"ПРИСТАНИЩЕ ВАРНА" ЕАД

УТВЪРДИЛ:
ИЗП. ДИРЕКТОР.....
(И.Гавраилов)

Дата: 20.03.2026 г.

ИНСТРУКЦИЯ

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

I. Правно основание

Чл.1(1)Настоящата Инструкция се издава на основание и във връзка с прилагането на :

- Регламент (ЕС) 2016/679;
- Закон за защита на личните данни;
- Действащия Закон за киберсигурност на България, транспониращ Директива (ЕС)2022/2555 (NIS2), доколкото „Пристанище Варна"ЕАД попада в обхвата на „съществени субекти" по смисъла на закона.

(2)Настоящата инструкция урежда вътрешните правила за обработване и защита на личните данни, като отчита задълженията на администратора както по режима на защита на личните данни, така и по режима на мрежова и информационна сигурност, без да допуска прехвърляне или ограничаване на отговорността по Регламент (ЕС) 2016/679.
Инструкцията се утвърждава, допълва, изменя и отменя от Изпълнителния директор на „Пристанище Варна" ЕАД.
(3)Подробните технически и организационни мерки по мрежова и информационна сигурност се уреждат в отделни вътрешни процедури по киберсигурност, като настоящата инструкция регламентира специфичните аспекти, свързани със защита на личните данни.

II. Цели на Инструкцията

Чл. 2. Инструкцията се приема с цел да регламентира:

- Създаване на организация и вътрешен ред при обработване на лични данни на физически лица;
- Задълженията на служителите, обработващи личнни данни в „Пристанище Варна"ЕАД;
- Осигуряване на подходящи технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от други незаконосъобразни форми на обработване, съобразно риска за правата и свободите на физическите лица;
- Осигуряване на ефективен достъп на субектите на данни до личните им данни и практическото упражняване на правата им съгласно Регламент (ЕС) 2016/679;
- Поддържане на точност и актуалност на обработваните лични данни.

- Гарантиране на прозрачност и информираност на субектите на данни относно обработването;
- Осигуряване на съответствие между режима на защита на личните данни и задълженията на дружеството като „съществен субект" по действащия Закон за киберсигурниост в България, без ограничаване на отговорността по защита на личните данни.

При съществени промени в нормативната уредба, в структурата на дружеството или в рисков профил, Инструкцията подлежи на незабавен преглед съвместно от Длъжностното лице по защита на личните данни и Офицера по киберсигурност.

III. Изисквания

Чл. 3. Изисквания към съдържанието на Инструкцията съгласно Регламент (ЕС) 2016/679:

- Индивидуализиране на администратора на лични данни.
- Общо описание на поддържаните регистри – категории лични данни и основание за обработване;
- Технологично описание на поддържаните регистри – носители на данни, технология на обработване, срокове за съхранение и предоставяни услуги;
- Определяне на длъжностите, свързани с обработване и защита на лични данни, както и техните права и задълженията;
- Определяне на взаимодействието между Длъжностното лице по защита на личните данни и Офицера по киберсигурност при управление на риска, внедряване на нови системи, оценка на въздействие и реагиране при инциденти;
- Оценка на въздействието върху защита на личните данни и определяне на съответно ниво на защита;
- Описание на предприетите технически и организационни мерки, съобразени с риска;
- Разграничаване между мерките по защита на личните данни и мерките по мрежова и информационнасигурност, уредени във вътрешни инструкции;
- Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.);
- Действия при киберинциденти и координация между Длъжностното лице по защита на личните данни и Офицера по киберсигурност, когато инцидентът представлява и нарушение на сигурността на личните данни;
- Предоставяне на лични данни на трети лица – основание, цел, категории лични данни и гаранции за защита;
- Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните и тяхното заличаване;
- Определяне на ред за изпълнение на задълженията по приложимото законодателство относно сигурността на обработване;
- Информацията се описва за всеки един от поддържаните регистри;
- Разширени изисквания по Регламент (ЕС) 2016/679.

IV. Обхват

Чл. 4. Инструкцията е задължителна за всички лица и служители, които обработват лични данни от името на „Пристанище Варна" ЕАД.

Разпоредбите в тази инструкция се прилагат и по отношение на външни обработващи лични данни, доколкото това е предвидено в договорите сключени с тях.

Чл. 5.(1)Оправомощените лица трябва да бъдат запознати със съдържанието и измененията на тази Инструкция, удостоверено с техния подпис.
(2)Провеждането на периодични обучения по защита на личните данни и информационна сигурност се координира съвместно с Длъжностното лице по защита на личните данни и Офицера по киберсигурност.

V. Обработване на лични данни на физическите лица

Чл. 6. Администратор на лични данни е „Пристанище Варна" ЕАД.
(1)Администраторът носи отговорност за доказване на съответсвтието с принципите по чл.5 от Регламент (ЕС) 2016/679 принцип на отчетност.
(2)При изпълнение на задълженията си администраторът осигурява координация между функциите по защита на личните данни и по киберсигурност, когато обработването се осъществява чрез мрежови и информационни канали.

Чл. 7.(1)Обработващи лични данни от името на администратора са Изпълнителният директор, а под негово ръководство - Финансов директор и Ръководителите на отдели:

- Отдел „Правен",
- отдел „Финансово счетоводна отчетност" (ФСО),
- отдел „Човешки ресурси и административно обслужване" (ЧРиАО),
- отдел „Безопасност и здраве при работа",
- отдел „Организация на труда, работната заплата и прогнозиране и анализ" (ОТРЗиПА),
- отдел „Маркетинг",
- отдел „Търговски, обществени поръчки и европрограми" (ТОПЕ),
- отдел „Фирмена сигурност",
- отдел „Статистика и ИСУ" (СИСУ),
- отдел "Оперативна експлоатация" (ОЕ),
- отдел „Складово експедиционен"
- сектор „Контейнерен терминал"
- отдел „Енергиен";

(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
- Организатор ЦПО, той и домакин;
- 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";
- Специалист ИСУ и проучване – отдел СИСУ;
- Организатор работна сила – отдел ОЕ;
- Дежурен енергетик.

