Kapitola

[Ochrana osobních údajů]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: bit schulungscenter
Poslední úprava: 14.8.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Ochrana osobních údajů

Úvod

Data se stávají čím dál tím cennějšími. Možnosti sběru a zpracování dat se v digitálním věku rapidně zvýšily, proto je soukromí dat otázkou, která se dotýká nás všech. Věděli jste, že evropské regulační orgány pro ochranu osobních údajů obdrželi od přijetí zásadního zákona EU o ochraně soukromí v květnu 2018více než 95 000 stížností na možné narušení údajů?

Chcete mít také v případě potřeby možnost uplatnit svá práva na ochranu osobních údajů? Důležitým předpokladem je pak základní znalost ochrany údajů! Kromě toho může mít narušení dat existenčně ohrožující důsledky pro společnosti, a proto byste měli i vy jako zaměstnanec mít základní znalosti o ochraně těchto údajů.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Po dokončení této výukové jednotky získáte základní znalosti o ochraně osobních údajů a zabezpečení dat do té míry, abyste mohli ve svém profesním životě dodržovat předpisy o ochraně osobních údajů a jako fyzická osoba získali větší kontrolu nad svými vlastními údaji.

Přehled výukových cílů a získaných kompetencí

V HVC_Ochrana osobních údajů_01 se dozvíte o účelu ochrany osobních údajů a právním základě ochrany údajů v Evropě. V HVC_Ochrana osobních údajů_02 obdržíte informace o věcném rozsahu použití GDPP. V HVC_Ochrana osobních údajů_03 se dozvíte, za jakých podmínek je shromažďování a zpracování osobních údajů ze zákona povoleno a jaké zásady je třeba dodržovat. V HVC_Ochrana osobních údajů_04 se seznámíte s povinnostmi zpracovatelů a správců dat v případě narušení dat. V LO_Ochrana osobních údajů_05 se dozvíte o právech subjektů údajů. V HVC_ Ochrana osobních údajů _06 obdržíte informace o důležitých cílech ochrany a opatřeních k ochraně dat v praxi. V HVC_Ochrana osobních údajů_07 se dozvíte, jak můžete přispět ke zlepšení ochrany dat ve vaší společnosti.

Hlavní výukové cíle	Dílčí výukové cíle
HVC_Ochrana osobních údajů_01: Znáte účel ochrany osobních údajů a evropský právní základ	DVC_Ochrana osobních údajů_01_01: Umíte definovat pojem soukromí dat. DVC_Ochrana osobních údajů_01_02: Umíte vysvětlit účel ochrany

	osobních údajů. DVC_Ochrana osobních údajů_01_03: Umíte vysvětlit, co je GDPR a co je jeho územní rozsah. DVC_Ochrana osobních údajů_01_04: Umíte definovat rozdíl mezi pojmy zpracovatel a správce dat DVC_Ochrana osobních údajů_01_05: Umíte vysvětlit, o čem je one-stop-shop mechanismus a jaké důsledky může mít porušení ochrany osobních údajů.
HVC_Ochrana osobních údajů_02: Znáte věcný rozsah použití GDPR	DVC_Ochrana osobních údajů_02_01: Umíte vysvětlit, na co se vztahuje pojem zpracování dat podle GDPR, a dokážete uvést příklady, kdy GDPR neplatí navzdory osobní povaze zpracovávaných údajů. DVC_Ochrana osobních údajů _02_02: Umíte vysvětlit, co se myslí pod pojmem osobní údaje a co jsou citlivá data.
HVC_Ochrana osobních údajů _03: Znáte principy a podmínky zpracování dat	DVC_Ochrana osobních údajů _03_01: Umíte pojmenovat důležité principy zpracování dat podle GDPR a důsledky porušení těchto principů. DVC_Ochrana osobních údajů _03_02: Umíte uvést příklady právního základu, který umožňuje zpracování dat s citlivými osobními údaji. DVC_Ochrana osobních údajů _03_03: Umíte vysvětlit, co je třeba vzít v úvahu, pokud se jako právní základ pro zpracování údajů použije souhlas subjektů. DVC_Ochrana osobních údajů _03_04: Pomocí příkladů dokážete vysvětlit, kdy je povoleno zpracovávat citlivá data.
HVC_ Ochrana osobních údajů _04: Znáte povinnosti zpracovatelů a správců dat v případě porušení ochrany údajů.	DVC_Ochrana osobních údajů _ 04_01: Umíte vysvětlit, co znamená narušení dat. DVC_Ochrana osobních údajů _04_02: Umíte vysvětlit, co musí zpracovatelé a správci dat udělat v případě narušení dat.
HVC_Ochrana osobních údajů_05: Znáte práva subjektů dat	DVC_Ochrana osobních údajů_05_01: Umíte pojmenovat práva subjektů údajů. DVC_Ochrana osobních údajů_05_02: Umíte vysvětlit, co znamená právo na informace a právo přístupu a jak obecně postupovat s žádostí o ochranu údajů.DVC_Ochrana osobních údajů_05_03: Umíte poskytnout základní vysvětlení toho, co znamená právo na opravu, právo na vymazání nebo na zapomenutí, právo na omezení zpracování a právo na přenositelnost dat, kdo je oprávněn vykonávat tato práva a co zvážit z hlediska nákladů a důsledků.
HVC_Ochrana osobních údajů_06: Znáte opatření na ochranu dat, která musí provést správce dat a zpracovatel.	DVC_Ochrana osobních údajů_06_01: Umíte vysvětlit pojem “privacy by design“, tak i “privacy by default“. DVC_Ochrana osobních údajů_06_02: Umíte pojmenovat důležité cíle ochrany dat. DVC_Ochrana osobních údajů_06_03: umíte vysvětlit, co znamená termín TOMs, kdo je zodpovědný za jejich implementaci podle GDPR, a uvést příklady standardů TOMs. DVC_Ochrana osobních údajů_06_04: Umíte uvést praktické příklady opatření na ochranu dat.
HVC_Ochrana osobních údajů_07: Víte, jak můžete přispět k ochraně dat ve vaší společnosti	DVC_Ochrana osobních údajů_07_01: Umíte vysvětlit, jak uvést do praxe zásady týkající se tzv. clear desk/ clear screen. DVC_Ochrana osobních

	údajů_07_02: Umíte určit některá kritéria pro bezpečné používání a nakládání s hesly.

1.Buduj znalosti - Účel ochrany osobních údajů a evropský právní základ

V dobách rostoucí digitalizace a vzestupu datové ekonomiky je ochrana osobních údajů jednou z klíčových otázek. Je tak ještě důležitější, aby každý věděl, co pojem **ochrana dat** ve skutečnosti znamená.

Definice
Ochrana osobních údajů, známá také jako ochrana informací, je aspektem bezpečnosti údajů, který se zabývá řádným nakládáním s **osobními údaji**. Jedná se především o ochranu osobních údajů jednotlivců před zneužitím.

Ochranu osobních údajů lze tedy interpretovat jako právo rozhodnout se sám za sebe,

- kdo
- v jakou dobu a
- do jaké míry

má přístup k vašim osobním údajům.

Účelem ochrany osobních údajů je proto zajistit **soukromí jednotlivců**.

