следващ вътрешен одит и одит на Сметната палата;
- всички останали носители на счетоводна информация – 3 г.

3. Предоставени услуги.

По този регистър се предоставя достъп до договори, допълнителни споразумения и др. подобни.

(3) Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.

1. В Регистър „Клиенти и доставчици" правомерен достъп до личните данни на контрагентите на „Пристанище Варна" ЕАД и/или техни упълномощени представители, при спазване принципа „Необходимо да се знае", имат служителите от отдел „Маркетинг", както и други лица, пряко ангажирани с оформяне и проверка законосъобразността на документите - Изпълнителен директор, Финансов директор и Ръководител отдел „Правен".

Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

2. Възможността за предоставяне на други лица на достъп до личните данни е ограничена и изрично регламентирана в чл. 7, ал. 7 от Инструкцията.

(4) Оценка на въздействие и определяне на съответно ниво на защита.

1. Общия брой на физическите лица, на които се обработват личните данни в Регистър „Клиенти и доставчици", заедно с архива е по-малко от 10000.

Оценка на нивото на въздействие на Регистър „Клиенти и доставчици"

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Регистър „Клиенти и доставчици"	**НИСКО**	**НИСКО**	**НИСКО**	**НИСКО**

2. За да се оцени въздействието, Администраторът отчита критериите за поверителност, цялостност и наличност. 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.

3. Администраторът отчита категориите на обработваните лични данни по „Специфични признаци", които се отнасят до физическата идентичност (три имена, ЕГН, адрес, телефонен номер), трудова дейност и социално-икономическа идентичност на група физически лица, чийто брой надхвърля 2, но е по-малък от 10000.

4. Минималното ниво на технически и организационни мерки, които следва да осигури за Регистър „Клиенти и доставчици" при **НИСКО НИВО НА ВЪЗДЕЙСТВИЕ** е **НИСКО НИВО НА ЗАЩИТА**.

(5) Описание на предприетите технически и организационни мерки.

1. Физическа защита. Организационни и технически мерки.

На територията на дружеството помещенията, където се обработват лични данни от Регистър „Клиенти и доставчици", са общо 2 (две), само в Пристанище Варна-Изток. Помещенията са в отдел „Маркетинг", където има обособено място и за архив на документи.

В същите помещения се разполагат елементите на комуникационно-информационните системи за обработване на лични данни. Сървърът, към който се свързват всички работни компютри от локалната мрежа на Регистъра се намира в изолирано помещение с ограничен достъп.

Създадена е организация на физическия достъп – до помещенията се допускат назначените да обработват лични данни служители.

Външни лица се допускат до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

В административните сгради се влиза с пропуск и придружител през физическа охрана и при видеонаблюдение.

Шкафовете за хартиените носители на данни в Регистъра се заключват, а помещенията са оборудвани с пожарогасителни средства.

2. Персонална защита.

Обработващите лични данни по този Регистър се запознават с Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, Регламент (ЕС) 2016/679 и настоящата Инструкция, в касаещия ги обем.

Лицата, обработващи лични данни, подписват декларация Образец № 4– съгласие за поемане на задължение за неразпространение на лични данни.

Голяма част от персонала преминава обучение по защита на личните данни.

Създадена е политика за несподеляне на критична информация между персонала чрез персонализиране на работната среда.

3. Документална защита.

Регистър „Клиенти и доставчици" се поддържа на хартиен носител с достъп само от упълномощените лица, определени в чл. 10 ал. 3.

Обработката се извършва в работно време.

Сроковете за съхранение са определени в чл. 10 ал. 2 т. 2.

Личните данни се размножават и разпространяват от назначените служители, само при необходимост за изпълнение на служебни задължения или ако са изискани по надлежния ред.

Унищожаването на документи с изтекъл срок на съхранение се извършва от назначена със заповед на Изпълнителния директор комисия.

4. Защита на автоматизирани информационни системи и/или мрежи.

Програмните продукти чрез които се обработват личните данни по регистъра са: програмите МИКРО АКАУНТ.

Тези програми се свързват с MSSQL сървър, намиращ се на физически сървър с контролиран достъп в същата сграда.

Оправомощените лица имат персонален достъп до работните компютри с потребителско име и парола и отделно за програмните продукти МИКРО АКАУНТ.

Сроковете за съхранение на личните данни са дефинирани за целия Регистър в чл. 10 ал. 2 т. 2.

Унищожаване/заличаване/изтриване на носители се осъществява съгласно създадените процедури.

Компютрите са в работните помещения в зоната на сигурност на охраняемия периметър.