(3)Конкретните права на достъп до регистрите се определят въз основа на принципа „необходимо да се знае", чрез вътрешни правила за управление на достъпа, съгласувани между Длъжностното лице по защита на личните данни и Офицера по киберсигурност.

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

Чл. 9. Регистър „Персонал и кандидати за работа"

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

Регистърът съдържа лични данни на служители и работници по трудови договори и изпълнители по граждански договори, както и данни на кандидати за работа 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 служат за служебни цели, свързани с трудови и граждански правоотношения и са 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)Обработването се извършва на основание:

- Чл.6, пар. 1, б. „б" и „в" от Регламент (ЕС) 2016/679;
- Приложимото рудово и осигурително законодателство;
- Чл.9, пар. 2, б. „б" от Регламента – за медицинските данни.

(3)В регистър **„Персонал и кандидати за работа"** 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.

(4) Технологично описание на Регистър **„Персонал и кандидати за работа"**

(4.1)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 електронен носител:

- На хартиен носител – чрез систематизиране и съхраняване в регламентирани архивни единици при контролиран достъп;
- В електронна форма – чрез автоматизирани информационни системи при прилагане на подходящи технически и организационни мерки, съобразени с риска за правата и свободите на физическите лица .
- Техническите мерки включват: контрол и управление на достъпа, удостоверяване на потребители, регистриране и проследимост на действията, защита на комуникациите, резервиране и възстановяване на данни, както и други мерки предвидени във вътрешни инструкции по мрежова и информационна сигурност.

- При обработване чрез мрежови и информационни системи мерките се администрират от Офицера по киберсигурност, като Длъжностното лице по защита на личните данни упражнява контрол относно законосъобразността на обработването.

(4.2)Срок на съхранение и заличаване на личните данни в Регистър **„Персонал и кандидати за работа"**.

След изтичане на нормативно установените или вътрешно определени срокове личните данни се заличават, унищожават или архивират съгласно приложимото законодателство и вътрешните инструкции за управление на документи и информация.

(4.3) Предоставени услуги.

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

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

(1)В Регистър **„Персонал и кандидати за работа"** правомерен достъп до кадровите досиета на персонала, при спазване принципа „Необходимо да се знае" имат служителите от отдел ЧРиАО и ФСО, както и други лица, пряко ангажирани с оформяне и проверка законосъобразността на документите – Изпълнителен директор, Ръководител отдел „Правен" и Ръководител, отдел „ОТРЗиПА", при извършване на одити – Специалист ИСУ и проучване от отдел СИСУ.

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, (3) от Инструкцията.

(6) Оценка на риска.

(1)Оценка на риска за правата и свободите на физическите лица се извършва периодично и при съществена промяна в обработването. Когато обработването е вероятно да породи висок риск, се извършва оценка на въздействието върху защитата на личните данни съгласно чл.35 от Регламент (ЕС)2016/679. Оценката се извършва със съдействието на Длъжностното лице по защита на личните данни и при необходимост – в координация с Офицера по киберсигурност.

(7) Описание на предприетите технически и организационни мерки.

(1)При обработването на лични данни се прилагат подходящи технически и организационни мерки, съобразени с риска, включително контрол на достъпа, разделяне на роли, регистриране на действията в информационните системи, архивиране и възстановяване на данни, защита на комуникациите във вътрешна инструкция по мрежова и информационна сигурност.

(2)Персонална защита.

Достъп до лични данни имат само лица, писмено оправомощени от администратора, след проведено обучение и подписана декларация за поверителност - Образец №4.

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

„Документална защита.

Документите, съдържащи лини данни се съхраняват в шкафове под ключ или архивни помещения с ограничен достъп. Обработката се извършва в работно време.

Сроковете за съхранение са определени в чл. 7,т.(4.2).

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.
(3)Защита напрограмните продукти и системите.
Информационните системи се защитават чрез механизми за контрол на достъпа, удостоверяване, регистриране на действия, архивиране и възстановяване на данни, съобразно изискванията на Регламент (ЕС) 679/2016 и вътрешни инструкции по мрежова и информационна сигурност.
Мерките се администрират от Офицера по киберсигурност, а тяхната пропорционалност и законосъобразност се наблюдава от Длъжносто лице по защита на личните данни.
(4)Носители на лични данни се унищожават по начин, който не позволява възстановяване на информацията, съгласно инструкция за управление на информацията.

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

При възникване на авария, произшествие, бедствие или технически инцидент, който може да засегне лични данни, се предприемат незабавни мерки за органичаване на последиците и защита на информацията съгласно вътрешните правила за непрекъсваемостта на дейността и информационната сигурност.
При инцидент, засягащ мрежови и информационни системи, се уведомява незабавно Офицера по киберсигурност.
Когато инцидентът представлява нарушение на сигурността на лични данни, се уведомява Длъжностното лице по защита на личните данни.
Извършва се съвместна оценка на риска за правата и свободите на физическите лица, като се определя необходимостта от уведомяване на надзорни орган в срок от 72 часа съгласно чл.33 от Регламент (ЕС) 2016/679.
За всички инциденти се води регистър, в който се вписват:

- Времето и предполагаемият период на възникване;
- Времето на установяване;
- Времето на докладване;
- Лицето извършило доклада;
- Последиците от инцидента;
- Предприетите коригиращи и превантивни мерки.

Възстановяването на данни се извършва по утвърдена процедура за архивиране и възстановяване, под контрола на Офицера по киберсигурност, като Длъжностното лице по защита на личните данни следи за законосъобразността на действията.

