БЪЛГАРСКА АСОЦИАЦИЯ НА УПРАВЛЕНСКИТЕ КОНСУЛТАНТСКИ ОРГАНИЗАЦИИ
пл. „Славейков“ 6, етаж 2, 1000 София, България
bamco@bamco.bg, bamco.bg

Процедура за управление на инциденти

Съдържание

1. Обхват, предназначение и ползватели

Тази процедура предоставя общи принципи и модели за подходи, които да намалят негативния ефект при нарушаване на сигурността на личните данни ("нарушаване на сигурността") при едно или и двете от следните обстоятелства:

- Личните данни идентифицират субектите на данни, които са жители на държавите-членки на Европейския съюз (ЕС) и страните в Европейското икономическо пространство (ЕИП), независимо от това къде тези данни подлежат на глобална обработка и
- Личните данни подлежат на обработка в ЕС и/или ЕИП, независимо от страната на пребиваване на субекта на данните.

Процедурата определя общите принципи и действия за успешно управление на реакцията при нарушението на сигурността, както и изпълнението на задълженията, свързани с уведомяването на надзорните органи и физическите лица, както се изисква от GDPR.

Всички служители, членове, контрагенти, и трети лица (доставчици), които работят или действат от името на БАУКО, трябва да са наясно и да следват тази процедура, в случай на нарушаване на неприкосновеността на личните данни.

2. Свързани нормативни и вътрешни актове

- EU GDPR 2016/679 (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО)
- Закон за защита на личните данни
- Насоки/Методически указания на Комисията за защита на личните данни
- Политика за защита на личните данни
- Политика за съхранение на личните данни

3. Определения

- „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); 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;
- „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;
- „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;
- „регистър с лични данни“ означава 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;
- „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;
- „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;
- „получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

- „трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;
- „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;
- „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;
- „генетични данни“ означава 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;
- „биометрични данни“ означава 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;
- „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;

4. Отговорно лице за реакция в случаи на инциденти

Координатор на БАУКО отговаря за реагиране при нарушаване на сигурността на личните данни.

Тя може да избере да добави допълнителни нарочни специалисти за целите на справянето с конкретно нарушение на личните данни.

5. Идентификация на инцидент и задължения за реакция

Инцидент, свързан с нарушаване на неприконсновеността на данните може да бъде кражба или загуба на носител на данни, влизане с взлом в помещенията на БАУКО, хакерска атака, неправомерно разкриване на данните на трети лица и други. Изброяването е примерно.

След като бъде съобщено на координатор на БАУКО или установено лично от нея, нарушение на неприкосновеността на личните данни, тя трябва да направи следното:

- Валидиране/отсяване на нарушението на сигурността на личните данни;
- Гарантиране, че адекватно и безпристрастно разследване (включително полицейско, при необходимост) е инициирано, проведено, документирано и приключено;
- Предприемане на мерки и преглед на предприетите корективи действия;
- Докладване констатациите на координатор на БАУКО;
- Ако е необходимо – в срок до 72 часа, докладване на Комисията за защита на личните данни.
- Координиране на вътрешните и външните комуникации
- Да се увери, че засегнатите субекти на данни са коректно уведомени, когато това се изисква.
- Координатор на БАУКО води регистър за всеки инцидент, свързан със сигурността на личните данни, който съдържа : дата на възникване, дата на установяване, описание на инцидента, на настъпилите последици, евентуално вреди и предприетите коректривни действия.

6. Процес за реакция при нарушение на сигурността на личните данни

Процесът на реакция при нарушаване на данните се инициира, когато някой, който забелязва, че възникне предполагаемо/съмнително или действително нарушение на лични данни, и уведоми координатор на БАУКО за отговор при нарушаване на данните. Комисията е отговорна да определи дали нарушението трябва да се счита за нарушение, засягащо личните данни.

Координатор на БАУКО е отговорна за документирането на всички решения. Тъй като тези документи могат да бъдат преразгледани от надзорните органи, те трябва да бъдат написани много точно и задълбочено, за да се осигури проследяемост и отчетност.

7. Уведомление за нарушение на личните данни: Обработващ към Администратор

Когато нарушаването на личните данни или предполагаемото нарушаване на данните засяга личните данни, които се обработват от името на БАУКО от трета страна, лице определено от организацията, действаща като обработващ лични данни, трябва да докладва нарушението на личните данни на координатор на БАУКО без неоправдано забавяне, в срок до 48 часа от узнаването.

Лице, определено от обработващия лични данни ще изпрати уведомление до администратора БАУКО, което ще включва следното:

- Описание на вида нарушение
- Категориите на засегнатите лични данни
- Приблизителен брой засегнати субекти на данни
- Име и данни за контакт на ръководителя на екипа за отговор при нарушения на данните/ДЛЗД
- Последиците от нарушението на личните данни
- Предприети мерки за справяне с нарушаването на личните данни
- Всяка информация, свързана с нарушаване на данните

Координатор на БАУКО ще регистрира нарушението на данните в регистъра за нарушаване на данните.

8. Уведомление за нарушение на личните данни: Администратор към надзорен орган

Когато нарушаването на личните данни или предполагаемото нарушаване на данните засягат личните данни, които се обработват от БАУКО като администратор на данни, от координатор на БАУКО се изпълняват следните действия:

1) Сдружението трябва да установи дали нарушението на личните данни трябва да бъде докладвано на надзорния орган.
2) За да се установи риска за правата и свободите на засегнатото/ите физическо/и лице/а, комисията трябва да извърши оценка последиците, засегнати от нарушението на данните.
3) Ако нарушаването на личните данни няма вероятност да доведе до риск за правата и свободите на засегнатите субекти на данни, не се изисква известие. Независимо от това, нарушението на данните трябва да бъде записано в регистъра за нарушаване на данните.
4) Надзорният орган трябва да бъде уведомен без неоправдано забавяне, но не по-късно от 72 часа от узнаването, ако нарушаването на личните данни може да доведе до риск за правата и свободите на субектите на данни, засегнати от нарушението на личните данни. Всички възможни причини за забавяне над 72 часа трябва да бъдат съобщени на надзорния орган.

Определен от председателя на УС координатор е длъжен да изпрати уведомления до надзорния орган, които ще включват следното:

- Описание на вида нарушение
- Категориите на засегнатите лични данни
- Приблизителен брой засегнати субекти на данни
- Име и данни за контакт на ръководителя на екипа за отговор при нарушения на данните или друго отговорно лице
- Последиците от нарушението на личните данни
- Предприети мерки за справяне с нарушаването на личните данни
- Всяка информация, свързана с нарушаване на данните

9. Уведомление за нарушение на личните данни: Администратор към субект на данни

Управителният съвет трябва да прецени дали нарушаването на личните данни е вероятно да доведе до висок риск за правата и свободите на субекта на данните. Ако отговорът е "да", координатор на БАУКО трябва да уведоми заинтересованите физически лица без ненужно закъснение.

Уведомлението на субектите на данните трябва да бъде написано на точен и ясен език и трябва да съдържа същата информация, посочена в раздел 8.

Ако поради броя на засегнатите субекти на данни е прекалено трудно да се уведоми всеки засегнат субект на данни, Комисията трябва да предприеме необходимите мерки, за да гарантира, че засегнатите субекти на данни са уведомени, като използват подходящи обществени канали.

10. Отговорност

Сдружението носи юридическа отговорност за нарушенията на тази политика и действащото законодателство в областта на защита на личните данни.

11. Влизане в сила и актуализация

Този документ влиза в сила от датата на утвърждаването му от Управителния съвет на БАУКО.