

„ЗММ СТОМАНА“ АД

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. /1/ Настоящите вътрешни правила за защита на личните данни, наричани по-нататък „**Правила/та**“, уреждат реда, по който „**ЗММ СТОМАНА**“ АД, ЕИК 118001790, седалище и адрес на управление: гр. Силистра, ул. „Гутракан“ № 16, тел. 086821058, www.stomana.net, info@stomana.net, наричано по-нататък „**Дружество/то**“ събира, записва, организира структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който стават достъпни, поддържа или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.

/2/ Дружеството обработва данни в качеството си администратор на лични данни.

/3/ Правилата са изготвени в съответствие с изискванията на Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г., наричан по-нататък Регламент/а и приложимото българско законодателство.

Чл.2. Обработването на лични данни е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, поддръждат или комбинирани, ограничаване, изтриване или унищожаване на данните.

Чл.3. Лични данни са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл.4. Личните данни се обработват при спазване на следните принципи:

- личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;
- личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели;
- личните данни трябва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;
- личните данни трябва да са точни и при необходимост да бъдат поддържани в актуален вид;
- личните данни се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни;
- личните данни се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

Чл.5. Обработването е законосъобразно, само ако и доколкото е извършено на поне едно от следните основание:

- субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

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

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

- обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

- обработването е необходимо за изпълнението на задача от обществен интерес;

- обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните.

Чл.6. При внедряване на нов програмен продукт за обработване на лични данни следва да се проверят възможностите на продукта с оглед осигуряване защита от неправомерен достъп, загубване, повреждане или унищожаване на лични данни.

Чл.7. За неизпълнение на задълженията, вменени на съответните служители във връзка с обработването и защитата на лични данни, последните носят дисциплинарна и имуществена отговорност по реда на трудовото и гражданското законодателство.

ЦЕЛИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл.8. Обработването на личните данни се извършва с **цел**:

- сключване, изпълнение и прекратяване на трудови и граждански договори, управление на човешките ресурси, изплащане на трудови възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на Дружеството в качеството му на работодател или възложител на работа;

- водене на финансово-счетоводната дейност на Дружеството;

- сключване, изпълнение и прекратяване на договори с клиенти на Дружеството;

- сключване, изпълнение и прекратяване на договори с доставчици на стоки и услуги;

- изпълнение на нормативно установени задължения;

- изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане;

- опазване имуществото на Дружеството и предотвратяване на кражби;

- защита на легитимни интереси на Дружеството;

- провеждане на заседания на Общото събрание и Съвета на директорите на Дружеството.

СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл.9. /1/ Дружеството събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, контрагент, лице, изпълняващо задълженията си към данъчни, осигурителни, митнически и други държавни органи и институции, като търговско дружество с органи на управление, като участник в досъдебни, съдебни, арбитражни и административни производства, при спазване на изискванията на Регламента и приложимото законодателство.

/2/ Личните данни, обработвани от Дружеството се отнасят до следните **СУБЕКТИ** на данни:

- работници и служители, кандидати за работа, страни по граждански правоотношения, включително по договори за управление;
- клиенти, доставчици на стоки и слуги, страни по търговски и граждански договори;
- участници в заседанията на органите на Дружеството, посетители и други лица;
- членове на Съвета на директорите;
- участници в досъдебни, съдебни, арбитражни и административни производства;

Чл.10. /1/ Поддържаните от Дружеството регистри с лични данни са:

1./ Регистър „Персонал“ - относно лицата, заети по трудови и граждански правоотношения, включително по договори за управление и на кандидатите за работа се обработват следните лични данни:

1.Физическа идентичност - име, презиме, фамилия, ЕГН, паспортни данни, дата и място на раждане, телефон, имейл адрес, пол /във връзка с декларациите за трудова злополука/, снимка /във връзка с издаване на служебен пропуск и представяне на дипломи и свидетелства/.

2.Образование и професионална квалификация - данни, свързани с образование, трудов опит, професионална и лична квалификация и умения.

3.Трудова и икономическа дейност – месторабота, длъжност, трудово възнаграждение, банкова сметка, общ трудов стаж и трудов стаж при конкретни условия на труд, категория труд, месечна зарплата, присъствия и отсъствия през календарен месец, автобиографична справка.

4.Медицински данни – данни, свързани със здравословното състояние, съдържащи се в документ за медицински преглед /при първоначално постъпване на работа и след преустановяване на трудовата дейност повече от 3 месеца/, болнични листове, работоспособност /решения на ТЕЛК, НЕЛК/, други медицински документи, когато това е предвидено в нормативен акт.

5.Брой на деца до 18 години /във връзка с изплащане на детски надбавки/.

6.Свидетелство за съдимост – когато за заемане на определена длъжност се изисква представянето му съгласно нормативен акт;

7.Възраст и пол – с оглед изискването на чл. 19, ал. 2 от Наредба № 23.02.1987 г. за задължителните предварителни и периодични медицински прегледи.

8.Номер на карта за достъп.

9.Други данни – когато се изискват от нормативен акт или обработването им е необходимо за изпълнение на правата и задълженията на Дружеството като работодател.

2./ Регистър „Контрагенти“ - относно клиенти, доставчици и страни по търговски и граждански договори – физически лица и представители на клиенти, доставчици и страни по търговски и граждански договори – юридически лица се обработват следните лични данни:

-име, презиме, фамилия, ЕГН, паспортни данни, адрес, длъжност, постоянен и настоящ адрес, телефон, имейл адрес;

-други данни – когато се изискват от нормативен акт или обработването им е необходимо за изпълнение на правата и задълженията на Дружеството.

3./ Регистър „Счетоводство“ - относно посочените във фактурите и другите счетоводни документи лица се събират следните лични данни:

-име, презиме, фамилия; ЕГН; длъжност; паспортни данни; адрес; телефон;

-други данни – когато се изискват от нормативен акт или обработването им е необходимо за изпълнение на правата и задълженията на Дружеството.