Věděli jste, že ochrana osobních údajů je v Evropě po léta **základním právem**? V posledních letech se však v praxi stala ochrana dat ještě důležitější. Technický vývoj a globální vytváření sítí usnadňují sběr, zpracování, ukládání, šíření a analýzu dat.

Příklad

V USA již existují některé velmi úspěšné společnosti, které se specializují na shromažďování osobních údajů. Mezi tyto záznamy patří například jméno, pohlaví, politická příslušnost, příjem a mnoho dalšího. Banky, pojišťovny nebo jiné podniky nakupují tato data za účelem získání podkladových informací, přijímání úvěrových rozhodnutí nebo optimalizaci marketingových aktivit.

Možná znáte skandál kolem Camebridge Analytics, která údajně použila takové údaje k významnému ovlivnění voleb amerického prezidenta Trumpa?

Příklady, jako jsou tyto, jasně ukazují, že je ochrana osobních údajů důležitá z toho důvodu, aby si lidé **udrželi kontrolu** nad svými soukromými informacemi. Hlavním cílem **obecného nařízení o ochraně údajů (GDPR)** je proto ochrana **osobních údajů.**

Od 25. května 2018 platí GDPR.

Toto evropské nařízení je přímo - tj. povinně - použitelné v **každém evropském členském státě**. Vnitrostátní právní předpisy mají tedy pouze doplňkový charakter. GDPR však také obsahuje určité úvodní doložky (např. věkové limity mohou být posouzeny národními zákony).

Co je GDPR přesně? Jedná se o právně závazné nařízení o ochraně fyzických osob v souvislosti se zpracováním **osobních údajů**. Ochrana firemních údajů hraje roli pouze tehdy, je-li osobně identifikovatelná (např. údaje zaměstnanců, zákazníků, dodavatelů).
Cílem GDPR je posílit práva jednotlivců, harmonizovat právní předpisy o ochraně údajů v EU a zlepšit vymahatelnost ochrany údajů jednotným vymáháním a vysokými pokutami.

S cílem poskytnout jednotlivcům větší kontrolu nad jejich osobními údaji se GDPR vztahuje nejen na veškeré zpracování osobních údajů **prováděné organizacemi v rámci EU, ale také na zpracování organizacemi mimo EU,** které nabízejí zboží a služby občanům EU. Takže pokud vás zajímá, zda se přísné pokyny EU na ochranu údajů vztahují také například na poskytovatele webových vyhledávačů se sídlem v USA, které nabízejí své služby evropským občanům nebo na sociální sítě, jako je Facebook, odpověď zní ano.

Je důležité, abyste se seznámili s některými důležitými pojmy zavedenými v GDPR. Podívejme se na ně nyní blíže:

Definice

Správce údajů je osoba (nebo podnik), která rozhoduje o účelech a způsobech zpracování osobních údajů, zatímco **zpracovatel údajů** zpracovává osobní údaje jménem správce (s výjimkou vlastních zaměstnanců správce údajů).

V určitých předpisech mohou existovat rozdíly v závislosti na tom, zda se jedná o zpracovatele údajů nebo správce údajů (např. pokud si subjekty údajů chtějí uplatnit svá práva).

GDPR rovněž stanoví, že v každém členském státě musí **být alespoň jeden nezávislý dozorčí orgán** pro ochranu údajů odpovědný za sledování uplatňování zákona o ochraně údajů.

Důležité
V případě přeshraničního zpracování údajů se použije tzv. “mechanismus jediného kontaktního místa”. To znamená, že občané EU mohou podat stížnost u orgánu **ochrany údajů svého členského státu,** bez ohledu na to, v kterém členském státě byly údaje zneužity.

Domníváte se, že vaše právo na soukromí bylo porušeno? Poté můžete podat stížnost u vnitrostátního orgánu pro zpracování údajů, který je oprávněn uložit řadu **sankcí**.

Důležité
Je důležité poznamenat, že GDPR **výrazně zvýšilo pokuty** pro ty, kdo pravidla porušují. V extrémních případech mohou nyní tyto pokuty činit až 20 milionů eur nebo v případě společností až 4 % celosvětového obratu za předchozí finanční rok.

Díky těmto číslům si můžete představit, o kolik důležitější se pro podniky stalo dodržování ochrany údajů.

1.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_01_01

Zadání: O čem pojednává termín ochrana osobních údajů?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Ochrana osobních údajů je také známá jako ochrana soukromých informací.**
- Ochrana osobních údajů se zabývá především správným nakládáním s důvěrnými firemními daty a jejich ochranou proti zneužití.
- **Ochrana osobních údajů může být interpretována jako právo kterékoli osoby rozhodnout se, kdo má přístup k jejím osobním údajům, kdy a do jaké míry.**
- Ochrana údajů nemá nic společného s bezpečností dat.

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: FO_01_02

Zadání: Ochrana osobních údajů je důležitá, pro který z následujících účelů?

Úkol: Vyberte správné možnosti podle zásady více správných odpovědí: Pouze jedna odpověď je pravdivá.

- Soukromí údajů je důležité pro to, aby banky mohly lépe rozhodovat o úvěrech.
- **Ochrana osobních údajů je důležitá, aby lidé měli kontrolu nad svými osobními údaji.**
- Ochrana osobních údajů je důležitá, aby společnosti mohly optimalizovat své marketingové aktivity.
- Ochrana údajů je důležitá, aby společnosti již nemohly zpracovávat osobní údaje.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_01_03

Zadání: Co je GDPR a za jakých podmínek se uplatňuje?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **GDPR je evropské nařízení, které je přímo použitelné v každém evropském členském státě.**
- GDPR je evropské nařízení, které mohou členské státy bez vlastních vnitrostátních právních předpisů o ochraně údajů dobrovolně dodržovat.
- GDPR se vztahuje na všechna důvěrná firemní data, jako jsou firemní tajemství nebo kalkulace ceny a nákladů.
- GDPR se vztahuje pouze na společnosti se sídlem v evropském členském státě, a proto se nevztahuje na Facebook, Google nebo jiné velké korporace se sídlem v USA.
- **Cílem GDPR je posílit práva jednotlivců a harmonizovat právní předpisy o ochraně údajů v EU.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_01_04

Zadání: Čemu se rozumí zpracovatel dat a co znamená správce dat podle GDPR?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Správce dat rozhoduje o účelu a způsobech zpracování osobních údajů.**
- Zpracovatel dat rozhoduje o účelu a způsobech zpracování osobních údajů.
- **Zpracovatel dat zpracovává údaje jménem správce dat.**
- Za zpracovatele dat se obvykle považují zaměstnanci správce dat.
- Správce dat zpracovává data jménem zpracovatele dat.

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: FO_01_05

Zadání: Paní Josefína H. žije v Rakousku a je přesvědčena, že německá společnost Easyshop porušila její práva na ochranu osobních údajů. Která z následujících tvrzení jsou správná?
Úkol: Vyberte správné možnosti podle zásady více správných odpovědí: Pouze jedna odpověď je pravdivá.

