	„СОТ – СИГНАЛНО ОХРАНИТЕЛНА ТЕХНИКА“ ЕООД	GDPR PROC_11	ДЛЗД Мариана Николова
	ПРОЦЕДУРА ПО УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ	Лист : 1 От : 2	Издание : първо

УТВЪРЖДАВАМ
УПРАВИТЕЛ : .....
/П. Виденов/

София, 21.05.2018 г.

I. Предназначение на процедурата

Тази процедура се прилага в случай на нарушение на сигурността на личните данни съгласно член 33 от ОРЗД „Уведомяване на надзорния орган за нарушение на сигурността на личните данни“ и член 34 от ОРЗД „Съобщаване на субекта на данните за нарушение на сигурността на личните данни“.

При изпълнението на процедурата следва да се има предвид, че ОРЗД прави разлика между администратор на лични данни и обработващ лични данни. Съгласно регламента не всички организации, участващи в обработката на лични данни, носят една и съща степен на отговорност. С оглед на това, всяка организация трябва да направи преценка дали се явява администратор или обработващ по отношение на дадена дейност по обработка на лични данни, или пък съвместен администратор.

Нормативна уредба: ***Член 33 и член 34 от Общия регламент за защита на данните (ОРЗД).***

II. Задължения и роли

Всички свързани със „СОТ“ ЕООД лица (служители, контрагенти, временно наети лица или служители на трети лица) и ръководители на „СОТ“ ЕООД трябва да са запознати и да прилагат настоящата процедура в случай на нарушение на сигурността на личните данни *(Политика за провеждане на обучение GDPR.POL_02).*

Всички служители, контрагенти или временно наети лица, са длъжни да докладват на Длъжностното лице по защита на данните и на Ръководителя на отдел ИТ за всяко нарушение на сигурността на личните данни.

III. Ход на процедурата

1. Процедура по уведомяване на Администратора.

Организацията уведомява Администратора без ненужно забавяне за всяко нарушение на сигурността на личните данни или за какъвто и да било друг инцидент, свързан със сигурността на данните. Контактните данни, необходими за уведомлението, се записват във вътрешния Регистър на нарушенията. В съобщението до Администратора се посочват всички необходими подробности за осъщественото нарушение. *(Уведомление от обработващия до администратора на лични данни за нарушение на сигурността (GDPR.FORM_10).*

Администраторът изпраща потвърждение за получаване на уведомлението *(по имейл, телефон, факс и пр.)*.

2. Процедура по уведомяване на надзорния орган.

Администраторът прави преценка дали е необходимо да се уведоми надзорния орган за нарушението. Съгласно член 33, параграф 1 от ОРЗД, не е необходимо да се изпраща уведомление, ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. За целта Администраторът извършва оценка на въздействието на нарушението съгласно приетата Методология за оценка на въздействието.

Ако установи, че съществува риск за правата и свободите на субектите на данни, Администраторът уведомява надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и не по-късно от 72 часа след като е узнал за него. В случай, че уведомлението не е направено в рамките на 72 часа, Длъжностното лице по защита на данните на „СОТ“ ЕООД уведомява надзорния орган при първа възможност, като към уведомлението излага и причините за забавянето.

Уведомлението до надзорния орган трябва да съдържа следната информация:

- описание на естеството на нарушението на сигурността на личните данни;
- категориите лични данни, засегнати от нарушението;
- категориите и приблизителният брой на засегнатите субекти на данни;
- приблизителното количество на засегнатите записи на лични данни;

- имената и контактните данни на Длъжностното лице по защита на данните;
- описание на последиците от нарушението на сигурността;
- предприетите или предложените от Администратора мерки за справяне с нарушението.

Когато и доколкото не е възможно цялата необходима информация да се подаде едновременно, тя се подава поетапно без ненужно забавяне *(уведомление от администратора на лични данни до надзорния орган за нарушение на сигурността на личните данни GDPR.FORM_09).*

Контактните данни на надзорния орган се записват в Регистър на нарушенията.

Уведомлението до надзорния орган се изпраща съобразно изискваната от надзорния орган форма на комуникация.

„СОТ“ ЕООД записва информация относно потвърждението от страна на надзорния орган за получаването на уведомлението.

3. Процедура по изпращане на съобщение до субекта на данните.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субекти на данните, „СОТ“ ЕООД, без ненужно забавяне, съобщава на засегнатите субекти на данните за нарушението. *(съобщение за нарушение от администратора на лични данни до субекта на данни GDPR.FORM_11).*

Съобщението до субекта/субектите на данни съдържа същата информация, която се изпраща и до надзорния орган, а именно:

- описание на естеството на нарушението на сигурността на личните данни;
- категориите лични данни, засегнати от нарушението;
- категориите и приблизителният брой на засегнатите субекти на данни;
- приблизителното количество на засегнатите записи на лични данни;
- имената и контактните данни на Длъжностното лице по защита на данните;
- описание на последиците от нарушението на сигурността;
- предприетите или предложените от администратора мерки за справяне с нарушението.

Съгласно ОРЗД, тази информация трябва да е описана на ясен и прост език.

„СОТ“ ЕООД предприема мерки да направи личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, например чрез криптиране.

„СОТ“ ЕООД предприема последващи мерки, които да гарантират, че няма вероятност да се материализира високият риск за правата и свободите на субектите на данни.

Ако нарушението засяга голям брой субекти на данни и записи на лични данни, „СОТ“ ЕООД взема решение, основано на оценка на количеството усилия, необходими за уведомяване поотделно на всеки субект на данни и на това дали по този начин би била възпрепятствана способността на „СОТ“ ЕООД да изпрати навреме нужните съобщения. Когато тази оценка покаже, че съобщаването до голям брой субекти би довело до непропорционални усилия, Администраторът прави публично съобщение или взема друга подобна мярка, с която да гарантира, че субектите на данни ще бъдат ефективно информирани.

Ако Администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от Администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията по параграф 3 на чл. 34 от ОРЗД.

Администраторът „СОТ“ ЕООД документира в Регистър на нарушенията всички нарушения на сигурността на личните данни, като посочва отнасящите се до тях факти, последиците и предприетите мерки за смекчаване на тяхното въздействие.

IV. Регистър на изданията (ревизиите)

Дата на изготвяне/промяна	Издание	Промени, основания	Изготвил	Подпис
21.05.2018 г.	първо	Регламент (ЕС) 2016/679	М. Николова	