



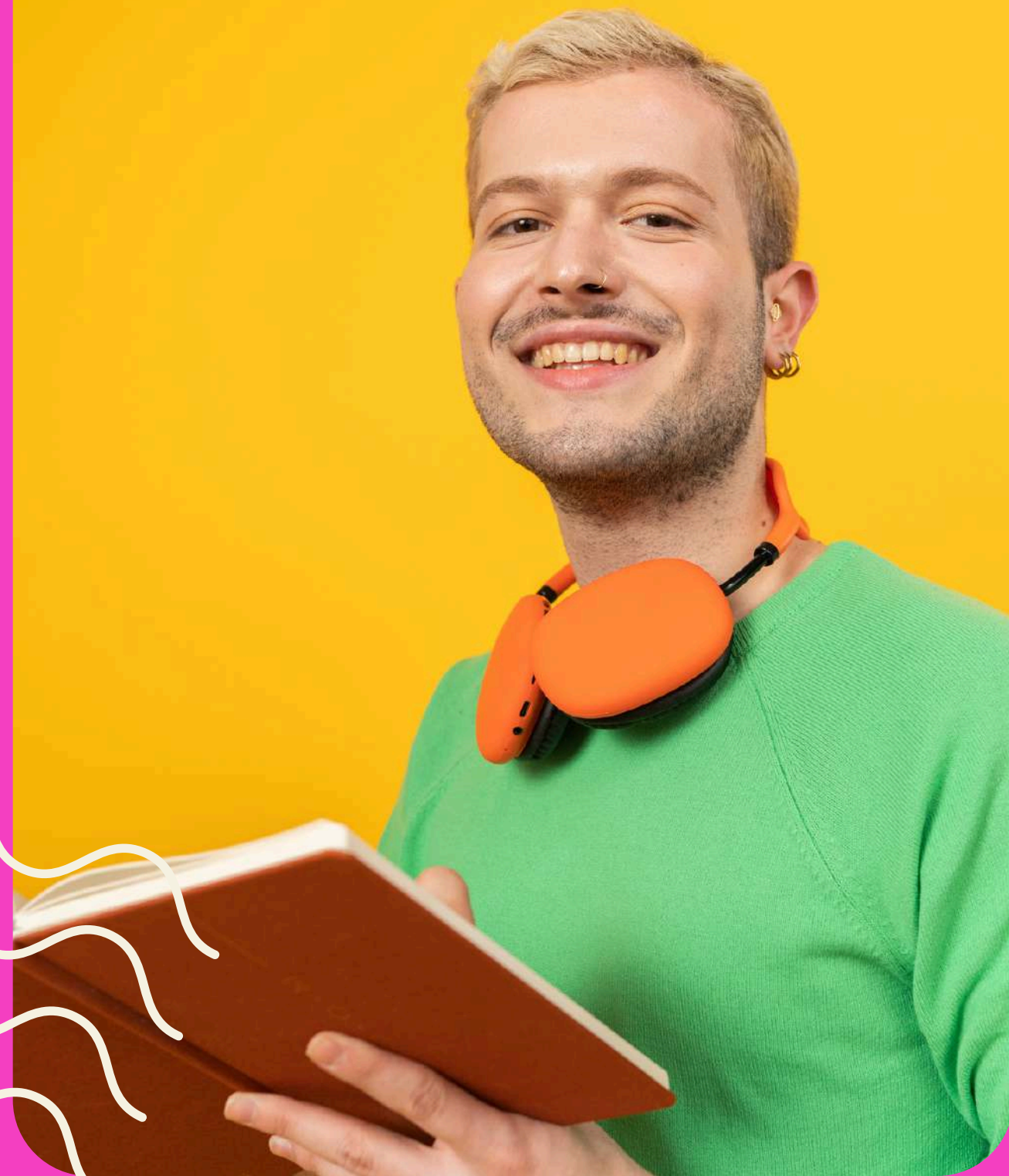
СЪВЕТИ ЗА

ДИГИТАЛНА

БЕЗОПАСНОСТ

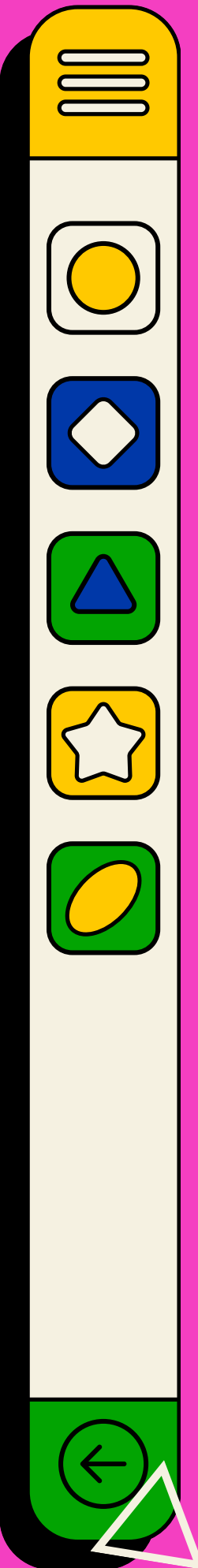


„Финансирано от Европейския съюз. Изразените възгледи и мнения принадлежат изцяло на техните автори и не отразяват непременно възгледите и мненията на Европейския съюз или на предоставящия орган Национална агенция, Център за развитие на човешките ресурси. За тях не носи отговорност нито Европейският съюз, нито предоставящият орган.“



Съдържание

- 1 Въведение
- 2 Сигурност на паролите
- 3 Осведоменост за фишинг атаки
- 4 Двуфакторна автентикация
- 5 Безопасност в социалните медии
- 6 Настройки за поверителност
- 7 Защита на личните данни
- 8 Заключение





Въведение

Добре дошли в нашето ръководство за съвети за дигитална безопасност! В днешния свят е важно да защитите себе си и личната си информация онлайн. Ето няколко съвета, които ще ви помогнат да сте в безопасност.





Сигурност на паролите

- Създавайте силни пароли с комбинация от букви, цифри и символи. Използвайте различна парола за всеки акаунт и ги сменяйте редовно. За да запазите личните си данни, използвайте силни пароли (да съдържат поне 12 знака, от които има малки и големи букви, цифри и специални символи). Старайте се да бъде колкото може по-необичайна и оригинална. Добра практика е да използвате подходяща запомняща се фраза. Не използвайте пароли, които могат да бъдат намерени в речник или са свързани с очевидни неща, които някой друг може да познае, като например части от Вашето име, името на детето или домашния Ви любимец, рождени дати, любимото Ви телевизионно/Интернет предаване и др. Добре би било, ако използвате мениджър за пароли. (Пример за силна парола: wH-1289757_etV#).



Сигурност на паролите

- Не използвайте лесни за отгатване пароли като „password123“ или „qwerty“. Вместо това използвайте уникална комбинация от букви, цифри и символи за всеки акаунт.
- Не използвайте една и съща парола за всичко - когато използвате една и съща парола за всеки от профилите си, излагате личните си данни на риск. Затова никога не използвайте една и съща парола два пъти. Ако някой разбере Вашата парола, а Вие я използвате на много места, то ще бъдете уязвими.
- Паролите трябва да се променят периодично – променяйте паролите си през определен период



Осведоменост за фишинг атаки



Бъдете внимателни за фишинг измами. Не кликвайте върху подозрителни връзки и не изтегляйте прикачени файлове от неизвестни податели. Ако получите имейл или текстово съобщение, което изглежда подозрително, свържете се директно с подателя, за да проверите автентичността му.