4./ Регистър „Участници в заседания“ - относно участници в заседания на СД и ОС на Дружеството и посетители се обработват следните лични данни:

- име, презиме, фамилия, ЕГН, адрес, паспортни данни, длъжност;
- други данни – когато се изискват от нормативен акт или обработването им е необходимо за изпълнение на правата и задълженията на Дружеството.

5./ Регистър „Защита на имущество“ - относно лица, преминаващи през входно-изходния пропускателен пункт и лица, намиращи се в определени участъци от територията му се обработват следните лични данни:

- видеообрази.

6./ Регистър „Производства“ - относно страните по досъдебни, съдебни, арбитражни и административни производства се обработват следните лични данни:

- име, презиме, фамилия, ЕГН, паспортни данни, постоянен и настоящ адрес телефон, длъжност;
- други данни, ако са необходими за целите на съответното производство.

/2/ За обработване на данните от регистрите по предходната алинея Дружеството

води Регистър на дейностите по обработване съгласно чл. 15 от тези правила.

Чл.11. Дружеството обработва чувствителни данни, доколкото това е необходимо за изпълнение на правата и задълженията му в областта на трудовото и осигурителното законодателство.

Чл.12. Клиентите, физически лица и физическите лица, представители на юридическите лица, работниците и служителите на Дружеството, кандидатите за работа и посетителите се идентифицират посредством официален документ за самоличност (лична карта, паспорт).

СЪГЛАСИЕ

Чл.13. /1/ В случаите, когато единственото основание за обработване на лични данни е съгласието на субекта на данни, то се счита, че последният е съгласен, ако е изразил това ясно и недвусмислено – чрез изявление или друг потвърждаващ акт. Ако съгласието за обработване на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по другите въпроси.

/2/ Субектите на данни могат да оттеглят съгласието си за обработване по всяко време, като оттеглянето следва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то трябва да се прекрати.

Чл.14. Декларациите за съгласие се съхраняват от Дружеството, докато се извършват действие по обработване на това основание и в определен срок след прекратяване на обработването, с оглед доказване спазването на принципа на отчетност, но не по-рано от изтичане на давностните срокове, в които се погасяват всички възможни претенции срещу Дружеството, които могат да възникнат във връзка с обработването на лични данни.

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕТО

Чл.15. /1/ Дружеството създава и поддържа Регистър на дейностите по обработването.

/2/ Регистърът на дейностите по обработването се поддържа в писмена форма, включително в електронен формат.

/3/ Регистърът съдържа задължително следната информация:

- името и координатите за връзка са администратора и на лицето, отговорно за личните данни;
- целите на обработването;
- категиорите на лични данни и категиорите субекти на данни;
- категиорите получатели, пред които са или ще бъдат разкрити личните данни, включително получатели в трети държави;
- предаването на лични данни на трети държави;
- когато е възможно, предвидените срокове да изтриване на различните категиории лични данни;
- когато е възможно, общо описание на техническите и организационни мерки за сигурност.

/4/ Дружеството може да включи в регистъра за дейностите и друга информация, като основание за обработване, местоположение на лични данни и др.

/5/ За постигането на по-голяма яснота и логическа последователност на Регистър на дейностите по обработването, последният може да се обособи в отделни подрегистри, като към датата на приемане на тези правила се поддържат подрегистри „Персонал“, „Контрагенти“, „Имущество“, „Дружествени органи“ и „Участия в програми и проекти“.

/6/ Регистрите се съхраняват в срок от 10 /десет/ години, считано от 1 януари на годината, следваща годината, в която е прекратена съответната дейност по обработване, респ. до изтичане на давностния срок, в който се погасяват всички възможни претенции срещу Дружеството, свързани с обработване и защита на личните данни, ако този срок изтича по-късно.

ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедури за обработване на личните данни, отнасящи се до лицата, заети по трудови и граждански договори, включително договори за управление и кандидатите за работа.

Чл.16. Личните данни, отнасящи се до лицата, заети по трудови и граждански договори, включително договори за управление, както и на кандидатите за работа **се събират:**

1. При постъпване/възлагане на работа по трудово или гражданско правоотношение, в изпълнение на нормативно задължение, регламентирано в Кодекса на труда, Кодекса за социално осигуряване, Търговския закон, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за държавния архив, Наредба № 4 от 11.05.1993 г. за документите, които са необходими за сключване на трудов договор, Наредба № РД-07-2/16.12.2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд, Наредба № 3/28.02.1987 г. за задължителните предварителни и периодични медицински прегледи на работниците, Наредба № Н-8/2005 г. и всички други нормативни актове, свързани с възникването, изпълнението и прекратяването на трудови и граждански правоотношения, по следните начини:

- устно интервю с лицето (при постъпване или в процеса на работа);
- на хартиен носител - чрез подаване на заявления за постъпване на работа, мотивационни писма, автобиографии и препоръки; насочващи писма Агенция по заетостта, чрез подаване на молби, сигнали, искания, възражения и жалби, свързани с

изпълнението, изменението и прекратяването на трудовите или граждански правоотношения;

-на електронен носител – чрез изпращане по имейл на молби, мотивационни писма, автобиографии, препоръки.

2.От външни източници - съдебни, финансови, осигурителни, данъчни и други институции, в изпълнение на нормативни изисквания.

3.При влизане на територията на Дружеството:

-чрез записване от дежурния портиер на имена и длъжност на работещите първа, втора и нощна смяна в тетрадка, съхранявана в портиерната;

-чрез записване на имена и длъжност на полагащите извънреден труд в списък, изготвян от отдел „Човешки ресурси“;

–чрез записване на номера на картата за достъп на съответния работник и служител.

Чл.17. Обработването на лични данни, отнасящи се за лица, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа е допустимо когато е необходимо за изпълнение на нормативно установени задължения, или е необходимо за изпълнение на задължения по договор, по който лицето, за което се отнасят данните е страна или за действия, предхождащи сключването на договор и предприети по искане на лицето, или когато лицето, за което се отнасят данните е дало изрично своето съгласие, или за целите на легитимните интереси на администратора.