- Paní Josefína H. se musí obrátit na orgán pro dohled nad osobními údaji v Německu, aby si uplatnila práva na ochranu údajů, protože společnost Easyshop má sídlo v Německu.
- **Orgán pro ochranu údajů může uložit sankce až do výše 20 milionů EUR za závažné porušení ochrany údajů.**

- Vzhledem k rozdílné právní situaci v oblasti ochrany údajů v Rakousku a Německu by měla paní Josefína H. nejprve zjistit, ve které ze dvou zemí by její stížnost na ochranu údajů mohla být úspěšnější.
- Paní Josefína H. by určitě měla hledat právníka, protože jako soukromá osoba se bohužel nemůžete obrátit na orgány dohledu nad osobními údaji.

2.Buduj znalosti - Věcný rozsah použití GDPR

Již víte, že **GDPR** lze aplikovat, jakmile jsou zpracovávány **osobní údaje fyzických osob**. Termín **zpracování** je však interpretován poměrně široce.

Definice
Podle GDPR „**zpracováváte**“ osobní údaje, jakmile je sbíráte, zaznamenáváte, organizujete, uspořádáváte, ukládáte, přizpůsobujete, měníte, čtete, dotazujete, používáte, zveřejňujete, porovnáváte, odkazujete, omezujete, mažete nebo ničíte přenosem, zpracováním nebo jakoukoli jinou formou poskytování.

V této souvislosti nezáleží na tom, zda je takové zpracování **zcela nebo částečně automatizované**. GDPR se může dokonce vztahovat na **neautomatizované zpracování** osobních údajů (např. v papírové formě). To je případ, pokud jsou data uložena nebo **mají být uložena ve strukturovaném systému souborů.**

Zajímá vás, co je podle GDPR považováno za souborový systém? V souladu s GDPR jakékoli shromažďování osobních údajů uspořádaných podle určitých kritérií již představuje **souborový systém**.

Příklad
Do oblasti působnosti GDPR patří například dotazníky, kartičky nebo soubory, které jsou tříděné podle jmen osob.

Zatímco na skupinu neuspořádaných poznámkových bloků s osobními údaji se nařízení GDPR vztahuje pouze v případě, že má být v určitém okamžiku podána strukturovaným způsobem.

Základem těchto nařízení je zajistit, aby úroveň ochrany nezávisela na použitých technikách zpracování údajů.

Pokud zvažujete, zda váš soukromý poznámkový blok s telefonními čísly přátel a rodiny podléhá GDPR, nebojte se. Zákon o ochraně údajů **se nevztahuje** na oblasti zpracování údajů v rámci **výhradně osobních nebo rodinných záležitostí** a nevstupuje v platnost ani v některých zvláštních případech, jako jsou činnosti v oblasti národní bezpečnosti.

Jak již víte, GDPR se zabývá ochranou osobních údajů. Co přesně, ale **osobní údaje** znamenají?

Definice
Osobními údaji se rozumí veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby (dále jen „subjekt údajů“).

Pokud se podíváte na následující příklady, rychle si všimnete, že z praktického hlediska **osobní údaje** jednoduše zahrnují vše, co **jakýmkoli způsobem odkazuje na fyzickou osobu**.

Příklad
Příklady osobních údajů: • jméno • rodinný stav • datum narození a věk • adresa trvalého bydliště, telefonní číslo, e-mailová adresa • číslo účtu nebo kreditní karty

Podle zákona o ochraně osobních údajů je však velký rozdíl v tom, zda se jedná například o ochranu Vaší e-mailové adresy nebo pokud se jedná o Vaši zdravotní anamnézu. Takzvaným **citlivým údajům** se dostává zvýšené ochrany.

Definice
Citlivá data jsou **zvláštní kategorií** osobních údajů, která odhalují - rasový a etnický původ, - politický názor, - náboženské nebo filozofické přesvědčení nebo - členství v odborech. To také zahrnuje zpracování genetických nebo biometrických údajů nebo údajů o zdraví nebo sexuálním životě fyzické osoby.

Příklad
Příkladem citlivých údajů jsou lékařské záznamy, otisky prstů, snímky duhovky nebo náboženské vyznání.

Co-funded by the
Erasmus+ Programme
of the European Union

Tato data obzvláště stojí za to chránit. Proto jsou pravidla zpracování citlivých údajů **extrémně striktní.**

2.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_01

Zadání: Které z následujících případů podléhají GDPR?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé

- **Marketingová společnost shromažďuje jména a e-mailové adresy telefonicky a ukládá je elektronicky.**
- **Malý řemeslný podnik vede seznam zákazníků (jména a telefonní čísla) v papírové podobě.**
- Státní úřednice Lisa S. je členkou orgánu národní bezpečnosti. Během své práce vyhodnocuje telefonní záznamy.
- **Pan Peter P. byl nedávno povýšen na výkonného ředitele dlouholetého rodinného podniku. Chce se soustředit na nové obchodní oblasti, a proto vymaže řadu položek ze stávající databáze zákazníků.**
- Studentka Sarah K. si zapisuje kontaktní údaje několika spolužáků.
- **Zaměstnankyně Maria S. hodnotí výsledky písemného průzkumu u zákazníků. Průzkum byl proveden prostřednictvím dotazníků v papírové podobě. Zákazníci byli požádáni, aby uvedli své poštovní směrovací číslo, ale uvedení jejich jména bylo nepovinné.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_02

Zadání: Které z následujících údajů jsou osobní údaje?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Jméno osoby
- Datum narození
- Adresa bydliště
- Sídlo společnosti
- Příjem
- Údaje o prodeji
- Fotografie zaměstnance na domovské stránce společnosti
- E-mailová adresa osoby
- E-mailová adresa společnosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_02

Zadání: Které z následujících údajů jsou citlivé?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Otisk prstu
- Lékařská anamnéza
- Věk
- Údaje o bankovním účtu
- Sexuální orientace
- Členství ve spolku

3.Buduj znalosti - Zásady a podmínky zpracování údajů

GDPR definuje **sedm klíčových principů**, které musí být při zpracování dat striktně dodržovány:

1. Data musí být zpracovávána **podle zákona, spravedlivě a transparentně**.
2. Údaje mohou být zpracovávány pouze pro **stanovené, výslovné a legitimní účely**.
3. Zpracování údajů musí **být omezeno na to, co je nezbytně nutné**.
4. Data musí být **přesná** a aktuální.
5. Osobní údaje musí být uchovávány ve formě, která umožňuje identifikaci subjektů údajů, **pouze po dobu nezbytně nutnou pro účely**, pro které jsou zpracovávány.
6. Osobní údaje musí být chráněny před **neoprávněným zpracováním** a **před náhodnou ztrátou nebo poškozením** vhodnými technickými (např. zálohami) a organizačními opatřeními (např. oprávněním k přístupu).
7. Správce musí být schopen prokázat soulad se zásadami ochrany údajů.