Реализацията на технически мерки се осъществява, като:

- потребителите се идентифицират име и парола;
- управление на регистрите от тип клиент-сървър-база данни;
- без външни връзки и свързване;
- софтуерната и хардуерната среда периодично и при необходимост се обслужва за вируси, нежелани програми и замърсяване от отдел ИТ. Ползва се UPS на сървъра;
- забранява се ползването на лични технически носители на информация (флаш памет, телефон, външен диск и др.), инсталиране на нелицензирани програми;
- ползването на Интернет на компютри с достъп до сървъра, където се обработват личните данни, да става само с криптирана връзка;
- личните данни се архивират на технически носител, периодично на всеки 90 дни от обработващия лични данни или от служител в отдел ИТ с цел запазване на информацията за съответните лица в актуален вид. Същото се извършва на външен диск, достъп до който има само обработващият лични данни;
- по разписание се правят резервни копия за възстановяване;

Обработването на лични данни става само в работно време от назначеното длъжностно лице.

(6) Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.).

При възникване и установяване на инцидент, се действа съгласно утвърдена Процедура в случай на нарушение на сигурността на личните данни

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. 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, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(7) Предоставяне на лични данни на трети лица – основание, цел, категории лични данни.

1. Данните на лицата не се изнасят извън сградата на администратора. Никое длъжностно или трето лице няма право на достъп до личните данни на клиентите и доставчиците на "Пристанище Варна" ЕАД, освен ако същото е изисквано по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). Достъпът на тези органи до личните данни на клиентите и доставчиците на "Пристанище Варна "ЕАД е правомерен.

2. Надлежен е начинът, при който съответният съдебен орган е изискал документи с лични данни, писмено с изрично искане, отправено до Изпълнителния директор на дружеството. В подобни случаи на органите на съдебна власт се предоставя копие от съдържащите се документи, заверени с подпис на Ръководителя на съответния отдел и печат на дружеството, освен ако няма изрично искане от съда да бъдат предоставени оригиналите. За идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира заинтересованото лице, но не и да препятства работата на органите на съдебна власт.

3. Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на

непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на дружеството.

4. Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до личните данни на клиентите и доставчиците на "Пристанище Варна" ЕАД.

5. Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица.

6. При внедряване на нов програмен продукт за обработване на лични данни следва да се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

7. За неизпълнение на задълженията, вменени на съответните длъжностни лица по тази инструкция и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган - предвиденото наказание в Закона за защита на личните данни и Регламент (ЕС) 2016/679. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

„Пристанище Варна" ЕАД не предоставя лични данни на други държави по този регистър.

(8) Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

Сроковете са веднъж на две, години или когато възникне основание за това.

(9) Определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни.

(1) След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни по този Регистър, данните трябва да се:

1. унищожат, или

2. прехвърлят на друг администратор, като предварително се уведоми за това комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни Регистърът се съхранява само в предвидените в закон случаи.

(3) В случаите, когато след постигане целта на обработване „Пристанище Варна" ЕАД иска да съхрани обработените лични данни като анонимни данни за исторически, научни или статистически цели, се уведомява за това комисията.

(4) Комисията за защита на личните данни може да забрани съхраняването за целите по ал.3, ако „Пристанище Варна" ЕАД не осигури достатъчната защита на обработените данни като анонимни данни.

(5) Решението на комисията по ал. 4 подлежи на обжалване пред съответния административен съд. Решението на административния съд не подлежи на обжалване. В случаите на отхвърляне на жалбата срещу решението на комисията, тогава „Пристанище Варна" ЕАД трябва да унищожи личните данни по Регистъра.

Чл. 11. Регистър „Обществени поръчки"

(1) Общо описание на поддържаните регистри - категории лични данни и основание за обработване в Регистър „Обществени поръчки".

1. Регистър „Обществени поръчки" обработва данни на контрагентите на „Пристанище Варна" ЕАД и/или техни упълномощени представители по време на дейността им по изпълнение на сключените договори и индивидуализиране на облигационно-правните правоотношения, в изпълнение на нормативните изисквания на Закона за счетоводството Търговския закон, Закона на задълженията и договорите , Закон за обществените поръчки, ПК-05 Доставки на стоки, избор на изпълнители на услуги и строителство, Инструкция за реда, организирането и използването на документите в архивохранилищата на ПВ, представляващи архивен фонд на ПВ и др. Обработваните данни за съответните лица са за служебни цели, свързани с облигационно-правните отношения за изготвяне на договори, допълнителни споразумения и др., за установяване на връзки с лицата по телефон, за изпращане на кореспонденция.

2. В регистърът се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, адрес, месторождение, телефони за връзка и др.
- трудова дейност: месторабота и заемана длъжност, професионален опит.
- социално-икономическа идентичност: текущо финансово състояние, участие в сдружения.

(2) Технологично описание на поддържаните регистри.

1. Носители на данни, технология на обработване.