Чл.18. При необходимост от поправка на личните данни, лицата предоставят такива на служителя, обработващ лични данни по негово искане или на основание нормативно задължение.

Чл.19. Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа се обработват с **ЦЕЛ:**

1.Индивидуализиране и администриране на трудовите и граждански правоотношения.

2.Управление на персонала.

3.Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за държавния архив, Наредба № 4 от 11.05.1993 г. за документите, които са необходими за сключване на трудов договор, Наредба № РД-07-2/16.12.2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд, Наредба № 3/28.02.1987 г. за задължителните предварителни и периодични медицински прегледи на работниците и всички други нормативни актове, свързани с възникването, изпълнението и прекратяването на трудови и граждански правоотношения.

4.Използване на събраните данни за съответните лица за служебни цели.

5.Използване на събраните данни за изготвяне на всякакви документи на лицата (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни) във връзка с възникването, изпълнението и прекратяването на трудови и граждански правоотношения, придобиване на пенсии, ползване на отпуски, изплащане на обезщетения, упражняването на други техни права.

6.Установяване на връзка с лицето посредством адрес, телефон, имейл адрес с цел предоставяне на информация, отнасяща се до изпълнение на задълженията му и упражняване на правата му по трудови или граждански договори.

7.Изготвяне на документи във връзка с изплащането на възнаграждения.

8.Упражняване на права и задължения по сключени трудови и граждански договори.

9.Водене на счетоводната отчетност на Дружеството.

10.Регистриране на влизанията и излизанията на територията на Дружеството.

Чл.20. Личните данни се събират на хартиени носители от служителите от отдел „Човешки ресурси“, „Счетоводство“, „Охрана на труда“, служители, провеждащи инструктажи и служителите, водещи присъствени книги, портиери. Записите от номерата на картите за достъп се събират на твърди дискове съгласно чл. 21, ал. 7 от тези правила.

Чл.21. /1/ Хартиените носители на лични данни се **СЪХРАНЯВАТ** в папки /трудова досиета/ за всеки служител, страна по трудов договор, папки с болнични листове, папки с потвърждения, че уведомленията по чл. 62, ал. 4 от КТ са изпратени до НАП, папки с потвърждения, че електронните уведомления със съдържанието от болничните листове са изпратени до НОИ, папки с граждански договори, папки за кандидати за работа, в тетрадки за проведени инструктажи, в присъствени книги, в тетрадки за работещите първа, втора и нощна смяна.

/2/ Трудовите досиета на служители по действащи трудови договори, папките с граждански договори и папките с кандидати за работа се подреждат в картотечни шкафове в стаята на отдел „Човешки ресурси“.

/3/ Трудовите досиета на служители, с които трудовите или гражданските договори са прекратени се подреждат в картотечни шкафове в стаята на отдел „Човешки ресурси“ и на стелажи в стая, предназначена за архивирани документи на отдел „Човешки ресурси“. В последната се съхраняват и ведомостите за заплати за периода от 1982 г. до 1997 г.

/4/ Ведомостите за заплати за периодите от 1967 г. до 1982 г. и от 1997 г. насам се съхраняват във втора стая, предназначена за архивирани документи на отдел „Човешки ресурси“.

/5/ Тетрадките за инструктаж и присъствените книги се съхраняват в стаите на съответните служители, които ги водят.

/6/ Актове за брак по вина на изпълнител се съхраняват в стаята на отдел „Охрана на труда“.

/7/ Записите с номерата на картите за достъп до територията на Дружеството се съхраняват на твърдите дискове на персоналния компютър на мениджъра, намиращ се в стаята на „Търговския отдел“ и на персоналния компютър на служителя от отдел „Човешки ресурси“, намиращ се в стаята на отдела.

Чл.22. /1/ Лицата, оправомощени да обработва лични данни, предприемат необходимите организационно-технически мерки за съхраняването и опазването на личните досиета и класъори с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

/2/ Досиета на служителите и данните на кандидатите за работа, не се изнасят извън сградата на Дружеството.

Чл.23. Техническата ЗАЩИТА на данните, отнасящи се до служители и кандидати за работа се осъществява посредством следните мерки:

-определяне на самостоятелни помещения, в които служителите от отдел „Човешки ресурси“ обработват данни и в които са разположени компютрите за обработване на данните и се съхраняват хартиените носители;

-определяне на самостоятелни помещения, в които служителите от отдел „Охрана на труда“, служители, провеждащи инструктажи и служителите, водещи присъствени книги обработват данни и в които помещения са разположени компютрите за обработване на данните и се съхраняват хартиените носители;

-заклучване на помещенията;

-предоставяне на достъп на работници и служители на Дружеството до стаята, в която работят служителите от отдел „Човешки ресурси“ само през работно време, в присъствието на служител от отдела и единствено с цел подаване и/или получаване на болнични листове, молби, заповеди, удостоверения, справки и други подобни документи;

-предоставяне на достъп на външни лица до стаята, в която работят служителите от отдел „Човешки ресурси“ само през работно време, след допускането им от дежурния портиер, в присъствието на служител от отдела и единствено с цел подписване или получаване на подписани договори и други документи, свързани с тях, подаване и/или получаване на автобиографии, болнични листове, молби, заповеди, удостоверения, справки и други подобни документи;

-инсталиране на сигнално-охранителна система в стаята на отдел „Човешки ресурси“ и в стаята за архив, в която се съхраняват документи и ведомостите за заплати за периодите от 1967 г. до 1982 г. и след 1997 г.;

-заклучване на помещенията, в които се съхраняват архивираните трудови досиета, ведомостите за заплати за период 1982 г. до 1997 г., книгите за инструктаж, присъствените книги, актовете за брак;

-обезопасяване на помещенията посредством противопожарни мерки;

-денонощна техническа охрана от СОТ;

-видео-наблюдение на територията на Дружеството и в коридора, в който са разположени стаите на администрацията;

-съхраняване на документите в шкафови и лавици;

-разполагане на шкафове по начин, позволяващ непосредствен, постоянен и пълен контрол върху тях от страна на служителите на отдела.

