Финансирано от Европейския съюз
NextGenerationEU

4.2. Защита на личните данни и поверителност

МУЛТИМЕДИЕН ТЕКСТ (ПОМАГАЛО) ТИП ЛЕКЦИЯ (УЧЕБНИК)/
БЕЗОПАСТНОСТ – БАЗОВО НИВО

ЩЕ НАУЧИТЕ:

- Да разпознавате своите лични данни.
- Да разпознавате потенциални рискове и заплахи свързани с личните данни.
- Да познавате базови концепции за GDPR и правилата за защита и управление на личните данни.

НОВИ ПОНЯТИЯ:

Понятие	Описание
Лични данни	Всяка информация, която може да бъде използвана за идентифицирането Ви.
Рискове свързани с личните данни	Опасности и заплахи, които могат да възникнат при злоупотреба с лични данни.

Финансирано от
Европейския съюз
NextGenerationEU

Съдържание

1 Лични данни

Лични данни са всяка информация, която може да бъде използвана за идентифицирането Ви и може да съществува, както, когато не сте свързани в мрежата - офлайн, така и, когато сте свързани - онлайн.

- Офлайн идентичност – това е личността от реалния живот, която представяте ежедневно у дома, в училище или на работа. В резултат, семейството и приятелите знаят подробности за личния Ви живот, включително пълното ви име, възраст и адрес.
- Онлайн идентичност - кой сте Вие и как се представяте пред другите онлайн. Това не е просто Вашето име, а също включва потребителското име или псевдонима, който използвате за вашите онлайн профили, както и социалната идентичност, която установявате и представяте в онлайн общности и уебсайтове.

Личните данни описват всяка информация за вас, като пример това могат да бъдат включително:

- Вашето име;
- Единен граждански номер (ЕГН);
- Дата и място на раждане;
- Адрес;
- Телефонен (мобилен) номер;
- Електронна поща (Email);
- Номер на лична карта;
- Номер на шофьорска книжка;
- Ученически/Факултетен номер;
- Информация за здравето;
- Потребителски имена;
- Пароли;
- Моминското име на майка Ви;
- Снимки или съобщения, които обменяте със семейството и приятелите.

Личните данни могат да бъдат записани още в:

- Образователни записи.

  Тези записи съдържат информация за вашите академични квалификации, оценки и постижения. Може също да включват й Вашата информация за контакт, записи за присъствие, дисциплинарни доклади, здравни и имунизационни записи, както и всякакви специални образователни записи, включително индивидуализирани образователни програми.

- Трудови и финансови досиета.

  Вашите финансови записи може да включват информация за вашите приходи и разходи. Вашата трудова документация може да включва чекове от заплати, извлечения от кредитни карти, кредитен рейтинг и данни за вашата банкова сметка.

- Медицинска документация.

Всеки път, когато посещавате лекар, лична информация относно вашето физическо и психическо здраве и благополучие се добавя към Вашите електронни здравни досиета.

Много фитнес гривни/часовници и други подобни умни устройства събират големи количества клинични данни, като Вашия пулс, кръвно налягане и нива на кръвна захар, които могат да се считат също за данни, които са част от медицинските Ви досиета.

- Данни, въведени в сайтове или системи, които използвате.

  Това включва всички лични данни, с които се регистрирате и идентифицирате в различни онлайн страници, социални медии и приложения или пък офлайн – в различни институции.

2 Потенциални рискове и заплахи

2.1 Знаете ли къде се съхраняват Вашите лични данни?

Най-често личните Ви данни се прехвърлят, съхраняват и показват чрез облака.

Често личните Ви данни се споделят с трети лица или се продават на компании с цел реклама или изграждане на Вашия покупателен профил.

Пример: Картите за лоялност в магазините, които са удобен начин да спестите пари от покупките си. Магазинът обаче използва тази карта, за да изгради профил на Вашето покупателно поведение, което може да се използва, за да Ви се изпращат специални оферти от различни маркетингови партньори.

Какво става, когато споделите със своите близки, приятели или колеги лична информация онлайн, например снимки.

Споделяйки с други, данните, които първоначално са били на Вашето мобилно устройство или персонален компютър, могат да бъдат споделени с непознати за Вас хора, който са познати на Вашите познати и който от своя страна си ги копират, свалят на техните устройства или споделят с техни приятели и познати.

В такива случаи Вашите лични данни излизат извън границите на конкретна организация или устройство, което е било под Ваш контрол.

2.2 С каква цел се злоупотребява с лични данни?

Личните Ви данни, т.е. Вашата чувствителна информация, може да бъде използвана от злонамерени лица с цел:

- Кражба на самоличност
  - Да се представят за Вас, нарушавайки поверителността Ви и потенциално причинявайки сериозни щети на репутацията Ви.
  - Да се възползват от облаги, който Вие използвате.
- Кражба или унищожение на чувствителна информация.
- Финансови злоупотреби (получаване на пари или изтегляне на заеми).

