ПРАВИЛА

за мерките и средствата за защита на личните данни

събирани, обработвани, съхранявани и предоставяни

от дружествата в групата на Евро Алианс

Раздел първи

ЦЕЛИ И ОБХВАТ

Чл.1. Настоящите Правила уреждат организацията и вътрешния ред на дружествата в групата на Евро Алианс, наричан по-нататък за краткост "групата на ЕАИ", като администратор на лични данни, както и нивото на технически и организационни мерки при обработване на лични данни и допустимия вид защита.

Чл.2. Правилата са изготвени в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО - Общ регламент относно защитата на данните (наричан по-долу: Регламентът), както и във връзка с привеждане дейността на групата на ЕАИ в съответствие с изискванията на Регламента и на нормативните актове и други относими актове, регламентиращи защитата на личните данни, като но не само разпоредбите на Закона за защита на личните данни (ЗЗЛД) и Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (Наредба № 1) и целят защита на интересите на клиентите - физически лица и физическите лица, представляващи юридическите, както и на служителите от групата на ЕАИ от незаконосъобразно и недобросъвестно обработване на личните им данни. В случай че правило установено в настоящите Правила противоречи на Регламента или на друг нормативен акт, касаещ защитата на лични данни, прилага се Регламентът, съответно нормативният акт.

Чл.3. Всички служители, работници, свързани лица, членове на управителните органи на дружество, част от групата на ЕАИ, контрагенти и други субекти, изпълняващи дейности по възлагане или по друг повод, обработващи, съхраняващи или получаващи лични данни на физически лица **са длъжни да спазват разпоредбите на настоящите Правила**, Регламента и посочените по-горе нормативни актове.

Раздел втори

ИЗПОЛЗВАНИ ТЕРМИНИ И ДЕФИНИЦИИ

Чл.4 За целите на настоящите Правила понятията по-долу имат следното значение:

1. **„Лични данни"** са всяка информация, отнасяща се до физически лица и физическите лица, представляващи юридическите на дружествата от групата на ЕАИ, както и тази, свързана с нейните служители, които са идентифицирани или чрез която същите могат да бъдат идентифицирани пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или

непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

2. **„Субект на лични данни/Субект"** – всяко физическо лице, което предоставя личните си данни или чиито лични данни се обработват или съхраняват.
3. **„Обработване на лични данни"** е всяко действие или съвкупност от действия, които групата на ЕАИ извършва по отношение на личните данни с автоматични или неавтоматични средства (събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване и др.).
4. **„Администратор на лични данни"** е всяко едно юридическо лице от групата на ЕАИ, което самостоятелно или чрез възлагане на друго лице обработва лични данни.
5. **„Обработващ лични данни"** – физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на Администратора.
6. **„Специфични признаци/чувствителни данни"** са признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето.
7. **„Генетични данни"** - лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице.
8. **„Биометрични данни"** - лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни. Обработването на снимки е обработване на биометрични данни, когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице.
9. **„Данни за здравословното състояние"** - означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние.
10. **„Регистър на лични данни" -** всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.
11. **„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
12. **„Криптиране"** – е процесът на кодиране на информацията по начин, който предотвратява достъпа на неоторизирани лица до нея.

13. **„Псевдонимизация"** – означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано.
14. **„Профилиране"** – е всяка форма на автоматизирано обработване на лични данни, при която използването на лични данни е с цел оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.
15. **„Трансгранично обработване"** означава или а)обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка;
16. **Дружество от групата на ЕАИ** – е всяко дружество, което може да е пряко или непряко под доминиращото влияние от страна на друго дружество в групата на ЕАИ, или може да упражнява доминиращо влияние върху такова дружество или заедно с такова дружество попада под доминиращото влияние на друго предприятие поради собственост, финансово участие или правилата, които се прилагат към него. Дружества в групата на ЕАИ (без изброяването да е изчерпателно) са „Евро Алианс Геотехника" АД, „Евро Алианс Тунели" АД, „Евро Алианс Кънстракшън" АД, „Евро Алианс Инженеринг" АД, „Евро Алианс Флийт" ООД, „Геоинженеринг клъстер" ООД, „Евро Алианс Изолации" ООД, „Евро Алианс Дизайн" ЕООД.
17. **Надзорен орган** – за територията на Република България, това е Комисия за защита на личните данни.

Раздел трети

ПРИНЦИПИ ПРИ СЪБИРАНЕ И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл.5. (1) Групата на ЕАИ спазва следните принципи при събиране и обработване на личните данни:

1. **Минимизация** – означава събирането на лични данни, които са подходящи и релевантни във връзка с целите, за които се обработват. Прилагането на принципа в процесите на събиране и обработване на лични данни се изразява в събирането на данни в минимален обем, необходим за изпълнение на целите, за които се събират.
2. **Законосъобразност/добросъвестност** – събирането, обработването и съхранението на личните данни се извършва в съответствие с нормативната уредба, добросъвестно и единствено за целите, за които са събрани данните.