Důležité
Porušení těchto zásad pravděpodobně povede k **maximálním pokutám.**

Věděli jste, že **zpracování osobních údajů je obecně zakázáno**, pokud nejsou splněny zvláštní podmínky? U necitlivých osobních údajů má GDPR k dispozici **celkem šest zákonných podkladů pro zpracování**:

1. **Zpracování dat je nezbytné pro splnění smlouvy** - např. zpracování údajů o adrese zákazníka pro online nákupy
2. **Zpracování dat je nezbytné pro splnění zákonné povinnosti** - např. povinnost zaměstnavatele zaznamenat pracovní dobu
3. **Zpracování dat je potřebné pro ochranu něčího života** - např. v případě epidemií nebo přírodních katastrof
4. **Osobní údaje jsou zpracovávány za účelem plnění konkrétních úkolů v rámci veřejného zájmu** nebo při výkonu úřední moci, které jsou stanoveny zákonem - např. v souvislosti s policejními dotazy
5. **Zpracování dat je nezbytné pro vaše oprávněné zájmy** nebo oprávněné zájmy třetí strany, pokud neexistuje pádný důvod k ochraně osobních údajů fyzické osoby, který převažuje nad těmito oprávněnými zájmy – např. kamerové snímání areálu společnosti jako ochrana před vloupáním
6. **Souhlas zainteresované osoby** - např. podepsáním nebo zaškrtnutím políčka na webové stránce.

Důležité
Prohlášení o souhlasu mohou dotčené osoby **kdykoli odvolat**!

Má-li být souhlas použit jako zákonný základ, musí být splněny určité požadavky a musí být rovněž zohledněn **věk subjektu údajů**.

Důležité
U osob, které ještě nedosáhly věku **16** let, je nutný souhlas rodičů nebo zákonného zástupce. Členské státy EU mohou stanovit nižší věkovou hranici pro získání souhlasu rodičů, která však nesmí klesnout pod 13 let.

Na zpracování citlivých údajů se **vztahují zvláštní požadavky**. V tomto případě je zpracování dat povoleno pouze ve **velmi specifických výjimečných případech**, např. v případě nehody za účelem zjištění životně důležitých údajů nebo pokud byly osobní údaje zveřejněny subjektem údajů.

3.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_01

Zadání: Jako zaměstnanec poradenské firmy zpracováváte různé údaje o zákaznících. Čeho byste si měli být vědomi?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Zpracování osobních údajů musí být omezeno na nezbytně nutnou dobu.**
- Stávající osobní údaje nesmí být aktualizovány.
- **Osobní údaje nesmějí být uchovávány po neomezenou dobu.**
- **Údaje musí být chráněny před neoprávněným zpracováním.**
- **V případě porušení základních zásad ochrany údajů mohou být uloženy maximální sankce.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_02

Zadání: V kterém z následujících případů je zpracování osobních necitlivých údajů zahrnuto do jednoho ze šesti právních základů, a tudíž povoleno?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Zákazník si koupí novou kuchyň a chce ji doručit do svého domu. Prodejce zaznamená adresu zákazníka a uloží ji do zákaznické databáze.**
- **Ve společnosti se zaznamenává a zpracovává pracovní doba všech zaměstnanců.**
- **Zákazník souhlasí se zpracováním svých osobních údajů a podepíše prohlášení o souhlasu.**
- Sportovní klub zveřejňuje v klubových novinkách informace svých členů, která se týkají narození jejich dětí a dat jejich svateb.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_03

Zadání: Představte si, že chcete zpracovávat osobní údaje. Vzhledem k nedostatku jiných právních základů budete potřebovat prohlášení o souhlasu osob, kterých se údaje týkají. Co byste měli vzít v úvahu?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Souhlas může subjekt údajů kdykoli odvolat.**
- **U osob, které ještě nedosáhly věku 16 let, je pro platný souhlas vyžadován souhlas rodiče nebo zákonného zástupce.**
- Členské státy EU mohou pro získání souhlasu rodičů stanovit vyšší věkovou hranici.
- **Členské státy EU mohou pro získání souhlasu rodičů stanovit nižší věkovou hranici.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_04

Zadání: V kterém z následujících případů je zpracování citlivých údajů povoleno?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Osoba v bezvědomí je po nehodě převezena do nemocnice. Zpracovávají se údaje jako krevní skupina, věk nebo alergie.**
- **Homosexuál v televizním rozhovoru otevřeně hovoří o své sexuální orientaci.**
- V žádném z těchto případů, protože zpracování citlivých údajů je bez výjimky přísně zakázáno.
- Zpracování citlivých údajů je povoleno pouze v jednom případě a to pokud k tomu subjekt údajů dá souhlas.

4.Buduj znalosti - Povinnost informovat o narušení dat

Předpokládejme, že začnete svůj pracovní den jako obvykle, ale náhle budete konfrontováni s následujícími událostmi:

- na Vašem firemním serveru došlo k útoku hackerů, který neoprávněným osobám umožnil získat přístup k osobním údajům nebo
- došlo k vloupání do služebního automobilu a byly odcizeny notebooky s osobními údaji.

Tyto události představují hrozbu pro ochranu osobních údajů.

Definice
Incidenty, které by mohly vést k náhodnému nebo nezákonnému zničení, ztrátě, změně nebo neoprávněnému přístupu k osobním údajům, se označují jako narušení údajů.

Povinností každého zpracovatele údajů je bezodkladně informovat správce údajů o každém **narušení dat.**

Důležité
Dojde-li k narušení dat, musí správce údajů splnit **ohlašovací a oznamovací povinnost**. To znamená: • **Orgán pro ochranu údajů** musí být informován do 72 hodin poté, co se správce o porušení dozvěděl, pokud by narušení mohlo představovat riziko pro práva a svobody subjektů údajů. • **Dodatečné oznámení subjektům údajů** je vždy nezbytné, pokud existuje **vysoké riziko** ohrožení práv a svobod subjektů údajů - např. pokud byla citlivá data ovlivněna narušením údajů.

4.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_04_01

Zadání: Co je z hlediska GDPR považováno za narušení údajů?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Neoprávněné osoby získaly přístup k osobním údajům v důsledku hackerského útoku.**
- **Zaměstnanec omylem smazal řadu údajů o zákaznících.**
- Byl odcizen notebook obsahující důležitá prohlášení o nové marketingové strategii společnosti.
- **Zaměstnanec personální agentury ztratil USB disk, na kterém byly uložen mimo jiné velký počet životopisů a poznámek o osobní situaci zákazníků.**

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: FO_04_02

Zadání: Ve zdravotní pojišťovně došlo ke kybernetickému útoku. Hackeři získali přístup k řadě zdravotních údajů pojištěných osob. Jaký je postup podle GDPR?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Existuje vysoké riziko narušení práv a svobod dotčených osob, takže správce údajů musí o tomto incidentu rovněž informovat dotyčnou osobu.**
- **Správce údajů musí informovat orgán ochrany osobních údajů do 72 hodin.**
- Zpracovatel údajů o tom informuje správce údajů do 72 hodin.
- Zpracovatel údajů musí uvědomit orgán ochrany osobních údajů do 72 hodin.
- Nejedná se o citlivá data, proto stačí informovat orgán ochrany osobních údajů. Správce údajů může upustit od oznámení subjektu údajů.