- Искане на откуп.

2.3 Как/от къде хакерите могат да получат достъп до Вашите данни?

- От лично споделена чувствителна информация за Вас.
- От не защитени или не достатъчно добре защитени онлайн споделени данни.
- Чрез имейл пощата – при отваряне на писма от непознат или при фишинг (phishing).
- Неправилна поддръжка и конфигурация на устройствата, които използвате.

2.4 Кой друг се интересува от Вашата онлайн самоличност?

- Вашият интернет доставчик.
  - Проследява онлайн активността Ви, дори биха могли да продават тези данни на рекламодатели с цел печалба.
  - При определени обстоятелства интернет доставчиците може да са задължени по закон да споделят Вашата информация с правителствени агенции за наблюдение или органи.
- Рекламодатели.
  - Целева реклама - Рекламодателите наблюдават и проследяват вашите онлайн дейности като навици за пазаруване и лични предпочитания и Ви изпращат насочени реклами.
- Търсачки и платформи за социални медии.
  - Тези платформи събират информация за Вашия пол, геолокация, телефонен номер, политически и религиозни идеологии въз основа на Вашата история на търсене и онлайн самоличност. След това тази информация се продава на рекламодатели за печалба.
- Уеб страниците, които посещавате.
  - Уебсайтовете използват бисквитки (cookies), за да проследяват вашите дейности и предоставят по-персонализирано съдържание. Това оставя следа от данни, която е свързана с вашата онлайн самоличност, която често може да се окаже в ръцете на рекламодатели!

3 Базови концепции за GDPR

3.1 Какво представлява General Data Protection Regulation (Регламент (ЕС) 2016/679, GDPR)?

- Общ регламент (задължителни правила) за защита на данните на физическите лица, който обединява законите за поверителност на данните в целия Европейски съюз (ЕС).
- Регламентът е одобрен от Европейския парламент на 14 Април 2016 г. и неговото прилагане влиза в сила от 25 май 2018 г.
- Прилага се за всички организации, които обработват и съхраняват лични данни.

- Предоставя правна рамка за запазване на личните данни на всеки, като изисква от компаниите да разполагат със стабилни процеси за обработка и съхранение на лична информация.
- Определя правилата по отношение на свободното движение на лични данни в рамките на Европейския съюз.
- Предоставя на хората по-голям контрол върху личната им информация, всеки има право да даде съгласие за обработване на личните му данни за една или повече конкретни цели, както и по всяко време да оттегли това си съгласие.

3.2 Принципи, свързани с обработването на лични данни

Според GDPR, се спазват принципите, свързани с обработването на личните данни. Някои по-важни са:

- Обработват се законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните (физическото лице, на което са данните), т.е трябва да бъдете информирани какво да очаквате, когато обработват Вашите лични данни.
- Събирани са за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.
- Подходящи, свързани с и ограничени до необходимото, във връзка с целите, за които се обработват (това осигурява „свеждане на данните до минимум“).
- Точни и при необходимост да бъдат поддържани в актуален вид.
- Съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.
- Обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки (гарантира се „цялостност и поверителност“).

Администраторът на данни (обработващият лични данни) определя целите и средствата за обработването на лични данни, носи отговорност и е в състояние да докаже спазването на принципите (осигуряване на „отчетност“).

3.3 Защита и управление на личните данни

Какво е киберсигурност?

Киберсигурността е непрекъснатото усилие за защита на лица, организации и правителства от цифрови атаки чрез защита на мрежови системи и данни от неоторизирано използване или увреждане.

Нива на защита основно са три:

- Лично ниво - трябва да защитите Вашата самоличност, Вашите данни и Вашите компютърни устройства.
- Организационно ниво - отговорност на всеки да защитава репутацията, данните и клиентите на дадена организация.

- Правителствено ниво - цифровата информация се събира и споделя, така нейната защита става още по-важна на правителствено ниво, където националната сигурност, икономическата стабилност и безопасността и благосъстоянието на гражданите са застрашени.

3.3.1 Правила за защита и управление на личните данни

За да предпазите личните си данни от злонамерени действия, добре е да познавате определени правила:

- Споделяйте личните си данни само с познати хора или при необходимост.
- Не споделяйте повече лични данни от необходимото.
- Винаги се интересувайте ЗАЩО искат Вашите лични данни и ИМАТ ЛИ ПРАВО да ги искат. Не предоставяйте личните си данни без предварително да сте наясно кой и с каква цел ги изисква.
- Винаги бъдете бдителни, когато предоставяте лична информация електронно – в уеб сайтове, през електронна поща или в социални медии.
- Не разпространявайте чужди лични данни, без разрешение или без необходимост.
- Не запазвайте паролите си за потребителски профили в браузърите на никакви устройства, особено на обществени такива.
- Заключвайте електронните си устройства по сигурен начин (код, сложна парола или пръстов отпечатък), за да не могат други хора да ги използват без Вашето съгласие.
- Проверявайте редовно кредитните си отчети и незабавно докладвайте всяка невярна информация, като молби за кредит, които не сте инициирали или покупки с вашите кредитни карти, които не сте направили.