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

(1)Лични данни от регистър „Персонал и кандидати за работа"се предоставят на трети лица само при наличие на правно основание, определена цел и в обем, необходим за постигане на съответната цел, при спазване на принципа на минимизиране.
(2)Кадровите досиета не се изнасят от извън сградата на администратора, освен когато това е изискано по надлежен ред от компетентен орган или съдебен орган.
(3)Достъп до кадрови досиета или данни, съдържащи се в тях, се предоставя на:

- Съд, прокуратура и следсвени органи;
- Контролни и ревизиращи държавни органи;
- Вещи лица, назначени от съд, при наличие на писмено искане или разпореждане, съдържащо правното основание, обхвата и целта на искането.

(4)В случаите по предходната алинея се предоставят заверени копия от документи освен ако изрично не са поискани оригинали.
Информирането на субекта на данните относно предоставянето на лични данни на компетентни органи се извършва, освен ако приложимото законодателство предвижда ограничение или забрана за такова уведомяване, или когато това би могло да възпрепятства изпълнението на законово установени правомощия на съответния орган.
(5)Когато предоставянето на данни представлява обработване от името на администратора, се сключва писмен договор или друг правен акт, съдържащ изискванията на чл.28 от Регламент (ЕС) 2016/679.
(6)Предоставянето по електронен път се извършва при прилагане на технически мерки за сигурност, под контрола на Офицера по киберсигурност, като законосъобразността и пропорционалността на предоставянето се наблюдават от Длъжностното лице по защита на личните данни.
(7)Съгласие на субекта не се изисква, когато предоставянето е неободимо за изпълнение на законово задължение или за упражняване на правомощия на компетентен държавен орган.
(8)Предоставяне на лични данни извън Европейския съюз не се извършва по този регистър.
(9)Решението за предоставяне или отказ за оредоставяне на лични данни се взема от администратора и се документира.
(10)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.

(10)Срок за провеждане на периодични прегледи и заличаване на данни
(1)Необходимостта от съхранение на личните данни от регистър „Персонал и кандидати за работа" се преглежда периодично, но не по рядко от веднъж годишно, както и при промяна в нормативната уредба или целите на обработването.
(2)След изтичане на нормативно установените или вътрешно определени срокове за съхранение личните данни се заличават, унищожават или архивират по начин, който не позволява тяхното възстановяване, освен ако съществува законово основание за по – нататъшното им съхраняване.
(3)Унищожаването на хартиени носители се извършва чрез физическо унищожаване, а на електронни носители – чрез технически средства, загарнтиращи невъзможност за възстановяване на информацията.
(4)Процесът по заличаване и унищожаване се документира.
(5)Оценката на законосъобразността на съхранение се извършва със съдействието на Длъжностното лице по защита на личните данни, а техническото изпълнение на заличаването в информационните системи се осъществява под контрола на Офицера по киберсигурност.

Чл. 10. Регистър „Клиенти и доставчици"

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

В Регистър „Клиенти и доставчици" се обработват данни на физически лица - контрагенти на „Пристанище Варна" ЕАД и/или техни упълномощени представители или лица за контакт, във връзка със сключване и изпълнение на договори, както и за изпълнение на законови задължения по приложимото законодателство.

Обработването се извършва на основание:

- Изпълнение на договор;
- Изпълнение на законово задължение;
- Легитимен интерес на администратора, когато е приложимо.

Лични данни могат да се обработват и във връзка с получени запитвания чрез електронна поща или други комуникационни канали, когато това е необходимо за предоставяне на информация, изготвяне на оферти или предприемане на действия по искане на субекта на данните преди сключване на договор.

(2)В регистъра се обработват следните категории лични данни:

- Идентификационни данни:имена,длъжност,фирма,служебен адрес;
- Данни за контакт:телефон, електронна поща;
- Данни съдържащи се в договори и счетоводни документи;
- Банкови данни, когато са необходими за разплащане.

По този регистър не се обработват специални категории лични данни.

(2) Технологично описание на поддържаните регистри.

(1)Личните данни се съхраняват на хартиен и електронен носител при прилагане на подходящи технически и организационни мерки, съобразени с риска.

- Хартиените документи се съхраняват в шкафове, които се заключват и в сграда с контролиран достъп.
- Електронните данни се съхраняват в информационни системи с контрол на достъпа с удостоверяване на потребители.

(2)Договорите, анексите и свързаните протоколи се съхраняват за срок от 5 години след прекратяване на договорното отношение, освен ако в приложим нормативен акт е предвиден по – дълъг срок или съществува необходимост от защита на правни претенции.

След изтичане на приложимите срокове личните данни се заличават или унищожават по реда на тази инструкция.

(3)По този регистър се осигурява административен достъп до договори и свързани документи единствено на оправомощени лица за целите на изпълнение на договорни и счетоводни задължения.

Техническите мерки се администрират от Офицера по киберсигурност, а законосъобразността на обработването на обработването се наблюдава от Длъжностното лице по защита на личните данни.

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

1. Достъп до лични данни в Регистър „Клиенти и доставчици" имат само служители, за коитотова е необходимо за изпълнение на служебните им задължения, при спазване на принципа „необходимо да се знае" , а именно:

- Служители от отдел „Маркетинг"
- Изпълнителен директор
- Директор направление"Експлоатация"

- Ръководител отдел „Правен"
- Оправомощени лица за извършване на вътрешни одити или проверки;
- На служители от отдел „Оперативна експлоатация" и „Складово – експедиционен" отдел пряко ангажирани с изпълнението на сключените договори, се забранява събирането или изискването на информация, която не е необходима за изпълнение на конкретната дейност, провеждането на устни запитвания извън служебната компетентност на служителя, изискването за сведения относно трети лица, включително това коя фирма изпраща дадено лице за извършване на превоз на стоки, когато тази информация не е необходима за изпълнение на конкретната дейност. Служителите нямат право да събират информация „за всеки случай", по лична преценка или извън рамките на определените в настоящата инструкция цели.

