Общ регламент относно защита на личните данни

(General Data Protection Regulation, или GDPR)

GDPR основни аспекти

1. Какво е GDPR и кого засяга?
2. Какво са лични данни?
3. Елементи на личните данни
4. Глоби
5. Роли в защитата на лични данни
6. Длъжностно лице по защита на лични данни
7. Основания за събиране и обработка на лични данни
8. Права на физическите лица във връзка с обработката на лични данни
9. Уведомления за поверителност
10. Какво предприе ИЗИРА?
11. Класификация на информацията и препоръки
12. Сигурност на информацията – ИТ и административни мерки
13. Уведомление при пробив във сигурността
14. Въпроси и отговори ?!

Какво е GDPR и кого засяга?

Общият регламент за защита на личните данни (Регламент 2016/679 - General Data Protection Regulation или GDPR) е ново законодателство на Европейския съюз, което задължава фирмите и институциите да спазват определени правила и процеси, когато събират, съхраняват и обработват информация за физически лица.

- Последните правила на ЕС за подобен тип информация са от средата на 90-те години, далеч преди развитието на онлайн търговията, социалните мрежи и анализите на големи масиви с данни.

- Регламентът унифицира политиката по този въпрос във всички 28 страни членки, което улеснява международните компании - те ще следват един стандарт в блока.

- GDPR влиза в сила на 25 май 2018 Chart

Какво са лични данни?

- **Обикновени лични данни** е широк термин, който включва: име, снимка, имейл адрес, банкови данни, публикации в социални мрежи, медицинска информация, дори и компютърен IP адрес. Такива са данните, чрез които едно лице може да бъде идентифицирано, като име, пол, възраст, ЕГН, имейл, снимка, банкови данни, IP адрес и др.

- **Чувствителните лични данни** са определени категории данни, които се ползват с по-високо ниво на защита. Такива са данните за здравето, биометрични данни, данни отнасящи се до расов или етнически произход, политически възгледи и др.

Елементи на личните данни

1. Общи елементи

1) Име
2) Пол
3) Възраст и дата на раждане
4) Семеен статус
5) Гражданство
6) Език
7) Статус на ветеран
8) Статус на неравностойно положение
9) IP адрес

2. Организационни елементи

1) Служебен/ Личен адрес
2) Служебен/ Личен телефонен номер
3) Служебен/ Личен и-мейл адрес
4) Идентификационни номера за служебни цели
5) Идентификационен номер издаден от властите
6) Информация за потвърждаване на самоличността

GDPR предвижда съществени наказания:

- до 20 млн. евро;
- 4 на сто от световния оборот на компанията, ако се установят несъответствия;
- Право на субекта на данните да търси обезщетение по съдебен път.

1. Субект

2. Администратор

3. Обработващ

4. Контролиращ орган

Има консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията на ИЗИРА и повишаването на осведомеността и обучението на персонала.

Лицето по защита на личните има следните задължения:

• Да информира и съветва ИЗИРА, обработващия лични данни и служителите, които извършват обработване;

• Да наблюдава спазването на правилата за защита на личните данни;

• Да си сътрудничи с надзорния орган;

• Да действа като точка за контакт за надзорния орган.

GDPR регламентира следните права на субекта на данни:

- Право на информация;
- Право да възрази;
- Право да ограничи достъпа до данни;
- Право да поправи данните си;
- Право на преносимост в машинно четим формат;
- Право да бъде забравен – данните му да бъдат изтрити;
- Право на претенции за обезщетение.

ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ

Принцип на прозрачността

- ✓ Четлива и лесно достъпна форма
- ✓ Ясен и опростен изказ
- ✓ Краткост
- ✓ Визуализация
- ✓ Безплатно

Какво предприе ИЗИРА?

ИЗИРА
ЗАСТРАХОВАТЕЛЕН БРОКЕР

• Изира сформира проект на групово и местно ниво;

• Идентифицира източниците, движението и крайните получатели на данни във всички процеси и ги описа;

• Идентифицира пропуските;

• Създава новите процеси, свързани с регламента;

• Променя и създава политики и стандарти

• Въвежда стандарт за класификация на информацията;

• Актуализира политиката за сигурност на информацията;

• Създаде политика за реакция при изтичане на информация.