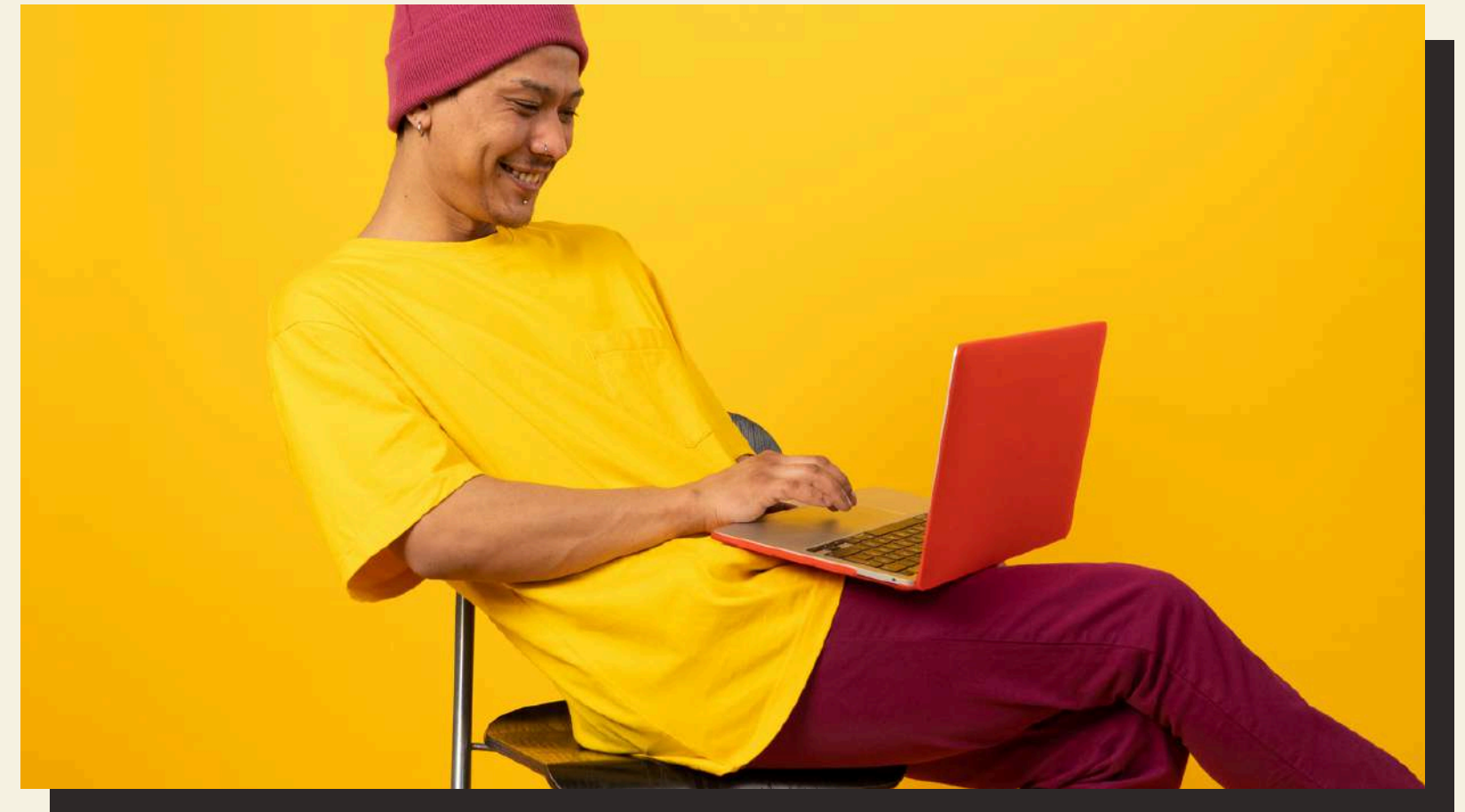


Осведоменост за фишинг атаки

Най-честите индикатори за фишинг атака са: неофициални или непознати имейл адреси на изпращача; изискване/настояване за изпращане на различен тип лични данни; използваното обръщение обикновено не е лично към Вас, а е общ поздрав или изобщо липсва такъв; посочените хипервръзки, към които Ви насочват, водят към непознати уеб страници или нямат нищо общо с изпращача; езикът и/или стилът на текста е лош или присъстват грешки, което често се дължи на автоматичен превод. Почти винаги присъства и предупреждение за лоши последствия, в случай, че не изпълните посоченото.

Двуфакторна автентикация

- Активирайте двуфакторно удостоверяване в акаунтите си за допълнителен слой сигурност. Това изисква да въведете код в допълнение към паролата си, за да получите достъп до акаунта си.
- Използвайте многофакторно удостоверяване при влизане от неизвестно устройство или изискване за потвърждение на имейл.





Безопасност в социалните медии

Бъдете внимателни какво споделяте в социалните мрежи. Не публикувайте лична информация като адрес или телефонен номер. Внимавайте какво споделяте и с кого го споделяте.





Настройки за поверителност

Проверете настройките си за поверителност в социалните мрежи и други онлайн акаунти. Уверете се, че споделяте информация само с хора, на които имате доверие.





Използвайте само защитени безжични (Wi-Fi) мрежи

Незащитените мрежи са много рискови. Злонамерено лице, използващо същата мрежа, може да открадне данните Ви или дори да поеме контрол върху Вашето устройство.