По този критерий попада начина на съхранение и невъзможността неоторизирани лица да манипулират личните данни на Регистъра. Данните са на хартиен и технически носител:

- На хартиен носител личните данни се съхраняват в папки за всеки клиент или доставчик. Данните се подреждат в специален шкаф, в помещение с ограничен достъп.
- На технически носител личните данни се въвеждат на компютър с твърд диск в мрежа. Компютърът е свързан в локална мрежа, със защитен достъп до личните данни. Местонахождението на компютъра е в помещение за самостоятелна работа на обработващите лични данни по регистъра. Достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият чрез известна само на него парола. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните, както и чрез поддържане на информацията на хартиен носител.

2. Срока на съхранение на личните данни в Регистър „Обществени поръчки".

Срока на съхранение на личните данни в Регистър „Обществени поръчки", съгласно Интегрирана система за управление, както следва:

- досиетата на доставчиците се съхраняват в отдел ТОПЕ за срок от 3 г., а след това се архивират за срок от 5 г.
- списъците на одобрените доставчици се съхраняват от отдел ТОПЕ за срок от 1 г., а след това се архивират за срок от 3 г.

3. Предоставени услуги.

По този регистър се предоставя достъп до договори, допълнителни споразумения и други подобни.

(3) Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.

1. В Регистър „Обществени поръчки" правомерен достъп до личните данни на контрагентите на „Пристанище Варна" ЕАД и/или техни упълномощени представители, при спазване принципа „Необходимо да се знае", имат служителите от отдел ТОПЕ, както и други лица, пряко ангажирани с оформяне и проверка законосъобразността на документите - Изпълнителен директор, Финансов директор, Ръководител отдел „Правен", Директор НТД и Ръководители на отдели в комисии.

Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

2. Възможността за предоставяне на други лица на достъп до личните данни е ограничена и изрично регламентирана в чл. 7, ал. 7 от Инструкцията и в случаите за:

- Профил на купувача, съгласно Закон за обществените поръчки;
- Служители на дружеството при застраховки при трудови злополуки и живот.

(4) Оценка на въздействие и определяне на съответно ниво на защита.

1. Общия брой на физическите лица, на които се обработват личните данни в Регистър „Обществени поръчки", заедно с архива е по-малко от 10000.

Оценка на нивото на въздействие на Регистър „Обществени поръчки"

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Регистър „Обществени поръчки"	**НИСКО**	**НИСКО**	**НИСКО**	**НИСКО**

2. За да се оцени въздействието, Администраторът отчита критериите за поверителност, цялостност и наличност. 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.

3. Администраторът отчита категориите на обработваните лични данни по „Специфични признаци", които се отнасят до физическата идентичност (три имена, ЕГН, адрес, телефонен номер), трудова дейност и социално-икономическа идентичност на група физически лица, чийто брой надхвърля 2, но е по-малък от 10000.

4. Минималното ниво на технически и организационни мерки, които следва да осигури за Регистър „Обществени поръчки" при **НИСКО НИВО НА ВЪЗДЕЙСТВИЕ** е **НИСКО НИВО НА ЗАЩИТА.**

(5) Описание на предприетите технически и организационни мерки.

1. Физическа защита. Организационни и технически мерки.

На територията на дружеството помещенията, където се обработват лични данни от Регистър „Обществени поръчки", са общо 2 (две), намиращи се само в Пристанище Варна-Изток. Помещенията са в отдел „Търговски, обществени поръчки и европрограми", където има обособено място и за архив на документи.

В същите помещения се разполагат елементите на комуникационно-информационните системи за обработване на лични данни. Само сървърът, към който се свързват всички работни компютри от локалната мрежа на Регистъра е в изолирано помещение с ограничен достъп.

Създадена е организация на физическия достъп – до помещенията се допускат назначените да обработват лични данни служители.

Външни лица се допускат до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

В административните сгради се влиза с пропуск и придружител през физическа охрана и при видеонаблюдение.

Шкафовете за хартиените носители на данни в Регистъра се заключват, а помещенията са оборудвани с пожарогасителни средства.

2. Персонална защита.

Обработващите лични данни по този Регистър се запознават с Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, Регламент (ЕС) 2016/679 и настоящата Инструкция, в касаещия ги обем.

Лицата, обработващи лични данни, подписват декларация Образец № 4– съгласие за поемане на задължение за неразпространение на лични данни.

Голяма част от персонала преминава обучение по защита на личните данни.

Създадена е политика за несподеляне на критична информация между персонала чрез персонализиране на работната среда.

3. Документална защита.

Регистър „Обществени поръчки" се поддържа на хартиен носител с достъп само от упълномощените лица, определени в чл. 11 ал. 3.

Обработката се извършва в работно време.

Сроковете за съхранение са определени в чл. 11 ал. 2 т. 2.

Личните данни се размножават и разпространяват от назначените служители, само при необходимост за изпълнение на служебни задължения или ако са изискани по надлежния ред.

Унищожаването на документи с изтекъл срок на съхранение се извършва от назначена със заповед на Изпълнителния директор комисия.

4. Защита на автоматизирани информационни системи и/или мрежи.