Чл.24. /1/ При обработване личните данни се въвеждат на твърд диск, на изолиран компютър.

/2/ Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само за обработващите лични данни. При работа с данните се използват специализирани софтуерни продукти по обработка на данните, относно възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други задължения (вноски по заеми, запори и пр.), трудов стаж, присъствени и неприсъствени дни и други подобни. Софтуерните продукти са адаптирани към специфичните нужди на администратора и са съобразени с нормативните изисквания.

/3/ Компютърът се намира в помещението на отдел „Човешки ресурси“.

/4/ Достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващия лични данни чрез парола за отваряне на тези файлове. Защитата на електронните данни от неправилен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, чрез периодично архивиране на данните на твърд диск, на отделен компютър, намиращ се в същата стая и отговарящ на посочените в предходните алинеи условия и изисквания, както и чрез поддържане на информация на хартиен носител в законоустановените срокове.

Чл.25. /1/ Право на **ДОСТЪП** до данните имат:

1.Лицата, за които се отнасят данните - по тяхно писмено искане.

2.Служителите от отдел „Човешки ресурси“.

3.Служителите от отдел „Охрана на труда“ – до документи, свързани с периодичните медицински прегледи и инструктажи.

4.Служителите, провеждащи инструктаж – до тетрадките с инструктажи.

5.Служителите от отдел „Човешки ресурси“ и служителите, отчитачи присъствия и отсъствия – до присъствените книги.

6.Портиерите – до тетрадките за работещите първа, втора и нощна смяна.

7.Други служители на Дружеството, ангажирани с оформянето, подписването или контрола върху законосъобразността на документите относно работниците и служителите – изпълнителен директор, заместник директор, главен счетоводител, мениджър, лицата, осъществяващи технически счетоводни операции по обработка на документите, лицата, осъществяващи правното обслужване на Дружеството.

8.Системният администратор и лица, обслужващите специализираните програмни продукти при сринове, повреди, профилактика

9. Държавни институции – съд, прокуратура, разследващи органи, контролно-ревизиращи органи /НАП, НОИ, ИА „ГИТ“ и др./ В тези случаи се представят копия от намиращите се в съответното досие документи, без да се изнасят оригинали, освен в предвидените в закона случаи.

10. Банки - във връзка с изплащане трудовите възнаграждения

11. Застрахователи - във връзка със сключване и изпълнение на договори за застраховки.

/2/ Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

Чл.26. /1/ Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството и на кандидатите за работа се съхраняват в **СРОКОВЕТЕ**, определени за съхраняването на документите, в които съответните данни са обективирани:

-ведомости за заплати - 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят /чл. 12, ал. 1, т. 1 от Закона за счетоводство и чл. 38, ал. 1, т. 1 от ДОПК/;

-неполучени от работниците или служителите трудови книжки, дневниците за издаване на трудови книжки и екземпляр от издадените удостоверения за трудов стаж – 50 години /чл. 8, ал. 1 от Наредба за трудовата книжка и трудовия стаж/;

-трудова договор, допълнителните споразумения към тях, заповеди за ползван неплатен отпуск над 30 работни дни, заповеди за изменение и прекратяване на трудово правоотношение – 10 години, считано от 1 януари на годината, следваща годината на прекратяването на трудовия договор;

-документи, необходими за сключване на трудов договор съгласно Наредба № 4 от 11.05.1993 г./ документи за придобито образование, специалност, квалификация, стаж по специалността, медицински преглед, свидетелство за съдимост, разрешение от инспекция по труда/, уведомления до НАП по чл. 62, ал 5 от КТ, длъжностни характеристики, решения на ТЕЛК и производствени характеристики до ТЕЛК, заповеди за налагане на дисциплинарни наказания и приложените към тях документи - 10 години, считано от 1 януари на годината, следваща годината на прекратяването на трудовия договор /с оглед възможните проверки на контролните органи за спазване на трудовото законодателство/;

-документи, отнасящи се до провеждане на обучение и инструктаж - не по-малко от 5 години /чл. 9, ал. 2 от наредба № РД-07-2/16.12.2009 г./;

-болнични листове – 5 години, считано от 1 януари на годината, следваща годината на представянето им /чл. 6, ал. 2 от Наредба за паричните обезщетения и помощи от ДОО/;

-потвърждения, че уведомленията по чл. 62, ал. 4 от КТ са изпратени до НАП и потвърждения, че електронните уведомления със съдържанието от болничните листове са изпратени до НОИ - 10 години, считано от 1 януари на годината, следваща годината, в която е направено съответното потвърждение /с оглед проверки на контролните органи за спазване на трудовото законодателство/;

-тетрадките за работещите първа, втора и нощна смяна се съхраняват през текущата и предходната година;

-документи за данъчно-осигурителен контрол, различни от горепосочените – 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани /чл. 38, ал. 1, т. 3 от ДОПК/;

-молби за кандидатстване за работа, автобиографии и препоръки на неприети кандидати – в срока, необходим за осъществяване на конкретната цел, която администраторът иска да постигне със събирането им, но не повече от 3 месеца от предоставянето им;

-документите, свързани със сключването и изпълнението на граждански договори за възлагане на работа – 5 години от прекратяване на гражданския договор,

освен ако приложим закон или приложим давностен срок по евентуална претенция срещу Дружеството, изискват друго;

-изявления, свързани с даване на съгласия, деклариране на факти и обстоятелства, поемане на задължения; декларации във връзка със защитата на лични данни - 10 години, считано от 1 януари на годината, следваща годината на прекратяването на трудовия договор /чл. 38, ал. 1, т. 3 от ДОПК с оглед възможните проверки на контролните органи за спазване на трудовото законодателство/, освен ако приложим закон или приложим давностен срок по евентуална претенция срещу Дружеството, изискват друго;

-други документи, от значение за данъчното облагане и задължителните осигурителни вноски – 5 години /чл. 38, ал. 1, т. 4 от ДОПК/;

-всички останали документи - в срока, необходим за осъществяване на конкретната цел, която администраторът иска да постигне със събирането им.