5.Buduj znalosti - Práva subjektů údajů

GDPR rozšiřuje **práva subjektů údajů**. Tato práva byste měli znát, abyste mohli uplatňovat svá práva a reagovat v souladu se zákonem v případě dotazů na ochranu údajů adresovaných Vaší společnosti.
Jak můžete vidět z obrázku, GDPR poskytuje jednotlivcům následující práva:

Co ale tato práva ve skutečnosti znamenají?
Podívejme se na ně blíže: Začněme **s právem na informace**. Pokud jsou vaše osobní údaje zpracovávány, je správce údajů povinen poskytnout Vám **v době shromažďování vašich údajů určité informace**, zejména:

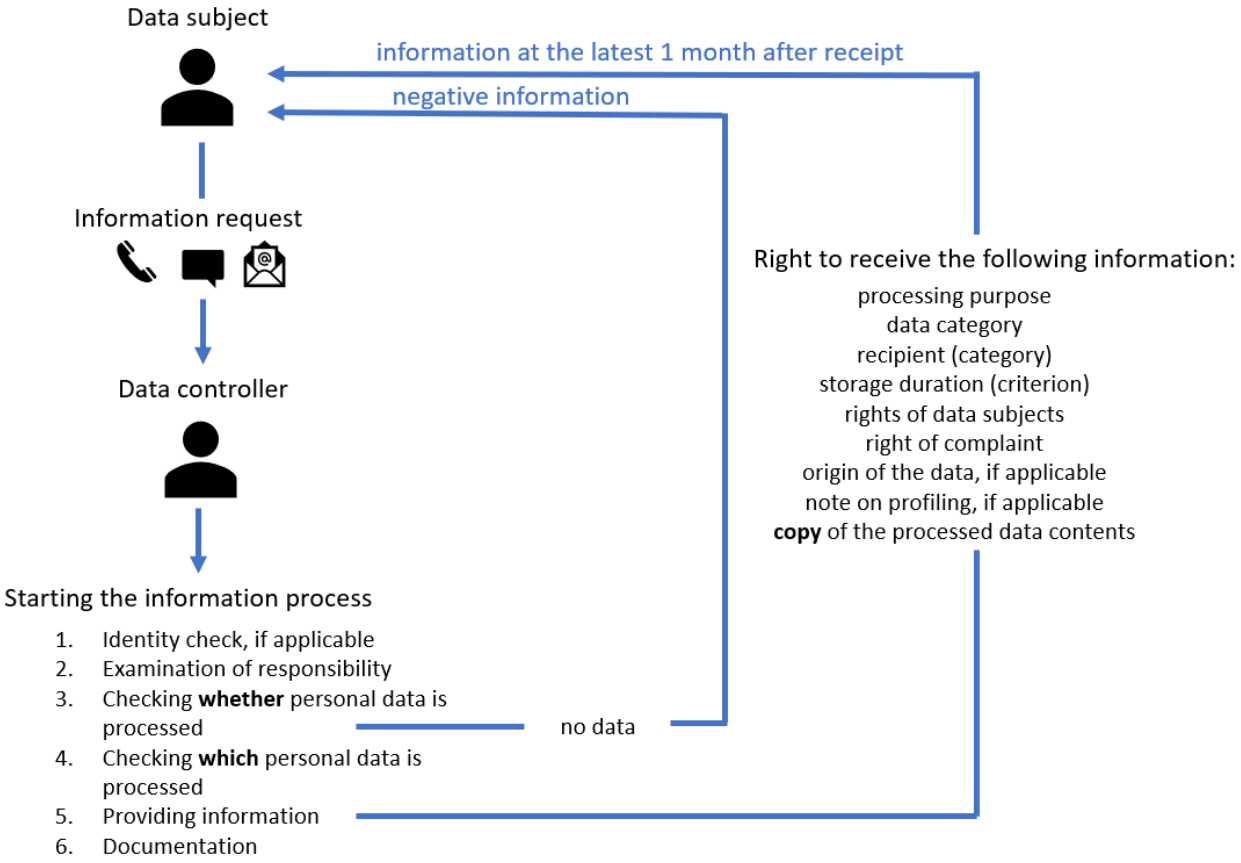
- **kdo** zpracovává vaše údaje (jméno a kontaktní údaje)
- **jaká data** zpracovává,
- **proč** tyto data zpracovává
- **jak dlouho** budou data uchovávána

Kromě toho GDPR vyžaduje, aby vám byly informace poskytnuty

- v přesné, jasné a snadno dostupné formě
- v jasném a jednoduchém jazyce a
- zdarma

K naplnění práva na informace musí správci údajů **aktivně** poskytovat jednotlivcům určité informace. Naproti tomu **právo na přístup** opravňuje každý subjekt údajů k získání kopie svých osobních údajů a dalších doplňujících informací týkajících se zpracování údajů.

Následující obrázek zobrazuje správnou reakci v případě, že subjekt údajů chce uplatnit své právo na přístup:



Jak vidíte na obrázku, žádost o informace lze podat osobně, písemně nebo telefonicky. Je důležité ověřit **totožnost** osoby, která žádost podala.

Dalším krokem je **přezkoumání odpovědnosti.**

Důležité
Práva subjektu údajů lze uplatnit pouze u **správce údajů**! Nicméně, I když má zpracovatel údajů **povinnost podpory**, měl by být požadavek na ochranu údajů zaslán přímo **správci údajů**. Bez výslovných pokynů nejste jako zaměstnanec **oprávněni poskytovat informace o osobních údajích**!

Jak jste si již mohli všimnout z obrázku, správce údajů musí reagovat na žádost o uplatnění práva na přístup, i v případě že nejsou zpracovávány žádné osobní údaje (**negativní informace**). Jsou-li však osobní údaje skutečně zpracovávány, mají jednotlivci **právo na přístup k těmto údajům**, na poskytnutí kopie zpracovávaných osobních údajů a právo na získání jakýchkoli dalších relevantních informací.

Důležité
V případě žádosti o ochranu osobních údajů je lhůta pro poskytnutí informací v zásadě **pouze jeden měsíc** po obdržení žádosti.

Poznámka
Předpisy, které jsme se dosud naučili v souvislosti s - formou žádosti o ochranu údajů (písemná, elektronická, osobní, telefonická) - povinností ověřit totožnost subjektu údajů v případě pochybností - odpovědností za požadavek na ochranu údajů (pouze správce údajů) - lhůtou pro odpověď na ochranu osobních údajů (1 měsíc) platí stejně pro všechna práva subjektů údajů!

Právo na opravu dává jednotlivcům právo požadovat opravu nesprávných, nepřesných nebo neúplných osobních údajů.

Jednotlivci mohou požádat o **vymazání osobních údajů**, pokud již například nejsou údaje zpracovávané společností dále potřebné nebo pokud byly údaje použity nezákonně.
Toto právo platí také **online** a je často označováno jako „**právo být zapomenut**“. Toto právo ukládá správci údajů povinnost přijmout veškerá přiměřená opatření k odstranění zveřejňovaných osobních údajů.

Právo na omezení zpracování je právo, které lze uplatnit pouze za **určitých podmínek.** Jako příklady lze uvést námitku subjektu údajů proti zpracování údajů, přičemž rozhodnutí o námitce stále čeká na vyřízení, nebo spor ohledně přesnosti údajů.