Оправомощените лица имат персонален достъп до работните компютри с потребителско име и парола.

Сроковете за съхранение на личните данни са дефинирани за целия Регистър в чл. 11 ал. 2 т. 2.

Унищожаване/заличаване/изтриване на носители се осъществява съгласно създадените процедури.

Компютрите са в работните помещения в зоната на сигурност на охраняемия периметър.

Реализацията на технически мерки се осъществява, като:

- потребителите се идентифицират име и парола и автентифицират с електронен подпис за НАП;
- управлението на регистрите от тип клиент-сървър-база данни;
- няма външни връзки и свързване;
- софтуерната и хардуерната среда периодично и при необходимост се обслужва за вируси, нежелани програми и замърсяване от отдел Информационни технологии (ИТ). Ползва се UPS на сървъра;
- забранява се ползването на лични технически носители на информация (флаш памет, телефон, външен диск и др.), инсталиране на нелицензирани програми;
- ползването на Интернет на компютри с достъп до сървъра, където се обработват личните данни, да става само с криптирана връзка;
- личните данни се архивират на технически носител, периодично на всеки 90 дни от обработващия лични данни или от служител в отдел ИТ с цел запазване на информацията за съответните лица в актуален вид. Същото се извършва на външен диск, достъп до който има само обработващият лични данни;
- по разписание се правят резервни копия за възстановяване;

Обработването на лични данни става само в работно време от назначеното длъжностно лице.

(6) Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.).

При възникване и установяване на инцидент, се действа съгласно утвърдена Процедура в случай на нарушение на сигурността на личните данни

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. 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, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(7) Предоставяне на лични данни на трети лица – основание, цел, категории лични данни.

1. Данните на лицата не се изнасят извън сградата на администратора. Никое длъжностно или трето лице няма право на достъп до личните данни на участниците в обществени поръчки в „Пристанище Варна" ЕАД, освен ако същото е изисквано по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). Достъпът на тези органи до личните данни на участниците в обществени поръчки в „Пристанище Варна" ЕАД е правомерен.

2. Надлежен е начинът, при който съответният съдебен орган е изискал документи, съдържащи лични данни, писмено с изрично искане, отправено до Изпълнителния директор на дружеството. В подобни случаи на органите на съдебна власт се предоставя копие от документите, заверени с подпис на Ръководителя на съответния отдел и печат на дружеството, освен ако няма изрично искане от съда да бъдат предоставени оригиналите. За идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира заинтересованото лице, но не и да препятства работата на органите на съдебна власт.

3. Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на дружеството.

4. Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до личните данни на участниците в обществени поръчки.

5. Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица.

6. При внедряване на нов програмен продукт за обработване на лични данни следва да се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

7. За неизпълнение на задълженията, вменени на съответните длъжностни лица по тази инструкция и по Закона за защита на личните данни, се налагат дисциплинарни

наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган - предвиденото наказание в Закона за защита на личните данни и Регламент (ЕС) 2016/679. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

„Пристанище Варна" ЕАД не предоставя лични данни на други държави по този регистър.

(8) Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

Сроковете са веднъж на две, години или когато възникне основание за това.

(9) Определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни.

(1) След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни по този Регистър, данните трябва да се:

1. унищожат, или

2. прехвърлят на друг администратор, като предварително се уведоми за това комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни Регистърът се съхранява само в предвидените в закон случаи.

(3) В случаите, когато след постигане целта на обработване „Пристанище Варна" ЕАД иска да съхрани обработените лични данни като анонимни данни за исторически, научни или статистически цели, се уведомява за това комисията.

(4) Комисията за защита на личните данни може да забрани съхраняването за целите по ал.3, ако „Пристанище Варна" ЕАД не осигури достатъчната защита на обработените данни като анонимни данни.

(5) Решението на комисията по ал. 4 подлежи на обжалване пред съответния административен съд. Решението на административния съд не подлежи на обжалване. В случаите на отхвърляне на жалбата срещу решението на комисията, тогава „Пристанище Варна" ЕАД трябва да унищожи личните данни по Регистъра.

Чл. 12. Регистър „Сигурност"

(1) Общо описание на поддържаните регистри - категории лични данни и основание за обработване в Регистър „Сигурност".

1. Регистърът набира и съхранява данни на лицата, които са субекти на контролно-пропускателния режим на „Пристанище Варна" ЕАД по време на дейността им по изпълнение на сключените договори с оглед индивидуализиране на лицата, които влизат, престояват и излизат от пристанището в изпълнение на нормативните изисквания на Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България, Закона за частната охранителна дейност и подзаконовите нормативни актове; използване на събраните данни за съответните лица за служебни цели за всички дейности, свързани с издаване на еднократни, временни и постоянни пропуски на лицата, имащи право на достъп до територията на „Пристанище Варна" ЕАД.