/2/ В случай на трудова злополука или професионално заболяване личните данни се съхраняват до изтичане на срока, в който се погасяват всички възможни имуществени и неимуществени претенции срещу Дружеството, произтичащи от съответната трудова злополука или професионално заболяване, когато този срок изтича след изтичането на съответния срок, посочен в предходната алинея.

/3/ При наличие на административен или съдебен спор относно възникването, изменението, прекратяването или изпълнението на трудови правоотношения и свързаните с тях възнаграждения и обезщетения, или при проверка от контролните органи във връзка със свързаните с трудовите правоотношения задължения за плащане на осигуровки, данъци и други публични задължения, личните данни се съхраняват до приключване на административния или съдебния спор с влязъл в сила акт, когато това настъпва след изтичане на съответния срок, посочен в предходните алинеи.

/4/ При използване на информационни системи, продукти или архиви, създадените данни в електронен вид се съхраняват съответно в сроковете по предходните алинеи.

Процедури за обработване на личните данни, отнасящи се до клиенти, доставчици, наематели, изпълнители, ползватели и лицата, посочени във фактурите и другите счетоводни документи.

Чл.27. /1/ Личните данни, отнасящи се до клиенти, доставчици, наематели, изпълнители и други ползватели се събират при сключване на договори за покупко-продажба на стоки и за предоставяне на услуги, договори за наем или заем за послужване, договори за ремонт, строителство, изработка, като и други търговски и граждански договори в изпълнение на нормативно задължение /Търговски закон, Закон за задълженията и договорите, Закон за данък върху добавената стойност, Закон за счетоводството, Закон за данъците върху доходите на физическите лица, Закон за корпоративното подоходно облагане и др./, при подаване и приемане на оферти, предложения и поръчки, при попълване на митнически документи и товарителници, при изнасяне и внасяне на стоки от и на територията на Дружеството, при изпращане и получаване на стоки в страната и чужбина, при извършване на превози, ремонти и други дейности, свързани с осъществяването от Дружеството търговска дейност, по следните начини:

-на хартиен носител – предложения за сключване на договори и анекси, приемане на предложения за сключване на договори и анекси, сключване на договори и анекси, изготвяне на митнически документи, товарителници, пътни листове, кореспонденция между контрагенти, рекламации, изпращане и получаване на документи и изявления;

-на електронен носител – изпращане по имейл на предложения за сключване на договори и анекси, на приемане на предложения за сключване на договори и анекси, на кореспонденция между контрагенти, рекламации и други документи и изявления;

-чрез записване на имена от дежурния портиер в специална тетрадка, в която се описват данни за фактури за стоки, които се внасят на или изнасят от територията на Дружеството.

/2/ Обработването на лични данни, отнасящи се до клиенти и доставчици е допустимо когато е необходимо за изпълнение на нормативно установени задължения, или е необходимо за изпълнение на задължения по договор, по който лицето, за което се отнасят данните е страна или за действия, предхождащи сключването на договор и предприети по искане на лицето, или когато лицето, за което се отнасят данните е дало изрично своето съгласие, или за целите на легитимните интереси на администратора.

Чл.28. Личните данни, отнасящи се до клиенти и доставчици се обработват с цел:

1.Индивидуализиране на търговски и граждански правоотношения.

2.Изпълнение на нормативните изисквания на Закон за митниците, Търговския закон, Закона за задълженията и договорите, Закона за данък върху добавената стойност, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за корпоративното подоходно облагане и други вътрешни и международни актове, които са свързани с възникването, изпълнението и прекратяването на търговски, граждански и данъчни правоотношения.

3.Използване на събраните данни за служебни цели.

4.Изготвяне на всякакви документи във връзка с възникването, изпълнението и прекратяването на търговски и граждански правоотношения.

5.Установяване на връзка с лицето посредством адрес, телефон, имейл, за изпращане на информация, отнасяща се до изпълнение на задължения по търговски и граждански договори.

6.Водене на счетоводната отчетност на Дружеството.

Чл.29. /1/ Личните данни, отнасящи се до клиенти, доставчици, наематели и други ползватели се съхраняват на електронни и хартиени носители.

/2/ Хартиените носители на лични данни се съхраняват в папки по клиенти, доставчици, наематели и други ползватели, папки с митнически документи, пътни листове, кочани с фактури, тетрадки с опис на фактури. Горепосочените документи и фактурите се подреждат в шкафове, разположени в стаите на отдели „Търговски“, „МТС“, „Счетоводство“, стаята за архив и портиерната.

/3/ Електронните данни се съхраняват в бази данни.

Чл.30. Лицата, оправомощени да обработва лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на фактури, договори, товарителници, митнически и други документи, съдържащи лични данни относно клиенти и доставчици на Дружеството, в това число ограничаване на достъпа до тях на външни лица и неотторизирани служители.

Чл.31. Техническата защита на данните, отнасящи се до клиенти и доставчици се осъществява посредством следните мерки:

-определяне на самостоятелни помещения, в които служителите от отдели „Търговски“, „МТС“, „Счетоводство“ и портиерна обработват и съхраняват данни и в които помещения са разположени компютрите за обработване на данните и хартиените носители;

-заклучване на помещенията;

-предоставяне на достъп до помещенията, в които работят служителите от горепосочените отдели само през работно време, в присъствието на служител от отдела и единствено с цел подаване и/или получаване на заявки, фактури, товарителници, митнически и други документи;

-предоставяне на достъп на външни лица до помещението, в което работят служителите от горепосочените отдели само през работно време, след допускането им от охраната, в присъствието на служител от отдела и единствено с цел подаване и/или получаване заявки, фактури, товарителници, митнически и други документи;

-инсталиране на сигнално-охранителна система в стаите, в които се съхраняват договори и счетоводни документи за минали периоди;

-обезопасяване на помещенията посредством противопожарни мерки;

-денонощна техническа охрана от СОТ;

-видео-наблюдение на територията на Дружеството и в коридора, в който се намират горепосочените помещения;

-съхраняване на документите в шкафови и лавици;

-разполагане на шкафове по начин, позволяващ непосредствен, постоянен и пълен контрол върху тях от страна на служителите на съответния отдел.