Ú**čelem práva na přenositelnost údajů j**e zajistit, aby jednotlivci mohli požadovat přenos osobních údajů, které zpřístupnili správci údajů, ve strukturovaném, běžném a strojově čitelném formátu. Právo platí pouze tehdy, jsou-li údaje zpracovávány na základě souhlasu nebo smlouvy. Pokud je to technicky proveditelné, můžete také požádat o přenos osobních údajů přímo k jinému správci údajů.

Příklad
Předpokládejme, že chcete změnit poskytovatele e-mailu. **Právo na přenositelnost dat** umožňuje požádat současného poskytovatele e-mailu o zaslání seznamu kontaktů novému poskytovateli e-mailu.

Subjekty údajů mají v zásadě **právo vznést námitku proti zpracování** osobních údajů. Uplatnění práva závisí na účelu a zákonném základu zpracování. Vždy máte například právo vznést námitku proti zpracování za účelem přímého marketingu. Pokud se však údaje zpracovávají například pro vědecký nebo historický výzkum nebo statistické účely, je právo vznést námitku omezenější.

GDPR poskytuje jednotlivcům **právo nepodléhat rozhodnutí založenému výhradně na automatizovaném zpracování**, včetně profilování.

Důležité
Práva na ochranu údajů mohou uplatňovat **pouze fyzické osoby**! Výkon práv subjektů údajů musí být **bezplatný**. Nedodržení těchto práv by mohlo vést k vysokým finančním sankcím.

5.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_01

Zadání: Díky GDPR jsou posílena práva jednotlivců. Jakých práv se mohou nyní jednotlivci dovolávat?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Právo vznést námitku proti zpracování**
- **Právo být informován**
- Právo na zveřejnění
- **Právo na přenositelnost dat**
- **Právo na opravu**
- **Právo na přístup**
- Právo na spravedlivou platbu za data

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_02

Zadání: Které z následujících výroků týkajících se práva na informace a práva na přístup jsou pravdivé?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Právo na přístup opravňuje subjekty údajů k získání kopie jejich zpracovaných osobních údajů.**
- Právo na informace je úplně stejné jako právo být informován.
- **Právo na přístup znamená, že osoba požadující informace má také právo být informována, pokud nejsou zpracovávány žádné osobní údaje, které se jí týkají (negativní informace).**
- **Právo na informace znamená, že správce údajů musí aktivně informovat subjekty údajů o konkrétních bodech zpracování údajů.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_02

Zadání: Školící společnost shromažďuje a zpracovává jména a kontaktní údaje účastníků kurzu při registraci pomocí registračního formuláře. Které body je třeba splnit, aby bylo dodrženo právo na informace?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Účastníci musí být informováni o určitých záležitostech týkajících se zpracování údajů (např. jméno a kontaktní údaje správce dat), jakmile jsou údaje shromážděny.**
- Neexistuje žádná povinnost poskytovat informace, protože se nejedná o citlivé údaje.
- Nejpozději 1 měsíc po získání osobních údajů musí odpovědná osoba splnit svou povinnost a informovat účastníky kurzu.
- V tomto případě není vyžadováno žádné prohlášení o souhlasu. Informační povinnost tedy také není povinná.
- **Informace musí být účastníkům kurzu poskytovány jasným, jednoduchým jazykem a zdarma.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_02

Zadání: Zákazník vás kontaktuje telefonicky. Chce vědět, jaká data ve Vaší firmě zpracováváte. Jak reagujete?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Ihned odpovídám na jeho dotaz.
- Na jeho dotaz odpovím, pokud zákazníka znám a žádné citlivé údaje nezpracovávám.
- Pokud zákazníka znám, odpovím na jeho dotaz.
- **Sdělím mu, že já osobně jako zaměstnanec nesmím poskytovat informace bez výslovných pokynů a žádám ho, aby svou žádost adresoval písemně osobě, která je odpovědná za zpracování údajů.**

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: FO_05_02

Zadání: Kdo je podle GDPR odpovědný za zodpovídání dotazů ohledně ochrany osobních údajů od dotčených osob?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Zpracovatel údajů
- **Správce údajů**
- Zaměstnanci, pokud mohou bez pochyby identifikovat dotčenou osobu.
- Pouze orgán pro ochranu údajů.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_02

Zadání: Pan P. již několik týdnů přijímá e-maily od společnosti, kterou nezná. Rozhodl se proto telefonicky požádat tuto společnost o informace, jaké osobní údaje o něm společnost má a odkud tato data získala.
Které z následujících tvrzení je správné?

Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Společnost může požádat pana P. o prokázání totožnosti, a to ještě před odeslání odpovědi na jeho žádost.**
- **Pokud pan P. od společnosti neobdrží žádnou odpověď nebo informaci do jednoho měsíce, může podat stížnost na úřad pro ochranu osobních údajů.**
- Pan P. může uplatnit své právo na informace pouze osobně na místě, po předložení průkazu totožnosti.
- Společnost je oprávněna požadovat poplatek za přenos informací v papírové podobě. Pro osoby žádající o informace musí být bezplatný pouze přenos v elektronické podobě.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_03

Zadání: Která z následujících tvrzení o právu na přenositelnost údajů jsou pravdivá?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Jednotlivci mohou požádat o přenos osobních údajů, které zpřístupnili správci údajů.**
- **Právo platí, pouze pokud jsou údaje zpracovávány na základě souhlasu nebo smlouvy.**
- Společnosti si mohou také nárokovat právo na přenositelnost dat.
- Právo na přenositelnost dat vám umožňuje požádat současného poskytovatele e-mailu o zaslání seznamu kontaktů novému poskytovateli e-mailu. Náklady na přenos dat nese nový poskytovatel e-mailu.
- **Nedodržení tohoto práva by mohlo vést k vysokým finančním sankcím.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_05_03

Zadání: Pan Klaus se minulý rok oženil a souhlasil s tím, že fotograf může zveřejnit jeho svatební fotografie na svých webových stránkách. Dnes je pan Klaus rozvedený a je naštvaný, že se zadáním jeho jména na Google jsou jeho svatební fotografie viditelné pro všechny. Které z následujících tvrzení je pravdivé?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Má právo odvolat svůj souhlas se zpracováním údajů svatebním fotografem.**
- **Má také právo požadovat, aby byly jeho fotografie zveřejněné na internetu smazány.**
- **Klausova bývalá manželka Lisa se odstěhovala. Má právo požadovat opravu svých zákaznických údajů (nová adresa).**
- Právo na omezení zpracování umožňuje svatebním fotografům nadále používat fotografie pro reklamní účely.

Co-funded by the
Erasmus+ Programme
of the European Union

6.Buduj znalosti - Opatření pro zabezpečení dat

V zájmu zajištění ochrany osobních údajů hraje otázka **bezpečnosti údajů** ústřední roli. Důležitými klíčovými slovy v této souvislosti jsou **”privacy by design”(tzv. záměrná ochrana osobních údajů)** a **”privacy by default” (“ochrana osobních údajů ve výchozím nastavení”)**.