• Създава регистри;

• Актуализира договори с посредници, доставчици, служители;

• Регламентира нови потребителски права в системите;

• Променя политиката за пароли за достъп;

• Подобрява сигурността в системите и крайните устройства;

• Провежда обучения;

• Ще има ДЛЗЛД от 25 май;

• Ще следи за прилагане на регламента.

Класификация на данните-стандарт

Стандартът за класификация на данните касае цялата електронна и хартиена документация на ИЗИРА, а не само личните данни:

- ел. писма
- документи – на хартия и електронни
- вербална, визуална и споделена

Класове на конфиденциалност:

- Публична информация – публикации в пресата, маркетинг брошури, публични уебсайтове
- Информация за вътрешно ползване – вътрени протоколи от проведени срещи, записки на хартия или в ел. вариант, кореспонденция, която не съдържа „чувствителни данни“
- Поверителна – информация, съдържаща чувстителна информация: здравен статус, пароли, информация за деца и техния здравен статус
- Строго поверителна – бизнес данни, които не са публикувани и не са публични, бизнес стратегии

• Публична информация – няма специални препоръки

• Информация за вътрешно ползване – Ел. файлове се съхраняват само на места посочени в инструкции от ИТ. Хартията се съхранява в незаключени шкафове.Трябва да се предприемат мерки да няма изтичане на информация. Унищожаването се извършва с шредери. Ел. данни се унищожават съгласно процедура и със знанието и съдействието на ИТ Дирекция. Е-майл кореспонденцията се изтрива.

• Поверителна информация, съдържаща чувствителна информация: здравен статус, пароли, информация за деца и техния здравен статус - Данните се съхраняват на криптирани устройства, когато са в ел. вариант и се изпращат криптирани по мейл. Физическите документи се съхраняват в заключени контейнери. Унищожаването се извършва съгласно процедура и е придружено с документация. ЦУ е информирано за тези действия.

• Строго поверителна – данните се съхраняват и разпространяват при необходимост само в криптиран вариант.

ПОЛИТИКА ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

ИТ МЕРКИ

АДМИНИСТРАТИВНИ МЕРКИ

И
Т

–

М
Е
Р
К
И

• Въвеждат се нови правила за употреба на пароли

• Нови правила за работа с мобилни устройства

• Правила за употреба на USB устройства и друга медия

• Правила за боравене, съхранение и унищожение на информация на ел. носители

• Нови правила за принтиране и сканиране на документи

• Обозначаване на документите, съобразно класификацията им

• Унищижаване, изтриване на данни

• Криптиране

• Кореспонденция по ел. Поща

• Работни сесии на работната станция, информационните системи

• Пароли и др. поверителна информация на екран, записка и ползване на „гръбчета“

• Интернет и социални мрежи

• Неодобрен софтуер

• Вируси и контрол

• Работа от дома и дистанционен достъп

А
д
м
и
н
и

• Въвеждат се нови правила за работа с документи на хартия и тяхната класификация;

• Правила за боравене, съхранение и унищожение на информация на хартия;

• Нови образци на документи;

• Политика на „чистото бюро“;

• Вербална комуникация;

• Контрол на достъпа;

• Грижа за техниката и мобилните устройства.

У
в
е
д
о
м
л
е
н

Докладван сигнал за изтичане на лични данни:

- по и-мейл
- уеб сайт
- офис, точка на продажба
- телефон
- кол център

Стъпки:

- Попълване на уведомление на докладващия, с точно описание на пробива
- Изпращане на уведомлението до длъжностно лице по защита на данните
- ИЗИРА изпраща уведомление до контролиращия орган в рамките на 72 часа
- ИЗИРА информира засегнатите субекти на данни
- ИЗИРА предприема мерки за обезопасяване
- Провеждане на разследване

В
Ъ
П
Р
О
С
И

И

?