THE DATA GAME

E-Book

на български

Съфинансирано от Европейския съюз

Изразените възгледи и мнения са единствено на автора(ите) и не отразяват непременно тези на Европейския съюз или на OeAD-GmbH. Нито Европейският съюз, нито предоставящият орган могат да бъдат държани отговорни за тях.
Номер на проекта: 2023-1-AT01-KA220-ADU-000157050

ПАРТНЬОРИ

Съфинансирано от
Европейския съюз

СЪДЪРЖАНИЕ

02
DataGame: Защо и за Кого?

05
Предговор

12
Глава 1: Светът на киберсигурността

18
Глава 2: Лек за най-слабото звено

21
Глава 3: Навигация из регулаторната рамка

29
Глава 4: Добри практики и стратегии

40
Глава 5: Иновации и възникващи тенденции

46
Глава 6: Казуси и истории на успеха

64
Глава 7: Практически знания и нагласи

71
Глава 8: Компетентностна рамка

81
Пътят напред

DATAGAME: ЗАЩО И ЗА КОГО?

DataGame е онлайн платформа за обучение, спонсорирана през инициативата Erasmus+ KA2 на Европейския съюз. Нашата цел е да подпомогнем професионалистите в областта на образованието за възрастни да повишат експертизата си в безопасното и сигурно администриране на лични данни в техните организации. Партньорството, което стои зад този проект, споделя богат опит в областта на професионалното обучение и цифровата квалификация и приобщаване. На линковете по-долу можете да разгледате някои от предишните ни инициативи:

През ноември 2023 г. се отправихме на двугодишно пътешествие, за да ви предоставим следните материали:

Електронната книга „DataGame“ - вашето ръководство за защита на личните данни в европейския контекст на обучението за възрастни, съдържащо най-новите актуализации, най-добрите практики, прозрения, знания и политически рамки, както и два уникални теста. Това е наръчник за всеки, който се интересува от повишаване на безопасността и сигурността в мрежата на своята организация.

The DataGame - онлайн обучение, базирано на игрови сценарии, което поставя реални предизвикателства, свързани с поверителността на данните в образованието за възрастни. Играчът ще трябва да взема решения, за да гарантира безопасността и сигурността на данните на своята организация, както и на данните на своите клиенти, за да научи и напредне в обучението.

Инструментариумът „DataGame" - инвентар с най-новия софтуер, курсове за обучение и полезни материали за защита на личните данни, които експертите в областта на образованието за възрастни, преподавателите и лицата, вземащи решения, могат да използват в своята работа.

Това, което четете в момента, е първият ни продукт - Електронната книга “DataGame”.
Тя е придружена от специално разработен речник, който ще ви помогне да се ориентирате в сложната терминология на защитата на личните данни. Него можете да изтеглите тук.

НА ДОБЪР ЧАС!

НАУЧЕТЕ ПОВЕЧЕ ЗА DATAGAME НА ТЕЗИ ЛИНКОВЕ:

ПРЕДГОВОР

Живеем в интересни времена.

Насред какофонията от информация, с която сме бомбардирани ежедневно - говорим от името на петте милиарда души, свързани с интернета днес - се намира огромна паралелна вселена от нули и единици, която представлява нашето минало, настояще и бъдеще. Тя вече е основното ни средство за споделяне на идеи и общуване. В много отношения, виртуалната реалност позволява на нашето културно и технологично развитие да напредне с такива бързи темпове през последните 30 години. В тази цифрова епоха ползите от съвременните технологии са неоспорими - от незабавни съобщения и биометрично сканиране, до проследяване на движения в реално време и цифрови плащания. Въпреки това, дори и по-семплите технологии идват със своя собствен набор от предизвикателства, особено в сферата на защитата на личните данни. Както се изразява британският математик Клайв Хъмби, помогнал за създаването на членската карта на Tesco, „Данните са новият петрол". Разбираемо е, ако това Ви звучи пресилено. Възможно е да имате някои предубеждения относно защитата на личните данни; че тя е излишна, че е скучно административна, или че е тема, която интересува само юристите.

Но какво всъщност представлява поверителността на данните?

Казано по-просто, това е онзи аспект на съхранение и използване на цифрова информация и комуникация, който отговаря за защитата на въпросните данни (данни в най-широкия смисъл на термина, представляващи даден физически обект, идея, споразумение, комуникация, търговски продукт, интелектуална собственост и прочие от реалния свят), като дава възможност и гарантира поверителността им чрез контрол на достъпа до тях и тяхното използване, обработка и

съхранение. Обикновено тези данни са свързани с хора. Това определение, обаче, не е напълно изчерпателно.

Аспекти на поверителността на данните

Поверителността на данните е сложна концепция, която съдържа аспекти от много различни области - правни, технически, социални, културни и междуличностни.

Нека започнем с правните дефиниции 

В правен контекст, защитата на личните данни е едновременно нормативната уредба, съдебната практика и политиките, които обявяват рамките на тази дейност в дадена държава или юрисдикция, и какви усилия са необходими за нейното подсигуряване. В случая с образованието за възрастни е важно да се запознаем с правните аспекти на защитата на личните данни, тъй като те могат да окажат пряко въздействие върху Вашата работа.
Например, какво се случва, когато вашата организация е обект на одит, нарушение на сигурността на данните или жалба от потребител? Тези правни определения оказват влияние и върху личния ви живот. Какви права имате като гражданин?

Тъй като всяка организация в ЕС е в стремежа си да интегрира цифрови инструменти и онлайн платформи в своята дейност, пейзажът на защитата на личните данни става все по-сложен. С Общия регламент за защита на данните (GDPR) и други разпоредби, които прекрояват глобалния пейзаж на цифровите мрежи, разбирането и прилагането на надеждни мерки за защита се превърна не само в правно задължение, но и в стратегическа необходимост.

Днес, обикновения контрол върху данните е още по-усложнен, тъй като защитата на данни включва цялостно разбиране на начина, по който данните те достъпват, използват, обработват и съхраняват.

Въпреки това, докато техническите и правните дефиниции осигуряват

рамка, социалните и културните аспекти на поверителността подчертават човешкия елемент на неприкосновеността на личния живот в цифров контекст.

Човешкият фактор (социален контекст/граници)

От друга страна, изследванията на Дана Бойд показват, че поверителността е също толкова свързана с разбирането и действието в рамките на социалните граници.

Проучвайки взаимодействието на подрастващи в тийнейджърска възраст със социалните медии, за да определи начините, по които технологиите влияят върху разбирането им за понятия като поверителност, тя дава следното определение за неприкосновеността на личните данни:

> Тя не е свързана с контрол върху данните, нито е свойство на данните. Става дума за колективно разбиране на границите на дадена социална ситуация - да знаеш как да действаш в рамките на тези граници с контрол върху ситуацията. Става дума за разбиране на аудиторията и знанието докъде ще стигне информацията. Става дума за доверие в хората, ситуацията и контекста.
>
> *Дана Бойд (2014 г.) - Това е сложно: Социалният живот на тийнейджърите в мрежата; стр. 54*

Това е един различен аспект на поверителността, който провокира значителни промени в методите за нейното проектиране в системите. За разлика от техническите и правните дефиниции, Бойд поставя в центъра социалното и културното разбиране, контекста и индивидуалния избор и осъзнатост. Защо? Когато се наведете, за да прошепнете нещо, другите разбират, че тази информация не е предназначена за споделяне. Когато изкрещите на площада, другите разбират, че искате да ви чуят колкото се може повече хора. Начинът, по който човек адаптира стила си на комуникация си според хората, с които общува, е силно повлиян от това как той определя и възприема

поверителността.

От друга страна, способността на хората да експериментират и да променят взаимодействието си с другите се е трансформирала значително с времето. Цифровите технологии и световната мрежа позволяват на всеки да разшири комуникацията си, което неизменно пренася проблемът с поверителността в контексти, които не са физически. Докато този нов хоризонт изменя свързаността ни по иновативен и изключително полезен в много аспекти начин, преминаването от физическия към онлайн света, също така, замъглява осъзнатостта ни за контекста, в който работим. Сферата на образованието за възрастни не прави изключение.

Какви са правилата на това пространство? Кой може да ни вижда и чува? С един човек ли говорим, или с група. Ако е с група, колко е голяма тази група и какви са нейните рамки, правила, очаквания?

Контекстуален интегритет 

Работата на Хелън Нисенбаум върху контекстуалния интегритет показва, че технологиите са променили степента, до която тези линии са прозрачни, както и са усложнили възприемането им. Това засяга не само потребителските интерфейси, но и основните начини, по които се проектирани системите и софтуерите.

Изборът на "настройки по подразбиране" в крайна сметка засяга неприкосновеността на личните данни на милиони хора. Решенията за сигурност и криптиране правят частните разговори достъпни за правоприлагащите органи и държавното наблюдение. Складовете за данни могат да вземат чувствителна информация, предназначена само за един човек, и да създадат пътища за достъп на служители и услуги за данни на трети страни.
Когато контекстът е изгубен или неясен, а при проектирането на системата не се отчитат социалните и културните дефиниции, технологията по същество пренебрегва човешкия аспект на

поверителност.

Тъй като доставчиците на услуги в областта на образованието за възрастни все повече използват цифрови услуги, за да повишат качеството и ефективността на работата си, значението на опазването на поверителността на лични данни не може да бъде надценено.

Защо тази електронна книга

Тук ще ви преведем през променящия се пейзаж, стоящ пред сектора на образованието и организационния мениджмънт като цяло, като ви предложим практически знания и най-добри практики за защита и отговорно управление на Вашите цифрови дейности.

Изграждайки стабилна рамка за поверителност и сигурност на данните, Вие не само ще сте по-способни да се ориентирате в нормативните уредби, адекватно и с точност спрямо Вашата работа, но и ще станете по-отговорни и етични в дигиталната си комуникация както с клиентите, така и с Вашите колеги.


Добре дошли на едно пътешествие, в което ще се научите да разбирате и да се справяте с неизбежните социални и правни последици от цифровизацията, които засягат поверителността на лични данни не само в образованието, но и в съвременния живот като цяло!

1

СВЕТЪТ НА КИБЕРСИГУРНОСТТА

Почти сме сигурни, че след като четете това, Вие живеете в Европа и още по-вероятно сте от България, Австрия, Гърция, Кипър или Ирландия. Дори и това да не е така, при всяко положение, в тази първа глава ще получите яснота относно начина, по който секторът на образованието за възрастни функционира в рамките на Европейкския Съюз. Тук ще се запознаете с регулациите, които определят неговото развитие по отношение на разпоредбите за защита на данните.
Но преди да стигнем дотам, ни трябва малко контекст.

Предисторията 

Киберпространството - големият брат на Интернета от 80-те години на миналия век - за пръв път се въвежда като термин от научно-фантастичния писател Уилям Гибсън в разказа „Burning Chrome" (1982г). В него Гибсън капсулира политическото и културното напрежение, което се надига в началото на XX век, отвъд обикновения стремеж на човека за технологично развитие. Разказът му описва едно мрачно бъдеще, в което могъщи корпорации упражняват огромен контрол чрез взаимосвързани компютърни мрежи.
В същата година, екшънът „TRON" представя една по-оптимистична гледна точка, изобразявайки "киберпространството" като сфера, в която всеки може безпрецедентно да изразява своите убеждения, без значение колко особени са те и без да се страхува, че ще бъде принуден да мълчи.
Тази втора визия - несъмнено по-позитивна и вдъхновяваща - кара технологичните утописти от Западния бряг на Америка да преосмислят киберпространството. То е един безопасен свят, в който могат да се реализират радикални мечти. Документалистът на Би Би Си Адам Къртис представя тези ранни дни на Интернет пространството като много сходни с хипи движението през 60-те години на миналия век - то е техно-културната революция срещу консуматорското общество и правителствения контрол.
За днес можем да кажем, че контролът на големите корпорации, упражняван чрез мощни компютърни мрежи, е общоприет факт. Именно киберпространството - паралелната реалност, предначертана да ни освободи от безкомпромисните неписани правила на

капитализма и постмодерното общество чрез своя безграничен потенциал за себеутвърждение и едновременно взаимственост - се превръща в поредния локус на властта.
През 1996г. бива създаден Законът за телекомуникациите, насочен към регулирането на регулирането на пазара - онова, което Киберпространството изначално е трябвало да промени. В същата година „Декларацията за независимост на киберпространството", написана от Джон Пери Барлоу, подкрепя гласа на хората, които вярват в суверенитета и независимостта на киберпространството от политики или правителствено влияние. Декларацията се застъпва за цялостна саморегулация въз основа на нормите и ценностите на "цифровата общност", но именно двама млади хакери, известни като „*Acid Phreak*" и „*Phiber Optik*", предвиждат идеалистичната ѝ фантазия. Те си поставят за цел да докажат необходимостта от регулаторна рамка над "световната мрежа". Обвинени в заговор за незаконно проникване във федерални системи, хакерите демонстрират последиците от липсата на контролиращи власти още през 1990г. Хакването на TRW (Thompson Ramo Wooldridge Inc. - голяма американска корпорация, отговорна за разработването на технологии от решаващо значение за стратегическата отбрана на САЩ по време на Студената война), от *Acid Phreak* и *Phiber Optik* разкрива как компанията използва цифрови софтуери за управление на кредитни и дългови системи, като си сътрудничи с банките за събиране на кредитни данни на гражданите, за да определя техните кредитни истории. Те символично крадат кредитната история на Барлоу и я публикуват онлайн по време на конференция, на която той се застъпва за цифровите права и обсъжда киберсвободите. По този начин хакерите показват, че зад мечтата на Барлоу стои нова сила отвъд политиката.