Защитата на личните данни за сигурността е от изключително значение в днешната дигитална ера, където преобладават онлайн заплахите и кражбата на самоличност. Един основен принцип, към който всеки трябва да се придържа, е никога да не споделяте лични данни за сигурност с никой друг. Личните данни за сигурност обхващат широк спектър от чувствителна информация, включително, но не само, пароли, ПИН номера, номера на социалното осигуряване, данни за кредитни карти и отговори на въпроси за сигурността.

**Защитете данните си
за сигурност**





Защитата на нашите компютри и мобилни устройства е от съществено значение в днешния взаимосвързан свят. Две важни практики, които допринасят за сигурността на устройството, са редовно актуализиране на операционната система и уеб браузъра и инсталиране на приложения изключително от официални магазини, като Apple App Store или Google Play Store. Тези прости, но ефективни мерки могат значително да подобрят сигурността на нашите устройства и да ги предпазят от различни онлайн заплахи.

Защитете компютъра и мобилното си устройство





Защитете ПИН кода си, никога не го споделяйте. Избягвайте да отговаряте на искания за данни за картата. Не приемайте помощ от непознати. Дръжте картата отделна и безопасна и я носете отделно, третирайте я като пари в брой. Използвайте надеждни устройства, дръжте картата на видимост. Наблюдавайте извлеченията от сметката си, съобщавайте незабавно на банката издателя на картата за наличие на несъответствия.

Защитете платежните си карти





Фишинг атаките са една от най-големите заплахи за сигурността, пред които е изправен бизнесът. Киберпрестъпниците използват техники, за да подмамат потребителите да мислят, че са истински податели, в опит да се откажат от данните за акаунта си, да инициират измамни плащания или да ги примамят към злонамерени уебсайтове чрез фалшификация по имейл. Най-често срещаната форма на фишинг е имейлът. Този имейл изглежда различно от официалния имейл на съответната компания, написан е на лош език или с граматически грешки, а подателят обикновено е с различен имейл адрес от този на съответната фирма/институция.

Пазете се от фишинг имейли





Какво представляват личните данни?



Лични данни са всяка информация, която помага на някого да разбере кой си ти, като например – името ти, рожденият ти ден, имейл адресът ти, телефонният ти номер или домашният ти адрес. Тази информация не е само записана някъде в документи, а може и да бъде информация за това как изглеждаш или звучиш, например снимки или видеоклипове, които си публикувал онлайн, или гласовите ти записи. Може дори да е информация за твоите интереси, като например неща, които търсиш онлайн, или видовете публикации, върху които кликваш най-много в социалните мрежи. Лични данни може също да бъде информация, която ти дори да не знаеш, че се събира за теб. Така например твоето лицево изображение може да бъде заснето от охранителна камера в търговски център или информация събрана от телефона ти, когато влезеш в публична безжична (Wi-Fi) мрежа, като тези в магазини или кафенета.





Категории за класификация на типове лични данни са:

- Доброволно предоставени данни - създават се и изрично се споделят от лица (Пр. профили в социални мрежи). Този тип данни може да включва видео файлове, снимки, текст или аудио файлове.
- Наблюдавани данни – улавят се чрез записване на действията на лица (Пр. данни за местоположението при използване на мобилни телефони или заснемане на лицево изображение от обществена камера).
- Изведени данни – заключение в следствие на анализ на доброволни или наблюдавани данни – (Пр. кредитен рейтинг).



Какви са данните в личен план и тези в дадена организация?

1. Лични данни в персонален план са всяка информация, която може да Ви идентифицира.
2. Лични данни в дадена организация са:
 - Традиционни: Данни за персонала - материали за кандидатстване, вестници, договори на служителите; Данни за подробности, свързани с покупка и продажба, производствени дейности и основни организационни операции; Интелектуални – патенти, търговски марки, продуктови планове, търговски тайни което позволява на организацията да спечели икономическо предимство пред своите конкуренти. Тази информация често се счита за търговска тайна и загубата ѝ може да се окаже катастрофална за бъдещето на една компания; Финансови - отчети за приходите и разходите, баланси, отчети за паричните потоци, които дават представа за състоянието на една компания.
 - Интернет на нещата (Internet of Things) и големи бази данни (Big Data): Internet of Things (IoT) - голяма мрежа от физически обекти, като сензори, софтуер и друго оборудване, които, свързани с интернет, могат да събират и споделят данни; Big Data – анализ на данните, събирани от IoT сензорите.



