Informační bezpečnost a GDPR

Technická a organizační opatření podle GDPR se zaměřením na nastavení operačního systému a souvisejících prvků

Úvod

Obecné nařízení o ochraně osobních údajů (GDPR) s sebou přineslo zvýšené nároky na správce a zpracovatele při práci s osobními údaji. Vedle práv a povinností vyplývajících z nařízení samotného se v praxi promítá zejména důraz na zajištění bezpečnosti a ochranu zpracovávaných údajů. To znamená zavádění vhodných **technických** a **organizačních** opatření a také schopnost **doložit**, že tato opatření byla přijata (tzv. „accountability“).

V následujícím textu jsou uvedena konkrétní opatření a praktiky (například nastavení oprávnění v souborovém systému, šifrování či zálohování), které lze ve vztahu k GDPR implementovat. Dokument dále obsahuje plné znění článků 24, 25 a 32 GDPR, které se k těmto opatřením přímo vážou.

---

1) Nastavení práv NTFS

Co to je:
NTFS (New Technology File System) v systémech Windows umožňuje detailní konfiguraci přístupu k souborům a složkám. Je tak možné přesně nastavit, kdo může data číst, upravovat, mazat či spouštět.

Vztah k GDPR:

Zásada omezení přístupu (need-to-know): Podle čl. 32 GDPR je jednou ze základních povinností správce omezit přístup k osobním údajům pouze na osoby, které je k výkonu své práce skutečně potřebují.

Ochrana důvěrnosti: Přesné nastavení oprávnění (read, write, modify apod.) brání neoprávněným osobám v přístupu k citlivým datům.

---

2) Nastavení diskových kvót

Co to je:
Diskové kvóty určují maximální kapacitu disku, kterou může konkrétní uživatel či skupina využívat.

Vztah k GDPR:

Organizační opatření: Ačkoliv nepředstavují přímý požadavek GDPR, mohou pomoci v rámci správy dat, například zamezením nekontrolovaného shromažďování velkého množství osobních údajů.

Minimalizace údajů (data minimization): GDPR vyžaduje zpracovávat jen nezbytné množství dat. Nastavení kvót může motivovat k tomu, aby se zbytečně nehromadila nepotřebná data.

---

3) Příkazy pro práci se soubory a adresáři (kopírování, přesun, mazání)

Co to je:
Základní operace s daty v souborovém systému (například prostřednictvím průzkumníka ve Windows nebo příkazové řádky).

Vztah k GDPR:

Zásada omezení uložení a výmaz: GDPR ukládá povinnost vymazat či anonymizovat osobní data, jakmile nejsou dále potřebná (např. na žádost subjektu údajů nebo po uplynutí zákonné lhůty).

Dokumentace procesů výmazu: Organizace musí být schopna prokázat, že data byla skutečně odstraněna (např. skartací či bezpečným elektronickým smazáním).

---

4) Komprimace dat

Co to je:
Snížení objemu dat pomocí kompresních algoritmů (např. ZIP, RAR).

Vztah k GDPR:

Technické opatření: Komprimace sama o sobě není zabezpečovací metodou, avšak často se kombinuje se šifrováním (např. zaheslované ZIP archivy).

Přenos dat: Při přenášení velkých objemů citlivých dat komprimace urychluje a usnadňuje bezpečný přenos, pokud je zároveň použito šifrování.

---

5) Šifrování dat

Co to je:
Převod čitelné podoby dat na nečitelnou, k jehož zpětnému převodu je potřeba příslušný klíč či certifikát.

Vztah k GDPR:

Jedno z hlavních bezpečnostních opatření (čl. 32 GDPR): GDPR přímo uvádí šifrování jako příklad vhodného technického opatření pro ochranu dat.

Minimalizace rizika úniku: V případě, že dojde k úniku (např. odcizení) databáze, zašifrovaná data zůstávají nečitelná bez příslušného klíče.

---

6) Nastavení periferního zařízení

Co to je:
Konfigurace tiskáren, USB portů, skenerů, přenosných disků a dalších zařízení, která mohou ukládat či jinak zpracovávat data.

Vztah k GDPR:

Prevence neoprávněného kopírování či tisku: Např. omezení možnosti tisknout citlivé dokumenty, kontrola přístupu k USB portům.

Bezpečnostní politika: Minimalizace rizika zneužití dat (např. zcizení na flash disku).

---

7) Záloha dat

Co to je:
Vytváření kopie dat pro případ ztráty, havárie nebo kybernetického útoku.

Vztah k GDPR:

Dostupnost osobních údajů (čl. 32 GDPR): Jedním z cílů GDPR je zajištění dostupnosti, aby data mohla být obnovena i po technické nehodě či útoku.

Retenční politika: Je nutné dbát na to, aby zálohy neobsahovaly osobní údaje déle, než je nutné, a aby byly rovněž řádně zabezpečeny (ideálně šifrované).

---

8) Záloha operačního systému

Co to je:
Kompletní záloha (image) disku obsahující celý operační systém, včetně nainstalovaných aplikací a nastavení.

Vztah k GDPR:

Zajištění funkčnosti a rychlé obnovy: U systému zpracovávajícího osobní údaje je obnova po havárii či ransomwarovém útoku zásadní pro zachování chodu organizace.

Stejná pravidla jako u klasické zálohy: Musí být dostatečně zabezpečená (nejlépe šifrovaná) a uchovávaná pouze po nezbytně dlouhou dobu.

---

9) Zabezpečení operačního systému

Co to je:
Soubor opatření a konfigurací (uživatelské účty, firewall, antivir, správa aktualizací, řízení služeb atd.) zajišťujících ochranu systému.