Нарушаването на тази разпоредба представлява нарушение на вътрешните правила и на тази инструкция и подлежи на дисциплинарна отговорност.

(2)Достъпът се предоставя въз основа на писмено оправомощаване и при определено ниво на достъп в информационните системи.

(3)Управлението на техническия достъп се осъществява под контрола на Офицера по киберсигурност, а спазването на принципите за законосъобразност и минимизиране се наблюдава от Длъжностното лице по защита на личните данни.

(4)Предоставянето на достъп на други лица се допуска само при правно основание и се документира.

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

(1) Обработването на лини данни в Регистър „Клиенти и доставчици" се подлага на периодична оценка на риска за правата и свободите на физическите лица.

(2)Оценката се извършва:

- При създаване или изменение на регистъра;
- При промяна в категориите данни и целите на обработването;
- При внедряване на нови технологии;
- Периодично, но не по – рядко от веднъж на две години.

(3)Когато обработването е вероятно да породи висок риск за правата и свободите на физическите лица, се извършва оценка на въздействието върху защитата на личните данни съгласно чл.35 от Регламент (ЕС) 2016/679.

(4)Подходящите технически и рганизационни мерки се определят въз основа на резултатите на оценката на риска и се прилагат съвместно от администратора, Офицера по киберсигурност и Длъжностното лице по защита на личните данни.

(5) Описание на предприетите технически и организационни мерки.

(1) Физическа защита.

Личните данни от Регистър „Клиенти и доставчици" се обработват и съхраняват в помещения в сграда с контролиран достъп.

(2)Служителите в отдела , обработващи лични данни и изпълнявайки служебните си задължения се запознават с тази инструкция и с всяка нова версия, преминават вутрешни обучеия по защита на личните данни и информационна сигурност, подписват декларация за поверителност Образец №4, работят при спазване на принципа „необходимо да се знае".

Спазването на изискванията се наблюдава от Длъжностното лице по защита на личните данни.

(3)Документална защита.

Регистърът се поддържа на хартиен и електронен носител. Хартиените документи се съхраняват в заключващи се шкафове на обособено място за архив.

Размножаване и предоставяне на документи се допуска само при служебна необходимост или при наличие на правно основание.
Унищожаване на документи с изтекъл срок на съхранение се извършва по установена процедура, която гарантира невъзможност за възстановяване на информацията.
(4)Защита на автоматизирани информационни системи.
Електронното обработване се извършва чрез информационни системи, при прилагане на подходящи технически и организационни мерки , включително:

- Контрол и управление на достъпа;
- Удостоверяване на потребители;
- Регистриране на действията;
- Архивиране и възстановяване на данни;
- Защита на комуникациитр.

Конкретните технически решения се уреждат с вътрешни процедури по мрежова и информационна сигурност.
Техническите мерки се администрират от Офицера по киберсигурност, а законосъобразността на обработването се наблюдава от Длъжностното лице по защита на личните данни.

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

При възникване на авария, технически инцидент или събитие, което може да засегне лични данни, се предприемат мерки за органичаване на последиците.
При инцидент, засягащ информационни системи се уведомява Офицера по киберсигурност.
Когато инцидентът представлява нарушение на сигурността на лични данни, се уведомява и Длъжностното лице по защита на личните данни.
Извършва се съвместна оценка на риска и при необходимост се подава уведомляние до надзорния орган в срок до 72 часа съгласно чл.33 от Регламент (ЕС)2016/679.
Всички инциденти се документират.
Възстановяването на данни се извуршва по утвърдена процедура под контрола на Офицера по киберсигурност.

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

Лични данни от Регистър „Клиенти и доставчици" се предоставят на трети лица само при наличие на правно основание и при спазване на принципите на законосъобразност, минимизация и необходимост.
(1)Данни могат да бъдат предоставяни на:

- Компетентни държавни органи при наличие на законово основание и писмено искане;
- Съдебни и контролни органи в рамките на техните правомощия;
- Външни обработващи лични данни при наличие на договор по чл.28 от Регламент (ЕС) 2016/679;
- Правни и одиторски консултанти при наличие на договорна поверителност.

(2)Предоставят се само данните, необходими за конкретната цел.
(3)всяко предоставяне се документира.
(4)Не се изисква съгласие на субекта на данни, когато обработванто се извършва въз основа на законово задължение или в рамките на упражняване на официални правомощия.
(5)Лични данни не се предоставят в трети държави или международни организации, освен при спазване изискванията на глава V от Регламента.

(8) Срок за провеждане на периодични прегледи и заличаване на данни
Необходимостта от съхранение на личните данни в Регистър „Клиенти и доставчици" се преглежда периодично не по – рядко от веднъж на две години или при настъпване на промяна в целите на обработването.

След изтичане на сроковете за съхранение данните се :
- Унищожават по вътрешна процедура и по сигурен начин
  или
- Архивират , когато това се изисква по закон.

(9) Прекратяване на обработването
(1) След постигане целта на обработване, личните данни се заличават или анонимизират, освен ако не съществува законово основание за тяхното по – нататъшно съхранение.
Под анонимизиране се гарантира, че лицето не може да бъде идентифицирано пряко или косвено.
Прехвърлянето на регистъра към друг администратор се допуска само при наличие на законово основание и при осигуряване на непрекъснатост на защитата.