Чл.32. /1/ При обработване на технически носител личните данни се въвеждат на твърд диск, на изолиран компютър.

/2/ Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само за обработващите лични данни. При работа с данните се използват специализирани софтуерни продукти по обработка на данните. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни и са съобразени с изискванията на Регламента и другите нормативни актове във връзка със защитата на личните данни.

/3/ Компютрите се намират в стаите на съответния отдел.

/4/ Достъп до операционната система, съдържаща файлове за обработка на лични данни, имат обработващите лични данни чрез парола за отваряне на тези файлове. Защитата на електронните данни от неправилен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, чрез периодично архивиране на данните на твърд диск, на отделен компютър, който отговаря на посочените в предходните алинеи условия и изисквания, както и чрез поддържане на информация на хартиен носител в законоустановените срокове.

Чл.33. Право на достъп до данните имат:

1. Лицата, за които се отнасят данните, по тяхно писмено искане.

2. Служителите от отдели „Търговски“, „МТС“, „Счетоводство“, които обработват лични данни.

3. Портиерите – фактури, тетрадките с опис на фактури, пратки, товарителници и други документи, съпътстващи товарите.

4. Служители на Дружеството, ангажирани с оформянето, подписването или контрола върху законосъобразността на документите – изпълнителен директор, заместник директор, главен счетоводител, мениджър, лицата, осъществяващи технически счетоводни операции по обработка на документите, лицата, осъществяващи правното обслужване на Дружеството.

5. Системния администратор и лица, обслужващите специализираните програмни продукти при сридове, повреди, профилактика

6. Държавни институции, с оглед изпълнение на нормативни задължения – съд, прокуратура, разследващи органи, контролно-ревизиращи органи /Агенция „Митници“, НОИ, НАП и др./. В тези случаи се представят копия от намиращите се в съответното досие документи, без да се изнасят оригинали.

Чл.34. Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

Чл.35. /1/ Личните данни, отнасящи се до клиенти, доставчици, наематели, изпълнители и други ползватели се съхраняват в **СРОКОВЕТЕ**, определени за съхраняването на документите, в които съответните данни са обективирани:

-договори, анекси към тях, документи и изявления, свързани с преддоговорни отношения и изпълнение по договори и други документи, съдържащи търговска

информация – 5 години от прекратяването на договора, или от съставянето на документа, или от извършването на изявлението, или от последното действие по изпълнението на договор, което от тези събития настъпи най-късно /чл. 38, ал. 1, т. 4 от ДОПК/;

-фактури и други документи и сведения, от значение за данъчно облагане и задължителни осигурителни вноски – 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани /чл. 38, ал. 1, т. 3 от ДОПК/, освен ако приложим закон или приложим давностен срок по евентуална претенция срещу Дружеството, изискват друго;

-служебна кореспонденция, извън горепосочените случаи – до изпълнение на целите, за която е създадена;

-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 /чл. 12, ал. 1, т. 2 от Закона за счетоводство/;

-всички останали носители на счетоводна информация – 3 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят /чл. 12, ал. 1, т. 3 от Закона за счетоводство/;

--извадки от сайта на НАП – „Електронни данни от получателя“ във връзка с подадени справки за закупено гориво – до 6 месеца, други документи - в срока, необходим за осъществяване на конкретната цел, която администраторът иска да постигне със събирането им.

-тетрадки с опис на фактури – до приключването на съответната тетрадка.

/2/ При наличие на административен или съдебен спор относно публични и частни задължения, изпълнения на договори, рекламации и др. подобни, личните данни се съхраняват до приключване на административния или съдебния спор с влязъл в сила акт, когато това настъпва след изтичане на съответния срок, посочен в предходната алинея.

/3/ При използване на информационни системи, продукти или архиви, създадените данни в електронен вид се съхраняват съответно в сроковете по предходните алинеи.

Процедури за обработване на лични данни, отнасящи се за участници в заседания на органите на Дружеството.

Чл.36. /1/ Личните данни, отнасящи се до участници в заседания на Съвета на директорите /СД/ и Общото събрание /ОС/ на Дружеството се събират по повод провеждане на съответното заседание.

/2/ Данните за участниците в заседанията на ОС и СД на Дружеството се обработват с цел:

1.Идентифициране на участници в заседанията.

2.Изпълнение на нормативните изисквания на Търговския закон.

/3/ Личните данни на участниците в заседанията се обработват в изпълнение на нормативни изисквания /Търговския закон, Закон за търговския регистър/ или въз основа на изрично съгласие.

/4/ Личните данни на участници в заседанията на ОС и СД на Дружеството се съхраняват на хартиени носители, подредени в папки. Папките се съхраняват в шкафове, намиращи се стаята на служителите от търговския отдел и в кабинета на изпълнителния директор.

/5/ Личните данни на участници в заседанията на ОС и СД на Дружеството се предоставят в Търговския регистър към АВ чрез електронен подпис като за целта се сканират оригиналите на приложените към заявленията документи.

/6/ Личните данни на участници в заседанията на ОС и СД на Дружеството се съхраняват в **СРОКОВЕТЕ**, определени за съхраняването на документите, в които съответните данни са обективирани, респ. сроковете, необходими за осъществяване на конкретната цел, която администраторът иска да постигне със събирането им, но не по-малко от 5 години /чл. 232, ал. 5 от Търговския регистър/.

/7/ При наличие на спор относно законосъобразността на взетите от органите на Дружеството решения на проведените заседания, личните данни се съхраняват до приключване на с влязъл в сила акт, когато това настъпва след изтичане на съответния срок, посочен в предходната алинея.

/8/ При използване на информационни системи, продукти или архиви, създадените данни в електронен вид се съхраняват съответно в сроковете по предходните алинеи.