ПРАВИЛА ЗА ЗАЩИТА И УПРАВЛЕНИЕ НА ЛИЧНИТЕ ДАННИ (1)

Когато сте онлайн, оставяте дигитална следа, която записва всичко, което правите в различните сайтове и приложения, но и личните Ви данни, които споделяте. За да защитите данните си по-добре, следвайте описаните стъпки:

- Запознайте се с настройките на профила си в социалните мрежи и изберете възможно най-сигурния (препоръчително да е поверителен режим).
- Преди да публикувате нещо онлайн, помислете добре за кого искате да е видимо, т.к. след това може да бъде трудно да го изтриете.
- Отнасяйте се с данните на другите така, както се отнасяте със собствените си данни.
- Преди да се отбележите от някое място (таг-ване, tag), имайте предвид, че това е споделяне на местоположението Ви, което може да Ви изложи на риск. Не давайте разрешение на приложението или сайта да използва местоположението Ви, освен ако не е необходимо.
- Не се оставяйте да бъдете „подведени” – изберете опцията, която е най-сигурна, а не най-лесната за избор! (Понякога сайтовете и приложенията се опитват да Ви подведат, като искат да предоставите повече лична информация, отколкото им е необходима. Обичайно бутонът, върху който искат да щракнете, е голям, ярък и в средата на екрана, докато другата опция е малка и се пропуска лесно).
Внимавайте за тези практики!



ПРАВИЛА ЗА ЗАЩИТА И УПРАВЛЕНИЕ НА ЛИЧНИТЕ ДАННИ (2)

- Без да бързате, внимателно прочете условията (Всеки сайт или приложение трябва да Ви предостави информация за това какво прави с личните Ви данни. Често тази информация е написана на сложен и неразбираем език, затова ако не сте сигурни, попитайте родител или потърсете човек, който да Ви даде компетентен съвет).
- Не избирайте просто върху „Приемам всички“ (Accept all) (Видите ли съобщение за поверителност или банер за бисквитки, помислете дали искате да ги приемете. Потърсете бутона, който Ви позволява да отхвърлите тези, които можете. В противен случай споделяте повече лична информация, което може да Ви навреди).
- Знайте стойността на личните си данни („Безплатните“ услуги не винаги са безплатни. Голяма част от личните данни, споделяни онлайн се използват от приложенията и сайтовете, за да се печелят пари от неща като реклами. Винаги мислете дали си заслужава да споделите твоите лични данни и какво получавате ли срещу тях).
- Не забравяйте, че контролът е в Вас (Когато споделяте личните си данни, Вие имате права върху тях, за които сайтовете и приложенията трябва да се съобразяват. Например Вие можете да поискате от тях достъп и копие от личните Ви данни или да изтрият профилите Ви).

ПРАВИЛА ЗА ЗАЩИТА И УПРАВЛЕНИЕ НА ЛИЧНИТЕ ДАННИ (3)

- Въвеждайте/предоставяйте точна информация за данните си (Никога не лъжете за възрастта си или за други данни, когато се регистрирате някъде, както и в социалните мрежи! Това може да доведе до лоши последствия за Вас, тъй като обикновено се съгласявате с определени условия и потвърждавате коректността на данните си).
- Изтрийте профила си, когато нямате нужда от него (Ако вече не използвате някое приложение или сайт, по-добре изтрийте профила си, защото той може да бъде хакнат след време и да се използва от други хора, което впоследствие да Ви навреди).

Заклучение



Като следвате тези съвети за дигитална безопасност, можете да защитите себе си и личната си информация онлайн. Пазете се!



**Съфинансирано от
Европейския съюз**

**„ФИНАНСИРАНО ОТ ЕВРОПЕЙСКИЯ СЪЮЗ. ИЗРАЗЕНИТЕ
ВЪЗГЛЕДИ И МНЕНИЯ ПРИНАДЛЕЖАТ ИЗЦЯЛО НА ТЕХНИТЕ
АВТОРИ И НЕ ОТРАЗЯВАТ НЕПРЕМЕННО ВЪЗГЛЕДИТЕ И
МНЕНИЯТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ИЛИ НА ПРЕДОСТАВЯЩИЯ
ОРГАН НАЦИОНАЛНА АГЕНЦИЯ, ЦЕНТЪР ЗА РАЗВИТИЕ НА
ЧОВЕШКИТЕ РЕСУРСИ. ЗА ТЯХ НЕ НОСИ ОТГОВОРНОСТ НИТО
ЕВРОПЕЙСКИЯТ СЪЮЗ, НИТО ПРЕДОСТАВЯЩИЯТ ОРГАН.“**