От една страна, интернетът наистина представлява една глобална среда, еманципираща свободата на словото. Универсална модалност, където се осъществява бизнес, култура, политика, наука и образование. В сферата на образованието, възможностите за предоставяне на по-добри и по-качествени услуги, с помощта на

цифровите технологии са безспорни. Те дават възможност за по-персонализирано обучение, при което преподавателите могат да адаптират съдържанието към специфичните нужди и темпото на всеки учащ. Този подход повишава ангажираността и разбирането, което води до по-ефективни академични резултати и по-високи постижения. Онлайн платформите и ресурсите също така предлагат достъп до изключително голям и съвременен набор от учебни материали - от академични статии и електронни книги до интерактивни курсове и уебинари. Това ниво на свързаност позволява на обучаемите да разширят знанията и уменията си извън традиционните класни стаи със собствено темпо и в удобно за тях време. Освен това, цифровите технологии улесняват използването на мултимедийно и интерактивно съдържание, което прави обучението по-динамично. Функции като виртуални симулации, игрови модули за обучение и разширена реалност могат да вдъхнат живот на сложни концепции, което ги прави по-лесни за разбиране и запаметяване. Отделно, възможността за свързване с колеги и преподаватели в световен мащаб чрез видеоконференции и онлайн форуми насърчава една по-богата среда за сътрудничество в учебната дейност.

Наред с тези възможности, обаче, идва нов и непознат тип уязвимост.

Интегрирането на онлайн платформи е неизменно свързано с използването на онлайн хранилища за съхранение на данни (Cloud Storage). Макар това от една страна да улеснява администрирането им, рискът от кибератаки при такъв вид услуги е голям, поради липсата на ресурси и нуждата от специфични конфигурации за гарантиране на сигурността на онлайн хранилищата, като например създаване на контрол на достъпа, криптиране и провеждане на редовни одити на сигурността. Киберпрестъпниците често таргетират малките и средни предприя именно по тази причина. Така образователните досиета, личните идентификатори и финансови данни, както и всякакъв друг вид чувствителна информация, е изложена на риск от **неоторизиран достъп, кражба на**

самоличност, финансови измами и други заплахи. Използването на услуги от трети страни често включва споделяне на данни между множество платформи, което значително усложнява управлението на сигурността на данните и увеличава риска от неправилно обработване на данни, както и разкриването им чрез лошо защитени връзки.

Проблеми с поверителността възникват и от неадекватните практики за управление на данните в образователните институции. Без стабилни политики и ясни насоки няма достатъчен надзор върху това кой има достъп до данните, как се съхраняват и колко дълго се пазят. Тази липса на контрол може да доведе до неоторизиран достъп от страна на персонала или външни лица, случайно изтичане на данни или неспазване на законовите изисквания.

Освен това използването на инструменти за анализ и проследяване на обучението - макар и полезно за персонализиране на учебния процес - може да породи опасения относно наблюдението на учениците и профилирането на данните. Без подходящото ниво на прозрачност и когнитивно благоприятни механизми за даване на съгласие (бисквитки), учащите не са наясно как се събират и използват техните данни, което е косвено нарушение на техните права на неприкосновеност на личния живот. Етичните последици тук подчертават необходимостта от яснота в комуникацията и създаването на политики, за да се гарантира, че данните се използват отговорно и с информираното съгласие на участващите лица.

Затова разбираме, че **ефективността на цифровото образование зависи** не само от самата технология, но и **от добросъвестните практики и етичните съображения на тези, които я използват и управляват**.

Така стигаме до сърцевината на нашата дискусия: **човешкият фактор** при обработката на лични данни.
Въпреки най-съвременните технологични предпазни мерки, отговорността в крайна сметка винаги пада върху преподавателите,

администраторите, управителите и обучаемите.

В следващата кратка и изчерпателна втора глава ще разгледаме концепцията за „**най-слабото звено**“. Тя ще положи основната стратегия за справяне със сериозния компромис, който нашите решения и поведение могат да представляват за защитата на личните данни.

2

ЛЕК ЗА НАЙ-СЛАБОТО ЗВЕНО

Както тъмните модели ни показаха през последните години, всички сме подвластни на собствените си когнитивни пристрастия. И тъй като интернет, въпреки автоматизацията си, е напълно безполезен без нашето взаимодействие с него, е съвсем уместно най-големият компромис със сигурността на дадена организация или система да бъдем ние самите. Независимо дали чрез фишинг атаки, социално инженерство, слаби практики за пароли или просто незнанието, че не се включват USB устройства, намерени на земята на път за работа - физическите лица често са основната причина за проблемите във веригата за сигурност.

В контекста на образованието за възрастни този въпрос е особено актуален. Преподавателите и администраторите боравят с огромни количества чувствителни данни - от информация за учениците до финансови документи - което ги прави основни мишени за кибератаки. Ето защо предизвикателството е да се намалят тези рискове, като на първо място се обърне внимание на човешките елементи в процеса на защита на данни. Това включва насърчаване на култура на информираност и бдителност, осигуряване на цялостно обучение за най-добрите практики за защита на данните, както и прилагане на стабилни политики за сигурност.

За пример, нека разгледаме случая на една образователна институция, която претърпява значителен пробив в данните вследствие на фишинг атака. Нападателят, представяйки се за доверен източник, подлъгва служител да разкрие идентификационни данни за вход в системата, които след това се използват за незаконен и потенциално вреден достъп до чувствителна информация.
Подобни инциденти са често срещани и подчертава значението не само на техническите предпазни мерки, но и на непрекъснатото обучение и осведомяване на персонала и обучаемите за тактиките, използвани от киберпрестъпниците (и как да ги смекчат) . Ето защо е от съществено значение да се възпитава мнителност и предпазливост, като хората се обучават да поставят под съмнение необичайните искания и да проверяват легитимността на цифровата комуникация,

преди да участват в нея.

За минимизирането или отстраняването на тези уязвимости е нужно да обсъдим практически методи, като например прилагане на многофакторно удостоверяване, провеждане на редовни одити на сигурността и насърчаване на среда, в която докладването на потенциални заплахи за сигурността се поощрява.

Именно като обърнем внимание на **човешкия фактор** в киберсигурността, можем значително да подобрим цялостната сигурност на образователните институции и да защитим по-добре поверените данни.

В следващите глави предстои да навигираме сложния пейзаж на регулации и разпоредби, които трябва да се спазват от професионалистите в областта на образованието за възрастни. Съответствието с тях не само защитава правата на лицата, чиито данни биват обработвани, но и предпазва институциите от сериозни санкции и увреждане на репутацията. Ще Ви предоставим изчерпателно ръководство за ориентиране в тези разпоредби, за да сте добре подготвени да изпълнявате правните си задължения и да поддържате адекватен стандарт за защита на данните.

3

НАВИГАЦИЯ НА РЕГУЛАТОРНАТА РАМКА

Съвремието ни обгръща с безброй правила, които трябва да познаваме, за да можем да се разпореждаме свободно в обществото, в което живеем, а последиците от девиантно поведение са сериозни. Това важи в пълна сила дори и за виртуалния свят. Като преподаватели, експерти или управители, работещи в сферата на образованието за възрастни, Вие неизменно сте обект на закона GDPR. Независимо от длъжността ви, ще бъдете подложени на съответното наказание за нарушаване на някоя от неговите клаузи в рамките на Вашата работа.
Преди да навлезем в подробност за практиките, които избягват това, трябва да знаете какво представлява регламентът - какви са възможните му дерогации и как те, както всички други закони, на които сте подчинени като член на организация, която предлага обучения за възрастни, се прилагат за Вас.

Ориентирането в безбройните правила и стандарти в цифровата епоха може да бъде обезсърчително, особено за тези, които обработват чувствителна информация на ежедневна база, без нужните знания за това. Общият регламент относно защитата на данните (ОРЗД/GDPR на англ.) е един от най-всеобхватните закони за защита на данните в световен мащаб и неговото значение за образованието за възрастни не може да бъде надценено. Като преподаватели, администратори или лица, вземащи решения, разбирането на GDPR е от решаващо значение не само за спазването на правните изисквания, но и за запазване на доверието на обучаемите, персонала и бизнес партньорите на организацията.

Какво представлява GDPR

GDPR определя правата на физическите лица и задълженията на организациите по отношение на обработката на лични данни. В регламента се набляга на **прозрачността**, **отговорността** и **сигурното обработване** на лична информация. Основните принципи включват **свеждане на данните до минимум**, **ограничаване на целите** и **изискване за изрично съгласие** за дейностите по обработване на данни. За работещите в сферата на образованието за

възрастни това означава, че всички събрани данни - независимо дали става въпрос за регистрация, управление на курсове или научни изследвания - трябва да се обработват с най-голямо внимание и в строго съответствие с насоките на GDPR.

Основни понятия и определения

Лични данни: Всяка информация, свързана с идентифицирано или подлежащо на идентифициране лице. Това може да включва имена, идентификационни номера, данни за местоположението, онлайн идентификатори и други фактори, специфични за самоличността на дадено лице.

Права на лицето (субекта на данни): Лицата имат право на достъп до своите данни - да коригират неточности, да ги изтриват, да ограничават обработката им и т.н. Разбирането на тези права е от съществено значение за преподавателите и администраторите, тъй като гарантира спазването на изискванията и укрепва доверието.

Администратор и Обработчик (на данни): Администраторът определя целите и средствата за обработване на лични данни, докато обработчикът обработва данните от името на администратора. В образователен контекст институцията обикновено действа като администратор на данни, докато услугите на трети страни (като онлайн хранилищата за данни, платформи за услуги и т.н.) могат да бъдат обработващи данни.

Законови основания за обработване: GDPR очертава няколко законни условия за обработване на лични данни, включително изрично съгласие, договорна необходимост, правно задължение, жизненоважни интереси, обществена дейност и легитимни интереси. Определянето на правилното основание за обработване на данни е от решаващо значение за спазването на изискванията.

Дерогации и изключения

Въпреки че ОРЗД се прилага в широк смисъл, съществуват

специфични последващи актове и изключения, които могат да се прилагат, особено в контекста на образованието и научните изследвания. Например регламентът позволява обработването на лични данни без изрично съгласие, ако това е необходимо за целите на научни или исторически изследвания или за статистически цели, при условие че обработването е пропорционално и спазва същността на принципите за защита на данните. Освен това, въпреки че ОРЗД установява строги правила за защита на личните данни, в него се признава и необходимостта от гъвкавост в определени контексти, и именно образованието и научните изследвания са едни от тях. Тези частични отмени на закона имат за цел да балансират защитата на данните с необходимостта от обществен и научен напредък.

Научни и исторически изследвания: Съгласно член 89 от ОРЗД личните данни могат да бъдат обработвани без изрично съгласие, ако това е необходимо за научни или исторически изследвания или за статистически цели. Това изключение е от решаващо значение за академичните и изследователските институции, които се нуждаят от достъп до големи масиви от данни, включително чувствителна информация. При обработването им обаче трябва да се спазват принципите за защита на данните - да се свеждат данните до минимум и да се прилагат предпазни мерки като псевдонимизация за защита на самоличността на субекта.

Обществен интерес и Официални органи: Образователните институции могат да обработват лични данни в обществен интерес или при упражняване на предоставените им официални правомощия. Например университет, провеждащ изследвания в областта на общественото здраве, може да обработва данни без изрично съгласие, ако те допринасят за познанията във въпросната област.

Пропорционалност и предпазни мерки: Дори когато се прилагат изключения, обработването трябва да бъде пропорционално, което означава, че трябва да се събира само необходимото количество данни и трябва да се прилагат предпазни мерки за защита. Това

включва мерки като анонимизиране или криптиране, които гарантират, че данните не могат лесно да бъдат проследени до отделните субекти.

Архивиране: За целите на архивирането в обществен интерес институциите могат да обработват лични данни без съгласие, при условие че обработката спазва принципите за защита на данните и включва подходящи гаранции.

Тези изключения позволяват на образователните и научноизследователските институции да изпълняват функциите си без административната тежест да получават съгласие във всеки случай, при условие че спазват основните принципи на ОРЗД.