3.3.2 Основни правила за защита на Вашата онлайн самоличност

Вашата онлайн самоличност също трябва да бъде защитена. Основните правила най-често са свързани с потребителското Ви име и паролата, която ползвате за вход.

Потребителско име – При избора на потребителско име за Вашия профил, е важно да не разкривате лична информация. Трябва да е нещо подходящо и уважително, но без да подсказва директно кой сте Вие, тъй като това може да Ви направи лесна мишена за киберпрестъпления или да привлече нежелано внимание.

Съвети, които да ви помогнат да генерирате Вашето потребителско име:

- Не използвайте пълното си име или части от адреса или телефонния си номер.
- Не използвайте потребителското си име, което използвате за имейл (електронна поща).
- Не използвайте една и съща комбинация от потребителско име и парола, особено при финансови сметки. Ако го направите, това Ви прави по-лесни за проследяване.
- Не избирайте потребителско име, което дава указания за вашите пароли, като поредица от цифри/букви или първата част на фраза от две части или отдела, в който работите (например: Ако отделът е Информационни технологии, популярно съкращение е - ИТ).
- Изберете потребителско име, което е подходящо за типа акаунт, т.е. личен, социален или бизнес.

Парола – При избора на парола, тя също не трябва да съдържа лична информация, което би довело до лесното й разгадаване. Препоръки са:

- Съставяйте сложни пароли и не ги споделяйте с никого. Сложните пароли се състоят от повече на брой символи, включват комбинация от големи и малки букви, цифри, служебни символи).
- Не използвайте едни и същи пароли за различните си профили и в различни уеб сайтове и системи.

Електронна поща - Друго свързано с онлайн самоличността Ви е, защитата на електронната Ви поща.

Правила за защита на електронната Ви поща по подходящ и сигурен начин, са:

- Добре изберете потребителското.
- Съставете силна парола.
- Използвайте двуфакторна автентикация (удостоверяване) – втори метод за удостоверяване, че сте Вие, чрез изпращане на кратко съобщение (SMS) до мобилния Ви телефон или чрез потвърдителен имейл на друга Ваша електронна поща.
- Бъдете бдителни към съобщенията, които получавате и не отговаряйте на съмнителни такива.

Подобни са правилата за различните системи, които използвате - профили към търговци в Интернет, социални мрежи и устройствата, който използвате.

4 Рисково поведение с лични данни

За успешното предпазване от потенциалните рискове и заплахи, трябва да се познава, т.нар. рисково поведение или това са индикаторите, които показват, че има нещо нередно/рисково. Една от най-честите измами с лични данни е фишинг.

Индикатори за фишинг (phishing) измама:

Електронна поща

- Неофициални имейл адреси на организации или непознат изпращач.
- Общи поздрави или липса на такива, т.е. не е лично обръщение към Вас.
- Правописни/пунктуационни грешки, лош език.
- Приканване за изпращане на лична информация и заплахи, в случай, че не го направите.
- Подвеждащи хипервръзки към непознати уеб страници или чрез изображения.

Фалшиви уеб сайтове

- Най-често URL адресът на сайта, не отговаря на името му.
- Логото прилича, но има различия в детайлите или е поставено на не обичайно място.
- Обикновено Ви предлагат да подобрят нещо за Вас, ако изпратите определени данни и присъства предупреждение какво ще се случаи, ако не го направите.

Друг индикатор е свързан с

Нежелана поща (спам, spam) – получаване на прекомерно количество съобщения с рекламно съдържание.

За нарушение на правата Ви, свързани с лични данни, се грижи Комисията за защита на личните данни (КЗЛД).

5 Използвани източници

- Данни, обхванати от правилата на ЕС за защита на данните, включително име, имейл, IP адрес и здравна информация. - https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_bg
- General Data Protection Regulation (GDPR) – Official Legal Text - https://gdpr-info.eu/
- GDPR Summary - https://www.gdprsummary.com
- Член 5. Принципи, свързани с обработването на лични данни | GDPR made searchable by Algolia. Chapters, articles and recitals easily readable - https://gdpr.algolia.com/bg/gdpr-article-5
- Полезна информация – КЗЛД - https://www.cpdp.bg/index.php?p=rubric&aid=54
- Защита на личните данни - http://www.daskalo.com/oubotevpirne/files/2021/10/Защита-на-личните-данни-презентация-кампания.pdf
- „Free online tech courses backed by Cisco's expertise and connected to real career paths. Discover your future today.“ - https://skillsforall.com/
- Ways to Recognize a Phishing Email: Email Phishing Examples - https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email