Процедури за обработване на личните данни от видео-наблюдение.

Чл.37. /1/ На определени участъци от територията и сградите на Дружеството – входно-изходен пропускателен пункт, коридор на втория етаж на административната сграда, халета, в които се съхраняват машини, оборудване, части, материали и други активи се осъществява денонощно видео-наблюдение.

/2/ Данните се предоставят доброволно от лицата при влизането им на територията на Дружеството. На главния вход са поставени предупредителни табели, че обектът се намира под постоянно видео-наблюдение.

Чл.38. /1/ Данните от видео-наблюдението се обработват с цел:

-опазване на имуществото на Дружеството от посегателства и кражби от външни лица;

-защита на личните данни, съхранявани в помещенията, находящи се в административната сграда;

-спазване на нормативни изисквания – Закон за управление на отпадъците.

/2/ Данните от видео-наблюдението не се обработват по начин, несъвместим с горепосочените цели и същите не се използват за наблюдение, мониторинг или контрол на субектите на данни.

/3/ Дружеството не осъществява видео-наблюдение в санитарно – хигиенните помещения /бани, тоалетни/, в стаите за отдих и преобличане, в стаите на администрацията.

/4/ Дружеството не осъществява видео-наблюдение с цел контрол на трудовата дисциплина, спазване на работно време, изпълнението на други трудови задължения и не използва данните за целите на дисциплинарни производства и производства за търсене на имуществена отговорност от работници и служители.

Чл.39. /1/ Видеозаписите се съхраняват на видеорекордер, монтиран в портиерната.

/2/ Видеозаписите се съхраняват в **срок** от 30 дни, след което се унищожават автоматично от твърдия диск на видеорекордера, като върху най-стария запис се записва новата информация.

/3/ При поискване на записи за определен период от страна на органите на МВР, съд, прокуратура, разследващи органи, Министерство на околната среда и водите и други компетентни държавни органи същите се предоставят на диск, флаш-памет или друг носител и се съхраняват съгласно указания от съответния компетентен орган срок.

Чл.40. /1/ Право на достъп до записите имат:

1.Лицата, за които се отнасят данните, по тяхно писмено искане направено в срока, в който данните са налични.

2.Мениджърът.

3. Лица, обслужващи специализираната видеотехника - при сринове, повреди, профилактика в присъствието на маркетинг мениджъра или изпълнителния директор.

4. Държавни институции, с оглед изпълнение на нормативни задължения – съд, прокуратура, разследващи органи, органи на МВР, контролно-ревизиращи органи /Министерство на околната среда и водите, НАП/.

/2/ Изпълнителният директор и други служители на Дружеството нямат свободен достъп до данните с оглед изискванията на чл. 38, ал. 2 и 4 от тези правила.

Чл.41. /1/ Физическата защита на личните данни се осъществява денонощно от дежурните портieri и от техническа охрана от СОТ.

Процедури за обработване на личните данни при досъдебни, съдебни, арбитражни и административни производства.

Чл.42. /1/ При възникване и водене на досъдебни, съдебни, арбитражни и административни производства документите, съдържащи лични данни се събират в отделни папки, които се съхраняват от упълномощения по конкретното производство адвокат.

/2/ Упълномощеният по случая адвокат съхранява книгата по съответното дело в **срок** от 5 години от приключването му /чл. 47, ал. 1 от Закона за адвокатурата.

ОБЩИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИ МЕРКИ ЗА ЗАЩИТА

Чл.43. /1/ **Техническата защита** на обработваните данни е организирана като елемент от общата физическа защита на територията на Дружеството и се осъществява посредством система от технически и организационни мерки, насочени към предотвратяване на нерегламентиран достъп до сгради и помещения, в които се обработват лични данни.

/2/ Конкретните мерки на техническа защита са посочени в настоящите правила при отделните процедури за обработване на данни.

Чл.44. **Персоналната защита** на обработваните данни се осъществява чрез:

-запознаване на служителите от съответните отдели с Регламента и другата нормативна уредба в областта на защитата на личните данни;

-запознаване на служителите от съответните отдели с политиката на Дружеството за защита на личните данни;

-запознаване на служителите от съответните отдели с опасностите за личните данни, обработвани от Дружеството, в качеството му на администратор на лични данни;

-даване на съгласие за поемане на задължение за неразпространяване на лични данни;

-обучение за реакция при събития, застрашаващи сигурността на данните.

Чл.45. /1/ **Документалната защита** се осъществява чрез установяване на процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение.

/2/ Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва от упълномощени служители при възникнала необходимост.

Чл.46. **Защита на автоматизирани информационни системи и криптографска защита** се осъществяват посредством:

-достъпът до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп. Достъпът се осъществява чрез парола;

-електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени и др.;

-архивиране на лични данни на технически носители се извършва периодично с оглед съхранение на информация;

-използване на електронен подпис;

-криптографски методи и средства за защита при пренасяне на информация, надеждна и защитена идентификация и автентификация на изпращача и на получателя на информация, осигуряване на конфиденциалност и интегритет на пренасяната информация.

Чл.47. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия и др., се осигурява посредством:

-въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни и файловете, които съдържат лични данни;

-антивирусни програми, проверки за нелегално инсталиран софтуер;

-периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител /архивни копия.

-периодични уведомяване на ръководството на Дружеството за предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

Чл.48. Архивиране на личните данни на технически носител се извършва с оглед запазване на информацията за съответните лица в актуален вид.

ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл.49. /1/ Дружеството документира дейностите по обработване на лични данни при спазване на принципа на отчетност.

/2/ Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

/3/ Обработването на данни, свързано с предаване на данни на трети лица, установени в страната или чужбина, съхранение на данни на сървъри, собственост на трети лица, въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:

-целите на обработването;

-категориите на лични данни и категориите субекти на данни;

-категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получатели в трети държави;

-предаването на лични данни на трети държави;

-когато е възможно, предвидените срокове да изтриване на различните категории

лични данни;

- когато е възможно, общо описание на техническите и организационни мерки за сигурност.