Други релевантни регламенти

Освен GDPR, работещите в сектора на образованието за възрастни трябва да са наясно и с други нормативни актове, които могат да окажат въздействие върху техните дейности по обработване на данни. Те включват национални закони за защита на данните, които допълват GDPR, специфични за сектора разпоредби и международни закони за институции, които работят отвъд международните граници. Нормативната уредба може да се различава значително в отделните държави от ЕС, което налага задълбочено познаване на местните закони.

България: В България Законът за защита на личните данни (**ЗЗЛД**) допълва GDPR, като предоставя конкретни насоки и изисквания. Комисията за защита на личните данни (**КЗЛД**) е националният орган, който отговаря за прилагането на тези закони. В контекста на образованието за възрастни институциите трябва да са наясно със специфичните разпоредби на ЗЗЛД относно периодите на съхранение на данните и обработката на чувствителни данни, като например образователни документи или здравна информация.

Австрия: Австрия прилага допълнителни мерки за защита на данните

чрез Datenschutsgesets (**DSG**). За доставчиците на образование за възрастни DSG включва разпоредби относно обработването на данни за научноизследователски и статистически цели, подобни на дерогациите от GDPR. Дерогацията обаче включва и по-строги изисквания за нарушения на сигурността на данните и процедури за уведомяване, които образователните институции трябва да спазват.

Гърция: Органът, който прилага законите за защита на данни в Гърция е **HDPA**. Гръцкото законодателство набляга на защитата на личните данни в публичните институции, включително в образователните такива. За използването на биометрични данни или електронни комуникации в образователните институции могат да се прилагат специални разпоредби, които изискват специално съгласие и строги мерки за сигурност.

Ирландия: Ирландският закон за защита на данните от 2018 г. допълва GDPR, като предвижда допълнителни правила за обработката на данни, особено по отношение на чувствителните лични данни. Ирландските разпоредби поставят силен акцент върху прозрачността и отговорността, като изискват от институциите да предоставят ясни уведомления за защита на личните данни и да поддържат подробни записи за дейностите по обработване на данни. Комисията за защита на данните (**КЗД**) следи за спазването на изискванията в Ирландия.

Кипър: Службата на комисаря за защита на личните данни (**OCPDP**) следи за спазването на изискванията за защита на данните в Кипър. Кипърският закон за защита на личните данни допълва ОРЗД и включва конкретни разпоредби относно обработката на данни в образователен контекст, като например обработката на ученически досиета и използването на образователни технологии. Освен това Кипър подчертава ролята на длъжностните лица по защита на данните (**ДЛЗД**) за осигуряване на съответствие в организациите.

Специфични за сектора разпоредби и международни съображения

В допълнение към националните закони, специфичните за сектора разпоредби могат да повлияят на практиките за защита на данните. Например:

Специфични насоки за образователния сектор: В много държави има специфични насоки за образователния сектор, които очертават най-добрите практики за защита на данните в образователната среда. Тези насоки често обхващат използването на технологии в класните стаи, защитата на данните на учениците и отговорностите на образователните институции за защита на личната информация.

Международни съображения: За институциите, работещи в чужбина, разбирането и спазването на международните закони е от решаващо значение. Това включва не само GDPR, но и разпоредби като Директивата за защита на личните данни в областта на електронните комуникации (ePrivacy Directive), която се отнася до електронните комуникации и може да окаже влияние върху начина, по който институциите боравят с платформите за онлайн обучение и цифровите комуникации.

Трансгранично предаване на данни: Може да се наложи институциите да прехвърлят лични данни отвъд граница, което се регулира от разпоредбите на GDPR относно международното прехвърляне на данни. Те трябва да осигурят адекватна защита на данните, като често използват механизми като стандартни договорни клаузи (**SCC**) или получаване на изрично съгласие от субектите на данни

Прилагане на практики за съответствие

За да осигурят съответствие с GDPR и други съответни разпоредби, институциите за обучение на възрастни трябва да прилагат всеобхватни политики и процедури за защита на данните. Това включва провеждане на редовни оценки на въздействието върху защитата на данните (**ОВЗД**) за идентифициране и намаляване на рисковете, създаване на ясни структури за управление на данните и

осигуряване на постоянно обучение на персонала и студентите относно принципите и най-добрите практики за защита на данните. Следващият казус е първият ни действителен пример в тази електронна книга. В глава 4 Ви очаква много по-подробно описание на най-добрите практики в сектора, за да можете да управлявате данните във Вашата организация в крак с най-новите стандарти, а глава 6 е изцяло посветена на реални казуси и успешни истории, за да ви покажем, че защитата на данните не е ниша, а просто изисква правилните инструменти, знания и нагласи.

Нарушение на GDPR в образователна среда 

Разгледайте следния пример за нарушение на данните в учебен център за възрастни. Хакер се възползва от уязвимост в онлайн платформата за обучение на институцията, като получава достъп до лични данни, включително имена, имейл адреси и информация за курсове. Последиците от инцидента не само излагат институцията на значителни глоби съгласно ОРЗД, но също така накърняват репутацията ѝ и подкопават доверието сред учениците и персонала.

В отговор институцията предприема няколко стъпки за подобряване на мерките си за защита. Тя извършва задълбочен преглед на дейностите си по обработка на данните, актуализира политиките си за защита, въвежда по-строг контрол на достъпа и осигурява допълнително обучение за целия персонал по киберсигурност и защита на данните. Тези мерки помагат на институцията да постигне съответствие със закона и затвърждава ангажимента ѝ да защитава личните данни на своята общност.

Поглед към бъдещето 

С неспирното развитие на цифровите технологии, регулаторната среда също ще се променя. За всеки, който работи в образователния сектор, е от съществено значение да бъде информиран за промените в законите и разпоредбите, като актуализациите на GDPR или въвеждането на нови стандарти за защита на данните. Като насърчават култура на спазване на правилата и дават приоритет на

защитата на данните като област, която е от голяма важност и не все още не получава вниманието, което заслужава, институциите за обучение на възрастни могат не само да избегнат правни капани, но и да изградят доверие и увереност сред своите обучаеми и персонал.

В следващата глава ще навлезем по-дълбоко в някои практически стратегии съобразеи със законодателството, както и полезни ресурси, на които можете да разчитате за изпълнението им.

4

ДОБРИ ПРАКТИКИ И СТРАТЕГИИ

Въпреки общата проблематика, която поражда нуждата от тази електронна книга, сложната мрежа от информация и най-различни възможности, предоставена от интернета, има и много положителни страни. Както виждате, тя може да бъде използвана в наша полза, а самото Ви участие тук е само малка част от глобалните усилия да се гарантира, че има достатъчно подкрепа за безопасното и добросъвестно използване на технологичните постижения.

Направили сме всичко възможно, за да разберем Вашите нужди като професионалисти в сферата на образованието, както и да стигнем до правилния път това да Ви подготвим да се справяте със сложностите, които идват с все по-широкото използване на цифровите технологии.

Въпреки невъзможността да се адаптираме изцяло към Вашите обстоятелства - което означава, че тази електронна книга несъмнено ще Ви остави с много въпроси - моля, имайте предвид, че добрите практики и стратегии, които ще прочетете тук, се отнасят до това как да гарантирате, че независимо от услугите, които Вашата организация предлага, тя следва общи стандарти за защита на данните, макар и по специфичен за дейността си начин. Това се отнася и към Всички ваши колеги, които взеха пряко или косвено участие в нашето изследване.

Можете да бъдете сигурни, че тук има нещо и за Вас.

Пейзажът 

Най-добрият ни залог тук е да ви предоставим най-подходящите ресурси, които можете да използвате, за да осигурите висок стандарт на киберсигурност във Вашата организация, независимо от това къде се намирате в ЕС. Тези ресурси могат да Ви послужат за бъдещи справки в областта на защита на личните данни, както и да се превърнат в основа, на която да стъпите.

Европейски комитет по защита на данните (**ЕКЗД**) и национални органи за защита на данните (ОЗД): Комитетът предоставя изчерпателни насоки относно спазването на ОРЗД, като предлага

документи, често задавани въпроси и решения, които разясняват прилагането на регламента. По подобен начин всеки член на ЕС има свой собствен ОЗД, който предлага локализирани насоки и ресурси, съобразени с националния контекст и законодателство. Използването на тези ресурси може да помогне на образователните институции по следните начини:

- **Разбиране на изискванията на ОРЗД**: Придобиване на подробна представа за разпоредбите на GDPR, които са от значение за образователния сектор.
- **Разработване на политики за защита на личните данни**: Създаване или усъвършенстване политиките за поверителност на данните, чрез използване на шаблони и насоки за добри практики.
- **Обучение и повишаване на осведомеността**: Провеждане обучения, като използване на насоките на ЕКЗД и ОЗД, за да се гарантира, че персоналът е добре информиран за своите роли в областта на защитата на данните.

Национални органи зазащита на данните (**ОЗД**): Органите за защита на данните на всяка държава членка предоставят важни, специфични за страната насоки относно законите за защита на данните, които могат да допълват или да се различават от ОРЗД. Тези локални съвети са от съществено значение за:

- **Местното съответствие**: Разбирането и спазването на националните разпоредби, които надхвърлят обхвата на GDPR.
- **Процедурите за уведомяване за нарушения**: Спазване на специфични процедури за уведомяване за нарушаване на сигурността на данните съгласно изискванията на местното законодателство.
- **Ръководството по местни въпроси**: Разглеждане на уникални проблеми, като например използването на онлайн хранилища или трансгранично пренасяне на данни, в рамките на местния контекст.

Международна асоциация на професионалистите по защита на личните данни (**IAPP**): IAPP е глобална организация, която предлага

ресурси, сертифициране и обучение в областта на защитата на личните данни. Техните материали са особено полезни за специалисти в областта на образованието, които искат да задълбочат познанията си за законите и практиките за защита на личните данни. Те предоставят:

- **Образователни ресурси**: Курсове и сертифициране за повишаване на знанията за поверителност на данните.
- **Възможности за работа в мрежа**: Връзки с други професионалисти в областта на защитата на личните данни за споделено обучение и подкрепа.

ЮНЕСКО: ЮНЕСКО предлага ръководства за политики и ресурси, насочени към защитата на личните данни в образованието. Тези ресурси се застъпват за защитата на данни на учениците и насърчаване на етичните практики при използването на образователни технологии. Те осигуряват:

- **Наръчници за политики**: Рамки за разработване на политики за защита на данните на учениците.
- **Етични насоки**: Най-добри практики за отговорно използване на образователните технологии.

Microsoft Education: Майкрософт предоставя ръководство, специално насочено към поверителността и сигурността на данните за образователните институции, което обхваща най-добрите практики за защита на личната информация при използване на цифрови инструменти. Ръководството им включва:

- **Мерки за сигурност на данните**: Стратегии за защита на данните в платформите на Microsoft.
- **Съответствие с изискванията за поверителност**: Осигуряване на съответствие със законите за защита на данните при използване на продуктите на Microsoft.

Агенцията за киберсигурност на Европейския съюз (**ENISA**): ENISA предлага обширни ресурси за киберсигурност и най-добри практики за защита на данните в различни сектори, включително този на

образованието. Те предоставят:

- **Насоки за киберсигурност**: Стратегии за защита на данните в образованието.
- **Инструменти за оценка на риска**: Инструменти за оценка и намаляване на рисковете при защита на данните.

European Schoolnet: Мрежата на европейските министерства на образованието European Schoolnet предлага ресурси и проекти, свързани с технологиите в образованието, включително най-добрите практики за защита на личните данни и сигурността. Те предоставят:

- **Образователни проекти**: Инициативи, насочени към безопасното интегриране на технологиите в училищата.
- **Насоки за добри практики**: Препоръки за защита на данните на учениците.

Световен форум за защита на данните: Онлайн платформа, предлагаща новини, информация и уебинари за защита на данните и неприкосновеността на личния живот. Тя предоставя специфично за сектора съдържание, включително сесии, свързани с образователния сектор, като:

- **Уебинари и семинари**: Обучения и актуализации на най-новите тенденции в областта на защитата на данните.
- **Прозрения за индустрията**: Статии и доклади по възникващи въпроси в областта на защитата на данните.

Coursera и **LinkedIn Learning**: Тези платформи предлагат онлайн курсове по киберсигурност и законовата рамка за защита на данните. Те предоставят:

- **Професионално развитие**: Помагат на професионалистите да бъдат в крак с най-добрите практики за защита на личните данни.
- **Програми за сертифициране**: Удостоверения, които показват експертни познания в областта.

Национална база данни за уязвимости (**NVD**): NVD се управлява от NIST и предоставя информационно хранилище за софтуерни

уязвимости. Въпреки че е базирана в САЩ, тя е ценен ресурс и за европейските организации поради всеобщия характер на цифровите софтуери. Базата редлага:

- **Сигнали за уязвимост**: Актуализации за най-новите заплахи за киберсигурността.
- **Инструменти за управление на риска**: Ресурси за управление и намаляване на рисковете за сигурността.