3. **Информираност/Прозрачност** – преди всяко събиране на лични данни от субекта, на същия следва да му се предостави ясна, еднозначна и вярна информация относно целите, за които се събират/обработват/съхраняват личните данни, как се съхраняват, колко време ще се съхраняват, на какво основание се събират и какви са правата на субекта във връзка с обработването на личните му данни.

4. **Точност** – данните се обработват и съхраняват при съблюдаване за тяхната точност и гарантиране на своевременното им поддържане в актуален вид, при необходимост от това, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват

5. **Защита на данните на етапа на проектирането** – събирането, обработването и съхранението на личните данни се извършва с такива технически средства и прилагането на други подходящи мерки, които осигуряват прилагането на настоящите принципи, включително събиране на минимално необходимия обем данни. Мерки се въвеждат към момента на определянето на средствата за обработване, така и към момента на самото обработване.

6. **Защита на данните по подразбиране** – ползване само на такива технически средства за защита или прилагането на други подходящи мерки, гарантиращи, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването, че данните се съхраняват за минимален срок, абсолютно необходим за постигане на целта на обработване и след това се заличават при спазване на съответните правила и процедури, че всеки достъп, предаване или споделяне на данни е допустим само при наличие на валидно правно основание за това. Прилагат се такива мерки, които активират по подразбиране най-стриктните настройки за поверителност, които не позволяват автоматично споделяне на данни, освен ако самото лице, за което се отнасят данните, не го разреши изрично.

7. **Цялостност и поверителност** – обработването на личните данни се осъществява по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

8. **Ограничение на съхранението** – личните данни се съхраняват във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни. Личните данни могат да се съхраняват и за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в Регламента с цел да бъдат гарантирани правата и свободите на Субекта на данните.

9. **Отчетност -** гарантира се спазването на настоящите принципи чрез поддържане на документация за дейностите по обработване, за които е отговорен Администратора.

(2) Групата на ЕАИ обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Личните данни, които групата на ЕАИ 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.

(3) Групата на ЕАИ поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

(4) Групата на ЕАИ спазва принципа за забрана на обработване на специални категории данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход; разкриване на политически, религиозни или философски убеждения; членство в политически партии или организации; сдружения с религиозни, философски, политически или синдикални цели; лични данни, които се отнасят до здравето, сексуалния живот или до човешкия геном), като изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от ЗЗЛД.

Раздел четвърти

СЪБИРАНЕ И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ. ОСНОВАНИЯ.

Основания

Чл.6. В Групата на ЕАИ се използват следните законосъобразни основания за събиране на лични данни:

1. **Договорно** – данните са необходими с оглед сключване на договор със субекта на данни или във връзка с пред договорни отношения със субекта на данни (в случаите, когато субектът предприема действия преди сключване на договор).
2. **Законово** – когато обработването е във връзка с изпълнение на законово задължение от Администратора.
3. **В обществен интерес** – когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора.
4. **С оглед легитимен/законно защитим интерес на Администратора** - 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.
5. **Въз основа на съгласие на Субекта** – в случай че не е налице някое от основанията, посочени в т. 1 – 4 по-горе, данни на Субекта могат да се събират, обработват и/или съхраняват въз основа на предварително дадено от него съгласие. Съгласието следва да бъде дадено във форма, от която може лесно да се определи неговото съдържание, да е ясно, конкретно, информирано и доброволно (да не са поставени условия за предоставяне на определена стока или услуга в зависимост от даването на съгласие).

Чл.7. (1) Субектът на личните данни изразява свободно своето съгласие относно обработването на отнасящи се за него лични данни.

(2) Субектите (физически лица и физическите лица, представители на юридическите) и служителите на групата на ЕАИ, се идентифицират посредством официален документ за самоличност (лична карта). Документът за самоличност задължително се копира като субектът изписва на копието „Съгласен/а съм с копирането" и се подписва върху

него. Оригиналът се връща на субекта, а копието се съхранява в архива на групата на ЕАИ за срок от 5 години.

(3) В случаите, когато данните не са получени от субекта, групата на ЕАИ 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.

Чл.8. Като администратор на лични данни групата на ЕАИ поддържа личните данни във вид, който позволява идентифициране на физическите лица.

Чл.9. Всички работници/служители на групата на ЕАИ при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни с субекти, в т. ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на трудовите/служебните им задължения.

Събиране на лични данни

Чл.10. (1) Преди да се съберат личните данни от Субекта следва да му се предостави информация (във вид, в който може да се докаже по несъмнен начин момента на предоставяне на информацията и обема на предоставената информация) относно:

1. Целите, за които се събират личните данни;

2. Срокът, за който ще се обработват и съхраняват личните данни;

3. Данните, които идентифицират администратора;

4. Координатите за връзка с Длъжностното лице по защита на личните данни;

5. Получателите на лични данни, ако има такива;

6. Правното основание за обработване на личните данни;

7. Правата на Субекта на коригиране, изтриване (в случай, че е налице такова), преносимост на данните и правото на жалба до Надзорния орган (Комисия за защита на личните данни).