Чл. 11. Регистър „Обществени поръчки"

(1) Общо описание на поддържаните регистри – категории лични данни и основание за обработване в Регистър „Обществени поръчки".
(1) В Регистър „Обществени поръчки" се обработват следните данни на контрагенти 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", ИК-517 „Инструкция за реда, организирането, обработването, съхраняването и използването на документите в архивохранилищата на ПВИ и ПВЗ, представляващи архивен фонд на „Пристанище Варна" ЕАД" 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 регистъра се обработват следните категории лични данни:
- Идентификационни данни: имена, длъжност, егн (при необходимост) фирма,служебен адрес;
- Данни за контакт: телефон, електронна поща;
- Данни свързани с професионална квалификация и опит;
- Данни съдържащи се в декларации по Закона за обществените поръчки;
- Други данни, изискуеми от нормативната уредба.

(2) Технологично описание на поддържаните регистри.
(1)Личните данни се обработват:
- На хартиен носител (досие на процедурата)
- В електронна среда чрез информационни системи

Хартиените документи се съхраняват в помещения в сграда с контролиран достъп.
Електронните данни се съхраняват в защитена информационна среда с :

- Контрол на достъпа;
- Удостоверяване на потребители;
- Регистриране на действия;
- Архивиране и възстановяване на данни.

Конкретните технически параметри се уреждат с вътрешни процедури по информационна сигурност.

(2)Личните данни в Регистър "Обществени поръчки" се съхраняват съобразно:

- Изисквания на Закон за обществените поръчки;
- Вътрешни правила за архивиране;
- Приложимите срокове по счетоводно и архивно законодателство.

След изтичане на сроковете данните се унищожават или архивират по установен ред.

(3) Предоставени услуги.

По този регистър се предоставя достъп до информация при наличие на правно основание,включително:

- Публикуване на информация в профил на купувача на официалния сайт на „Пристанище Варна"ЕАД port-varna.bg;
- Предоставяне на документи на контролни органи;
- Достъп на участници по реда на закона.

(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 имат само:

- Служители, ангажирани с подготовка и провеждане на процедурите;
- Членове на комисии;
- Ръководители на съответните структурни звена;
- Изпълнителният директор в рамките на правомощията си;
- Длъжностното лице по защита на личните данни (за контролни функции)
- Офицерът по киберсигурност (за техническа сигурност)

Достъпът се предоставя при спазване на принципа „необходимо да се знае", а лицата подписват декларация за поверителност и носят дисциплинарна и имуществена отговорност при нарушение.

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

(1) В Регистър „Обществени поръчки"се извършва оценка на риска въз основа на :

- Категориите обработвани данни;
- Броя засегнати лица;
- Публичния характер на процедурите;
- Вероятността от неразрешен достъп;
- Възможни последици за субектите на данни.

Оценката се извършва периодично, не по – рядко от веднъж на две години или при съществена промяна в обработването.

С оглед естеството на обработваните данни и нормативните изисквания за регистъра се прилага **средно ниво на защита**, включващо засилени организационни и технически мерки.

При установяване на повишен риск Администраторът предприема допълнителни мерки съгласно Регламен (ЕС) 2016/679.

(5) Описание на предприетите технически и организационни мерки.

(1) Физическа защита.

Личните данни в Регистър „Обществени поръчки" се обработват в помещения с контролиран достъп.

Достъп до помещенията имат само оправомощени служители. Външни лица се допускат единствено при служебна необходимост и в присъствието на упълномощено лице.

- Хартиените документи се съхраняват в заключващи се шкафове или на обособено място в помещението на служителите. Информационните системи са разположени в защитени зони със съответните мерки за физическа защита.

(2) Персонална защита.
Обработващите лични данни по този Регистър :

- Се определят съгласно трудови договори и служебните им задължения;
- Преминават обучение по защита на данни и информационна сигурност;
- Подписват декларация за поверителност;
- Работят при спазване на принципа „необходимо да се знае"

Спазването на изискванията се контролира от Длъжностното лице по защита на личните данни.
(3) Документална защита.
Регистър „Обществени поръчки" се поддържа на хартиен носител и електронен носител.
Размножаване и предоставяне на документи се допуска само при наличие на правно основание или служебна необходимост.
Унищожаването на документи с изтекъл срок на съхранение се извършва по установена процедура, гарантираща невъзможност за възстановяване на информацията.
(4)Електронното обработване се извършва чрез защитена информационна среда при прилагане на подходящи технически и организационни мерки, включително:

- Контрол и управление на достъпа
- Удостоверяване на потребителите;
- Логване на действията;
- Архивиране и възстановяване на данни;
- Защита на комуникациите.

Конкретните технически параметри се уреждат с вътрешни процедури по информационна сигурност.
Мерките се администрират от Офицера по киберсигурност, а законосъобразността на обработването се наблюдава от Длъжностното лице по защита на личните данни.
Обработването на лични данни става само в работно време от назначените длъжностни лица.

(6) Действия при аварии и инциденти

При възникване на инцидент засягащ лични данни или информационни системи, се предприемат незабавни мерки за ограничаване на последиците.
Инцидентите се докладват без неоправдано забавяне на :

- Офицера по киберсигурност – при технически инциденти;
- Длъжностото лице по защита на личните данни – когато е налице нарушение на сигурността на лични данни.

Извършва се оценка на риска и при необходимост се подава уведомление до надзорния орган в срок до 72 часа съгласно чл.33 от Регламент (ЕС)2016/679.
Всички инциденти се документират.
Възстановяването на данни се извършва по утвърдена вътрешна процедура под контрола на Офицера по киберсигурност.

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

(1)Лични данни от Регистър „Обществени поръчки" се предоставят на трети лица само при наличие на правно основание и в обем, съответстващ на конкретната цел.
Данни могат да бъдат предоставяни на :

- Компетентни държавни и съдебни органи;
- Контролни органи в рамките на техните правомощия;
- Участници в процедурите при условия на публичност, предвидени в Закон за обществените поръчки;
- Външни обработващи лични данни при наличие на договор по л.28 от Регламент (ЕС) 2016/679.