Използвайки тези ресурси спрямо начина, по който се отнасят към Вашата работа, Вие ще бъдете на сигурен път към разработването на стратегия за защита на данните във Вашата организация, независимо на кое ниво. Намерли сме за Вас насоки за прилагане, разработване и поддържане на надеждни мерки за поверителност и защита на данните, които могат да Ви послужат като основен източник на знания в областта. Моля, изтеглете придружаващия файл, за да получите пълната версия на ресурсите.

Първото нещо, което трябва да знаете, преди да приложите каквито и да било процедури за защита, е какви точно данни, как и защо ще ги събирате.
Оттук произтича всичко останало.

Киберхигиена

Компютърната хигиена, често наричана „киберхигиена“, е основен аспект от поддържането на сигурността във всяка организация. Тя подпмага предотвратяването на пробиви в данните и други инциденти на сигурността, които могат да възникнат от най-простите ежедневни действия. Ето някои от най-добрите практики за поддържането на компютърна хигиена.

Силни пароли и удостоверяване на автентичността:

- **Използвайте силни, уникални пароли**: Служителите трябва да създават силни, уникални пароли за *всеки* свой акаунт. Силната парола включва комбинация от главни и малки букви, цифри и специални символи.

- **Избягване на повторното използване на пароли**: Повторното използване на пароли в различни акаунти е често срещано и носи голям риск от пробиване в дългосрочен план. Всеки акаунт трябва да има уникална парола, тъй като само една компрометирана парола може да доведе до множество пробиви.
- **Двуфакторна автентификация** (**2FA**): Където е възможно, 2FA винаги трябва да е включена за допълнително ниво на сигурност. Тази опция добавя втора форма на проверка, като например код, изпратен на мобилно устройство, в допълнение към паролата.
- **Национален институт за стандарти и технологии** (**NIST**): NIST предоставя изчерпателни насоки за създаване и управление на сигурни пароли и многофакторно удостоверяване. Специална публикация на NIST 800-63B

Редовни актуализации на софтуера:

- **Поддържайте системите и софтуера актуализирани**: Уверете се, че всички операционни системи, софтуер и приложения са актуализирани с най-новите пачове за сигурност. Тези актуализации често са насочени към уязвимости, които могат да бъдат използвани от киберпрестъпници.
- **Автоматични актуализации**: Когато е възможно, включете опцията за автоматични актуализации, за да сте сигурни, че системите Ви винаги работят с най-новите версии.
- **Агенцията за киберсигурност и инфраструктурна сигурност (CISA)** подчертава значението на поддържането на актуален софтуер за защита от уязвимости, които могат да бъдат използвани от нападатели. Те препоръчват редовно да проверявате и да прилагате актуализации на всички софтуери и системи. CISA „Keeping Up with Patches".

Електронна поща и фишинг:

- **Бъдете предпазливи с имейлите**: Служителите трябва да бъдат обучени да разпознават фишинг имейли и да избягват да кликат върху подозрителни връзки, или да изтеглят прикачени файлове от непознати податели.

- **Проверявайте исканията за чувствителна информация**: Винаги проверявайте автентичността на всяко искане за чувствителна информация, дори и да изглежда, че идва от надежден източник. Това може да включва директна връзка с подателя на искането чрез известна и надеждна контактна информация.
- **Федералната търговска комисия (FTC)** предоставя съвети за разпознаване и избягване на фишинг измами. В тях се подчертава, че трябва да се внимава с нежеланите имейли и да не се клика върху подозрителни връзки. Как да разпознаваме и избягваме фишинг измами

Безопасно сърфиране в интернет:

- **Използване на сигурни връзки**: Служителите трябва да се уверяват, че използват сигурни, криптирани връзки (HTTPS в URL кода), когато сърфират в интернет, особено когато притежават достъп до чувствителна информация.
- **Избягвайте обществения Wi-Fi**: Обществените Wi-Fi мрежи могат да бъдат несигурни. Служителите трябва да избягват достъпа до чувствителна информация през тях и, при необходимост, да използват VPN.
- **Агенцията на Европейския съюз за киберсигурност (ENISA)** предоставя палитра от ресурси за безопасно използване на интернет, като препоръчва използването на сигурни уебсайтове (HTTPS), избягване на подозрителни сайтове и предпазливост при изтеглянето на файлове.

Сигурност на устройствата:

- **Подсигурявайте устройствата си**: Винаги заключвайте компютрите, лаптопите и мобилните устройства, когато не сте на бюрото си, дори за кратко време.
- **Защита на USB и външни устройства**: Избягвайте да използвате непознати или ненадеждни USB устройства и външни устройства. Използвайте криптирани USB устройства за прехвърляне на поверителна информация.
- **Институтът SANS** предлага насоки за защита на устройствата,

като например заключване на екрани, криптиране на данни и използване на сигурни пароли. Информираност за сигурността на Института SANS.

Архивиране на данни: 

- **Редовни резервни копия**: Редовно създавайте резервни копия на важни данни на сигурни места. Уверете се, че тези копия са криптирани и се съхраняват отделно от основните системи.
- **Тестване на резервните копия**: Периодично тествайте резервните копия, за да се уверите, че данните могат да бъдат успешно възстановени.
- **Международната организация по стандартизация (ISO)** предоставя стандарти за управление на информационната сигурност, които включват насоки за стратегии за архивиране на данни, за да се гарантира целостта и наличността на данните. ISO/IEC 27031:2011.

Сигурен достъп и разрешения: 

- **Ограничаване на достъпа до чувствителни данни**: Достъпът до чувствителни данни трябва да бъде ограничен до тези, които се нуждаят от тях, за да изпълняват служебните си задължения. Прилагане на принципа на най-малките привилегии.
- **Използвайте контрол на достъпа, основан на роли (RBAC)**: Използвайте RBAC, за да гарантирате, че служителите имат достъп само до данните и системите, необходими за техните роли.
- **Центърът за интернет сигурност (CIS)** предлага контроли за управление на достъпа и потребителските права, като гарантира, че само упълномощени потребители имат достъп до чувствителна информация. CIS Controls v8.

Физическа сигурност: 

- **Защитени работни станции**: Уверете се, че работните места са физически обезопасени, като оборудването, като компютри и твърди дискове, е заключено, за да се предотврати кражба.
- **Изхвърляне на данни по подходящ начин**: Използвайте

подходящи методи за премахване на чувствителни данни, като например унищожаване на документи или използване на софтуер за изтриване на данни за цифрови файлове.

Обучение и повишаване на осведомеността за сигурността: 

- **Редовно обучение**: Осигурете редовно обучение и актуализации относно най-новите заплахи за сигурността и най-добрите практики. Поддържайте служителите информирани за фишинг, зловреден софтуер и други киберзаплахи.
- **Симулирани атаки**: Провеждайте симулирани фишинг атаки, за да тествате и подобрите способността на служителите да разпознават и да реагират на фишинг опити.
- **Институтът SANS** предоставя разнообразни обучителни материали за повишаване на осведомеността и обучение на служителите относно най-добрите практики за сигурност. SANS Security Awareness (Информираност за сигурността)

Готовност за реакция при инциденти: 

- **Докладване на инциденти**: Насърчавайте служителите да докладват незабавно на ИТ екипа или на екипа по сигурността за всяка подозрителна дейност или инцидент, свързан със сигурността.
- **План за реагиране**: Разполагайте с ясен план за реакция при инциденти, в който са описани стъпките, които трябва да се предприемат в случай на нарушаване на сигурността на данните или друг инцидент, свързан със сигурността.
- **Националният център за киберсигурност (NCSC)** предлага насоки за създаване на план за реагиране при инциденти, в който подробно се описва как да се управлява и реагира ефективно на инциденти със сигурността. Управление на инциденти на NCSC

Важно е тези практики не само да се прилагат, но и **редовно да се преразглеждат** и укрепват чрез непрекъснато обучение и актуализации. Създаването на **култура на сигурност** в организацията, при **която всеки служител разбира значението на**

добрата киберхигиена, е от ключово значение за поддържането на сигурна среда.

Заключавайки тази глава ние сме длъжни да подчертаем още веднъж и значението на това да останете информирани и проактивни в постоянно променящия се пейзаж на защитата на данните.

В глава 5 ще разгледаме последните иновации и нововъзникващите тенденции в областта на защитата на данните, като ви предоставим информация за бъдещите развития, както и как да се подготвите за тях. Нека продължим напред с нагласата, че цифровите технологии тепърва ще се развиват и това да поддържаме нашата информираност е от ключово значение за ефективната ни навигация в този непрестанно променящ се пейзаж.

5

ИНОВАЦИИ И ВЪЗНИКВАЩИ ТЕНДЕНЦИИ

До този момент би трябвало да сте достатъчно добре запознати с основните разпоредби за защита на данните, рисковете и методите за осигуряване на съответствие на Вашата организация с GDPR, за да знаете, че едва ли това, което предлага проектът DataGame, ще се окаже достатъчно, за да покрие всички подробности по темата.

Ето защо тук идва моментът да ви успокоим, че това далеч не е нашата цел.

Всъщност, основното послание, което се опитваме да Ви предадем тук, е, че човек не може да не направи всичко възможно, за да остане информиран и по този начин да е наясно с възможностите си. Ние високо ценим индивидуалната отговорност да бъдем в крак с това, което предстои в областта на киберсигурността.

От наша страна най-добрият ни залог е да ви предоставим преглед на най-новите тенденции и да ви дадем някои съвети как да бъдете в крак с всичко, което със сигурност ще последва.

Възходът на изкуствения интелект и машинното обучение в областта на защитата на данните

Изкуственият интелект (AI) и машинното обучение (ML) правят революция в защитата на данните, като предоставят усъвършенствани инструменти за наблюдение, откриване и реагиране. Тези технологии повишават сигурността чрез идентифициране на необичайни модели и потенциални нарушения в реално време, което позволява бързи действия и намаляване на потенциалните щети.

Системи за наблюдение и сигнализиране

Решенията за сигурност, базирани на изкуствен интелект, използват машинно обучение за непрекъснато наблюдение на мрежовата активност, откриване на аномалии и предоставяне на предупреждения в реално време за потенциални инциденти със сигурността. Тези системи анализират големи обеми от данни, за да идентифицират

заплахи, като например неоторизиран достъп или нарушаване на сигурността на данните, които могат да останат незабелязани от човека. Примери за такива инструменти са:

- Darktrace: Използва изкуствен интелект за автономно откриване и реагиране на киберзаплахи.
- Splunk: Анализира машинно генерирана *big data* за подробности и открития в областта на сигурността.
- IBM QRadar: интегрира анализи и машинно обучение за определяне на приоритетите на заплахите.

Професионален съвет: Внедряването на решения за сигурност, базирани на изкуствен интелект, може значително да намали човешките грешки чрез автоматизиране на процесите на откриване и реагиране, като гарантира непрекъснато спазване на стандартите за защита на данните.

Блокчейн: **Нова граница за сигурността на данните**

Блокчейн технологията предлага децентрализиран и сигурен метод за съхранение на данни, известен с приложението си в криптовалутите. Нейният децентрализиран характер гарантира, че данните са разпределени в множество възли, което прави подправянето им почти невъзможно. Тази технология се използва все по-често за защита на личните данни и осигуряване на прозрачност при обработката на данни.

Децентрализираният характер на блокчейн

В блокчейн данните се съхраняват в разпределена мрежа от възли (отделни компютри). Всеки възел поддържа копие на блокчейн и потвърждава транзакциите, като гарантира, че данните не могат да бъдат променяни без консенсус от цялата мрежа. Тази функция осигурява надеждна рамка за сигурност за различни приложения, включително академични записи.

Примери в образованието:

- Blockcerts на MIT Media Lab: Система за издаване и проверка на базирани на блокчейн академични удостоверения.

- Blockchain на Sony Global Education: Защита на академични записи и сертификати, като улеснява надеждната проверка на удостоверенията.

Забавен факт: Някои университети вече използват дипломи, базирани на блокчейн, които в близко бъдеще могат да се превърнат в стандарт за цифрови удостоверения!

Бъдещето на съгласието: Динамично и детайлно съгласие 

Традиционните механизми за даване на съгласие за обработване на данни се развиват към по-динамични и гранулирани модели. Тези нови системи позволяват на физическите лица да управляват предпочитанията си за данните в реално време, като посочват какви данни искат да споделят и за какви цели.

- OneTrust: Предоставя платформа за управление на съгласието и предпочитанията.
- TrustArc: Предлага инструменти за динамично управление на съгласието, което позволява цялостен контрол върху настройките за поверителност на данните.

Творческа идея: Разработете завладяващ и лесен за използване панел за управление на предпочитанията за данни на обучаемите и персонала, който прави настройките за поверителност достъпни и лесни за разбиране.