2. Към дейността по сигурността влиза и видеонаблюдение на подходите към КПП, охраняемия периметър и прилежащите паркинги. Записите с видеообрази се съхраняват на отделно устройство.

3. В регистърът се обработват следните категории лични данни:

- физическа идентичност: имена и паспортни данни, като ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.;
- физическата идентичност на лицето: видеообраз за движението на служителите и посетителите към подходите, сградите и по охраняемия периметър;
- копиране на лични документи с директен запис в охраняем сървър.

(2) Технологично описание на поддържаните регистри.

1. Носители на данни, технология на обработване.

По този критерий попада начина на съхранение и невъзможността неоторизирани лица да манипулират личните данни на Регистъра. Данните са на хартиен и технически носител:

- На хартиен носител личните данни се съхраняват в папки, подредени в шкаф, който се заключва. Обработката на тези данни е от назначено за обработването длъжностно лице. Това става в специално помещение, което също се заключва;
- На технически носител личните данни се въвеждат директно на твърд диск в защитен сървър в мрежа. Сървърът е в изолирано помещение с контрол на достъпа. Влизането в операционната система става чрез парола, известна само на оторизираното длъжностно лице. Защитата на техническите данни от неправомерен достъп, повреждане, изгубване или унищожава се осигурява чрез система от мерки: определяне на роли и отговорности (администратор, ползвател), идентификация и автентификация, лицензирани програмни продукти, антивирусни програми, контроли на сесията, копия/резервни копия за възстановяване, процедури за унищожаване/заличаване/изтриване на носители и чрез поддържане на информацията на хартиен носител.

2. Срока на съхранение на личните данни в Регистър „Сигурност".

Срока на съхранение на личните данни в Регистър „Сигурност" е:

- съгласно Закон за българските лични документи по чл. 30 от 5 до 10 г.;
- съгласно Закона за частната охранителна дейност за видеозаписи по чл. 30 – 30 дни.

3. Предоставени услуги.

По този регистър не се предоставят услуги.

(3) Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им.

1. В Регистрър „Сигурност" правомерен достъп, освен служителите от отдел „Вътрешен ред и сигурност", при спазване принципа „Необходимо да се знае", имат и други лица, пряко ангажирани с оформяне и проверка законосъобразността на издаваните пропуски - Изпълнителен директор и Главен юрисконсулт.

2. Задълженията на длъжностните лица, обработващи лични данни са описани в Нормативни изисквания на Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България и подзаконовите нормативни актове, Инструкция за контролно-пропускателния режим, Инструкция за оператор-охранител и Инструкция, относно „механизма на обработване на лични данни и защитата им от незаконни форми на обработване в регистрите в Пристанище Варна ЕАД". Видеонаблюдението е с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

3. Възможността за предоставяне на други лица на достъп до личните данни е ограничена и изрично регламентирана в чл. 7, ал. 7 от Инструкцията.

(4) Оценка на въздействие и определяне на съответно ниво на защита.

1. Общия брой на физическите лица, на които се обработват личните данни в Регистър „Сигурност" е по-малко от 10000.

Оценка на нивото на въздействие на Регистър „Сигурност"

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Регистър „Сигурност"	**СРЕДНО**	**СРЕДНО**	**СРЕДНО**	**СРЕДНО**

2. За да се оцени въздействието, Администраторът отчита критериите за поверителност, цялостност и наличност. 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.

3. Администраторът отчита категориите на обработваните лични данни по „Специфични признаци", които се отнасят само до физическата идентичност на група физически лица, чийто брой надхвърля 2, но е по-малък от 10000.

4. За определяне ниво на въздействие „СРЕДНО" се отчита също така, характера и целите на обработваните лични данни, а именно за контролно-пропускателния режим на територията на „Пристанище Варна" ЕАД, където по смисъла на Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България, контролно-пропускателните пунктове се явяват и гранична зона.

5. Минималното ниво на технически и организационни мерки, които следва да осигури за Регистър „Сигурност" при **СРЕДНО НИВО НА ВЪЗДЕЙСТВИЕ** е **СРЕДНО НИВО НА ЗАЩИТА**.

(5) Описание на предприетите технически и организационни мерки.

1. Физическа защита. Организационни мерки и технически мерки.

На територията на дружеството помещенията, където се обработват лични данни от Регистър „Сигурност", са общо 2 (две):

- в Пристанище Варна-Изток са 1 (едно) помещение на контролно-пропускателния пункт.

- в Пристанище Варна-Запад са 1 (едно) помещение на контролно-пропускателния пункт.

В същите помещения се разполагат елементите на комуникационно-информационните системи за обработване на лични данни. Сървърът, към който се свързват всички работни компютри от локалната мрежа на Регистъра е в друго изолирано помещение с ограничен достъп.

Създадена е организация на физическия достъп – до помещенията се допускат назначените да обработват лични данни служители.

Достъпът на Външни лица до помещенията, в които се обработват лични данни е през гише.

