ПРАВИЛНИК

за механизма на набиране, обработване и съхранение на лични данни и защитата им от незаконни форми на обработване в „Енергомонтаж” АД гр. Бургас

Чл. 1. Настоящият правилник се издава на основание Общия регламент за защита на личните данни (Регламент (ЕС) 2016/679, GDPR) Закон за защита на личните данни (ЗЗЛД) и подзаконовите актове по прилагането им, ръководствата и насоките на Комисията за защита на личните данни (КЗЛД) и Работната група по чл. 29 (след 25.05.2018 г. – на Европейския комитет по защита на данните) и има за цел да регламентира:

(1) Набирането, воденето, поддържането и защитата на лични данни за всички физически и юридически лица пряко или косвено свързани с "Енергомонтаж" АД.

(2) Задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

(3) Необходимите технически и организационни мерки за защита на личните данни на физически и юридически лица от незаконосъобразно и недобросъвестно обработване.

(4) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността.

Чл.2. За целите на настоящият правилник понятията по-долу имат следното значение:

(1) „Лични данни” означава всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице. Отделни данни, които когато се съберат заедно могат да доведат до идентифициране на конкретно лице, също представляват лични данни. Лични данни, които са били деидентифицирани, кодирани или псевдонимизирани, но могат да бъдат използвани за повторно идентифициране на дадено лице, остават лични данни.

(2) „Обработване на лични данни” е всяко действие или съвкупност от действия, които се извършват по отношение на личните данни с автоматични или неавтоматични средства (събиране, записване, организиране, структуриране, съхранение, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване и др.).

(3) „Администратор на лични данни” е "Енергомонтаж" АД, което самостоятелно или чрез възлагане на друго лице обработва лични данни.

(4) „Длъжностно лице по защита на личните данни /ДЛЗД/” е лице, което е служител в дружеството или изпълнява функции по поръчение, на което са възложени

задълженията във връзка със защитата и процесите по обработка на лични данни, уредени в този Правилник.

(5) „Обработващ лични данни” е лице или организация, което въз основа на договор обработва лични данни, предоставени от Дружеството, за уговорените цели.

(6) "Субект" е физическо лице и физически лица, представители на юридическите

(7) „Съгласие на физическо лице” е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява те да бъдат обработвани.

Чл.3.(1) "Енергомонтаж" АД обработва само законно събрани лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, които дружеството събира и обработва следва да бъдат точни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстващи на целите, за които се обработват.

(2) Дружеството обработва законосъобразно, добросъвестно и прозрачно личните данни, като спазва принципа данните да се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели, както и предварително информира субекта за обработката.

(3) "Енергомонтаж" АД поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на субектите за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

(4) "Енергомонтаж" АД в качеството си на Администратор на лични данни е разработил "Кодекс на поведение", който може да бъде намерен на интернет страницата на дружеството, а именно: www.energomontage-bs.com. Всички субекти пряко или косвено свързани с дружеството са длъжни да спазват правилата определени с цитирания кодекс.

Чл.4.(1) Субекта - притежател на личните данни - изразява свободно своето съгласие относно обработването на отнасящи се за него лични данни, които са предоставени с точно определена цел.

(2) Документите за съгласие се съхраняват от дружеството, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

(3) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган, свързано с

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

(4) Субекта има право по всяко време на обработването да поиска коригиране, блокиране или унищожаване (изтриване) на събрани за него лични данни, в случаите, когато оспорва тяхната точност или обработването им е незаконосъобразно.

(5) В случаите, когато данните не са получени от субектите, "Енергомонтаж" АД го информира за целите и правното основание на обработването, за категориите предоставени данни и техния източник, за получателите, на които ще бъдат предоставени, както и за правото му на достъп до неговите лични данни.

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

(7) Субекта има право да бъде уведомен при нарушение на защитата на данните, което вероятно ще доведе до висок риск за неговите права.

(8) Субекта има право на защита по съдебен или административен ред, в случай че правата му са били нарушени.

(9) Субекта има право да поиска информация относно личните си данни и дружеството е длъжно в срок до 1/един/ месец да се произнесе по искането на лицето.

Чл.5. Обработването на личните данни се извършва, когато:

(1) Това е необходимо за изпълнение на нормативно установено задължение.

(2) Субектите, за което се отнасят данните, са дали своето изрично съгласие.

(3) Обработването е необходимо за 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.

(4) Това е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице.

(5) Обработването е необходимо за изпълнение на задача от обществен интерес или е за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни.

Чл. 6. Цел на набиране и използване на лични данни

(1) За всички дейности, свързани с възникване, изменение и прекратяване на трудовите, служебните и граждански правоотношения - за изработване на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни) - цитираните лични данни се набират при постъпване/възлагане на работа по горецитираните правотношения. Данните се предоставят на хартиен носител на представляващия администратора на лични данни на основание нормативно задължение с оглед преценка за годността на постъпващия/изпълнителя да заеме съответната длъжност или за извършване на определената работа. След съгласуване решението на представляващия със съответнините длъжностни лица и одобрение на кандидатстващият за работа, всички събрани лични данни се предоставят на обработващия лични данни и/или лицето, действащо под негово или на администратора ръководство, за възникване и последващо обработване на правоотношението.

(2) За установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по служебни правоотношения, трудови и граждански договори;

(3) За 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

(4) За водене на счетоводна отчетност спрямо всички субекти

5) За всички дейности, свързани с възникване, изменение и прекратяване на договори и всякакви документи, свързани с нормалното функциониране и осъществяване дейността на дружеството /с клиенти, доставчици/ - набират се данни, необходими за законовите задължения на дружеството

Чл. 7. Съхранение на лични данни

(1) "Енергомонтаж" АД събира и обработва лични данни автоматизирано и неавтоматизирано /хартиен носител/.