**** На субекта следва да се предостави възможност за избор относно начина на предоставяне на личните си данни – на хартия, след непосредствена среща/интервю, в електронен вид (по e-mail) или по друг подходящ начин, по който могат да бъдат коректно и правилно възприети.***

(2) В процеса на събиране на личните данни се събират само такива, които са необходими с оглед целите, за които ще се обработват и в минимален обем. Законосъобразно е събирането, обработването и съхранението на данни в следните неизчерпателно изброени хипотези и обеми:

2.1. За сключване на облигационен договор или друг двустранен акт, който не подлежи на нотариално удостоверяване се събират лични данни относно име, ЕГН и адрес за кореспонденция и в случаите, когато това е необходимо – относно административен адрес на недвижим имот.

2.2. За сключване на облигационен договор или друг двустранен акт, който подлежи на нотариално удостоверяване се събират лични данни относно име, ЕГН, номер на лична карта (или друг документ за самоличност) и постоянен адрес по лична карта (или

друг документ за самоличност) и в случаите, когато това е необходимо – относно административен адрес на недвижим имот.

2.3. С цел изпълнение на нормативните актове, регламентиращи трудовите правоотношения Администратора (в качеството му на работодател) събира данни относно:

2.3.1. идентификацията на работника (име, ЕГН и адрес за кореспонденция);

2.3.2 относно икономическата му идентичност, когато е поискал изплащане на трудовото му възнаграждение по банкова сметка (данни относно банковата му сметка);

2.3.3. относно здравословното му състояние, когато е упражнил правата си по Кодекса на труда с оглед установяване на облекчен режим на работа, защита при уволнение по смисъла на чл. 333 от Кодекса на труда и др. (Експертно решение на лекарска комисия, болничен лист и др.), както и в случаите при постъпване на работа, с оглед сключването на трудовия договор;

2.3.4. данни относно съдебно минало, когато за заемане на длъжността нормативен акт изисква удостоверяване на данни относно присъди и осъждания (свидетелство за съдимост);

2.4. С цел охраняване на законните си интереси и неприкосновеност на имуществото си Администраторът осъществява видеонаблюдение на собственото му имущество и контрол на достъпа до него. Всички лица с достъп до имуществото на Администратора се информират предварително, по разбираем и конкретен начин за извършваното видеонаблюдение. На служителите и работниците на Администратора се осигурява достъп до имуществото, включително недвижимото чрез контролиран достъп и по – конкретно чрез карти за достъп, позволяващи идентификацията на съответния служител/работник осъществил достъпа. За целите и за охраняваните законни интереси на Администратора служителите/работниците на администратора се уведомяват предварително по ясен и конкретен начин към момента на предоставяне на карта за достъп.

2.5. Събиране и обработване на лични данни за маркетингови цели е допустимо само след изрично, информирано и свободно дадено съгласие на Субекта. При обработване на лични данни за маркетингови цели субектът има право на възражение срещу такова обработване, включително профилиране. Преди събиране на личните данни за целите на директния маркетинг субектът на данни изрично следва да бъде уведомен за правото му на възражение. Когато субектът на данни упражни правото си на възражение обработването на личните данни за целите на директния маркетинг се прекратява незабавно.

2.6. Автоматизирано обработване на лични данни за целите на профилирането при подбор на персонал - Субектите на данни следва изрично да бъдат уведомени, че данните им ще се обработват с цел профилирине при подбор на персонал, както и относно нивото на автоматизирано вземане на решения при това профилиране. Лични данни, които разкриват расов произход, политически възгледи, религиозни или други убеждения, както и лични данни относно здравето, съдебно минало или сексуалния живот не се обработват автоматизирано. Незабавно след приключване на конкретната процедура по подбор данните събрани в тази връзка се унищожават, освен ако Субектът не е дал изричното си съгласие за съхранението им с цел ползването им в

последващи процедури по подбор на персонала. Във всички случаи това съхранение не може да по-дълго от една календарна година, считано от датата на предоставяне на съгласието.

Обработване и съхраняване

Чл.11 При обработването и съхраняването на лични данни от Администраторът или от трети лица, действащи по възлагане на администратора се прилагат следните мерки:

(1) Съхраняване и обработване на документи, съдържащи лични данни на хартиен носител:

1.1. В случаите на обработване на лични данни, съдържащи се на хартиен носител обработващите ги лица нямат право да оставят носителите с лични данни без надзор и на общодостъпни места, като следва да извършват обработването по начин, който не позволява неоторизирано възприемане от трети лица, неоторизирано копиране, предаване и др. подобни действия.

1.2. За времето, за което трае обработването на лични данни, съдържащи се на хартиен носител последните се съхраняват в заключващи се шкафове (тип каса и други подобни) достъп до които имат само лицата оправомощени по силата на договор, закон или друго правно основание да извършват обработката.

1.3. В случаите, в които се предоставят копия на документи, съдържащи и данни, които не са необходими за целите на обработването, последните се заличават. Копия на документи съдържащи биометрични данни не се съхраняват, освен ако не е налице законно защитим интерес или нормативно основание за съхраняването им. При невъзможност за отделяне на необходимите личните данни от биометричните, последните се заличават от обработващите ги лица.