Интернет на нещата (IoT) и поверителност на данните 

Интернет на нещата обхваща мрежа от физически устройства, свързани с интернет, които могат да събират и обменят данни. В образователната среда това включва интелигентни класни стаи и технологични аксесоари, които поставят нови предизвикателства пред защитата на личните данни поради огромните количества данни, които генерират.

Прилагане на мерки за сигурност за устройствата на IoT:

За да се защитят данните, събирани от IoT устройствата, трябва да бъдат взети следните мерки:

- Сегментиране на мрежата: Изолиране на IoT устройствата в отделни мрежи, за да се ограничи разпространението на потенциални пробиви.
- **Редовно актуализиране на фърмуера**: Уверете се, че устройствата са актуализирани, за да се предпазят от уязвимости.
- **Силна автентификация**: Използвайте надеждни методи за удостоверяване, за да защитите достъпа до устройствата.

Идея за активност: Организирайте семинари на тема „Сигурност на интелигентните устройства“, за да обучите персонала и учениците си за защитата на техните лични устройства и данни.

Подготовка за бъдещи разпоредби и стандарти

С развитието на технологиите се развиват и разпоредбите за защита на данните. Поддържането на информираност за предстоящи промени, като например актуализации на GDPR или нови международни разпоредби, е от решаващо значение за поддържане на съответствие със закона.

Как да останете информирани и да бъдете проактивни:

- **Абонирайте се за бюлетини**: Бъдете в крак с актуализациите на организации като Международната асоциация на професионалистите по защита на личните данни (IAPP).
- **Участвайте в конференции и уебинари**: Участвайте в събития като семинари на Европейския комитет по защита на данните (EDPB).
- **Професионални мрежи**: Включете се във форуми и групи като LinkedIn, фокусирани върху поверителността и защитата на данните.

Примери за проактивни мерки:

- **Редовни одити**: Провеждайте редовни одити, за да гарантирате спазването на новите разпоредби.
- **Правни консултации**: Работете с правни експерти за тълкуване и прилагане на законите за защита на данните.

Доза вдъхновение: Отнасяйте се към защитата на данните не

само като към правно задължение, но и като към ангажимент за почтеност и отговорност, поставяйки стандарт във вашата област.

Непрекъснато обучение и професионални мрежи:

- Австрийско компютърно общество (OCG)
- Българска асоциация за компютърна техника (ACM)
- Кипърско компютърно общество (CCS)
- Гръцки орган за защита на данните (HDPA)
- Ирландско компютърно общество (ICS)

Мостът между иновациите и реалното въздействие

Както вече разбрахме, изкуственият интелект, блокчейн технологията, механизмите за динамично съгласие, интернетът на "нещата" и постоянно адаптиращата се регулаторна среда допринасят за скоростни развития в практиките за защита на личните данни. Технологичните постижения на новото време предлагат обещаващи решения на сложните предизвикателства, пред които са изправени всички организации при отговорното и сигурно управление на големия обем от данни, които генерират на ежедневна база.
Разбирането на тези технологии обаче е само първата крачка. Тяхното прилагане и осезаемите ползи, които те носят на образователните институции (и не само), непосредствено подлежат на внимателно разглеждане от всяко ниво на йерархията в една организация.

В следващата глава сме Ви подготвили казуси и истории на успеха, които подчертават как такива иновативни решения се прилагат в реални обстановки, както и как организации със слаби или липсващи процедури за поверителност и защита на данните са успели да преодолеят предизвикателството да гарантират, че услугите им отговарят на стандартите. Ще разгледаме случаи на успешна навигация в сложния пейзаж на защита на данните, на предизвикателства, превърнати във възможности, както и на установяване на нови стандарти за поверителност и сигурност. С това целим да Ви дадем практическа представа и вдъхновение, като покажем най-добрите практики и научените уроци от практиката.

6

КАЗУСИ И ИСТОРИИ НА УСПЕХА

Време е за малко мотивация!

Великите учители знаят, че мотивацията е твърде мимолетен фактор в кривата на компетентностното развитие, за да окаже съществено влияние върху резултите от него. Въпреки това, в правилния момент малка доза мотивация може да изиграе важна роля.

Ето защо, преди да споделим с Вас историите на някои Ваши колеги относно придобиването на нужните знания, инструменти и умения, необходими за справяне с възникващи проблеми на защитата на данните в една образователна институция, трябва да Ви предупредим, че те най-вероятно ще бъдат приложими за Вашия случай само донякъде.

НО - щом те могат, значи и Вие можете!

Казус 1

Coursera - Навигация в спазването на глобалните изисквания за защита на данните

Coursera, една от най-големите онлайн платформи за обучение в световен мащаб, се сблъска със значителни предизвикателства с влизането в сила на GDPR през 2018г. Огромното количество лични данни, включително информация за студентите и техните навици на учене, с които компанията разполага в международен мащаб, биват от ден до пладне подложени на стриктно спазване на палитра от нови административни разпоредби. Преди това подходът на Coursera към управлението на данните е бил стандартен за индустрията, фокусирайки се върху събирането и използването на данни с цел персонализация и маркетинг.

Всъщност, много организации от този бранш подценяват сложността и строгостта, необходими за спазването на GDPR. Нагласата често е била, че малки промени в съществуващите им политики за сигурност и поверителност на данните ще бъдат достатъчни. В случая с Coursera е налице е представата, че тъй като компанията предлага предимно

безплатни курсове, финансовите транзакции са това, което привлича по-голямо регулаторно внимание. Тя обаче се оказва съвсем погрешна и организацията е принудена да предприеме сериозни мерки за повишаване на сигурността, за да запази интегритета както на своя бранд, така и на клиентите си.

Реакция и инициативи:

- **Цялостен преглед на съответствието** - Coursera извършва обстоен преглед на практиките си за събиране, съхранение и обработка на лични данни. Прегледът разкрива пропуски, особено в управлението на съгласието и свеждането на данните до минимум.
- **Въвеждане на система за управление на съгласието** - Coursera разработва и внедрява цялостна система за управление на съгласието. Това позволява на потребителите да имат цялостен контрол върху това какви данни споделят и как те се използват, което е в съответствие с изискванията на GDPR за прозрачност и контрол на потребителите.
- **Обучение и повишаване на осведомеността на персонала** - Съществена част от предприетите мерки са и обученията на персонала на всяко ниво от йерархията относно спазването на GDPR. Това включва разбиране на нюансите на регламента и как той се прилага към всяка роли.

Пътят, който Coursera изминава, за да адаптира дейността си съгласно новопостъпилия регламент за защита на личните данни, е примерен. Компанията осъзнава значението на проактивното управление на данните и необходимостта от непрекъснато подобряване на своите практики, като подчертава нуждата от ясна комуникация с потребителите относно техните права върху данните в този процес.

Вътрешната реакция на компанията е смесица от съпротива и неизбежно приемане. Служителите се адаптират към нови работни процеси и регулярни проверки за съответствие. От гледна точка на клиентите, въпреки първоначалните опасения за това как тези

промени ще повлияят на потребителското изживяване, прозрачната комуникация и видимата ангажираност на Coursera към защитата на потребителя помагат за изграждането на доверие.

Опитът на Coursera поставя еталон за други EdTech компании, демонстрирайки важността на привеждането на организационната дейност в съответствие със строгите закони за защита на данните, както и стойността на прозрачността и проактивната нагласа при адаптацията към регулаторни промени.

Казус 2

Университет Гринуич - укрепване на основите

Университетът в Гринуич, Обединеното кралство, се сблъсква със сериозно нарушение на сигурността през 2016г., при което чувствителни информация, свързана със студенти и служители на университета, биват изложени на риск онлайн. Нарушението се дължи на стар микросайт, създаден от отдел за конференция за обучение през 2004 г. Сайтът не е бил изведен от експлоатация по подходящ начин, което го е направило уязвим и води до изтичането на имена, адреси, телефонни номера, а в някои случаи и здравна и финансова информация.

В голяма степен инцидентът е следствие от подценяване на нуждата от строги мерки за защита на личните данни и прекомерно разчитане на наследени остарели системи. Убеждението, че съществуващите мерки са достатъчни, довежда до несериозно отношение към актуализацията на протоколите за сигурност и обучението на персонала. Инцидентът, впоследствие, изиграва ключова роля в предстоящите промени.

Реакция и инициативи:

- **Цялостен одит и анализ на пропуските** - Университетът извършва пълен одит на практиките си за сигурност и обработка на данни. Това включва идентифициране на слабите места в системата, в случая използването на остарял софтуер и

недостатъчно обучение на персонала.

- **Преразглеждане на политиката** - Въведени са нови политики за защита, съобразени с изискванията на GDPR, като се набляга на по-строг контрол на достъпа и криптиране на данните.
- **Програми за обучение и повишаване на осведомеността** - Въведени са задължителни сесии за обучение на всички членове на персонала, в които се подчертава значението на защитата на данните и ролята на всяка длъжност в организацията в опазването на чувствителна информация.

Университетът се сблъсква по трудния начин с необходимостта от проактивно управление на данните. Нарушението в сигурността на системата се явява като катализатор за промяна, която води до по-сигурна и осведомена институционална култура. Персоналът, който първоначално се съпротивлява на новите протоколи, постепенно се адаптира, осъзнавайки важността на своята роля в защитата на данните.

Въпреки първоначалната загриженост и отпор от страна на студентите и университетския персонал, ангажираността и прозрачността при справянето с проблема и подобряването на мерките за защита помогат не само да се възстанови доверието към институцията, но и подчертават именно нуждата от въвеждане на регламенти като GDPR. В по-широка перспектива инцидентът служи като урок за други образователни институции, както и всички организации, които дигитализират дейността си.

Казус 3

Университет на Източна Англия (UEA) - Инцидент с пробив на данни през имейл сървър

През 2017 г. Университетът на Източна Англия (UEA) претърпява сериозен пробив в системата, когато член на персонала изпраща чувствителна лична информация по имейл към злонамерени получатели вследствие на фишинг измама. Компрометираните данни включват имена и адреси на студенти, разкривайки критични

уязвимости в практиките на комуникация и обработка на данни на UEA.

Преди нарушението UEA разчита на стандартни мерки за сигурност, които инцидентът разобличава. Показват се слабости в обучението на персонала, строгостта на процедурите и автоматизираните предпазни мерки. Университетът разчита на основни политики за защита на данните и надценява подготовката на персонала, което допринася за нарушението. В резултат на това UEA изплаща 140,000 лири обезщетение на засегнатите студенти, подчертавайки финансовите рискове и рисковете за репутацията, свързани с подобни инциденти.

Реакция и инициативи:

- **Преразглеждане на политиката:** UEA извършва задълбочен преглед на своите процедури за обработка на данни и комуникация. Това включва прилагането на по-строги протоколи за управление и предаване на чувствителна информация, като се набляга на ограничаването на достъпа само до упълномощени лица.
- **Засилено обучение на персонала:** Университетът въвежда задължителни програми за обучение относно защитата на данните и спазването на GDPR. Тези сесии са фокусирани върху практическите стратегии за безопасно боравене с данни, разпознаване на опити за фишинг и проверка на получателите на имейли при споделянето на чувствителна информация.
- **Инвестиции в системи за предотвратяване на загубата на данни (DLP):** UEA въвежда усъвършенствани DLP технологии за наблюдение и защита на данните в движение. Тези системи са предназначени да предотвратяват неразрешено предаване на чувствителна информация и да гарантират спазването на развиващите се стандарти за защита на данните.

Този казус служи като повратна точка за UEA, водейки до значителни подобрения в подхода им към защитата на данните. Университетът дава приоритет на създаването на култура на висока осъзнатост

в сферата на дигиталната сигурност чрез последователни обучения, технологични инвестиции и прозрачна комуникация в процесите. По този начин се насърчава бдителността и проактивната нагласа в опазването на личните данни.

Макар инцидентът първоначално да предизвика безпокойство сред студентите и персонала, бързата реакция на UEA и откритата комуникация около случая помагат за бързото възстановяване на доверието към учебното заведение, а последващите проучвания и регулярната обратна връзка покават повишена осведоменост и ангажираност по отношение на отговорностите за защита на данните.

Опитът на UEA сега често се цитира като поучителен пример, като се подчертава значението на стабилни стратегии за защита на данните, редовни обучения и интегриране на съвременни защитни мерки в образователните институции. Случаят доказва как дори утвърдени организации са уязвими към човешки грешки, но могат да използват подобни инциденти за стимулиране на значими културни и оперативни промени.

Казус 4

FutureLearn - Управление на промените след навлизането на GDPR

През 2018 г. FutureLearn, водеща платформа за онлайн обучение, се сблъсква със значителни предизвикателства при адаптацията си към изискванията на Общия регламент за защита на данните (GDPR). С разнообразна потребителска база, обхващаща множество държави от ЕС, спазването на строгите разпоредби на GDPR придобива съществено значение за запазване на доверието на потребителите и избягване на потенциални санкции.