Предоставят се само данни, необходими за съответната цел.
Всяко предоставяне се документира.
Лични данни не се предоставят в трети държави или международни организации, освен при спазване изискванията на глава V от Регламента.

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

Необходимостта от обработване и съхранение на личните данни в Регистър „Обществени поръчки" се преглежда периодично не по – рядко от веднъж на 2 години или при съществена промяна в целите, обема или правното основание на обработването.
При прегледа се оценява:

- Дали данните продължават да са необходими;
- Дали сроковете за съхранение са изтекли;
- Дали са налице законови основания за архивиране.

(9) Прекратяване на обработването

(1) След постигане целите на обработването или при отпадане на правното основание, личните данни се:

- Заличават по сигурен начин;
- Унищожават; или
- Архивират, когато това се изисква от закон.

(2) Прехвърлне на регистъра към друг администратор се допуска самопри наличие на законово основание и при гарантиране на непрекъснатост на защита на личните данни.

(3)При съхраняване на данни за исторически, статистически или отчетни цели се прилагат подходящи мерки за минимизация и, когато е възможно , анонимизация.

(4)Унищожаването или заличаването се документира.

Чл. 12. Регистър „Сигурност"

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

(1.1)Регистър „Сигурност"обхваща лични данни на:

- Служители;
- Контрагенти;посетители;
- Лица, подлежащи на контролно – пропускателен режим;
- Водачи на МПС;
- Други лица, които влизат или пребивават на територията на „Пристанище варна"ЕАД

Обработването се извършва с цел:

- Гарантиране сигурността на обектите и инфраструктурата;
- Контрол на достъпа;
- Защита на персонала и имуществото;
- Предотвратяване и разкриване на противоправни действия.

Правно основание:

- Изпълнение на законово задължение;
- Защита на обществен интерес;
- Легитимен интерес на администратора,

Съгласно приложимото национално законодателство и Регламент (ЕС) 2016/679.

(1.2)Видеонаблюдение.

В рамките на дейността по сигурност се извършва видеонаблюдение на :

- Входно – изходните пунктове
- Охраняемия периметър
- Прилежащите зони за сигурност.

Видеонаблюдение не се извършва в помещения, където се засяга личното достойнство на лицата.

(1.3)Категории лични данни, които могат да се обработват в Регистър „Сигурност"

- Идентификационни данни: имена, ЕГН/ЛНЧ , при необходимост номер на документ за самоличност;
- Данни за контакт;
- Регистрационен номер на МПС;
- Данни съдържащи се в пропуск;
- Видеообраз;
- Данни от дневници за достъп.

Копия на документи за самоличност може да се извършва само когато това е изрично предвидено в закон или нормативен акт.

(2)Носители на технология и обработване

Личните данни се обработват:

- На хартиен носител (заявление ФК)
- В електронна среда чрез защитени информационни системи
- Чрез системи за видеонаблюдение

Системите са разположени в защитена среда с контролиран достъп.

Прилагат се технически и организационни мерки , включително:

- Контрол- на достъпа
- Удостоверяване на потребители;
- Регистриране на действия;
- Резервно копие;
- Процедури за сигурно унищожаване.

Конкретните технически параметри се уреждат с утвърдени вътрешни процедури по информационна сигурност.

(3)Срок на съхранение:

Личните данни се съхраняват за срок, необходим за постигане на целите на обработването и съобразно приложимото законодателство.

Видеозаписите се съхраняват до 30 дни, освен когато са необходими за разследване или защита на правен интерес.

Данните за контролно – пропускателния режим се съхраняват за срок, определен във вътрешна процедура по сигурността.

(4)Предоставяне на данни:

Лични данни от Регистър „Сигурност" могат да бъдат предоставяни на :

- Компетентни държавни органи;
- Правоохранителни органи;
- Съдебни органи;
- Други органи в рамките на техните законови правомощия.

Предоставянето се документира. Не се предоставят данни в трети държави, освен при наличие на законово основание и при спазване изискванията на глава V от Регламент (ЕС) 2016/679,

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

1. В Регистър „Сигурност" правомерен достъп до лични данни имат:
   - Служители от отдел „Фирмена сигурност"
   - Оправомощени длъжностни лица, ангажирани с издаване и контрол на пропуски;
   - Изпълнителен директор в рамките на правомощията ми;
   - Главният юрист при правна необходимост;
   - Длъжностното лице по защита на личните данни – за контролни функции;
   - Офицерът по киберсигурност – относно техническата сигурност;
   - Определени служители при извършване на вътрешни одити

Достъп се предоставя при спазване на принципа „необходимо да се знае"
На всички изброени длъжностни лица , достъп се предоставя единствено и само за целта на изпълнение на трудовите задължения, като задължително преминават обучение по защита на личните данни, подписват декларация за поверителност и носят дисциплинарна и имуществена отговорност при нарушение.

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

(1) За Регистър „Сигурност" се извършва периодична оценка на риска с оглед на :
   - Естеството на обработваните данни (идентификационни данни, видеообраз);
   - Обема на засегнатите лица;
   - Значението на обекта като охраняема гранична зона;
   - Възможните последици при неправомерен достъп.

Оценка се извършва не по – рядко от веднъж на две години ли при съществена промяна в обработването.

С оглен характера на дейността и инфраструктурата се прилага средно към високо ниво на защита, съобразено с изискванията на Регламент (ЕС) 2016/679 и приложимото национално законодателство.

(5) Описание на предприетите технически и организационни мерки.