(2) В дружеството се съхраняват следните видове лични данни:

1. физическа идентичност – имена, ЕГН, адрес, телефон, паспортни данни;

2. образование – документ за придобито образование, квалификация правоспособност;

3. трудова дейност – съгласно приложените документи за трудов стаж и професионална биография;

4. медицински данни – карта за предварителен медицински преглед за постъпване на работа и последващи медицински прегледи;

5. професионална биография - данните са от значение при избора на подходящо за съответната длъжност лице. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо;

6. свидетелство за съдимост, когато се изисква;

7. фирмени данни - необходими за сключване на договори и обработка на счетоводни документи.

(3) Срока на съхранение на лични данни на физическите и юридическите лица, получени за изпълнение на горецитираните цели, се съхраняват до осъществяване на целите, за които се обработват или до нормативно определените срокове.

Чл. 8. Унищожаване на данните

(1) Унищожаване на личните данни се извършва от Дружеството или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

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

Чл. 9. "Енергомонтаж" АД предприема следните мерки за защита на личните данни:

(1) Програмно-технически средства за защита при пренасяне на информацията, надеждна и защитена идентификация и автентификация, осигуряване конфиденциалност и интегритет на пренасяната информация.

(2) Осъществява се контролиран достъп до помещенията в които се съхраняват личните данни.

(3) Оборудването в което се съхраняват личните данни е със заключващи се устройства.

Чл. 10. Длъжности свързани с обработването и защитата на личните данни - права и задължения

(1) Длъжностното лице по защита на личните данни е определено със заповед на Администратора на лични данни.

(2) Определеното длъжностно лице неможе да заема ръководна длъжност, пряко свързана с обработка на лични данни. То трябва да има необходимите експертни познания и да е запознат с всички нормативни документи в областа на защитата на лични данни /законодателство и практика/.

(3) Лицето по защита на информацията има следните правомощия:

1. да информира и да дава съвети на администратора или на обработващия данни, както и на техните служители за задълженията им съгласно закона за защита на данните;

2. да следи за спазването от страна на организацията на цялото законодателство във връзка със защитата на данните, включително при одити, дейности за повишаване на осведомеността, както и обучение на персонала, участващ в операциите по обработване;

3. да действа като звено за контакт за искания от страна на физически лица относно обработката на личните им данни и упражняването на техните права;

4. осигурява организацията по водене на информацията, съгласно предвидените мерки за гарантиране на адекватна защита;

5. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водената информация;

6. контролира спазването на правата на потребителите във връзка с информацията и програмно- техническите ресурси за тяхната обработка;

7. определя ред за съхраняване и унищожаване на информационни носители;

8. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;

9. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

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

11. да извършва оценка на въздействието върху защитата на лични данни при наличие на риск;

12. той задължително провежда предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

(4) Обработващи лични данни в "Енергомонтаж" АД са следните длъжвости: Изп. Директор, Главен счетоводител, Оперативен счетоводител.

(5) Обработващите лични данни са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

да ги обработват само и единствено от името на администратора;

2. да използват личните данни, до които имат достъп, само и единствено съобразно целите и средствата, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да не разпространяват личните данни, до които имат достъп;

да се запознаят с нормативната база, вътрешните правила и политики на дружеството относно защитата на личните данни;

4. да са запознати с правилата за реакция при събития, застрашаващи сигурността на данните;

5. да актуализират личните данни (при необходимост);

6. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

7. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

8. да не изнасят и съхраняват личните данни извън специално определените за целта места;

9. да не използват личните данни по нерегламентиран начин /фалшифициране и друг вид злоупотреба/;

10. след прекратяване на договора с обработващият лични данни, той няма право на достъп до същите;

11. администраторът може да назначи обработващ лични данни /външна организация/, като за целта сключва договор или споразумение при следните условия:

- ✓ обработването може да се извършва само при документирани инструкции от администратора;
- ✓ обработващият данни гарантира, че лицата, упълномощени да обработват личните данни, са се ангажирали с поверителността или са подчинени на съответното правно задължение за поверителност;
- ✓ обработващият данни трябва да предлага минимално ниво на сигурност, определено от администратора;

- ✓ администраторът трябва да съдейства при осигуряването на съответствие с ОРЗД.

Чл.10. (1) Право на достъп до данните имат:

1. Лицата, за които се отнасят данните, по тяхно изрично писменно или усно искане;

2. Достъп до личните данни на лицата, съдържащи се на технически или хартиен носител има само обработващият лични данни и/или лицето, действащо под негово или на администратора ръководство при обработване на лични данни, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има прекият ръководител.

3. Държавни органи, надлежно легитимирали се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

(2) Личните данни не се предават на трети лица, освен в случаите когато това се налага да бъдат защитени жизненоважните интереси на Вас или е за целите на спазването на законово задължение, което се прилага спрямо нас, като администратор на лични данни.

Чл. 11. Нарушения на сигурността

(1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Длъжностното лице, отговорно за личните данни, като му предоставят цялата налична информация.

(2) ДЛЗД извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) ДЛЗД докладва незабавно на съдружниците в 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, ДЛЗД предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, ДЛЗД може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай той уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

(6) 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, ДЛЗД организира уведомяването на КЗЛД. Уведомяването следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението. Уведомлението трябва да съдържа следната информация:

1. описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. името и координатите за връзка на Лицето, отговорно за личните данни;

3. описание на евентуалните последици от нарушението на сигурността;

4. описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(7) 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.

(8) Дружеството води регистър на нарушенията на сигурността, който е в електронен фермат и съдържа следната информация:

1. дата на установяване на нарушението;

2. описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);

3. описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

4. предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Дружеството;

5. предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

Изп. Директор:.....

/инж. Н. Апостолов/