1.4. Достъпът до личните данни от оторизирани служители или други лица от името на Администратора се извършва на принципа на диференцирането, като лицето има достъп само до такива данни и в такъв обем необходими за изпълнение на конкретната работа/задача. Нивата на достъп са определени в длъжностната характеристика на служителите/работниците на Администратора (в това число „Стандарт на работното място") и в информационната система (КИИС)

(2) Предаване на документи, съдържащи лични данни на хартиен носител:

2.1. Предаване на данните между различните структури в дружество или между различните дружества в групата на ЕАИ се извършва чрез анонимизирането им и/ или в непрозрачни пликове с отбелязване *гриф „Лични данни„*. Достъп до данните, които се предават може да има само лицето, което е посочено като получател, като всички лица, имащи достъп до личните данни и които не са получател, но участват в процеса по предаване на документите, са задължени да предадат данните само и единствено на получателя и да положат необходимата грижа данните да не се обработват от лица, които не са получателят, включително да съдействат за законосъобразното и сигурно предаване на получателя.

2.2. До предаването на личните данни на получателя им, същите се съхраняват в определени за това заключващи се шкафове (тип каса или други подходящи).

(3) Мерки относно информационната система и информационната сигурност на личните данни

3.1. Въвеждане на криптиране на интернет връзката посредством протокол (https) за защита на комуникацията в компютърната мрежа, както и гарантиране на сигурност при пренасяне на данни между отделни интернет потребители.

3.2. Осигуряване на достъп до информационната система посредством потребителско име и парола. Посредством тях се задава потребителска роля, която дефинира нивото на достъп.

3.3. Извършване на ежегоден одит за ниво на достъп до информационната система

3.4. Периодичен одит (на всеки 6 месеца) от независими експерти и удостоверяване на степента на сигурност на информационната система от външни атаки.

3.5. Запазване в поверителност от трети лица (включително служители на Администратора) на данните за вход към информационната система.

3.6. Достъп до информационната система единствено през вътрешна мрежа и прокси сървър. При необходимост издаване на поименен достъп до информационната система за връзка към нея от разстояние.

(4) Мерки за защита при унищожаване на лични данни. Начин на унищожаване на лични данни.

4.1. След изтичане на сроковете за съхранение и обработване на личните данни на субектите или след отпадане на основанието за съхранението и/или обработването им, носителите на лични данни се унищожават.

4.2. Унищожаването се извършва от комисия, назначена със заповед на изпълнителния директор на Администратора или упълномощено от него лице. Комисията документира действията си по унищожаване на данните в протокол.

4.3. Унищожаването се извършва чрез шредер - за хартиените носители и чрез заличаването им от информационната система - за електронните/магнитните носители.

4.4. Обработващите лични данни от името на Администратора или негови представители (по силата на изрично упълномощаване) на всеки два месеца извършват одит на видовете, обема и носителите на личните данни, които се обработват и съхраняват, както и на основанията за тяхното съхранение и обработване и определят личните данни, които подлежат на унищожаване. Резултатите от извършения одит се посочват в протокол и се предоставят на длъжностното лице по защита на данните.

4.5. На всеки три месеца длъжностното лице по защита на данните извършва, на самостоятелно основание, одит на видовете, обема и носителите на личните данни, които се обработват и съхраняват, както и на основанията за тяхното съхранение и обработване и определя личните данни, които подлежат на унищожаване. Резултатите от одита се документират в протокол.

Права на субектите:

Чл.12. (1) Субектите на лични данни имат следните основни права:

1. Право на достъп - Субекта на лични данни има право на достъп до собствените му лични данни, които се обработват. Субектът им право да получи информация относно

целите, за които се обработват личните му данни и категориите лични данни, които се обработват, срокът на съхраняване на личните му данни (когато е възможно да се определи), средствата на обработката, получателите, на които могат да бъдат предоставени данните, съществуването на автоматизирано вземане на решения, включително профилиране, както и право на копие от личните му данни, които се обработват.

2. **Право да иска изтриване на личните данни** – Субектът може да поиска от Администратора изтриване на личните му данни в разумен срок. Администраторът е длъжен да изтрие личните данни, ако последните се обработват въз основа на предварително съгласие на Субекта, обработването е незаконосъобразно или основанията за обработването са отпаднали. Не подлежат на изтриване лични данни, които се обработват във връзка с действащ договор, във връзка с признат правен интерес на Администратора, във връзка с правни претенции, включително тяхното предявяване или във връзка със законово основание/право. При процедурата по изтриване на личните се прилага нарочна вътрешна инструкция.

3. **Право на коригиране** – Субектът на данни има право да иска коригирането им от Администратора в разумни срокове.

4. **Право на ограничаване на обработването** - Субектът на данни има право да иска ограничаване на обработването на данните му, когато се оспорва точността на личните данни, обработването е неправомерно, но субектът не е поискал изтриването им, или когато са налице хипотезите на чл. 18 от Регламента.