(1)Физическа защита.
Личните данни се обработват в контролирани зони с ограничен достъп.
Контролно – пропускателните пунктове са обезпечени с физическа охрана и видеонаблюдение.
Хартиените носители се съхраняват в заключващи се шкафове или помещения с контролиран достъп.
(2)Персонална защита.
Обработващите лични данни преминават обучение по защита на личните данни, подписват декларация за поверителност и работят при спазване на вътрешните процедури по сигурност.
Контролът по спазването се осъществява от Длъжностното лице по защита на личните данни.
(3)Документална защита.
Регистърът„Сигурност" се поддържа на хартиен и електронен носител.
Обработката се извършва само в работно време.Размножаването и предоставянето на данни се допуска само при наличие на правно основание.
Унищожаването на документи се извършва по утвърдена процедура, гарантираща невъзможност за възстановяване.
(4)Защита на автоматизирани информационни системи и/или мрежи.
Електронно обработване се извършва в защитена информационна среда при прилагане на :

- Контрол и управление на достъпа;
- Удостоверяване на потребители;
- Криптирана комуникация;
- Логване на действия;
- Архивиране и възстановяване;
- Процедури за сигурно унищожаване на носители.

Конкретните технически параметри се уреждат във вътрешни процедури по информационна сигурност и не се описват детайлно в настоящата инструкция.

Техническата сигурност се администрира от Офицера по киберсигурност.

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

При възникване на инцидент, засягащ лични данни или ситема за сигурност:

- Се предприемат незабавни мерки за ограничаване на последиците;
- Се уведомява Офицера по киберсигурност;
- Когато е налице нарушение на сигурността на лични данни, се уведомява Длъжностното лице по защита на личните данни.

Извършва се оценка на риска и при необходимост се подава уведомление до надзорния орган до 72 часа съгласно чл.33 от Регламент (ЕС) 2016/679.
Всички инциденти се документират.
Възстановяването на данни се извършва по утвърдена процедура под контрола на Офицера по киберсигурност.

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

(1)Лични данни от Регистър „Сигурност" се предоставят на трети страни само когато:

- Това е предвидено в закон;
- Е необходимо за изпълнение на законово задължение;
- Е необходимо за защита на жизненоважни интереси;
- Е необходимо за установяване, упражняване или защита на правни претенции.

Предоставянето се документира.
(2)Предоставяне на лични данни на държавни органи
Лични данни (идентификационни данни и данни за достъп) могат да бъдат предоставяни на :

- Главна дирекция Гранична полиция
- Органи на Министерство на вътрешните работи
- Прокуратура
- Съд
- Разследващи органи
- Други компетентни държавни органи

При наличие на надлежно правно основание и писмено искане.
Предоставят се копия на документи, освен ако законът не изисква оригинал.
Администраторът може да откаже предоставяне, когато искането е незаконосъобразно.
(3)Уведомяване на субекта.
Субектът на данните се уведомява за предоставянето, освен когато това не е забранено със закон, уведомяването би възпрепядствало разследване или съществува риск за националната сигурност.
(4) Ревизиращи и контролни органи.
Правомерен е достъпът на надлежно легитимиани контролни органи, когато това е в рамките на техните законови правомощия.

(5)Забрана за международен трансфер на данни.
По този регистър не се извършва трансфер на лични данни в трети страни или международни организации, освен при законово основание и при спазване на глава V от Регламент (ЕС) 2016/679.
(6)Нови информационни системи.
При внедряване на нов софтуерен продукт, включващ обработване на лични данни, се извършва предварителна оценка на съответсвтието с изискванията за защита на личните данни и при необходимост – оценка на въздействието (DPIA).
(7)Отговорност.
Нарушенията на настоящата инструкция водят до :

- Дисциплинарна отговорност по Кодекса на труда;
- Административно – наказателна отговорност по Закон за защита на личните данни;
- Имуществена отговорност;
- Други форми на отговорност съгласно приложимото законодателство.

(8) Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.
Не по – рядко от веднъж на две години се извършва преглед на :

- Необходимостта от обработване;
- Срокове за съхранение;
- Актуалност на данните.

При отпадане на основанието данните се заличават или унищожават по установен ред.

(**9) Прекратяване на обработването**
(1) След постигане целта на обработване на личните данни:

- Се унищожават по сигурен начин; или
- Се съхраняват, когато това е изискуемо от закон.

VI. Осигуряване на права на достъп на субектите на данни

Чл. 13. Права на достъп и други права
Физическите лица имат право на достъп да упражняват правата си съгласно чл.12-23 от Регламент (ЕС) 2016/679.
(1)Подаване на искане.
Искането може да се подаде:

- Писмено;
- По електронен път;
- Лично или чрез упълномощено лице.
- Администраторът може да изисква информация за идентификация.

(2) Срок за отговор.
Администраторът отговаря в срок до 1 месец, който може да бъде удължен с още два месеца при сложност или множество искания. Удължаването се мотивира.
Информацията се предоставя безплатно, освен когато исканията са явно неоснователни или прекомерни.
(3)Ограничения.
Достъп може да бъде ограничен, когато това е предвидено в закон и е необходимо за:

- Национална сигурност;
- Обществен ред;
- Предотвратяване и разследване на престъпления;
- Защита на права и свободи на други лица.

(4)Обжалване.
Субектът има право да подаде жалба до Комисия за защита на личните данни или да потърси защита по съдебен ред.

VII. Актуализация на лични данни

Чл.14.(1)Актуализация на лични данни представлява коригиране, допълване или заличаване на неточни , непълни или остарели данни.
Актуализация на лични данни се извършва:

- По искане на субекта на данни, когато същият установи неточност или непълнота и при необходимост представи доказателства;
- По инициатива наадминистратора при наличие на достоверен източник на информация;
- При установена техническа или фактическа грешка при обработването.

(2) При извършване на актуализация на лични данни се документират:

- Основание за промяната;
- Датата на извършването;
- Лицето, извършило актуализацията;
- Източникът на новата информация (когато е приложимо).