Преди въвеждането на GDPR, процедурите на FutureLearn отразяват нормите в индустрията, като дават приоритет на събирането на данни с цел анализ и персонализация. Взимат се основни мерки за криптиране и потребителите могат да избират бисквитките си, но

въвеждането на GDPR разкрива ограниченията на тези практики. Акцентът на GDPR върху правата на потребителя, прозрачността и минимизирането на личните данни налага по-холистичен подход към защитата на чувствителна информация в платформата.

Реакция и инициативи:

- **Оценки на въздействието върху защитата на данните (ОВЗД)** - FutureLearn провежда холистично оценяване, за да идентифицира рисковете, свързани обработката на лични данни. Този процес помага на платформата да приоритизира мерките за смекчаване на последиците, напр. ограничаване на събирането на данни до строго необходимото и подосигуряване на чувствителната потребителска информация с усъвършенствани технологии за криптиране.
- **Гранулирани механизми за съгласие** - FutureLearn обновява своите системи за съгласие, давайки възможност на потребителите да упражняват по-голям контрол върху личните си данни. Платформата въвежда подробни известия за поверителност, които позволяват на потребителите да преглеждат и променят предпочитанията си за споделяне на данни по всяко време. Тези механизми са в съответствие с изискванията на GDPR за прозрачност и овластяване на потребителите.
- **Назначаване на Длъжностно лице по защита на данните (ДЛЗД)** - За да се гарантира постоянното спазване на изискванията, FutureLearn назначава ДЛЗД, което отговаря за надзора на политиките за защита на данните и провеждането на редовни одити, като представлява и точка за контакт за субектите на данни и регулаторните органи.

Прилагането на мерки за съответствие с GDPR се оказва трансформиращ опит за FutureLearn. Във вътрешен план служителите се сблъскват с първоначални предизвикателства, свързани с адаптирането към новите процедури. Платформата обаче се справя с тези пречки чрез специално разработени обучения и ясна комуникация за нуждата от сериозен подход при защитата на данни.

Въпросните мерки не само улесняват прехода, но и насърчават култура на отговорност и сигурност в организацията.

От гледна точка на потребителите промените се приемат добре. Проучванията, проведени след внедряването, показват, че потребителите оценяват повишената прозрачност и контрола върху информацията, която споделят. Много съобщават, че се чувстват по-уверени при използването на платформата, което допринася значително за повишаване на доверието към нея, а с това и нейната репутация.

Този казус подчертава значението именно на проактивното спазване на международните закони за защита на данните, особено за цифровите платформи с глобална потребителска база. Като дава приоритет на прозрачността и овластяването на потребителя, платформата не само изпълнява регулаторните изисквания, но и укрепва отношенията си със своите партньори и клиенти. Урокът тук е, че адаптирането към регулаторните промени може да бъде и стратегическа ход към изграждане на доверие в и към организацията, както и повишаване на надеждността на нейните услуги.

Казус 5

Университет „Еразъм“ - баланс между сигурността и достъпността на данните

През 2020 г. университетът „Еразъм“ става жертва на таргетирана фишинг атака, която компрометира чувствителни данни, включително лична информация на студенти и служители. Инцидентът разкрива уязвимости в инфраструктурата за киберсигурност на университета и подчертава предизвикателствата, свързани с балансирането на сигурността на данните със свободния достъп, необходим за академични цели.

Преди нарушението университетът работи при относително отворена политика за достъп до данни, за да улесни научните изследвания и административната ефективност. Този подход произлиза от

убеждението, че академичният характер на институцията я прави по-малко привлекателна за киберпрестъпниците. Фишинг инцидентът обаче разкрива критични пропуски в подхода на университета към сигурността на данните, което налага сериозна преоценка на приоритети.

Реакция и инициативи:

- **Усъвършенствана рамка за киберсигурност** - Университетът „Еразъм" обновява своята инфраструктура за киберсигурност след атаката. Мерките включват въвеждането на многофакторна автентикация (MFA) за защита на потребителски акаунти и прилагането на усъвършенствани протоколи за криптиране на чувствителни данни както при обмен, така и в съхранение.
- **Кампания за повишаване на осведомеността** - Признавайки, че пробивът е следствие от фишинг атака, университетът стартира цялостна кампания за повишаване на осведомеността относно такив тип измами. Инициативата включва:
  - Редовни сесии за обучение на персонала и студентите за разпознаване и избягване на опити за фишинг.
  - Упражнения със симулирани фишинг атаки, в които се тества и подобрява реакцията на общността към този вид кибератаки.
  - Разработване на вътрешна система за докладване, която насърчава бързото докладване на подозрителни имейли или дейности.
- **Преразглеждане на контрола на достъп до данни** - За да намали рисковете, университетът приема по-строги политики за достъп до данни, основани на принципа на "най-ниски привилегии". Достъпът до чувствителни данни бива ограничен до упълномощени лица със строго категоризирана дейност спрямо съответните данни, което намалява възможността за злоупотреба или случайно излагане на риск.

Тази фишинг атака води до ключови промени в университета „Еразъм". Инцидентът подчертава необходимостта от постоянна бдителност

към променящото се естество на заплахите за киберсигурността в академичните институции, които не могат да бъдат подценявани. Балансирането на достъпността със солидни мерки за сигурност се превръща в ключов елемента.

Както и при другите казуси, пробивът първоначално предизвиква опасения сред персонала и студентите относно потенциалната злоупотреба с техните данни. Такива инциденти много често провокират паника и недоверие. “Еразъм” университетът реагира бързо, като поддържа прозрачна комуникация относно атаката и стартира кампания за повишаване на фишинг осведомеността, а повишените мерки за сигурност включват не само оперативни, но и културни промени. Киберсигурността започва да се разглежда като споделена отговорност. Този подход доказано работи за превенцията и значителното намаляване на риска във всякакъв вид институции и е примерен.

Успешна иновация 1

Университетът в Никозия, глобален лидер в блокчейн образованието, отрано признава трансформационния потенциал на блокчейн технологията за повишаване на сигурността и поверителността на данните в академичната документация.

Какво е блокчейн?
Това е децентрализиран цифров регистър, който записва, съхранява и проверява данни по начин, устойчив на фалшифициране. Този метод подсигурява идеална за защита на чувствителна информация във всяка сфера, включително тази на образованието, където може да бъде интегриран в различни операции.

Защо блокчейн?
Университетът идентифицира належаща нужда от справяне с неефективността и уязвимостта на традиционните системи за управление на данни. Конвенционалните мерки за съхранение на

информация стават все по-податливи на фалшифициране, неоторизиран достъп и административни грешки.

Тъй като университетите боравят с огромни количества чувствителни данни, търсенето на сигурни и прозрачни решения за управлението им е значително. Това търсене се обуславя от повишената осведоменост относно поверителността и сигурността в днешно време, регулаторните изисквания като GDPR и необходимостта от надеждни процеси за проверка в един все по-дигитален свят.

Първоначално блокчейн се сблъска с критики заради това, че се разглежда като нишова технология, свързана предимно с криптовалути. Скептиците поставят под въпрос мащаба на регистъра, регулаторните последици и практичността за нефинансови приложения. Въпреки това, когато университетът проучва децентрализираните и неизменни характеристики на блокчейн - наред със способността му да осигурява прозрачност и сигурност - стана ясно, че тези характеристики могат ефективно да се справят с тези предизвикателства.

Инициативи:

- *Система за издаване на удостоверения, базирана на блокчейн*: Университетът разработва система, базирана на блокчейн, за издаване и проверка на академични удостоверения. Всяка диплома или сертификат се съхранява като криптографски защитен блок. Това гарантира, че удостоверенията са защитени от фалшифициране, като същевременно остават лесно достъпни и за студентите, и за завършилите чрез уникални цифрови ключове. Дипломантите могат да споделят удостоверенията си директно с работодатели или институции, без да изискват проверка от трета страна, което намалява административните разходи и повишава доверието в автентичността на техните квалификации.
- *Пилотни програми и ангажираност:* За да се справи със скептицизма и да демонстрира надеждността на системата, университетът стартира пилотни програми, включващи избрани

студентски кохорти. Тези програми демонстрират как удостоверенията с помощта на блокчейн могат да бъдат издавани по сигурен начин и незабавно проверявани от работодателите с помощта на прости цифрови инструменти. Чрез ангажиране на заинтересованите страни - включително студенти, преподаватели и индустриални партньори - университетът събира ценна обратна връзка, която помогна за усъвършенстване на функционалността на системата и за преодоляване на опасенията относно практическото ѝ приложение.

- *Съвместна научноизследователска и развойна дейност*: Университетът в Никозия започва да си партнира с други образователни институции и експерти в областта на блокчейн. Сътрудничеството е насочено към оптимизиране на механизмите за консенсус (процесът, чрез който се валидират блоковете), за да се осигури ефективност, без да се прави компромис със сигурността. Тези партньорства се занимават и с въпросите на регулаторното съответствие, като гарантират, че системата не само спазва международните стандарти за защита на данните като GDPR, но и е една стъпка пред тях, обменяйки информация за текущите пречки в поддържането на сигурността и поверителността на лични данни.

Въздействие:

Възприемането на блокчейн технологията има широкообхватни ползи за университета:

- *Повишена сигурност на данните*: Неизменчивостта на блокчейн гарантира, че академичните записи не могат да бъдат променяни или фалшифицирани.
- *Оптимизирани административни процеси*: Проверяването на удостоверения се прехвърля от трети страни (организации), които действат като посредници - директно към блокчейна. Нуждата от такива посредници, които носят свой риск за киберсигурността, отпада, тъй като удостоверенията се съхраняват директно в децентрализирания цифров регистър.
- *Повишено доверие към академичната база*: Работодателите и

институциите придобиват по-голяма увереност в автентичността на удостоверенията благодарение на прозрачния процес на проверка, който блокчейн технологията предлага.

Ползи от страна на заинтересованите страни: Студентите оценяват възможността да контролират собствените си удостоверения, а служителите признават повишаването на ефективността от автоматизирането на тези процеси.

Перспектива:

Инициативата на Университета в Никозия подчертава как блокчейн технологията може да революционизира управлението на данни в образованието, като осигури сигурни и прозрачни решения за удостоверяване на самоличността. Всяка институция, която търси иновативни начини за повишаване на сигурността на данните, като същевременно подобрява оперативната ефективност, би имала голяма полза от имплементирането на Блокчейн в тази насока. , Университетът в Никозия служи именно за пример как нововъзникващите технологии могат да се справят с реални предизвикателства в академичния свят.

Успешна иновация 2

Разширявайки своите цифрови услуги и платформи за онлайн обучение, Държавният университет на Джорджия (GSU) се сблъсква с все по-големи предизвикателства при опазването на чувствителни данни на студентите, персонала и институциите, с които работи.

През последните години образователни институции като GSU са все по-честа мишена за киберпрестъпниците поради огромните си хранилища на ценна информация, включително лични, финансови данни и интелектуална собственост. От друга страна, традиционните мерки за киберсигурност правят университета уязвим за все по-сложни кибератаки, включително такива подсилени с изкуствен интелект и усъвършенствани тактики за социално инженерство.

Киберпрестъпниците използват силно персонализирани фишинг имейли (spear phishing), гласов фишинг (vishing) и претекст схеми, за

да манипулират хората да разкрият поверителна информация или да предоставят неоторизиран достъп към такава. Тези атаки често имитират доверени източници, като ИТ отдели или университетски администратори, което ги прави особено трудни за откриване. Нещо повече, нападателите започват да използват изкуствен интелект, за да автоматизират и усъвършенстват тези тактики, което допълнително увеличават тяхната успеваемост.

Предизвикателството

Преди да въведе усъвършенствани мерки за сигурност, GSU разчита на конвенционални системи, които работят реактивно - откриват заплахите след възникването им. Общичт консенсус е, че тези мерки са адекватни поради историческата липса на големи пробиви и подценяването на развиващия се пейзаж на киберзаплахите. Ограниченията във финансирането също играят роля, тъй като киберсигурността често е отхвърляна като приоритет в полза на оперативните нужди. Това краткосрочно мислене обаче не взима предвид дългосрочните разходи от подценяването на киберсигурността, включително потенциалните правни отговорности, оронването на репутацията и скъпо струващите усилия за отстраняване на нередностите. Високопрофилните инциденти в други институции обаче подчертават уязвимостта на традиционните защити. Например нападателите, които залагат на социалното инженерство като тактика (подобно на тези при пробива в MGM Resorts през 2023 г.), показват колко лесно могат да бъдат откраднати идентификационни данни, включително на ИТ служители. Признавайки, че съществуващите системи не могат да се справят с тези нови заплахи, ръководството на GSU решава да предприеме проактивен подход, като възприема изкуствения интелект (ИИ) като основен елемент от своята стратегия за киберсигурност.