5. **Право на преносимост** – Субектът на данни може да изиска от Администратора предоставяне на личните му данни в подходящ формат, така че Субектът да ги предостави на друг администратор или да поиска от Администратора директното им предоставяне на друг администратор.

6. **Право на възражение** – Субектът може да възрази срещу обработването на негови лични данни, когато обработването се извършва при изпълнение на задача от обществен интерес или упражняване на официални правомощия, когато обработването е във връзка с защитим правен интерес на Администратора или трета страна, когато се обработват данни за целите на директния маркетинг, включващ и профилиране, когато данните се обработват за целите на научни, исторически изследвания или за статистически цели.

7. **Право на жалба** – Ако субектът на данни счита, че обработването на личните му данни нарушава разпоредбите на Регламента може да подаде жалба до надзорния орган. Упражняването на това право не възпрепятства упражняването на правата на съдебна защита по общия исков ред.

(2) Упражняването на правата по т. 1 – т. 6 от Субектите се извършва чрез писмено сезиране на Администратора, обработващия личните данни от името на Администратора или длъжностното лице по защита на личните данни.

(3) Писмените искания, чрез които се упражняват правата на субектите съдържат:

1. Данни относно Субекта, който упражнява съответното право в обем, който позволява идентифицирането му;

2. Посочване на категориите данни, за които се упражнява съответното право;

3. Посочване на конкретното искане/право, което се упражнява и обстоятелствата, които обосновават упражняването му, както и законово, договорно или друго основание за упражняване на правото;

4. Подпис на Субекта, подал искането.

(4) Искането се обработва от Администратора/обработващия лични данни в срок до 5 работни дни от постъпването му, в случай че не е налице правна или фактическа сложност относно обективното изпълнение на искането.

(5) В случаите, в които Администраторът/обработващият лични данни следва да извърши определени действия, в резултат на упражняване на право на субекта по т. 1 – 6 по-горе, той ги извършва в разумен срок, не по-кратък от 3 работни дни от постъпване на искането. В същия срок Администраторът/обработващият лични данни уведомява Субекта за конкретните мерки и действия предприети в изпълнение на искането му и упражняване на съответното право.

(6) Подаването на искането, обработването и уведомяването на Субекта са безплатни за последния.

Раздел пети

ОПИСАНИЕ НА РЕГИСТРИТЕ ВОДЕНИ ОТ АДМИНИСТРАТОРА

Чл.13. Групата на ЕАИ може да поддържа по преценка на всяко едно дружество следните регистри:

(1). „Персонал";
(2). „Видеонаблюдение";
(3). „GPS контрол"
(4). „Деловодство";
(5). „Външни посетители";
(6). „Счетоводство";
(7). „Контрагенти";

Чл.14. Всеки един от поддържаните регистри съдържа информация относно: 1) името и координатите за връзка на администратора, а когато е приложимо и на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива; 2) целите на обработването; 3) описание на категориите субекти на данни и на категориите лични данни; 4) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации; 5) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, документация за подходящите гаранции; 6) предвидените срокове за изтриване на различните категории данни; общо описание на техническите и организационни мерки за сигурност.

Чл.15. За защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване групата на ЕАИ организира и предприема мерки, съобразени

със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Раздел шести

ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ - НОСИТЕЛИ НА ДАННИ, ТЕХНОЛОГИЯ НА ОБРАБОТВАНЕ, СРОК ЗА СЪХРАНЕНИЕ И ПРЕДОСТАВЕНИ УСЛУГИ

Чл.16. (1) Групата на ЕАИ поддържа водените регистри в писмена форма, включително в електронен формат.

Чл.17. (1) В **регистър „Персонал"** се съхраняват следните видове лични данни:

1. физическа идентичност – имена, ЕГН, адрес, телефон, данни по документ за самоличност;

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;

5. свидетелство за съдимост, когато се изисква;

6. формуляр по образец;

7. декларация по чл. 333 ал.1, т.3 КТ;

8. банкова сметка;

9. месечен доход;

(2) Физическата защита на личните данни от регистъра е организирана като елемент на общата физическа защита на сградите и работните помещения при строг контрол на достъп до тях.

(3) Данните в регистъра се събират, обработват и съхраняват в отдел „ТРЗ" на хартиен и технически носител, посредством автоматизирани софтуерни продукти – Омекс, WorkStream.

(4) Личните данни в регистър "Персонал" се набират при подаване на документи за постъпване на работа по трудово и служебно правоотношение, за попълване на трудовото досие, издаване на различни справки и сл. бележки, провеждане на подбор по документи и интервюта.

Чл.18. (1) **Регистър „Видеонаблюдение"** се попълва с данни от автоматично денонощно видеонаблюдение (видео образ) за движението на служителите и посетителите към подходите на сградите на групата на ЕАИ и помещенията с определен статут. Записите с видео образи се съхраняват на отделен персонален компютър, монтиран в помещение на сградата.

(2) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на групата на ЕАИ. На входовете на сградата са поставени предупредителни табели, че обектът се намира под постоянно видеонаблюдение. Данните от този регистър се съхраняват 14 дни.

