

ЗАЩИТА НА ЛИЧНИ ДАННИ

Основна идея: Личните данни трябва да се събират, използват и споделят само при ясна цел, с необходимото съгласие и с подходящи мерки за защита.

1. Какво са лични данни?

Лични данни са всяка информация, която се отнася до определен човек и позволява той да бъде разпознат пряко или косвено. Това включва не само име и ЕГН, но и онлайн идентификатори, местоположение, снимки, глас, здравни и финансови данни.

КАКВО СА ЛИЧНИ ДАННИ?

Лични данни са всяка информация, чрез която човек може да бъде разпознат **пряко или косвено**.

**Идентификационни**

Данни, които директно идентифицират човек.

Примери:

- име, фамилия
- ЕГН, дата на раждане
- лична карта, паспорт
- снимка

**Контактни**

Данни, чрез които може да се свържете с човек.

Примери:

- адрес (домашен)
- телефонен номер
- e-mail адрес

**Онлайн данни**

Данни, свързани с онлайн активността.

Примери:

- IP адрес
- потребителски профили
- идентификатори (напр. cookie ID, device ID)

**Финансови**

Данни, свързани с финансовото състояние.

Примери:

- банкова сметка / IBAN
- данни от платежна карта
- доходи, плащания
- кредитна история

**Здравни**

Данни за физическото и психическото здраве.

Примери:

- диагнози
- медицински изследвания
- лечение, предписани лекарства
- информация от болнични досиета

**Биометрични**

Уникални физически характеристики.

Примери:

- лице (разпознаване на лице)
- пръстов отпечатък
- ирис на окото, ретина
- гласов отпечатък

**ПРАВИЛО:** събирайте и споделяйте само данните, които са действително необходими за конкретната цел, и ги пазете сигурно.

2. Нормативна защита на личните данни

Работата с лични данни е подчинена на правила, които защитават правата на хората и ограничават неправомерното събиране и използване на информация.

Документ / правило	Какво защитава	Практически смисъл
GDPR	личните данни на гражданите	данните се обработват законосъобразно, прозрачно и само за конкретна цел
Закон за защита на личните данни	правата на физическите лица	определя националните правила и контрола
Закон за авторското право	произведения и съдържание	чужди текстове, снимки, музика и програми не се използват без право

Важно: Наличието на информация в интернет не означава, че тя може свободно да се копира, публикува или използва.

3. Права на човека при обработване на данни

- да знае кой събира данните и с каква цел;
- да получи достъп до съхраняваните за него данни;
- да поиска поправка на неточни данни;
- в определени случаи да поиска изтриване или ограничаване на обработването;
- да възрази срещу определени начини на използване;
- да оттегли съгласието си, когато обработването се основава на съгласие.

Практическа задача 1: Изберете сайт или приложение и открийте какви лични данни събира. Запишете целта, правното основание и начините за управление на настройките.

4. Електронен подпис

Електронният подпис е информация в електронна форма, която е свързана с електронен документ и се използва за идентифициране на подписващия. Той подпомага доказването на авторството и целостта на документа.

КАК РАБОТИ ЕЛЕКТРОННИЯТ ПОДПИС?



Електронният подпис доказва:

- кой е подписал
- че документът не е променян
- кога е извършено подписването

Вид	Характеристика	Примерна употреба
Обикновен	електронни данни, свързани с документа	потвърждение в онлайн услуга
Усъвършенствен	свързан уникално с подписващия и позволява откриване на промени	договори и вътрешни документи
Квалифициран	усъвършенствен подпис с квалифицирано удостоверение и защитено устройство	официални документи и административни услуги

Важно: Квалифицираният електронен подпис има най-висока степен на доверие и в много случаи е равностоен на саморъчен подпис.

5. Бисквитки (cookies)

Бисквитките са малки текстови файлове, които уебсайтът записва в браузъра. Те могат да бъдат необходими за работата на сайта, да запомнят предпочитания или да се използват за анализ и реклама.

БИСКВИТКИ (COOKIES)

Малки текстови файлове, които сайтът записва в браузъра, за да **запомни информация** за посещението.

 Сесийни изтриват се при затваряне на браузъра напр. в кошница, на сесия	 Постоянни остават за определен срок напр. предпочитания	 На сайта създадени от посещенния сайт напр. език, форми	 От трети страни създадени от външни услуги напр. реклами, анализи
---	---	--	---



Преди да приемете:

прочетете целта • изберете само необходимите категории • променяйте настройките при нужда

Практическа задача 2: Отворете настройките за поверителност на браузъра. Проверете как се управляват бисквитките, как се изтриват и как се блокират бисквитки от трети страни.

6. Цифрова самоличност

Цифровата самоличност е съвкупността от данни, профили, идентификатори и действия, чрез които човек е разпознаван в дигитална среда. Тя може да включва потребителско име, имейл адрес, профилна снимка, публикации, история на дейността и данни за използваните устройства.

Подход	Ползи	Рискове
Една самоличност за много услуги	По-лесно влизане и управление	Пробивът в основния профил може да засегне много услуги
Отделни профили	По-добро разделяне на учебни, лични и публични дейности	Повече пароли и настройки за управление
Свързани профили	Бързо споделяне и възстановяване	Данните могат да бъдат обединявани и проследявани между услуги

Важно: Използвайте различни пароли, включвайте многофакторно удостоверяване и преглеждайте кои приложения са свързани с основния ви профил.

Практическа задача 3: Карта на цифровата самоличност

Без да записвате реални пароли или чувствителни данни, посочете три вида онлайн профили, които човек може да използва. За всеки профил отбележете какви данни съдържа, с кои други услуги е свързан и какъв би бил рискът при загуба на достъп.