Инициативи

- *Изкуствен интелект в сигурността и поверителността на лични данни:* GSU внедрява инструменти за сигурност, базирани на ИИ, като Darktrace и CrowdStrike. Тези системи използват алгоритми за

- машинно обучение, за да анализират огромни количества мрежови данни в реално време. За разлика от традиционните системи, които разчитат на предварително определени правила, решенията, управлявани от ИИ, откриват аномалии, като идентифицират необичайни модели на поведение - например опити за неоторизиран достъп или необичайни трансфери на данни - които подсказват за потенциални заплахи. С това проактивно идентифициране на уязвимостите и неутрализиране на заплахите в реално време, тези инструменти осигуряват ниво на защита, което традиционните системи няма как да постигнат.

Емпиричен подход в изграждането на стратегия: Изследователската група за киберсигурността на GSU въвежда научен подход за оценка на ефективността на своите инструменти и политики за сигурност. Чрез изучаване на начина, по който нападателите действат в екосистемата на киберпрестъпността - включително методите, средствата и целите на хакерите - университетът разработва точни стратегии за намаляване на рисковете. Този подход гарантира, че всеки внедрен инструмент е подкрепен от измерими резултати, а не от предположения.

Програми за повишаване на осведомеността: Признавайки, че човешкият фактор е най-слабото звено в защитата на киберсигурността, GSU стартира всеобхватни програми за обучение на студенти и служители. Тези програми се фокусират върху разпознаване на опити за фишинг, опазване на личната информация, както и разбирането на това как точно нападателите прилагат стратегии за социално инженерство. Насърчавайки културата на осведоменост за киберсигурността, GSU дава възможност на своята общност да приема по-голяма отговорност да изгради автономност в защитата срещу кибератаки.

Академична интеграция: За да продължи ангажимента си към иновациите, GSU въвежда магистърска програма за надеждни системи с изкуствен интелект през своя Център за информационна сигурност и защита на личните данни (INSPIRE). Тази програма дава възможност на специалисти да придобият експертен опит в сферата на киберсигурността и изкуствения интелект, като

- същевременно разглеждат критични въпроси относно справедливостта, прозрачността и етиката при технологичното развитие и имплементирането на иновативни технологии.

Одити и актуализации: GSU институционализира редовни одити на сигурността, за да идентифицира проактивно слабостите в своята ИТ инфраструктура. Тези одити включват стрес тестове на системите срещу симулирани атаки и подсигуряване на съответствие с регулаторните рамки като GDPR. Редовните актуализации гарантират, че всички крайни точки - сървъри, преносими компютри и работни станции - остават защитени срещу новооткрити уязвимости.

Въздействие:

Приемането на мерки за сигурност, управлявани от изкуствен интелект, революционизира способността на GSU да защитава чувствителните данни от все по-сложни киберзаплахи. Преминаването от реактивни защити към проактивни механизми за откриване, подкрепени от машинно обучение, има следните ползи:

- Университетът съкращава времето за реакция от часове или дни до няколко секунди.
- Заплахи като неоторизиран достъп или ексфилтрация на данни биват неутрализирани, преди да причинят значителни щети.
- Нововъведените основани на доказателства практики гарантират непрекъснато подобряване на протоколите за сигурност въз основа на реални резултати.

Освен това, интегрирането на киберсигурността в академичните програми подкрепя подготовката на бъдещи специалисти за възникващите предизвикателства в сферата, наблягайки върху етичните съображения, които са от решаващо значение за укрепване на доверието в технологиите.

Перспектива:

Случаят на GSU демонстрира как образователните институции могат да използват авангардни технологии не само за справяне с непосредствените предизвикателства в областта на

киберсигурността, но и за проактивното предвиждане на бъдещи рискове. Съчетавайки иновативни инструменти с практически основани практики и академични програми, посветени на развиване на нови специалисти, GSU създава модел подражание в защитата на цифровата среда, като същевременно е пионер в квалифицирането и акредитирането на бъдещи поколения. Този далновиден подход подчертава значението на ранното възприемане на иновациите - съществен урок за други институции, които се ориентират във все по-сложния пейзаж на киберзаплахите.

Заключение

Пътят на всяка институция ни предлага ценни уроци - от стриктното преразглеждане на политиките за защита на данни в Университета в Гринуич до пионерското имплементиране на блокчейн в удостоверяване на самоличността в Университета в Никозия. Тези примери показват, че успехите не представляват праволинейно спазване на изискванията, а насърчаване на култура на осведоменост, отговорност и креативност. С други думи, **да бъдеш в крак с времето и със стъпка напред**.

Тези казуси и истории на успеха подчертават необходимостта от цялостен подход, който съчетава организационната среда и политика, технологичния напредък и образованието, за да се създаде сигурна и надеждна учебна и работна среда.

А защо, вместо просто да се поучим от тези случаи, да не ги адаптираме в собствения си контекст?

За тази цел ще ни е нужна определена подготовка и нагласа.

Затова, в следващата глава сме Ви подготвили нещо, което ще помогне на Вас и Вашия екип да затвърдите своите знания и нагласи относно въвеждането на по-строга и надеждна рамка за съхранение и администриране на чувствителна информация. Предстоящите въпросници имат за цел да Ви ангажират, да насърчат критичното Ви мислене и нагласата Ви за учене.

Връщаме се назад - с перспектива за бъдещето - към класната стая!

7

ПРАКТИЧЕСКИ ЗНАНИЯ И НАГЛАСИ

Сега е моментът да проверите знанията си и да видите как точно сегашната Ви нагласа за учене може да Ви бъде полезна в предстоящите Ви начинания в света на сигурността и поверителността!

Като преподаватели, нашето DataGame партньорство е насочено както към практическата и теоретичната част, но към психологическия аспект в ученето. Затова искаме да овластим Вашето прогресивно и сигурно развитие, а не просто да Ви бомбардираме с информация, която *може би* ще Ви бъде полезна.

И така - време е да разберете от *какво* сте направени!

Нагласи и предпочитания

Въпреки разделенията си, човешкият мозък функционира като цялостен орган. И все пак, всеки от нас с времето изгражда свои предпочитания, определящи в какъв ред и доколко те се активират. Тези предпочитания могат да предвидят как ще реагираме в различни ситуации.

Текущият куиз има за цел да Ви провокира да се замислите за своите тенденции на учене, възприемане и прилагане на нова информация. Тематично за нашия контекст - ще видите как точно се ангажирате с новостите и неизбежните отговорности в контекста на поверителността и защитата на лични данни. Той ще насърчи самосъзнанието Ви, подчертавайки както силните Ви страни, така и областите, които можете да подобрите.
Няма „правилни“ или „грешни“ отговори - това е Вашата възможност да опознаете по-добре начина си на мислене!

Моля, последвайте тази връзка, за да попълните куиза. Когато сте готови, запомнете Вашата оценка и преминете към следващата страница, където можете да видите ценна за Вас информация.

Самооценка

Всеки отговор в куиза е съгласен с четирите квадранта на мозъка (*въз основа на концепцията на Neuro-Agility за предния и задния дял на лявото и дясното полукълбо*). Десетте въпроса се отнасят до различни аспекти на обучението в областта на защитата на личните данни. Те са достатъчно общи, за да бъдат приложени независимо от Вашата работна позиция, и достатъчно конкретни, за да ви дадат ясна представа как бихте реагирали в определени ситуации.

Таблицата с квадрантите на следващата страница разделя човешкия мозък на **четири части**, като всеки квадрант съответства на определен „*тип*". Въпреки че хората използваме всеки от тях; когато вземаме решение, действаме в определена ситуация или дори просто мислим, нашите предпочитания (*ляво/дясно полукълбо, преден/заден дял)* се развиват. Съответно, с времето те все по-точно предвиждат водещи или преобладаващи в нас поведения, съответстващи на начина, по който оптимизираме функциите на квадрантите.

Като се позовавате на стойностите във всеки квадрант в таблицата, можете да интерпретирате резултата си:

- Първата стойност (**1000 / *хилядни***) се отнася до **Анализатора**
- Втората стойност (**100 / *стотици***) се отнася за **Стратега**
- третата стойност (**10 / *десетици***) се отнася за **Изпълнителя**
- Четвъртата стойност (**1 / *единици***) се отнася за **Съветника**

Как? Ако резултатът Ви е по-малък от **4 знака**, например, това означава, че не сте избрали нито един отговор, който да съответства на Анализиращия тип. Съответно, ако **нямате единици**, не сте дали нито един отговор в Съветващия тип.
Всички **нули** също означават липса на отговори в даден квадрант.
Въз основа на всяко от числата във Вашия резултат можете да определите в колко от зададените ситуации ще реагирате като Анализатор, Стратег, Изпълнител или Съветник.
Ето един пример:


EXAMPLE
2305
Анализатор
Логичен
Аналитичен
Академичен
Фактически
Реалистичен
Вербален
Точен
Подробен
Стойност:
1000
Стратег
Творчески
Цялостен
Практически
Експериментален
Спонтанен
Футуристичен
Визуален
Общителен
Стойност:
100
Действащ
Целеустремен
Решителен
Конкурентен
Независим
Нетърпелив
Чувствителен
Сдържан
Изпълнител
Стойност:
10
Чувствителен
Сърдечен
Верен
Разбиращ
Подкрепящ
Дипломатичен
Съпричастен
Състрадателен
Съветник
Стойност:
1
EXAMPLE
2305

Изпълнители

Изпълнителите са ориентирани към действието и са отдадени на работата си докрай, като рядко се нуждаят от двойна проверка. Често получават незабавни резултати, проявяват силно чувство за постоянство и посрещат предизвикателствата с усмивка. Те са склонни да се изказват по-ярко, а исканията им могат да прозвучат като заповед. Изпълнителите вземат бързи решения, обичат да решават проблеми и са трудолюбиви и самостоятелни.

Изпълнителите трябва да имат предвид следното:

Изпълнителите могат да изглеждат безчувствени към другите хора и понякога очакват твърде много от другите. Поради прибързаността си понякога не обръщат внимание на рисковете и опасностите. Тъй като са трудолюбиви, те често могат да поемат твърде много работа и не обичат ограниченията. Понякога могат да са нетърпеливи, защото искат да постиганат бързи резултати. Това може да доведе до липса на гъвкавост и непреклонност.

Анализатори

Анализаторите имат силно изявено аналитично мислене и са ориентирани към детайлите. Като цяло те са много спретнати, дисциплинирани и мислят в дълбочина. Изглеждат изключително компетентни, прецизни и проявяват дипломатичност в работата и взаимодействието си с хора. Освен това са изключително отдадени на качеството и подхождат отговорно в живота.

Анализаторите трябва да имат предвид следното:

Анализаторите могат понякога да бъдат нерешителни или неадаптивни в методите си на изпълнение на работата. Често им липсва спонтанност и понякога трудно се доверяват на другите хора. Лесно могат да затънат в твърде много подробности. В определени ситуации анализаторите могат да бъдат големи песимисти и да се вторачват в "грешки". Не обичат конфликтите.

Стратези

Стратезите са носители на мечти и възможности. Те разширяват границите. Като цяло са оптимистични, ориентирани към взаимоотношенията и умеят да общуват с лекота. Обичат да създават приятна атмосфера и са ентусиазирани по отношение на живота и хората. Те са убедителни и често да правят добро впечатление със своята дружелюбност и общителност.

Стратезите трябва да се съобразяват със следното:

Понякога на стратезите им липсва способността да изпълняват своите идеи и задачи. Те са склонни да надценяват способностите си, но могат да бъдат и импулсивни. Трудно им е да казват „не" и заради това често поемат твърде много задачи. Освен това са често са прекалено оптимистични по отношение на крайните резултати и заради това могат да премълчават проблемите. Поради силната си креативност, стратезите могат да правят прибързани заключения и са склонни да манипулират.

Съветници

Съветниците са силно подкрепящи и лоялни хора. Те вдъхват стабилност и сигурност, и това ги прави лесно предвидими и надеждни. Лесно и приятно е общуването с тях. Ориентирани са към това да помагат и могат да бъдат много добри слушатели. Хората често се чувстват в безопасност около тях. Съветниците умеят да съхраняват взаимоотношенията.

Съветниците трябва да имат следното предвид:

Съветниците често се противопоставят на промените и могат да бъдат твърде снизходителни. По отношение на взаимоотношенията, те могат да бъдат нерешителни и притежателни, но и избягват конфликтите. Изпитват затруднения при спазването на крайните срокове и са склонни да отлагат задачите. Те имат добри идеи, но не са толкова инициативни.

Знания и компетенции

Подготвили сме за Вас още един въпросник, за да проверите не само какво сте научили досега, но и да получите още една възможност да придобиете нови знания. Няма нищо лошо в това да тествате наученото, за да видите колко от информацията в тази електронна книга е останала със Вас; какво сте пропуснали; и дали можете да вземете правилното решение в непредвидени обстоятелства.