В контролно-пропускателните пунктове винаги има оператор. Сградите са с физическа охрана и видеонаблюдение.

Шкафовете за хартиените носители на данни в Регистъра се заключват, а помещенията са оборудвани с пожарогасителни средства.

2. Персонална защита.

Обработващите лични данни по този Регистър се запознават с Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, Регламент (ЕС)

2016/679, Правилник за контролно-пропускателния режим, Инструкция, относно „механизма на обработване на лични данни и защитата им от незаконни форми на обработване в регистрите в Пристанище Варна ЕАД" и настоящата Инструкция, в касаещия ги обем.

Лицата, обработващи лични данни, подписват декларация Образец № 4– съгласие за поемане на задължение за неразпространение на лични данни.

Голяма част от персонала преминава обучение по защита на личните данни.

Създадена е политика за несподеляне на критична информация между персонала чрез персонализиране на работната среда.

3. Документална защита.

Регистър „Сигурност" се поддържа на хартиен носител с достъп само от упълномощените лица, определени в чл. 12 ал. 3.

Обработката се извършва в работно време.

Сроковете за съхранение са определени в чл. 12 ал. 2 т. 2.

Личните данни могат да бъдат размножавани и разпространявани от назначените служители, само ако е необходимо в изпълнение на служебни задължения или ако са изискани по надлежния ред.

Унищожаването на документи с изтекъл срок на съхранение се извършва от назначена със заповед на Изпълнителния директор комисия.

4. Защита на автоматизирани информационни системи и/или мрежи.

Програмния продукт чрез които се обработват личните данни по регистъра е специална програма за копиране на лични документи директно в охраняемия сървър.

„Пристанище Варна"-Запад има VPN криптирана връзка с Пристанище Варна-Изток, където се намира физическия сървър в зоната на сигурност. Физическия сървър за личните данни се намира в административната зона на сигурност, в изолирано помещение със строго контролиран и ограничен достъп, оборудвано с метална врата, климатик и СОТ.

Оправомощените лица са с персонален достъп с потребителско име и парола до операционната система на работните компютри и отделно за програмата за охрана.

Сроковете за съхранение на личните данни са дефинирани за целия Регистър в чл. 12 ал. 2 т. 2.

Унищожаване/заличаване/изтриване на носители се осъществява съгласно създадените процедури.

Компютрите са в работните помещения в зоната на сигурност на охраняемия периметър.

Реализацията на технически мерки се осъществява, като:

- потребителите се идентифицират с име и парола;
- управление на регистрите от тип клиент-сървър;
- външните връзки и свързване между Пристанище Варна-Изток и Пристанище Варна-Запад е през криптирана връзка VPN;
- софтуерната и хардуерната среда периодично и при необходимост се обслужва за вируси, нежелани програми и замърсяване от отдел Информационни технологии (ИТ). Ползва се UPS на сървъра;
- забранява се ползването на лични технически носители на информация (флаш памет, телефон, външен диск и др.), инсталиране на нелицензирани програми;
- ползването на Интернет на компютри с достъп до сървъра, където се обработват личните данни, да става само с криптирана връзка;
- личните данни се архивират на технически носител, периодично на всеки 90 дни от обработващия лични данни или от служител в отдел ИТ с цел запазване на информацията за съответните лица в актуален вид. Същото се извършва на външен диск, достъп до който има само обработващият лични данни;
- по разписание се правят резервни копия за възстановяване;

Обработването на лични данни става само в работно време от назначеното длъжностно лице.

(6) Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.).

При възникване и установяване на инцидент, се действа съгласно утвърдена Процедура в случай на нарушение на сигурността на личните данни

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. 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, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(7) Предоставяне на лични данни на трети лица – основание, цел, категории лични данни.

1. „Пристанище Варна" ЕАД **предоставя** лични данни за физическа идентичност, като имена и паспортни данни от личните документи на физическите лица, на трети лица - на Гранична полиция от Министерство на вътрешните работи. **Предоставянето на лични данни на трета страна е законосъобразно в съответствие с чл. 363 т. 1 ал. За от Закона за защита на личните данни.** Никое длъжностно или трето лице няма право на достъп до личните данни на "Пристанище Варна" ЕАД, освен ако същото е изисквано по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). Достъпът на тези органи до личните данни на лицата е правомерен. Предоставят се данни и в случаите за:

- Профил на купувача, съгласно Закон за обществените поръчки;
- Служители на дружеството при застраховки при трудови злополуки и живот.

2. Надлежен е начинът, при който съответният съдебен орган е изискал документи, съдържащи лични данни, писмено с изрично искане, отправено до Изпълнителния директор на дружеството. В подобни случаи на органите на съдебна власт се предоставя копие от документите, заверени с подпис на Ръководителя на съответния отдел и печат на дружеството, освен ако няма изрично искане от съда да бъдат предоставени оригиналите. За идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира заинтересованото лице, но не и да препятства работата на органите на съдебна власт.

3. Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на дружеството.

4. Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до личните данни на физическите лица.

5. Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица.

6. При внедряване на нов програмен продукт за обработване на лични данни следва да се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

7. За неизпълнение на задълженията, вменени на съответните длъжностни лица по тази инструкция и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган - предвиденото наказание в Закона за защита на личните данни и Регламент (ЕС) 2016/679. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

„Пристанище Варна" ЕАД не предоставя лични данни на други държави по този регистър.

(8) Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

Сроковете са веднъж на две, години или когато възникне основание за това.

(9) Определяне на ред за изпълнение на задълженията по чл. 25 от Закона за защита на личните данни.

(1) След постигане целта на обработване на личните данни или преди преустановяване на обработването на личните данни по този Регистър, данните трябва да се:

1. унищожат, или

2. прехвърлят на друг администратор, като предварително се уведоми за това комисията, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни Регистърът се съхранява само в предвидените в закон случаи.

(3) В случаите, когато след постигане целта на обработване „Пристанище Варна" ЕАД иска да съхрани обработените лични данни като анонимни данни за исторически, научни или статистически цели, се уведомява за това комисията.

(4) Комисията за защита на личните данни може да забрани съхраняването за целите по ал.3, ако „Пристанище Варна" ЕАД не осигури достатъчната защита на обработените данни като анонимни данни.

(5) Решението на комисията по ал. 4 подлежи на обжалване пред съответния административен съд. Решението на административния съд не подлежи на обжалване. В случаите на отхвърляне на жалбата срещу решението на комисията, тогава „Пристанище Варна" ЕАД трябва да унищожи личните данни по Регистъра.

VI. Осигуряване на достъп на лицата до личните им данни

Чл. 13. (1) Физическите лица имат право на достъп до личните си данни, в свободно избрана от тях форма, за което подават писмено заявление до обработващия лични данни, и/или лицето, действащо под негово или на администратора ръководство при обработване, в това число и по електронен път по реда на Закона за електронния документ и електронния подпис, лично или чрез упълномощено по нотариален ред лице. Подаването на заявление е безплатно.

(2) При упражняване на правото си на достъп заинтересованото лице има право по всяко време да поиска от администратора:

1. Потвърждение за това, дали отнасящите се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват.

2. Съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

3. Информация за логиката на всяко автоматизирано обработване на лични данни, отнасящи се до него, поне в случаите на автоматизирани решения от Закона за защита на личните данни.

(3) Правото си на достъп до лични данни по начина, посочен по-горе, лицето може да упражни безплатно веднъж на 12 месеца, а при смърт - правото му се упражнява от неговите наследници.

(4) Ако при осъществяване достъпа до лични данни по искане на едно лице е възможно да се разкрият лични данни за друго лице, администраторът е длъжен да предостави достъп само до частта от тях, отнасяща се до заинтересованото лице.

(5) Освен на достъп до лични данни, физическите лица имат право по всяко време да поискат от администратора да:

1. Заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на Закона за защита на личните данни и Регламент (ЕС) 2016/679.

2. Уведоми третите лица, на които са разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с горното, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

(6) Заявлението съдържа име, адрес на лицето и други данни, които го идентифицират:

- ЕГН, месторабота, описание на искането, предпочитана форма за предоставяне на исканата информация, подпис, дата на подаване на заявлението и адрес на кореспонденцията; - пълномощно, когато заявлението се подава от упълномощено лице.

(7) Заявлението се завежда в общия входящ регистър на администратора.

(8) Няма пречка заинтересованото лице да поиска този достъп да се осъществи в широко разпространените форми:

1. Устна справка.

2. Писмена справка.

3. Преглед на данните от самото лице или от изрично упълномощеното от него такова;

4. Предоставяне на копие от исканата информация;

5. Предоставяне на исканата информация по електронен път, освен в случаите, когато това е забранено от закон;

6. Предоставяне на копие от исканата информация на предпочитан носител, освен в случаите, когато законът забраняват това.

(9) При подаване искане за осигуряване на достъп представляващият администратора разглежда заявлението за достъп или разпорежда на обработващия лични данни и/или лицето, действащо под негово или на администратора ръководство при обработване личните данни да осигури искания от лицето достъп в предпочитаната от заявителя форма. Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен от деня на подаване на искането, съответно 30-дневен, когато обективно се изисква по-дълъг срок за събиране на всички искани данни на лицето и това сериозно затруднява дейността на администратора. В посочените срокове, по заявлението на лицето администраторът на лични данни взема решение за предоставяне на пълна или частична информация или мотивирано отказва предоставянето й.