7. Лични данни и услуги с изкуствен интелект

Приложенията с изкуствен интелект могат да обработват въведени текстове, изображения, глас, местоположение, файлове и данни за начина на използване. Част от информацията може да бъде изпратена към външна услуга, съхранявана за определен срок или използвана за подобряване на системата. Затова преди използване трябва да се прецени дали споделянето е необходимо и разрешено.

Не въвеждайте без разрешение	Защо е риск	По-безопасен подход
Имена, ЕГН, адреси и телефони	Позволяват пряко разпознаване	Използвайте измислени или обезличени данни
Пароли, кодове и документи за самоличност	Могат да доведат до злоупотреба с профил или самоличност	Никога не ги поставяйте в заявка
Здравни, финансови и семейни данни	Са чувствителни и могат да причинят вреда	Работете само с разрешени учебни примери
Поверителни училищни документи и снимки	Може да съдържат данни за други хора	Премахнете личните данни или не качвайте файла

Преди да споделите данни с AI услуга, проверете:

- необходими ли са данните за задачата;
- имате ли право да ги споделяте;
- може ли човекът да бъде разпознат пряко или косвено;
- как услугата съхранява, използва и изтрива информацията;
- може ли същата задача да се изпълни с обезличени или примерни данни.

Практическа задача 4: Оценка на риска при AI услуга

Разгледайте следните ситуации и определете дали данните могат да бъдат споделени:

- 1) снимка на списък с имена и оценки;
- 2) измислена таблица с примерни резултати;
- 3) медицински документ;
- 4) обезличен текст без имена.

Обосновете решението си и предложете по-безопасен вариант.

8. Управление на поверителността в браузъра

Поверителността не се изчерпва с приемане или отказ на бисквитки. Браузърът позволява управление на разрешенията за местоположение, камера, микрофон, известия, изскачащи прозорци и проследяване. Частното сърфиране не прави потребителя анонимен – то основно ограничава запазването на историята и бисквитките на използваното устройство.

Настройка	Какво контролира	Препоръчително действие
Бисквитки от трети страни	Проследяване между различни сайтове	Блокирайте ги, когато не са необходими
Разрешения на сайтове	Камера, микрофон, местоположение и известия	Разрешавайте само за надеждни сайтове и за необходимото време
История и запазени данни	Посетени страници, формуляри и файлове	Изтривайте ненужните данни и не запазвайте чувствителна информация на общ компютър
Персонализирани реклами	Използване на интереси и дейност за рекламно профилиране	Прегледайте настройките и изключете персонализацията при необходимост

Практическа задача 5: Проверка на настройките

Отворете настройките Privacy and security на браузъра. Проверете бисквитките от трети страни, разрешенията за камера, микрофон и местоположение, изтриването на данни за сърфиране и настройките за персонализирани реклами. Не променяйте служебни или училищни настройки без разрешение.

9. Добри практики за защита на лични данни

КАК ПАЗИМ ЛИЧНИТЕ СИ ДАННИ?

1



Минимално споделяне

Не публикувайте повече информация от необходимото.

2



Силни пароли и многофакторно удостоверяване

Използвайте различни пароли и допълнително потвърждение при вход.

3



Проверка на получателя

Преди изпращане проверете адреса и прикачените файлове.

4



Настройки за поверителност

Ограничете кой вижда публикации, снимки и профилна данни.

5



Актуализации и защита

Поддържайте системата, браузъра и защитния софтуер актуални.

6



Резервни копия

Съхранявайте копие на важните данни на отделно място.

- Не изпращайте лични документи чрез незащитени канали.
- Проверявайте адреса на сайта и връзката HTTPS.
- Не публикувайте снимки и данни на други хора без разрешение.
- Използвайте различни пароли и многофакторно удостоверяване.
- Ограничете разрешенията на приложенията до необходимото.
- Изтривайте стари профили и ненужни данни.

10. Практическо упражнение

Ситуация: Училищен клуб създава онлайн форма за регистрация на участници. Определете:

- кои данни са действително необходими;
- кои данни не трябва да се събират;
- как ще бъде обяснена целта на събирането;
- кой ще има достъп;
- колко време ще се пазят данните;
- как участниците могат да поискат промяна или изтриване.

11. Обобщение

Ключово понятие	Най-важното
Лични данни	Информация, чрез която човек може да бъде разпознат.
GDPR	Правила за законосъобразно и прозрачно обработване.
Електронен подпис	Свързва подписващия с електронен документ и подпомага проверката на целостта.
Бисквитки	Малки файлове за функции, предпочитания, анализ или реклама.
Минимално споделяне	Събират се и се предоставят само необходимите данни.
Цифрова самоличност	Данни и профили, чрез които човек е разпознаван в дигитална среда.
AI услуга	Може да обработва въведени данни; споделят се само разрешени и необходими данни.
Настройки за поверителност	Управляват бисквитки, проследяване и разрешенията на сайтовете.

12. Въпроси за самопроверка

1. Какво означава понятието „лични данни“?
2. Дайте три примера за онлайн лични данни.
3. Кои права има човекът при обработване на негови данни?
4. Каква е ролята на електронния подпис?
5. Какво представлява цифровата самоличност?
6. Какви са ползите и рисковете от използването на един профил за много услуги?
7. Какво са бисквитките и защо се използват?
8. Каква е разликата между частно сърфиране и анонимност?
9. Какви лични данни не трябва да се въвеждат в AI услуга без разрешение?
10. Как може да се намали рискът чрез обезличаване на данните?
11. Кои разрешения на сайтовете трябва да се преглеждат периодично?
12. Кои мерки намаляват риска при работа с лични данни?