/4/ Протоколите се изготвят от служителите, които извършват съответната обработка на данни по указание на лицето, отговорно за личните данни.

/5/ Протоколите, съдържащи горепосочената информация са част от регистъра на дейностите по обработването.

/6/ Протоколите се съхраняват в срок от 10 /десет/ години, считано от 1 януари на годината, следваща годината, в която са съставени, респ. до изтичане на давностния срок, в който се погасяват всички възможни претенции срещу Дружеството, свързани с обработване и защита на личните данни, ако този срок изтича по-късно.

НАРУШЕНИЯ НА СИГУРНОСТТА

Чл.50. /1/ Лицата, идентифицирали признаци на нарушение на сигурността на данните са длъжни да докладват незабавно на лицето, отговорно за личните данни, като му предоставят цялата налична информация.

/2/ Лицето, отговорно за личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи, дали е осъществено нарушение на сигурността и кои данни са засегнати.

/3/ Лицето, отговорно за личните данни, докладва незабавно на ръководството на Дружеството наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

/4/ След съгласуване с ръководството на Дружеството, лицето, отговорно за личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

/5/ При спешност, когато съгласуване с ръководството на Дружеството би забавило реакцията и би нанесло големи щети, лицето, отговорно за личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай лицето, отговорно за личните данни, уведомява незабавно ръководството на дружеството за предприетите мерки и съобразява по следващи действия с получените инструкции.

Чл.51. /1/ В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на Дружеството, лицето, отговорно за личните данни, организира уведомяването на КЗЛД.

/2/ Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване за нарушението.

/3/ Уведомлението до КЗЛД съдържа следната информация:

а) описание на естеството на нарушението на сигурността на личните данни, включително, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) името и координатите за връзка на лицето, отговорно за личните данни;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително мерки за намаляване на евентуалните неблагоприятни последици.

/4/ Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, лицето, отговорно за

личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл.52. /1/ Дружеството води регистър на нарушенията на сигурността, който съдържа следната информация:

- дата на установяване на нарушението;
- описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението;
- описание на извършените уведомявания на КЗДЛ и засегнатите лица, ако е било извършено;
- предприетите мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Дружеството;
- предприети мерки за ограничаване на възможността от по следващи нарушения на сигурността.

/2/ Регистърът се води в електронен формат от лицето, отговорно за личните данни.

ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл.53. /1/ Дружеството може при необходимост да предоставя личните данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор.

/2/ В случаите на предоставяне на обработването на обработващ, Дружеството:

- изисква достатъчни гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;
- сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламента;
- ако е възможно информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

/3/ Обработване на лични данни от обработващ извън ЕС/ЕИП е допустимо само когато:

- Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;
- налице са подходящи мерки за защита, като например Обвързващи корпоративни правила /ОКП/, стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;
- субектът на данните е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове, или
- трансферът е необходим за една от целите, изброени в Регламента.

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл.54. /1/ Оценка за въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработката на лични данни, извършвана от Дружеството. Оценка на въздействието се извършва за високорискови дейности по обработване.

/2/ Оценката на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:

-първоначално въвеждане на нови технологии или прехода към нови технологии;

-автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;

-обработване на чувствителни данни в голям мащаб;

-машабно, систематично наблюдение на публично обществена зона.

/3/ За оценката се съставя протокол, който се предоставя при поискване на КЗЛД.

УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл.55. /1/ Унищожаване на личните данни се извършва от дружеството или изрично упълномощено лице, без да бъдат накърняване правата на лицата, за които се отнасят данните, обект на унищожаване, и при спазване на разпоредбите на относимите нормативни актове.

/2/ Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

/3/ Унищожаването на данни на хартиен носител се извършва чрез изгаряне или нарязване с шредер машина. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

ЛИЦЕ, ОТГОВОРНО ЗА ЛИЧНИТЕ ДАНИ И ЛИЦА, ОТГОВАРЯЩИ ЗА ОБРАБОТКАТА НА ДАНИ

Чл.56. Лицето, отговорно за личните данни и лицата, отговарящи за обработката на данни са физически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите Правила.

Чл.57. Лицето, отговорно за личните данни:

-подпомага Дружеството и лицата, обработващи лични данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на лични данни;

-осигурява нормалното функциониране на горепосочените системи за защита;

-осъществява контрол през целия процес на събиране и обработване на данните;

-изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

-периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;

-уведомява Дружеството своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;

-води регистъра на дейностите по обработване;

-контролира унищожаването на данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;

-преупълномощава физически и юридически лица, които да осъществяват защитата на личните данни.

Чл.58. /1/ Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложени задачи налагат това.

/2/ При възлагане на дейности, налагащи обработка на лични данни от регистрите на Дружеството, доставчиците на услуги следва да спазват приложимите нормативни изисквания относно обработката на личните данни и посочените в тези Правила процедури.

/3/ Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др. Гореспоменатите органи могат да изискват данните по надлежен ред във връзка с изпълнението на техните правомощия.

ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл.59. /1/ Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

/2/ Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса по седалището на Дружеството или официалната електронна поща.

/3/ Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на неговите лични данни, обработването на които не отговаря на изискванията на закона.

/4/ Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

/5/ Дружеството е длъжно в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако Дружеството установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.

/6/ субектите на данни имат също правото да:

- оттеглят съгласието си за обработване по всяко време;
- възразят срещу употребата на личните им данни за целите на директния маркетинг;
- искат информация за основанието, въз основа на което личните им данни се предоставени за обработване извън ЕС/ЕИП;
- възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;
- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
- подават жалби до КЗЛД;

-в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене.

ПРОМЕНИ НА ВЪТРЕШНИТЕ ПРАВИЛА

Чл.60. Дружеството може да променя тези Правила по всяко време. Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат. Настоящите Правила са приети и влизат в сила от 23.05.2018 г.

Утвърдил от името на Дружеството:

.....

Инж. Никола Митиков – изп. директор