(3) Физическата защита на личните данни се осъществява от денонощна физическа охрана.

Чл.19. (1) **Регистър „GPS контрол"** се попълва с данни от автоматично денонощно осъществяван контрол за движението на служебните автомобили, предоставени на разположение на служителите/ работниците на дружествата от групата на ЕАИ. Записите с получената GPS информация се съхраняват на отделен персонален компютър, монтиран в помещение на сградата.

(2) Данните в регистъра се предоставят доброволно от лицата при предоставени на тяхно разположение на съответния служебен автомобил, посредством подписване на приемо-предавателен протокол в който е изрично посочено, че движението на служебния автомобил се контролира с GPS система. Данните от този регистър се съхраняват 365 дни.

(3) Физическата защита на личните данни от регистъра е организирана като елемент на общата физическа защита на сградите и работните помещения при строг контрол на достъп до тях.

(4) Данните в регистъра се събират, обработват и съхраняват на сървър на доставчика на услугата, посредством автоматизирани софтуерни продукти от Отговорник автопарк и GPS контрол в дирекция „Администрация".

(5) Личните данни в регистър "GPS контрол" се набират при предоставяне на служител/ работник на групата ЕАИ на служебен автомобил, който да бъде използван само при и по повод изпълнение на служебни задължения.

Чл.20. (1) **Регистър „Деловодство"** съдържа следните лични данни за физическите лица – служители на групата на ЕАИ: три имена и длъжност.

(2) Данните в регистъра не се предоставят на трети лица.

(3) Физическата защита на личните данни от регистъра е организирана, като данните се обработват и съхраняват в заключващи се помещения и строг контрол на достъпа до тях.

Чл.21. Регистър „Външни посетители" съдържа трите имена на респондентите и посетителите на групата на ЕАИ.

Чл.22. (1) **Регистър „Счетоводство"** съдържа следните данни – три имена, ЕГН, номер на лична карта, адрес, банкова сметка, данъчна служба по местоживеене, месечен доход;

(2) Данните в регистъра не се предоставят на трети лица.

(3) Физическата защита на личните данни от регистъра е организирана, като данните се обработват и съхраняват в заключващи се помещения и строг контрол на достъпа до тях.

(4) Данните в регистъра се събират, обработват и съхраняват в отдел „Счетоводство" на хартиен и технически носител, посредством автоматизиран софтуерен продукт ERP. Документите се съхраняват на хартиен носител в папки/класьори и в електронен формат посредством ERP система. След изтичането на една година документите съхранявани в отдел „Счетоводство" се изпращат в архив, където се съхраняват определен период от време.

Чл.23. Регистър „Контрагенти" съдържа следните лични данни за физическите лица, представляващи Юридическите лица: три имена и ЕГН или при физически лица контрагенти – три имена, ЕГН, номер на лична карта, адрес, банкова сметка.

(2) Физическата защита на личните данни от регистъра е организирана като елемент на общата физическа защита на сградите и работните помещения при строг контрол на достъп до тях.

Чл.24. Групата на ЕАИ предприема следните мерки за защита на личните данни:

(1) програмно-технически – криптографски методи и средства и защита при пренасяне на информацията, надеждна и защитена идентификация и автентификация на изпращача и на получателя на информацията и осигуряване конфиденциалност, интегритет на пренасяната информация, специализирани софтуерни програми и антивирусни програми.

(3) физически – система от мерки по защита на сградите, помещенията и съоръженията, в които се създават, обработват и съхраняват лични данни и контрола върху достъпа до тях;

(4) организационни и административни – регламентирани с правила и заповеди на представляващите групата на ЕАИ;

(5) нормативни, предвидени в законови и подзаконови нормативни актове.

Чл.25. (1) Сроковете за съхранение са съобразно описанията в част 2 от съответния регистър, както следва:

1. за Регистър „Персонал" - 50 години за ведомости и трудови досиета, 3 години за болнични;

2. за Регистър „Видеонаблюдение" – 14 дни;

3. за Регистър „GPS контрол" – 1 година.

4. за Регистър „Деловодство" – според номенклатурата на делата;

5. за Регистър „Външни посетители" – 3 месеца;

6. за Регистър „Счетоводство" – за първични счетоводни документи 5 години, за облигационни договори минимум 10 години;

7. за Регистър „Контрагенти" – договорите минимум 10 години.

(2) Групата на ЕАИ следва да спазва технологията за безопасно поддържане и съхранение, обновяване, заличаване, унищожаване и т.н на лични данни.

Раздел седми

ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ

Чл.26. (1) При необходимост и наличието на законови предпоставки за това, дружествата от групата на ЕАИ назначават Длъжностно лице по защита на данните, което следи за законосъобразното обработване на личните данни от Дружествата от групата на ЕАИ в качеството им на Администратор и/или обработващ лични данни.

(2) Длъжностно лице по защита на данните е длъжно да:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;

2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водените регистри;

3. осъществява контрол по спазване на изискванията за защита на регистрите;

4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

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

6. специфицира техническите ресурси, прилагани за обработка на личните данни;

7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, като чрез регистрация на всички извършени действия с регистрите в компютърната среда.

