ВЪТРЕШНА ПРОЦЕДУРА

на „Арсенал“ АД за уведомяване при нарушаване на сигурността на личните данни

Настоящата процедура се прилага в случаите на нарушение на сигурността на личните данни, съгласно член 33 и член 34 от Общия регламент относно защитата на данните (ЕС) 2016/679 (GDPR).

Нарушение на сигурността на данни е налице, когато личните данни, обработвани от „Арсенал” АД, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта на личните данни. В този смисъл, нарушение на данните възниква, когато има нарушение на сигурността, водещо до инцидентно или незаконно унищожаване, загуба, изменение, нерегламентирано разкриване на данни, които се предават, съхраняват или по друг начин се обработват.

Процедурата се прилага и при постъпили указания от Комисията по защита на личните данни при обстоятелства, настъпили в случаите на пробив въпреки технологичните мерки, които дружеството е предприело за защита на сигурността на личните данни, обект на нарушението.

1. След като в съответния работник/служител на „Арсенал” АД, явяващ се длъжностно лице, обработващо личните данни под ръководството на Администратора, се породи съмнение за извършено нарушение на сигурността на личните данни, той трябва да уведоми длъжностното лице за защита на данните, което определя дали конкретното събитие представлява нарушение на лични данни и да уведоми изпълнителния директор за събитието.

2. В случай на нарушение на сигурността на личните данните, при което съществува вероятност да се породи риск за правата и свободите на физическите лица, Администраторът (чрез съответния служител), без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението Комисията за защита на личните данни.

В уведомлението се съдържа най-малко следното:

- 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;

- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

- описание на евентуалните последици от нарушението на сигурността на личните данни;

- 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.

3. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

4. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

5. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

6. В съобщението до субекта на данните се посочва най-малко следната информация:

- описание на естеството на нарушението на сигурността на личните данни;
- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- 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.

7. Администраторът уведомява всяко физическо лице за настъпилото нарушение на сигурността на личните данни в разбираема форма на прост и ясен език.

8. Съобщение до субекта на данните не се изисква ако:

- Администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях;
- Администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
- то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

9. Администраторът на лични данни 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. Тази документация дава възможност на надзорния орган да провери дали е спазен член 33 от ОРЗД.

Настоящата процедура е утвърдена от Изпълнителния директор на „Арсенал“ АД и може да се допълва и изменя по реда на нейното утвърждаване.