ПРОГРАМА

I. Модул: Правни аспекти

1. Общи понятия

Преглед на българското законодателство и подзаконова уредба за защита на данните. Новите моменти в GDPR

- Права на субекта на данни, уведомяване за нарушения, кодекси за поведение
- Ролята на надзорния орган и на надзорния съвет
- Обработка, съгласие, легитимен интерес
- Международни трансфери на данни
- Нарушения и наказания

2. Искания за достъп

Характеристики и дефиниции на заявката за достъп до информация. Как да се отговори на искането, какви задължения има DPO и как да реагира ефективно?

- Заявка за достъп до информация – (Subject Access Request -SAR)
- Обработка, изключения на SAR
- Даване на достъп
- Преносимост на данните и тяхното въздействие върху SAR
- Предизвикателства и най-добри практики

II. Модул: Технически аспекти

3. Оценка на въздействието върху защитата на данните (Data Protection Impact Assessment - DPIA) – чл.35

Разработване и прилагане на оценка на въздействието, известен също като "Оценка на въздействието върху защитата на данните".Наблюдение на резултатите и предприемане на коригиращи действия, ако е необходимо.

Как да идентифицираме предварително проблемите? Превенция и намаляване разходите и потенциални щети при пробив.

- Разлика между риск и криза
- Профилиране на данни, анонимизация, псевдонимизация
- Въздействие на защитата на данните като изискване за GDPR
- Защо се изискват DPIAs
- Процесът на DPIA - Провеждане на DPIA
- Анализ на инструментите за DPIA
- Подход, базиран на риска
- Наблюдение на резултатите и отговор на риска
- Разходи за несъответствие

4. Управление на пробив в информационната система и нарушение на сигурността на личните данни (Data Breach)

Пробивите в системите за сигурност е все по-често срещани. Вероятността вашата организация да претърпи атака, която да доведе до такъв пробив и изтичане данните се увеличава непрестанно Изграждането на система за информационна сигурност е инвестиция в бъдещата сигурност на данните и репутацията на организацията ви. Тук ще се разгледат основните фактори, които могат да доведат до пробив и изтичане данните и процедурата, която трябва да бъде изработена и следване в подобен случай.

- Приемане на вътрешна процедура и/или план за действие в случай на нарушение на сигурността на личните данни.
- Определяне на отговорен служител/екип за реакция при нарушение на сигурността на личните данни, инструктаж на персонала, др.
- Създаване на вътрешна организация за своевременно уведомяване на КЗЛД в срок до 72 часа от узнаването за нарушението.
- Съобщаване на субекта на данните за нарушение на сигурността на личните данни

III. Модул: Практически познания

5. Одит за защита на данните

Способността да проведем свои собствени одити за защита на данните е безценно умение, което гарантирате, че вашата организация отговаря на законовите изисквания.
Ще се разгледат областите, които трябва редовно да бъдат наблюдавани и подготовка и готовност в случай на одит от Службата по надзор.

- Извършване Одит на данни по GDPR
- Одит на данни и управление на риска
- Одити за защита на данните: вътрешни, външни и регулаторни
- Инструменти за одит на данни
- Процесът на одит на данни
- Сертификация за защита на данните
- Най-добри практики

6. Практически насоки. Документи по управление на лични данни и отчетност

- Създаване и редовно актуализиране на вътрешен регистър на дейностите по обработване на лични данни
- Приемане на вътрешна инструкция/правила/процедури/политика за защита на личните данни
- Преглед и актуализиране на договореностите с обработващите лични данни с цел включване в тях на всички задължителни реквизити съгласно чл. 28
- Преглед и актуализиране на декларациите или другите форми за документиране на съгласието на субекта на данните, когато съгласието на субекта на данните е единственото правно основание за обработване с цел привеждането му в съответствие с изискванията на чл. 4, пар. 11
- Преглед и актуализиране на правното основание за предаване (трансфер) на данни към получатели в трети страни.
- Управление на архивите. Регулаторни и законодателни изисквания
- Електронна система за управление на документи
- Съхранение на електронни документи и документи на хартиен носител
- Отчетност и управление на записите
- Най-добри практики

Организиран от:

Център за правни изследвания към УНСС

Алианс за защита на личните данни

Адрес: 1700 София, Студентски град "Хр. Ботев", УНСС

Тел. +359 898712668