

ПРИЛОЖЕНИЕ №5: ПРОЦЕДУРА ЗА ИЗВЕСТЯВАНЕ ПРИ НАРУШЕНИЕ В СИГУРНОСТТА НА ДАННИТЕ

Обхват

Настоящата процедура се прилага в случай на нарушение на сигурността на личните данни съгласно член 33 и член 34 от ОРЗД. Всички служители на организацията са длъжни да бъдат запознати и да спазват настоящата процедура в случай на нарушение на сигурността на личните данни. Всички служители, изпълнители или временно нает персонал са отговорни за докладване на всяко нарушение на сигурността на личните данни на отговорното лице по защита на данните и Отдел/отговорник „Правни въпроси“.

Уведомление за нарушение от обработващ данни до администратор на данни

Организацията докладва всяко нарушение на сигурността на личните данни или инцидент, свързан със сигурността, на администратора на данни без ненужно забавяне. Информацията за нарушението се вписва в Регистъра на нарушенията в сигурността на данните („Регистъра“), като организацията предоставя на администратора цялата информация за нарушението. Уведомяването за нарушението се извършва по имейл, факс, поща и др. данни за контакт, посочени в договора с администратора. Уведомяването се извършва в писмена форма и получаването му се потвърждава от администратора в същата форма.

Уведомление за нарушение от администратор на данни до надзорен орган

Организацията, след вземането на становище от отговорното лице по защита на данните, определя дали надзорният орган трябва да бъде уведомен в случай на нарушение като преценява дали има вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на субектите на данните, засегнати от нарушението на сигурността на личните данни, като извърши оценка за въздействието върху защитата на данните.

Ако съществува вероятност за риск за субектите на данните, отговорното лице по защита на данните докладва нарушението на сигурността на личните данни на надзорния орган без ненужно забавяне и не по-късно от 72 часа. Ако уведомяването на надзорния орган за нарушение на сигурността на личните данни не бъде извършено в рамките на 72 часа, отговорното лице по защита на данните го предава по електронен път с обосновка за забавянето.

Ако не е възможно да се предостави цялата необходима информация наведнъж, отговорното лице по защитата на данните ще предостави информацията на етапи без ненужно допълнително забавяне.

Уведомление за нарушение от администратор на данни до субект на данни

Ако има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на субекта на данните, отговорното лице по защитата на данните уведомява засегнатите субекти на данни в писмена, включително електронна форма, незабавно и на ясен и прост език. Администраторът на данни впоследствие взема мерки, които гарантират, че вече няма вероятност да настъпят рискове за правата и свободите на субектите на данни.

Ако нарушението засяга голям брой субекти и техните лични данни, организацията взема решение въз основа на оценка на количеството усилия, положени за уведомяването на всеки един субект на данни поотделно, и дали то ще възпрепятства възможността и да предостави уведомлението в рамките на определения срок. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че засегнатите лица да бъдат в еднаква степен ефективно информирани.

Ако организацията не е уведомила субектите на данните и надзорният орган отчете вероятност нарушението на сигурността на личните данни да породи висок риск, отговорното лице по защита на данните ще съобщи за нарушението по гореописания ред.

Регистър на нарушенията в сигурността на личните данни

Отговорното лице по защитата на данните документира всяко нарушение в сигурността на личните данни. Нарушенията се документират като бъдат вписани в Регистъра на нарушенията в сигурността на личните данни, воден във всяка организация. Регистърът по-специално включва следната информация:

- a. категориите засегнати лични данни;
- b. приблизителният брой на засегнатите субекти на данни;
- c. приблизителното количество на засегнатите лични данни.
- d. името и координатите за връзка на длъжностното лице по защита на данните;
- e. последиците от нарушението;
- f. всички предприети мерки за справяне с нарушението;
- g. всякаква информация, свързана с нарушението на сигурността на данните.
- h. в случай че надзорният орган определи конкретен контакт във връзка с нарушение, тази информация също ще бъде отразена в Регистъра.