Подготовка на документи за предварителна проверка

по чл. 17б, ал. 1 от ЗЗЛД

Когато администратор на лични данни в заявлението за регистрация е посочил обработване на определени категории данни по чл. 5, ал. 1 от Закона за защита на личните данни (ЗЗЛД), съгласно чл. 17б, ал. 1 от ЗЗЛД Комисията за защита на личните данни (КЗЛД) задължително следва да извърши предварителна проверка преди вписване в регистъра по чл. 10, ал. 1, т. 2 от ЗЗЛД.

Предвид гореизложеното, Комисията започва производство по чл. 28, ал. 1, т. 2 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация. В тази връзка на администратора на лични данни се изпраща писмо за подготвяне и изпращане (в двуседмичен срок) до Комисията на комплект от копия на документи, заверени "Вярно с оригинала", а това са както следва:

1. Инструкция (вътрешни правила, заповед) за мерките за защита на личните данни, съгласно чл. 23, ал. 4 от ЗЗЛД и чл. 3, ал. 3 от Наредба № 1 от 7 февруари 2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (ДВ, бр. 25 от 23 март 2007 г.), цитирана в заявлението Ви за регистрация, съдържаща описание на видовете регистри, които сте заявили и мерките за защита на личните данни в тях;

В чл. 23, ал. 4 от ЗЗЛД е регламентирано, че администратора на лични данни определя с утвърдена от него инструкция (вътрешни правила, заповед) за предприетите технически и организационни мерки за защита на данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване при осъществяване на дейността си.

В същия текст е определено, че мерките за защита трябва да са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени. В тази връзка, съгласно чл. 23, ал. 5 от ЗЗЛД, Комисията определя с наредба минималното ниво на технически и организационни мерки, както и допустимия вид защита.

В "Държавен вестник", бр. 25 от 23 март 2007 г. е обнародвана Наредба № 1 от 7 февруари 2007 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (наредбата).

В чл. 5, ал. 1 от Наредбата е посочено съдържанието, което администраторът на лични данни трябва да има в предвид при изготвянето на инструкцията, а именно:

- определяне на нива на чувствителност за обработваните лични данни и препоръчителен вид на носителя на данните за трайно съхраняване (хартиен, електронен, технически);

- определяне на лицата, които отговарят за обработката на лични данни, техните права и задължения;

- списък от задължителни и препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразено вида и чувствителността на данните;

- спецификация на техническите ресурси, прилагани за обработка на личните данни;

- организационна 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 е препоръчително да се създава системен файл-дневник, достъпен само за системния администратор и лицето по защита на личните данни;

- мероприятия за защита на техническите и информационните ресурси при аварии, произшествия и бедствия (пожар, наводнение и др.);

- средства за предотвратяване на умишлено повреждане или нерегламентиран достъп до личните данни;

- ред за съхраняване и унищожаване на информационни носители;

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

- 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.

Съдържанието на инструкцията трябва да се има предвид и се описва за всеки отделен регистър с лични данни.

2. *Заповед, с която се определят служителите, обработващи личните данни;* /при наличие/

Заповед (вътрешен акт), с която се определят (поименно и/или по заемана длъжност) служители на администратора на лични данни, които ще отговарят за обработването на съответните регистри с лични данни, както и имащите достъп до тях.

3. *Доклад, съдържащ описание на:*

- *местоположение на обектите, в които ще се обработват данните;*

В свободен текст се записват местоположението (адреса) на обектите (офис, сграда), в които се обработват регистрите с лични данни.

- *начин на охрана на обектите – СОТ, ведомствена охрана и др.;*

В свободен текст се описва начина на охрана на обектите, в които ще се обработват регистрите с лични данни.

- *организация на достъпа до помещенията;*

В свободен текст се описва кой има достъп до помещенията, в които се обработват лични данни (упълномощени служители, външни лица и др.) – списък на упълномощени лица, баджове за упълномощени лица, заключване на помещенията, защитна сигнализация и охрана, алармена система, абонамент за СОД, специален вход, с цифров код, с магнитна карта, с гласов анализатор и др.

- *ограничаване на достъпа до данните;*

В свободен текст се описва предприетите мерки за ограничаване на достъпа до данните – поставени метални решетки на врати и прозорци, специализирана (еднопосочна) брава, заключване на регистрите в шкаф/каса и др.

(освен ако информацията не е отразена в Инструкцията по т. 1)

4. При обработка на личните данни чрез информационни системи, следва да представите заверено копие и доклад, съдържащ описание на:

- *компютърната мрежа;*

В свободен текст се описва изградената компютърна мрежа – комуникационен хардуер, софтуер, компютри и други устройства, свързани в една система, която позволява на група потребители да ползват заедно общи бази данни, софтуер, периферни устройства и др.

- *ограничаване на достъпа и защита на електронните данни;*

В свободен текст се описва предприетите мерки за ограничаване на достъпа до данните – дефинирани потребителски имена и пароли за достъп до операционната система и/или специализиран софтуер за обработка на данните, дефинирани права на достъп до данните, парола за отваряне на файлове, автоматична регистрация на всеки достъп, на извършени операции, на нелигитимен достъп и др. Описват се предприетите мерки за защита на електронните данни – поддържане на копие, периодично архивиране, "заключване" на файловете – "само за четене" и/или "само за запис", антивирусна защита, защитна стена, криптиране на данните и др.

- *защита при предаване на данни по електронен път;*

В свободен текст се описва предприетите мерки за защита при предаване на данните по електронен път – криптиране, електронен подпис, специализирани устройства и др.

(освен ако информацията не е отразена в Инструкцията по т. 1)