Vztah k GDPR:

Čl. 32 GDPR – Bezpečnost zpracování: Organizace by měly přijmout vhodná technická opatření proti neoprávněnému či nezákonnému zpracování.

Privacy by Design a by Default (čl. 25 GDPR): Bezpečný základní stav systému (např. nastavení silných hesel, pravidelných aktualizací) je předpokladem pro bezpečné zpracování osobních údajů.

---

10) Aktualizace operačního systému

Co to je:
Pravidelná instalace oprav a záplat (Windows Update, Linux patch management atd.).

Vztah k GDPR:

Základní prvek ochrany: Neaktuální systém s neopravenými chybami je zranitelnější vůči útočníkům a zvyšuje riziko úniku či narušení integrity dat.

Článek 32 GDPR – Bezpečnost: Aktualizace OS patří mezi nejzásadnější kroky při zajištění kybernetické bezpečnosti.

Shrnutí k vazbě na GDPR

Veškeré výše uvedené postupy a opatření (od nastavení oprávnění v souborovém systému až po pravidelnou údržbu a zálohování systému) se přímo nebo nepřímo vážou k několika klíčovým požadavkům GDPR, a to zejména k:

- **Bezpečnosti zpracování (čl. 32 GDPR)**
- **Principu odpovědnosti (accountability),** tedy schopnosti doložit, že bylo učiněno vše pro ochranu dat
- **Zásadám důvěrnosti, integrity a dostupnosti osobních údajů**

Tato opatření zabraňují neoprávněnému přístupu (důvěrnost), ztrátě a poškození dat (integrita) a pomáhají zajistit, aby byla v případě potřeby dostupná (dostupnost).

Plné znění vybraných článků GDPR

Pozn.: Text je převzatý z **Úředního věstníku Evropské unie** (veřejný zdroj), kde je oficiálně publikováno znění nařízení.

****Článek 24**

Odpovědnost správce**

S ohledem na povahu, rozsah, kontext a účely zpracování i na rizika pro práva a svobody fyzických osob různé závažnosti a pravděpodobnosti provede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování se provádí v souladu s tímto nařízením. Tato opatření jsou podle potřeby přezkoumávána a aktualizována.

Pokud je to přiměřené s ohledem na činnosti zpracování, zahrnují opatření prováděná správcem zavedení vhodných politik ochrany osobních údajů.

Dodržování schváleného kodexu chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 může být využito jako prvek pro prokázání splnění povinností správce.

****Článek 25**

Záměrná a standardní ochrana osobních údajů**

S ohledem na nejnovější poznatky, náklady na provedení a povahu, rozsah, kontext a účely zpracování a rovněž na rizika pro práva a svobody fyzických osob různé pravděpodobnosti a závažnosti zavede správce jak při určování prostředků zpracování, tak při samotném zpracování vhodná technická a organizační opatření, například pseudonymizaci, jež jsou navržena tak, aby účinně prováděla zásady ochrany údajů, jako je minimalizace údajů, a začlenila do zpracování nezbytné záruky za účelem splnění požadavků tohoto nařízení a ochrany práv subjektů údajů.

Správce zavede vhodná technická a organizační opatření, aby zajistil, že ve výchozím nastavení budou zpracovávány pouze osobní údaje, které jsou nezbytné pro každý konkrétní účel zpracování. Tato povinnost se vztahuje na množství shromážděných osobních údajů, rozsah jejich zpracování, dobu jejich uložení a jejich dostupnost. Zejména musí být tato opatření zavedena tak, aby nebyly osobní údaje bez zásahu fyzické osoby zpřístupněny neurčitému počtu osob.

Dodržování schváleného kodexu chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 může být využito jako prvek pro prokázání splnění požadavků uvedených v odstavcích 1 a 2 tohoto článku.

****Článek 32**

Zabezpečení zpracování**

S ohledem na nejnovější poznatky, náklady na provedení a povahu, rozsah, kontext a účely zpracování a rovněž na rizika pro práva a svobody fyzických osob různé pravděpodobnosti a závažnosti přijme správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku; přitom zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztrátu, pozměnění, neoprávněné poskytnutí přenášených, uložených či jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Při posuzování vhodné úrovně zabezpečení se bere zvláštní ohled na rizika, jež představuje zpracování, zejména náhodné či protiprávní zničení, ztrátu, pozměnění, neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů anebo neoprávněný přístup k nim.

Dodržení schváleného kodexu chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 může být využito jako prvek pro prokázání splnění požadavků uvedených v odstavci 1 tohoto článku.

Správce a zpracovatel přijmou opatření, aby zajistili, že každá fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, je zpracovává pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Závěr

Implementací výše zmíněných **technických** a **organizačních** opatření lze významně přispět k naplnění požadavků, které GDPR na správce a zpracovatele osobních údajů klade. Patří mezi ně zejména:

- zajištění přísného **řízení přístupu** (např. NTFS práva, omezení periferií),
- důsledná **správa životního cyklu dat** (smazání po uplynutí doby, nastavené kvóty),
- použití **kryptografických technik** (šifrování, zabezpečení přenosů),
- **zálohování** s přihlédnutím k době uchování a dalším požadavkům GDPR,
- pravidelné **aktualizace** a **údržba** systémů.

Nejedná se však o konečný výčet – každá organizace by měla vyhodnocovat rizika pro práva a svobody subjektů údajů a dle výsledků je snižovat pomocí přiměřených opatření. Důležitá je také **dokumentace** všech kroků, aby bylo možné prokázat soulad s GDPR (princip accountability). Tím se posiluje důvěra nejen ze strany dozorových úřadů, ale i samotných subjektů údajů, a naplňuje se cíl GDPR – chránit osobní údaje a práva fyzických osob v digitální době.

Odkazy:

https://uoou.gov.cz/

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_cs.htm