Definice
Termínem ”privacy by design” se rozumí ochrana údajů prostřednictvím technologického návrhu. To znamená, že již při vývoji nových technologií musí být zajištěna vhodná řešení v souladu s ochranou údajů. Například při vývoji nových softwarových programů a zařízení nesmí být ignorovány důležité zásady ochrany dat, jako je minimalizace dat. ”Privacy by default” znamená ochrana údajů prostřednictvím příslušného výchozího nastavení. Odpovědná osoba musí pomocí vhodného výchozího nastavení zajistit, aby byly zpracovávány pouze ty osobní údaje, které jsou naprosto nezbytné.

Stále si nejste jisti, co ”privacy by design” a ”privacy by default” ve skutečnosti znamená? Podívejme se na pár příkladů:

Příklad
”Privacy by design”: Začlenění konceptů mazání do softwaru pro zpracování dat nebo používání pseudonymizace (nahrazení osobně identifikovatelného materiálu umělými identifikátory) a šifrování (šifrování zpráv tak, aby je mohli číst pouze oprávněné osoby).

”Privacy by default”: Poskytovatel sociální sítě musí například zajistit, aby osobní údaje uživatelů nebyly od začátku zveřejňovány přednastavením své aplikace. Osoby, které aplikaci používají, by neměly nejprve měnit nastavení z „veřejné“ na „soukromé“.

Co však lze konkrétně udělat pro zlepšení bezpečnosti dat? Nyní se seznámíte s některými vhodnými opatřeními:

- Definice cílů ochrany údajů
- TOMs - technická a organizační opatření (z angl.“ technical and organizational measures“)

Podívejme se nyní na jednotlivá opatření trochu blíže:

Za základní cíle ochrany údajů se považuje

- **Integrita:** Údaje jsou věrné originálu a nebyly poškozeny ani změněny neoprávněnými stranami.
- **Dostupnost:** Údaje jsou k dispozici oprávněným osobám kdykoli a kdekoli je potřebují. Systém zpracování dat je do určité míry tolerantní k poruchám a chybám.
- **Důvěrnost:** Data jsou přístupná pouze oprávněným osobám.

GDPR požaduje, aby správce a zpracovatel provedli **vhodná technická a organizační opatření (TOMs)** při zpracování údajů za účelem zajištění úrovně ochrany přizpůsobené riziku.

Jak již víte, GDPR zavazuje k ochraně soukromí již **záměrně** (privacy by design”) **a ve výchozím nastavení (“privacy by default”).**

Přesná opatření, která je třeba přijmout k ochraně osobních údajů, jsou však v konečném důsledku odpovědností správce údajů a zpracovatele. **Příkladem TOMs** je pseudonymizace a šifrování dat, informací a školení zaměstnanců nebo automatické zálohování.

Následující příklad ukazuje, jak lze opatření na ochranu údajů uvést do praxe.

Příklad
Předpokládejme, že jste zaměstnáni ve společnosti, která používá **databázi zákazníků**. Tato databáze zákazníků je umístěna na serveru. Pro zajištění odpovídající úrovně ochrany osobních údajů zákazníků jsou myslitelná například tato opatření na ochranu údajů: • Přístup ke všem údajům o zákaznících je možný pouze pomocí **přihlašovacího hesla a uživatelského jména.** • Místnost, ve které je server umístěn, je zamčena **klíčem.** • Každé použití je **zaznamenáno**, jak přihlášení, tak odhlášení, jako i změny datových záznamů. Každému přihlášení je přiřazena osoba. • **Práva ke čtení a zápisu** jsou distribuována pouze podle potřeby. • Pokud je to možné, zákazníci se nezaznamenávají pod skutečným jménem, ale pod **ID uživatele.** • Jsou prováděny pravidelné **zálohy**, které jsou také testovány na integritu v určitých časových intervalech. • Všechny **TOMs podmínky** jsou kontrolovány čtvrtletně. • Zaměstnanci dostávají e-mailem **jasné instrukce**, jak zacházet s osobními údaji, **základní školení o ochraně údajů** a pravidelná **specifická oznámení o ochraně údajů.**

6.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_06_01

Zadání: Co se rozumí pod pojmy “privacy by design“ a “privacy by default“?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- “Privacy by design“ znamená ochranu údajů prostřednictvím příslušných (navrhovaných) přednastavení.
- **“Privacy by default“ znamená zajištění soukromí prostřednictvím vhodných přednastavení.**
- **“Privacy by design“ znamená ochranu údajů prostřednictvím vývoje technologií.**
- **Aplikace je přednastavena tak, že osobní údaje nemohou prohlížet ostatní uživatelé. Toto je příklad „privacy by default“..**
- V softwarovém programu jsou všechna data, která nejsou nezbytně nutná, uložena anonymně. Toto je příklad pro “privacy by default“.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_06_02

Zadání: Jaké jsou důležité cíle ochrany v oblasti ochrany údajů?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Integrita**
- **Dostupnost dat**
- Otevřený přístup k datům
- **Důvěrnost**
- Vysoká doba uchovávání

- Transparentnost dat

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_06_03

Zadání: Co se rozumí pod pojmem TOMs a kdo odpovídá za jejich provádění podle GDPR?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Zkratka TOMs označuje technická a organizační opatření pro ochranu údajů.**
- Zkratka TOMs znamená technicky závazná opatření pro ochranu údajů.
- **Správce údajů a zpracovatel dat jsou odpovědní za provedení vhodných TOMs.**
- Pouze správce údajů je odpovědný za provedení vhodných TOMs.
- Orgán pro ochranu údajů je odpovědný za přesná opatření, která je třeba přijmout k ochraně osobních údajů.
- **Příkladem TOMs je školení zaměstnanců.**
- **Příkladem TOMs jsou automatické zálohy nebo pseudonymizace.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: : FO_06_04

Zadání: Která z následujících opatření lze v praxi použít k ochraně údajů?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Pravidelné zálohy.**
- **Základní školení v oblasti ochrany údajů pro všechny zaměstnance.**
- **Abyste získali přístup k údajům o zákaznících, potřebujete přihlašovací heslo a uživatelské jméno.**
- Pokud je to možné, zákazníci jsou zaznamenáváni pod svým skutečným jménem, nikoli pod svým ID.

Ukládá se co nejvíc dat na technicky co nejdelší možnou dobu

7.Datová bezpečnostní opatření – co můžete udělat VY?

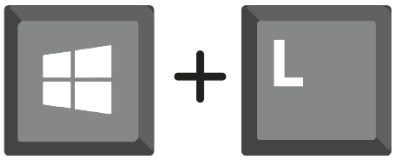
Kromě technické složky je zvláště důležitá také **osobnostní složka**. Zjistěte nyní, jak Vy sami **můžete** přispět k lepší ochraně dat ve Vaší společnosti:

Důležitým opatřením na ochranu údajů je tzv. zásada **Clear Desk/Clear Screen.**

Definice
Zásada Clear Desk se vztahuje na pokyny, aby zaměstnanci ve své nepřítomnosti zamykali všechny důvěrné dokumenty a nenechávali je otevřené na pracovišti. To má zabránit neoprávněným osobám (jako jsou návštěvníci, zákazníci, úklidový personál) v přístupu k údajům v těchto dokumentech.

Kromě toho by všichni zaměstnanci měli být vybízeni k tomu, aby přijali zásady tzv. Clear Screen. To znamená, že všichni uživatelé jsou povinni se od PC odhlásit při odchodu z pracoviště nebo PC uzamknout, pokud dojde pouze ke krátkému přerušení práce.