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

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

10. 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. ;

11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл.27. Законният представител на съответното дружество от групата на ЕАИ определя със заповед списъка на лицата, които обработват лични данни в групата на ЕАИ. Списъците се изготвят поотделно за всеки регистър.

Чл.28. Служителите на групата на ЕАИ са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

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

3. да актуализират регистрите на личните данни (при необходимост);

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

5. 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;

Чл.29. (1) За неспазването на разпоредбите на правилата и инструкцията служителите на групата на ЕАИ носят отговорност по Закона за защита на личните данни, Кодекса на труда и др. нормативни актове.

(2) Ако в резултат на действията на съответен служител на групата на ЕАИ 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.

Чл.30. (1) Групата на ЕАИ използва програмно техническите средства за защита на личните данни.

Чл.31. (1) Право на достъп до данните в регистър „Персонал" имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане изразено писмено;

2. Ръководителите на съответното дружество - при изпълнение на правомощията им по Закона за статистиката, Кодекса на труда, Закона за държавния служител и др.

3. Обработващите и операторите на лични данни – служителите от отдел „ТРЗ", отдел „Счетоводство" и служителите от фирмата, която обслужва групата на ЕАИ със съответната програма, лица, осъществяващи технически операции по обработката и контрол на данните, адвокати.

4. 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) Данните от регистъра не се предават на трети лица.

(3) Защитата на помещенията, в които се съхраняват личните данни се постига с контролиран достъп с чип-карта, СОТ-аларма с код и ключ, видеонаблюдение.

(4) Длъжностните лица, събиращи и обработващи лични данни в регистър „Персонал" имат следните права и задължения:

1. да използват личните данни при спазване разпоредбите на Кодекса на труда, Закона за държавния служител /при възникване на трудови и служебни правоотношения/.

2. да използват личните данни изпълнение на задълженията по Закона за здравното осигуряване /ЗЗО/.

3. да не изнасят и съхраняват личните данни извън специално определените за целта места, регламентирани с режим на специален достъп;

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

(5) Право на достъп до данните в регистъра имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

2. Ръководителите - при изпълнение на правомощията им по закон.

3. Обработващите и операторите на лични данни – служителите от външната охранителна фирма, осъществяващи технически операции по обработката и контрол на данните.

4. 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.

(6) Данните от регистъра не могат да бъдат предавани по електронен път.

(7) Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

Чл. 32. (1) Право на достъп до данните в регистър „Видеонаблюдение" имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

2. Ръководителите - при изпълнение на правомощията им по закон.

3. Длъжностното лице, което поддържа регистър „Видеонаблюдение" трябва да следи за изправността на ползваната апаратура.

4. Обработващите и операторите на лични данни – служителите от външната охранителна фирма, осъществяващи технически операции по обработката и контрол на данните.

5. 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.

6. Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

(2) Данните от регистъра не могат да бъдат предавани по електронен път.

(3) Длъжностното лице, което поддържа регистър „Видеонаблюдение" трябва да следи за изправността на ползваната апаратура.

(4) Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

Чл.33. Право на достъп до данните в регистър „Деловодство" имат:

(1). Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

(2) Ръководителите - при изпълнение на правомощията им по закон.

(3) Обработващите и операторите на лични данни – служителите от отдел „ТРЗ", служителите на фирмата, която обслужва групата на ЕАИ със съответната програма и лица, осъществяващи технически операции по обработката на данните – само за определена група документи, адвокати.

(4) Данните от регистъра не се предават на трети лица.

Чл.34. Данните, съхранявани в регистър „Посетители" се предоставят на :

(1) физически лица, за които се отнасят данните;

(2) на лица, ако е предвидено в нормативен акт;

(3) на лица, обработващи личните данни.

Чл.35. Данните, съхранявани в регистър „Счетоводство" се предоставят на:

(1) физически лица, за които се отнасят данните;

(2) съответните ТД на НАП;

(3) съответните ТП на НОИ.

Чл.36. Право на достъп до данните в Регистър „Контрагенти" имат :

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

2. Ръководителите - при изпълнение на правомощията им по закон.

3. Обработващите данните лица.

4. Данните от регистъра могат да бъдат предавани по електронен път на Евростат, когато това е необходимо за производство на европейска статистическа информация.

Раздел осми

ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ОПРЕДЕЛЯНЕ НА СЪОТВЕТНО НИВО НА ЗАЩИТА

Чл.37. Оценка на въздействие е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

Чл.38. Нива на защита:

(1) За Регистър „Персонал" се определя степен на защита – „средно ниво";

(2) За Регистър „Видеонаблюдение" се определя степен на защита – „ниско ниво";

(3) Регистър „Деловодство" е определена степен на защита - „ниско ниво";

(4) Регистър „Външни посетители" се определя степен на защита – „ниско ниво";

(5) За регистър „Счетоводство" се определя „ниско ниво" на защита;

(6) За Регистър „Контрагенти" се определя степен на защита „ниско ниво";

Раздел девети

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл.39. Групата на ЕАИ е предприело мерки за защита, както технически така и организационни, а именно:

1. личните данни се съхраняват в шкафове със заключващи се устройства;

2. работата и съхранение при работата с компютърни системи е подсигурена с анти вирусни програми, пароли за достъп;

3. използване на електронен подпис.