Актуализацията се извършва без неоправдано забавяне.

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

Чл.15. (1)Когато обработването се основава на съгласие, администраторът следва да може да докаже, че субектът на данните е дал:

- Свободно изразено;
- Конкретно;
- Информирано;
- Недвусмислено съгласие.

(2) Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието:

- не засяга законосъобразността на обработването, извършено преди оттеглянето;
- е също толкова лесно, колкото и даването на съгласието.

(3) Когато се прави оценка дали съгласието е било свободно изразено, се отчита дали изпълнението на договор или услуга е поставено взависимост от съгласие за обработване на данни, които не са необходими за изпълнение на договора
(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 искания и уведомления във връзка с упражняване на права по Регламент (ЕС) 2016/679 и Закон за защита на личните данни в „Пристанище Варна" ЕАД е: гр. Варна 9000 пл. "Славейков" №1 тел.: 052/ 69 2232 факс: 052/ 63 2953, или на електронен адрес: gdpr@port-varna.bg , както и лично в деловодството на дружеството.

X. Контрол при обработване на лични данни

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

Длъжностното лице по защита на личните данни:

- наблюдава спазването на нормативните изисквания;
- участва в оценка на риска и оценки на въздействие;
- сътрудничи с надзорния орган – Комисия за защита на личните данни.

КОНТРОЛЪТ НЕ ОСВОБОЖДАВА РЪКОВОДИТЕЛИТЕ НА ОТДЕЛИ И СТРУКТУРНИ ЗВЕНА ОТ ОТГОВОРНОСТ ЗА СПАЗВАНЕ НА ИЗИСКВАНИЯТА В РАМКИТЕ НА ТЯХНАТА КОМПЕТЕНТНОСТ.

Допълнителни и заключителни разпоредби

1. ИК-530 v.03/26 Инструкция за обработване и защита на личните данни на физическите лица в „Пристанище Варна" ЕАД влиза в сила от 10.03.2026 г.
2. Настоящата Инструкция отменя ИК-530 v.02/23 от 10.05.2023 г.
3. Изпълнителния директор утвърждава следните образци от документи:

- Образец №1. Декларация за информираност и съгласие (когато е приложимо);
- Образец №2. Декларация за поверителност на служители;
- Образец №3. Заявление за упражняване на права по чл.15-22 от Регламент (ЕС) 2016/679
- Образец №4. Искане за коригиране на лични данни;
- Образец №5. Искане за ограничаване на обработването;
- Образец №6. Искане за изтриване („право да бъдеш забравен");
- Образец №7. Искане за преносимост на данни (когато е приложимо);
- Образец №8. Искане за възражение срещу обработването;
- Образец №9. Протокол за унищожаване на лични данни

(Образците са неразделна част от Инструкция ИК-530 v.03/26)

Изготвил:
Длъжностно лице по защита на личните данни

(Виктория Ивайлова).....

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

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №1 – ДЕКЛАРАЦИЯ ЗА ИНФОРМИРАНО СЪГЛАСИЕ

От: .....

ЕГН/ЛНЧ: .....

Адрес: .....

Декларирам, че съм запознат/а с информацията относно обработването на личните ми данни.

Давам своето свободно, конкретно, информирано и недвусмислено съгласие.

Съгласието може да бъде оттеглено по всяко време.

Дата: ..... **Декларатор:** .....

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №2 – ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ НА СЛУЖИТЕЛ

Име: .....

Длъжност: .....

Декларирам, че ще обработвам лични данни единствено в рамките на служебните си задължения.

Няма да предоставям лични данни на неоторизирани лица.

Запознат/а съм с отговорността по действащото законодателство.

Дата: ..... **Декларатор:** .....

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №3 – ЗАЯВЛЕНИЕ ЗА УПРАЖНЯВАНЕ НА ПРАВА

До: .....

От: .....

ЕГН/ЛНЧ: .....

Адрес за кореспонденция: .....

Телефон/Имейл: .....

Моля да упражня следното право (отбележете):

□ Право на достъп

□ Право на коригиране

□ Право на изтриване

□ Право на ограничаване

□ Право на възражение

□ Право на преносимост

Описание на искането:

.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №4 – ИСКАНЕ ЗА КОРИГИРАНЕ НА ЛИЧНИ ДАННИ

От: .....

ЕГН/ЛНЧ: .....

Описание на искането:

.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №5 – ИСКАНЕ ЗА ОГРАНИЧАВАНЕ НА ОБРАБОТВАНЕТО

От: .....

ЕГН/ЛНЧ: .....

Описание на искането:

.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №6 – ИСКАНЕ ЗА ИЗТРИВАНЕ НА ЛИЧНИ ДАННИ

От: .....

ЕГН/ЛНЧ: .....

Описание на искането:

.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №7 – ИСКАНЕ ЗА ПРЕНОСИМОСТ НА ДАННИ

От: .....

ЕГН/ЛНЧ: .....

Описание на искането:

.....
.....
.....
.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №8 – ИСКАНЕ ЗА ВЪЗРАЖЕНИЕ СРЕЩУ ОБРАБОТВАНЕ

От: .....

ЕГН/ЛНЧ: .....

Описание на искането:

.....
.....
.....
.....
.....

Дата: .....

Декларатор: .....

ИК-530 v.3/26

„ПРИСТАНИЩЕ ВАРНА" ЕАД

ОБРАЗЕЦ №9 – ПРОТОКОЛ ЗА УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Днес, ..., комисия в състав:

1. .....

2. .....

3. .....

Установи, че лични данни по съответния регистър са с изтекъл срок на съхранение.

Начин на унищожаване:

□ Шредиране

□ Софтуерно заличаване

□ Физическо унищожаване

Подписи:

.....

.....

.....