Tip
Pro rychlé uzamčení počítače v operačních systémech Windows stačí stisknout klávesu se symbolem „Windows“ + „L“ společně.



Kromě toho má smysl nastavit **automatický zámek počítače se spořičem obrazovky chráněným heslem** po dobu nepoužívání počítače.

Důležité
Nikdy neukládejte poznámky o heslech přímo na pracovišti, např. pod deskou stolu nebo jako post-It na obrazovce.

Tím se dostáváme k dalšímu důležitému problému v souvislosti s opatřeními na ochranu údajů: Správné používání a bezpečné zacházení s **hesly**:

Příklad
Následující příklady hesel jsou velmi nevhodné, avšak bohužel stále velmi populární: • Heslo1 • Jméno_příjmení_Datum narození • Číselné řetězce jako 123456 Tato hesla byste nikdy neměli používat. Jsou snadno hacknutelné a proto velmi rizikové.

Bojíte se, že je Vaše heslo příliš slabé? Možná máte pravdu. Pro vytvoření silného hesla je třeba mít na paměti následující aspekty:

Poznámka
• Délka hesla (alespoň 10 znaků) • Kombinace písmen a čísel, speciálních znaků, velkých a malých písmen • Nepoužívejte křestní jména ani příjmení, data narození ani triviální hesla, například 123456 nebo qwertz. • Měňte své heslo v rozumných intervalech. • Heslo vždy udržujte v tajnosti a neposílejte ho nezašifrované e-mailem. • Nepoužívejte soukromá přihlašovací hesla (např. Pro Facebook, online zákaznické účty) pro profesionální účely.

7.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_07_01

Zadání: Společnost, pro kterou pracujete, vyžaduje zásady clear desk/clear screen. Co to znamená?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Pokud nejste u svého pracovního stolu, měli byste zamknout všechny své důvěrné dokumenty.**
- **Při odchodu z pracoviště byste se měli odhlásit z počítače.**
- Na ploše počítače byste neměli ukládat nic nepotřebného.
- **Pro rychlé uzamčení počítače s operačním systémem Windows stačí stisknout kombinaci kláves „Windows“ a „L“.**
- Na pracovním stole byste neměli nechávat vaše soukromé věci.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: FO_07_02

Zadání: Co byste měli vzít v úvahu při výběru hesla?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Pokud je pravděpodobné, že zapomenete své heslo, poznamenejte si ho na místo, ke kterému máte vždy snadný přístup (například post-it v práci).
- Snažte se nepoužívat žádné speciální znaky.
- **Nepoužívejte stejné heslo pro soukromé a profesionální účely.**
- **Nezapomeňte zvolit dostatečně dlouhé heslo.**
- Hesla s vaším příjmení v kombinaci s jménem nebo datem narození jsou relativně bezpečná.

Zdroje

jusline.at: https://www.jusline.at/gesetz/dsgvo

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

wko.at: https://www.wko.at/site/it-safe/kmu-handbuch.pdf

arbeiterkammer.at: https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/FAQ_DSGVO.pdf

dsb.gv.at: https://www.dsb.gv.at/documents/22758/116802/dsgvo_leitfaden.pdf/640015cb-eb90-4702-bf29-ca4fa2d32aca

wko.at: https://media.wko.at/epaper/Leitfaden-Sicherheitsmassnahmen-DSGVO/#20

wko.at: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/datenschutz-grundverordnung-fragen-und-antworten.html#heading_1__Bin_ich_von_der_DSGVO_betroffen_

wko.at: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-oesterreichisches-datenschutzgesetz.html

bmf.gv.at: https://www.bmf.gv.at/en/data-protection.html

gdpr.eu: https://gdpr.eu/eu-gdpr-personal-data/

gdpr-info.eu: https://gdpr-info.eu/

ico.org.uk: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf)

ec.euorpa.eu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

cyberthreatportal.com: https://cyberthreatportal.com/types-of-data-security-measures/

Zapamatujte si

Shrnutí

Termínem **ochrana údajů** se rozumí **ochrana osob** před zneužitím jejich osobních údajů.

Ochrana osobních údajů fyzických osob je také hlavním cílem evropského obecného nařízení o ochraně údajů (GDPR). Od 25. května 2018 se GDPR uplatňuje přímo ve všech členských státech EU a vnitrostátní předpisy na ochranu údajů jsou pouze doplňkové povahy.

Kromě **nových definic** znamená GDPR **rozšíření práv subjektů údajů**, zvýšení povinností v oblasti zpracování údajů a přísnější sankce za porušování ochrany údajů. Provádění GDPR sledují nezávislé dozorčí orgány v každém členském státě.

Objektivní rozsah použití GDPR je omezen na zpracování **údajů s osobním odkazem**. GDPR se vztahuje nejen na data zpracovávaná automaticky, ale také na data zpracovávaná ručně, pokud jsou (nebo mají být) uložena v systému souborů.

Podle GDPR jsou osobními údaji veškeré informace týkající se **identifikované nebo identifikovatelné fyzické osoby**. Takzvané **citlivé údaje**, jako jsou údaje o zdravotním stavu nebo náboženské či politické orientaci, se považují za zvláštní kategorie údajů. Kromě souhlasu subjektu údajů existují i další podmínky pro zákonné zpracování necitlivých údajů. Zpracování **citlivých údajů** je povoleno pouze ve výjimečných případech.

Platné prohlášení o souhlasu musí být učiněno dobrovolně, pro zvláštní účel zpracování, informovaným a jednoznačným způsobem a může být kdykoli odvoláno.

Zásadami pro zpracování údajů v souladu s GDPR jsou zákonnost a transparentnost, omezení účelu, minimalizace a správnost údajů, omezení uchovávání, integrita a důvěrnost.
Jakmile mají být osobní údaje zpracovány, musí být subjekt údajů **informován** o určitých aspektech zpracování údajů. Informace musí být subjektům údajů poskytovány transparentně a snadno dostupnou formou, v jasném a jednoduchém jazyce a zdarma.

GDPR vyžaduje ochranu dat prostřednictvím výchozího nastavení (**"privacy by default"**) a technologického designu vhodného pro ochranu dat (**"privacy by design"**).

V případě **narušení údajů** je správce údajů povinen uvědomit orgán pro ochranu údajů do 72 hodin, pokud nelze vyloučit ohrožení práv a svobod subjektů údajů.

V rámci GDPR byla **posílena práva subjektů údajů**. Je tedy třeba věnovat pozornost žádostem o přístup, opravu, vymazání, přenesení údajů nebo námitky proti zpracování. Pouze správce údajů je odpovědný a oprávněný odpovídat na žádosti o ochranu údajů a zabývat se otázkami ochrany údajů subjektů. Zpracovatelé dat však mají takzvanou povinnost podpory.

V zájmu dostatečné ochrany údajů je nezbytné vytvoření **koncepce ochrany údajů** a zapojení **vyškoleného personálu**. Na základě toho lze přijmout různá opatření, která zabrání porušování zákonů o ochraně údajů a jejich závažným důsledkům.