Раздел десети

ПРОЦЕДУРА ПО РАЗРЕШАВАНЕ НА СПОРОВЕ МЕЖДУ АДМИНИСТРАТОР И СУБЕКТ НА ДАННИТЕ

Чл.40. (1) В случай на възникнал спор между Администратора и Субект на лични данни, Администраторът или упълномощено от него лице, в срок от 7 работни дни от установяване на спора отправя покана за разрешаване на спора до Субекта на адреса посочен за кореспонденция.

(2) Страните следва да разрешат спора при съблюдаване законните интереси на Субекта и на Администратора, в дух на добра воля и сътрудничество. За времето на преговорите по разрешаване на спора, страните водят протокол с отразяване на исканията, направени в процеса на преговорите и взетите решения.

(3) В случай че спорът между страните не бъде разрешен, това обстоятелство се отразява в протокола.

(4) Срокът за доброволно разрешаване на спора е 30 работни дни, считано от датата, на която са се провели първите преговори, а при правна и фактическа сложност – 45 работни дни.

(5) Постигнатото съгласие на страните за разрешаване на спора се посочва в писмено двустранно споразумение.

Раздел единадесети

ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

Чл.41. Групата на ЕАИ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от групата на ЕАИ – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/и уведомяване на съответните органи;

3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

Раздел дванадесети

СЪТРУДНИЧЕСТВО С НАДЗОРНИЯ ОРГАН

Чл.42. (1). В случаите на нарушение на правилата относно обработването, събирането и съхранението на личните данни:

1.1. В случай че Администраторът установи нарушение на сигурността на личните данни същият е длъжен да докладва на Надзорния орган в срок до 72 часа. В случай че е невъзможно спазването на срока от 72 часа, Администраторът докладва на Надзорния орган в първия възможен момент, като посочва и аргументира причините за забавеното докладване.

Задължението по предходния абзац отпада, ако са налице достатъчно и категорични данни, че нарушението на сигурността на личните данни няма да породи риск за правата и свободите на физическите лица, чиито са данните.

1.2. В уведомлението, до надзорния орган се посочва най-малко:

1.2.1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

1.2.2. посочване на името и координатите за връзка на длъжностното лице по защита на данните или на други лица, от които може да се получи повече информация;

1.2.3. описание на евентуалните последици от нарушението на сигурността на личните данни;

1.2.4. описание на предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

1.3. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

2. В случаите, когато е необходимо осъществяване на консултация с Надзорния орган Администраторът, упълномощено от него лице или длъжностното лице по защита на данните отправят писмено запитване, съдържащо:

2.1. описание на обстоятелствата, които са наложили искането за консултация;

2.2. предложения за разрешаване на въпросите по конкретното консултиране;

2.3. друга информация, релевантна за конкретната консултация.

Раздел тринадесети

ПРЕДАВАНЕ НАЛИЧНИ ДАННИ В ТРЕТИ ДЪРЖАВИ

Чл.43. (1) Предаване на лични данни на трета държава или на международна организация, се осъществява само след получаване на конкретни гаранции, че правилата за сигурността по настоящите Правила се прилагат като минимален стандарт за защита на личните данни, които подлежат на предаване.

(2) Получаването на горепосочените гаранции не е необходимо, в случай че администраторът в тази трета държава се е присъединил към настоящите Правила.

(3) Предаването на лични данни в трета държава е допустимо и когато администраторът, на който се предават е:

1. доказал, че са налице ефективни правни средства за защита на личните данни, които подлежат на предаване;

2. приел е задължителни фирмени правила, съответстващи на Регламента;

3. налице е одобрен кодекс/правила за поведение по смисъла на чл. 40 от Регламента, който се прилага от Администратора или последният е сертифициран по смисъла на Регламента.

(4) Допустимо е предаването на лични данни в трета държава и в случаите, когато надзорния орган е дал разрешение за това.

Раздел четиринадесети

ОТГОВОРНОСТИ

Чл.44. (1).За неизпълнение на задълженията по настоящите Правила и по нормативните актове, касаещи защитата на личните данни виновните лица носят, както гражданска, така и дисциплинарна отговорност.

(2) Ако в резултат от действията на съответното лице по обработване на лични данни са произтекли вреди за лицето, чиито данни се обработват или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако извършеното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Раздел петнадесети

ПРИЕМАНЕ И ИЗМЕНЕНИЕ НА НАСТОЯЩИТЕ ПРАВИЛА

Чл.45. Настоящите Правила се приемат от представляващите на всяко дружество в групата на ЕАИ. Неразделна част от Правилата са съответните декларации представляващи Приложение № 1, 2, 3 и 4.

Одобрил:

Изпълнителен директор