(10) При искане за заличаване, блокиране на лични данни, поради неправомерно обработване, несъответстващо на Закона за защита на личните данни и Регламент (ЕС) 2016/679, администраторът взема решение и извършва съответното действие в 14-дневен срок от подаване на заявлението или мотивирано отказва извършването им. При искане за уведомяване на трети лица, на които са разкрити личните данни за извършеното заличаване, коригиране, блокиране, администраторът на лични данни взема решение в 14-дневен срок и незабавно уведомява третите лица или мотивирано отказва да извърши уведомяването.

(11) Администраторът на лични данни уведомява писмено заявителя за решението или отказа си в съответния срок лично срещу подпис или по пощата с обратна разписка. Липсата на уведомление се смята за отказ.

(12) Когато данните не съществуват или предоставянето им е забранено със закон, на заявителя се отказва достъп до тях с мотивирано решение. Администраторът отказва пълно или частично предоставяне на данни на лицето, за което те се отнасят, когато от това би възникнала опасност за отбраната или националната сигурност или за защита на класифицираната информация и това е предвидено в специален закон. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган и срок.

(13) Решението на администратора е недопустимо, когато:

1. Има правни или други съществени последици за физическото лице.
2. Е основано единствено на автоматизирано обработване на лични данни, предназначено да оценява лични характеристики на физическото лице.

(14) При постановяване на недопустимо решение, прието в нарушение на Закона за защита на личните данни и Регламент (ЕС) 2016/679, физическото лице има право да поиска от администратора да преразгледа решението.

(15) Решението не се счита недопустимо, когато:

1. В взето по време на сключването или изпълнението на договор, при условие че подадената от съответното физическо лице молба за сключване или изпълнение на договора е била удовлетворена или че съществуват подходящи мерки, гарантиращи законните му интереси.
2. Е уредено в закон, предвиждащ и мерки за защита на законните интереси на лицето.
3. Достъп до личните данни на лицата, съдържащи се на технически носител има само обработващият лични данни и/или лицето, действащо под негово или на администратора ръководство при обработване на лични данни.

VII. Актуализация на лични данни

Чл. 14. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в дружеството. Актуализация на лични данни се извършва:

1. По искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ.

2. По инициатива на обработващия лични данни - при наличие на документ, даващ основание за актуализация.

3. При установена грешка при обработката на личните данни от страна на „Пристанище Варна" ЕАД.

(2) При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето, обработващо личните данни.

VIII. Условия за даване на съгласие за обработване на лични данни

Чл. 15. (1) Когато обработването се извършва въз основа на съгласие, администраторът трябва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни – това става с утвърдена Декларация за предоставяне на лични данни.

(2) Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това. Оттеглянето на съгласие е също толкова лесно, колкото и даването му.

(3) Когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали е в изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор.

(4) Ако по някаква причина е необходимо обработване на лични данни на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 16 години. Ако детето е под 16 години това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

IX. Адрес за кореспонденция

Чл. 16. Адресът, на който се приемат молби за достъп и предоставяне на лични данни от регистрите на „Пристанище Варна" ЕАД, е: гр. Варна 9000 пл. "Славейков" № 1 тел.: 052/ 69 2232 факс: 052/ 63 2953, или на електронен адрес: headoffice@port-varna.bg

X. Контрол при обработване на лични данни

Чл. 17. Контролът по изпълнението на настоящата Инструкция ще се осъществява от длъжностно лице по защита на личните данни на „Пристанище Варна" ЕАД, определено със заповед.

Допълнителни разпоредби

1. Инструкция за обработване и защита на личните данни на физическите лица в „Пристанище Варна" ЕАД влиза в сила от 25.05.2018 г.

2. Настоящата Инструкцията отменя Инструкция от 2007 г. относно механизма на обработване на лични данни и защитата им от незаконни форми на обработване в

регистрите "Персонал", "Клиенти и доставчици" и "Сигурност", водени в "Пристанище Варна" ЕАД.

3. Изпълнителния директор утвърждава следните образци от документи:

- Образец № 1. Декларация за съгласие за обработка на лични данни на физическо лице в Регистър „Персонал".
- Образец № 2. Декларация за съгласие за обработка на лични данни на физическо лице в Регистри „Клиенти и доставчици" и „Обществени поръчки".
- Образец № 3. Декларация за съгласие за обработка на лични данни на физическо лице в Регистър „Сигурност".
- Образец № 4. Декларация за съгласие за поемане на задължение за неразпространение на лични данни.
- Образец № 5. Заявление за достъп до лични данни.
- Образец № 6. Искане за коригиране на лични данни на физическо лице.
- Образец № 7. Искане за ограничаване на обработването на лични данни на физическо лице.
- Образец № 8. Искане за изтриване на лични данни на физическо лице.
- Образец № 9. Искане за прекратяване обработването на лични данни на физическо лице.

Изготвил:
Старши юрисконсулт:.....
(Мила Атанасова)

Съгласувал:
Р-л отдел „Правен":.....
(Галин Иванов)

Одобрил:
Админ. директор:.....
(Мариела Петкова)