Наясно сме, че това в известна степен е тест на паметта. Също така, обаче, е и добър начин да разберете доколко сте способни да свържете предоставената информация, с Вашия професионален контекст. Като сложим картите на масата, човешката памет е силно асоциативна и се влияе от нашите емоции, желания и мотиви.
Така че в този смисъл, това е и тест за Вашата ангажираност с темата.

Тестът не е задължителен и сте напълно свободни да продължите с останалата част от книгата. Насърчаваме Ви да се забавлявате с ученето, а не да го правите от чувство за необходимост. Само тогава резултатите могат да бъдат удовлетворяващи.

Така че, пригответе се! Финалната права е зад ъгъла!

Последвайте тази връзка, за да попълните теста.

8

КОМПЕТЕНТНОСТНА РАМКА

Направихте ли тестовете?!
Ако сте, тази глава ще Ви е още по-полезна!

Както вече знаем, ползите от прилагането на цифровите технологии в образованието идват с все по-големи отговорности за институциите. Тъй като количеството информация, която е нужна за предоставяне на образователни услуги, нараства заедно с подновяването на най-различни платформи за обучение (предоставящи лични акаунти с достъп до модули, курсови работи, оценки, библиотека, външни източници на информация, форуми, чатове, лекции, записи и т.н.), с това се отваря и ново поле на знания и компетенции.

За да могат адекватно да отговорят боравят с цифровите инструменти, служителите в тези институции трябва да знаят какви са изискванията на регулаторните органи, определящи законната рамка при администрирането на лична информация за образователни цели, както и да имат нужния ресурс, за да могат правят това безопасно и съгласно закона.

Уменията, необходими за ефективното управление на личните данни, са изключително разнообразни. Ето защо в тази глава сме се постарали да представим една компетентностна рамка, която обхваща знанията и уменията на "обикновения Джо" в четири степени на компетентност.

Независимо дали тепърва започвате или сте готови да ръководите за цели инициативи за защита на личните данни, това е **картата на „обикновения Джо"**, с която можете да проправите своя път на реализация в един нов свят на (кибер)възможности!

В добрия случай тя е хумористично проницателна, а в лошия - просто разграфява четири етапа на развитие по ниво на отговорност, нужни качества за изпълнение и няколко съвета за подобрение.

Ниво 1: “Будният” Джо

Будният Джо тепърва навлиза в света на киберсигурността. Обикновено той може да обясни само, че сферата на защитата на лични данни е прекалено сложна, защото всъщност няма понятие от важността ѝ.

Будният Джо се съгласява със всички бисквитки и понякога се унася по конспиративни теории в съмнителни уебсайтове. Може да е бил на обучение или семинар по правата и защитите на субектите на данни покрай работа, но само за да си потвърди виждането, че “заешката дупка” стига твърде далеч. По-добре е да се занимава. Той използва пиратски “Windows” вкъщи, тегли си филми от “PirateBay” и мрази двуфакторните проверки, защото смята, че му губят времето.

Въпреки вежливостта и бодростта си, Будният Джо има много какво да научи и съответно предоставя риск за всяка организация, в която би работил с лични данни.

Отговорности:

- Всичко, което не включва работа с лични данни.

Знания и умения за подобрение:

- Основно разбиране за това какво представляват личните данни (имена, номера, имейл и IP адреси, и др.).
- Познаване на основните принципи за защита на личните данни (законосъобразност, справедливост, прозрачност).
- Познаване на значението на :съгласието” и минимизацията.
- Запознаване с политиките за защита на личните данни на организацията.

Съвети:

- Посещавайте обучения и семинари за защита на личните данни.
- Бъдете в крак с политиките за защита на данните
- Сверявайте източниците си на информация

Level 2: Работливият Джо

Работливият Джо е осъзнал рисковете, свързани с администрирането на лични данни и е развил силно чувство за отговорност. Макар знанията му да не са големи, отдадеността му е завидна.

Работливият Джо вероятно два-три пъти се е справял с проблем, свързан с опазването на дадено цифрово устройство от киберзаплаха и е видял какви могат да бъдат последиците от компроментирането му. Той проявява адекватна способност да преценява отговорността в работата си спрямо организацията, в която оперира, както и към клиентите, с които работи, по отношение на спазването на законовата рамка за защита на данните.

Задачата обаче не е толкова лесна! Използване на силни пароли, поддържане на двуфакторни проверки, предпазливост при споделяне, изтриване на ненужни файлове, организиране и криптиране...

Понякога Работливият Джо се претоварва.

Отговорности:

- Прилагане на мерки за защита при събирането и обработването на лични данни.
- Редовен преглед на процедурите за съхранение, достъп и изтриване на лични данни.

Знания и умения за подобрение:

- Запознаване на всички релевантни изисквания на GDPR (права на субекта на данни и правила за обработване на данни).
- Способност за оценка на рисковете в ежедневните операции.
- Познаване на основни техники за криптиране и анонимизиране на данни.
- Разбиране на периодите на съхранение и безопасното унищожаване на данни.
- Управление на достъпа според роли и отговорности.

- Комуникиране на въпроси, свързани с поверителността и защитата на данни с колеги и обучаеми.
- Търсене на подкрепа и менторство за непознати казуси.

Съвети:

- Потърсете наставничество от длъжностно лице по защита на данните (ДЛЗД) или експерт в областта.
- Започнете да участвате в одити за поверителност или оценки на риска.
- Не спирайте да учите за техниките за безопасно съхранение и предаване на данни.

Ниво 3: ДжоПро

ДжоПро е човекът, на когото се обаждате, когато стане напечено. Той е минал през окопите и познава до болка изискванията на GDPR. За неспециалистите често говори на технически жаргон, но те могат само да се учат от мъдрите му думи.

ДжоПро не се плаши от регламентите за защита на личните данни и вижда себе си като техен доверен пазител. Той е преминал от простото спазване на правилата към активното им прилагане в работата си. Може на един дъх да обясни разликата между криптиране и хеширане на данни, гарантира спазването на политиките за поверителност в организацията и предвижда умело рисковете от иновациите.

ДжоПро живее това, за което говори и само неговата амбиция може да доведе до падение.

Отговорности:

- Водене на оценки и одити на процедурите за защита.
- Подобряване на стратегиите в различните отдели.
- Подпомагане на ДЛЗД при навременната адаптация към нормативните изисквания за защита на данните.

Знания и умения за подобрение:

- Задълбочено разбиране на GDPR, CCPA и други актуални закони за защита на личните данни.
- Структуриране и проектиране на одити и оценки на риска според дейностите и нормативните изисквания.
- Усъвършенстване на методите за криптиране и протоколите за прехвърляне на данни.
- Водене на обучения за защита на личните данни по отдели.
- Изготвяне на мерки за реакция при инциденти и проектиране на сигурни системи за обработка на данни.

Съвети:

- Помислете за сертификати за напреднали като CIPP или CIPM.
- Ръководете по-големи проекти за защита на личните данни, включително, но не изрично - одити за защита на данните в цялата организация или стратегии за реакция при инциденти и нови видове киберзаплахи.
- Бъдете в крак с променящите се разпоредби, иновативните технологии и софтуер, като посещавате уебинари, четете и обменяте информация и опит с други специалисти.

Ниво 4: Майстор Джо

Майстор Джо е оракул в сферата на поверителността. Той е не само експерт спрямо принципите и разпоредбите, но и лидер в оформянето на стратегиите за защита на личните данни.

Майстор Джо познава тънкостите в закона и може да открие рисковете за съответствие светлинни години преди да станат реалност. Той е архитект на рамката за защита във всяка организация.

Постигнал отличително ниво на компетентност, Майстор Джо ръководи уверено инициативи за защита на личните данни, като разбира в детайли техните правни, етични и технически аспекти. Колегите му разчитат не само за съвет как да спазват правилата, но и как да интегрират поверителността във всеки аспект от своята дейност.

Майстор Джо има визията за свят, в който нарушенията в киберсигурността вече не съществуват и „privacy-by-design" е втора природа за всеки експерт, който работи с лични данни на трети лица. Неговото дълбоко разбиране за постоянно променящия се цифров пейзаж го прави водач при управлението на промените в начинът, по който споделяме и пазим личната си информация във все по-свързаната мрежа от равноправни членове на едно глобално общество.

Отговорности:

- Разработване и ръководене на стратегии за защита на личните данни в различни сфери на влияние.
- Съветник на ръководства по отношение на спазването на изискванията за поверителност и намаляването на риска от киберзаплахи.
- Ръководи разработването на политики, процеси и програми за обучение в областта на защитата на личните данни.
- Управление на инциденти и планове за митигация на риска

актуално спрямо правните изисквания на съответните разпореждения.

Знания и умения за подобрение:

- Ангажираност с международните разпоредби за защита на личните данни и трансграничните отношения.
- Управление на защитата на личните данни в сложни организации, свързани с масови услуги и споделяне на данни с трети страни.
- Лидерство в управлението на доставчици, инциденти, както и оценки на въздействието и мерките за защита.
- Разширени познания за техниките за подобрение на неприкосновеността на личния живот (PETs) в цифровото инженерство.

Съвети:

- Продължавайте да разширявате знанията си чрез професионални сертификати в различни сфери на сигурността и участвайте в изследвания и форуми.
- Поемайте глобални проекти и ориентирайте другите в различните юридически разпоредби за защита на личните данни.
- Бъдете не само в крак, но и съучастник в създаването на бъдещите цифрови технологии. Пишете статии, участвайте в беседи и бъдете активни в своята професионална общност.

9

КАКВО СЛЕДВА?

Приближавайки се до края е уместно да Ви информираме какво още можете да очаквате от нас.

Тази електронна книга е само първата част от DataGame и по характер, и по структура. Тя е ръководство за потребителя преди да премине към практиката. Защото всички сме първо потребители, а после администратори на данни.

Играта на "DataGame" ще бъде образователна, базирана на реални сценарии, в които можете да се озовете. Тя ще позволява на играча, независимо дали в истинския живот той е преподавател, експерт или директор в образователна институция (или подобен доставчик на услуги в публичния сектор), да се потопи в едно прогресивно обучение и да придобие ценни умения в управлението на лични данни съгласно дейността, както и законовата рамка, в която тя попада.

Ще се сблъскате с реални предизвикателства в симулирана среда в няколко различни сфери на сигурността:

- Правни въпроси: Ориентация в международните и националните закони за защита на данните, ролите на администраторите на лични данни, управлението на декларациите за поверителност на данните и уведомленията за нарушения.
- Регистрация: Подсигуряване на процесите за записване, идентификация и удостоверяването на потребителите, и поддържане прозрачност относно използването на данните им.
- Работа с данни: Прилагане на решения за сигурно съхранение, криптиране и контрол на достъпа - успешното съхранение на данни, изтриването им и предпазването им от нарушения.
- Осведоменост: Разработване и интегриране на програми за грамотност и обучение, както на персонал, така и на публични лица за отговорното управление на данни.
- Иновации: Използване на напреднали технологии като ИИ, и Блокчейн, и адаптация спрямо опасенията за сигурността сфързани с онлайн платформи и алтернативни методи обмен на информация.

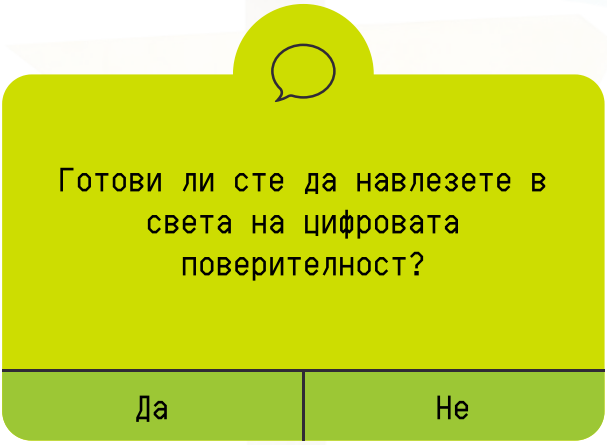
- Комуникация: Ясно съобщаване на практиките за управление, създаване на механизми за обратна връзка и справяне с инциденти, свързани с лични данни.

Срокът за провеждане на DataGame е определен за пролетта на 2025 г. Можете да следите актуализациите за нейното разработване чрез връзките, посочени на стр. 6

...Но това не е всичко.

Очаква Ви още един продукт - Инструментариумът на DataGame:
В него ще намерите колекция от ресурси, с които да подсилите набора си от инструменти за защитата на лични данни във Вашата работа.

Останете с нас!



Автори

Катрин Зигъл
Константинос Сурулас
Урания Капу
Паула Пейн
Теодора Теодору
Росен Петков

Редактор

Росен Петков

Дизайн

Паула Пейн
Росен Петков

Издател

die Berater Unternehmensberatungs GmbH Wipplingerstr. 32 A-1010 Vienna

ISBN 978-3-9519738-0-7

Лиценз