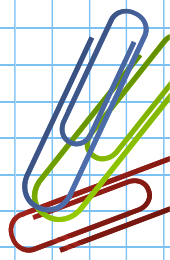

PŘÍRUČKA PRO ZAMĚSTNANCE

příručka

crp-gdpr 2018

Úvod do GDPR

Zkratka GDPR označuje Nařízení Evropského parlamentu rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Toto nařízení je přímo aplikovatelné, platí i v případě, že by k němu nebyla vytvořena národní legislativa. Cílem je sjednotit přístup k ochraně osobních údajů napříč EU. Jedná se o evoluci dřívější legislativy. Některé oblasti se příliš nemění, jiné jsou naopak zcela nové nebo výrazně upravené.

Tato publikace slouží pro základní rychlou orientaci v Nařízení a v dopadech do různých oblastí.

1 Základní pojmy GDPR

1.1 Pojmy definované přímo v nařízení (výběr)

Subjekt údajů

Identifikovaná nebo identifikovatelná fyzická žijící osoba. Je jí fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Osobní údaj

Veškeré informace o subjektu údajů.

Zpracování osobních údajů

Jakákoli činnost s osobními údaji, např. shromažďování, uložení, použití, zkombinování, předání, zpřístupnění, ale také jejich výmaz či zničení apod.

Každé zpracování musí mít stanoveno konkrétní účel (důvod, proč je prováděno) a tento účel musí být oprávněný, tzn., musí existovat tzv. právní základ, který jej legitimizuje.

Zpracování může být založeno na těchto právních základech:

- Souhlas subjektu údajů se zpracováním osobních údajů.
- Plnění či uzavření smlouvy se subjektem údajů.
- Právní povinnost správce.

- Ochrana životně důležitých zájmů subjektu údajů.
- Veřejný zájem nebo výkon veřejné moci.
- Oprávněný zájem správce.

Správce

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

Jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Zpracovatel

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Pověřenec na ochranu osobních údajů

Odborně kvalifikovaná osoba jmenovaná správcem, která dohlíží na zpracování osobních údajů, kontroluje soulad s pravidly nařízení a chrání zájmy subjektů. Je kontaktní osobou pro subjekty údajů a pro dozorový orgán.

Organizačně je podřízen vedení organizace, jeho činnost v oblasti ochrany osobních údajů by však měla být nezávislá a v této oblasti by neměl ze strany organizace přijímat žádné pokyny.

Při své práci využívá dále uvedené agendy a komunikuje se všemi odpovědnými pracovníky.

1.2 Nové pojmy zavedené v metodikách

Níže uvedené role a názvy agend nejsou z hlediska nařízení závazné. Z požadavků nařízení však potřeba takových rolí a agend nepřímo vyplývá, jinak celý systém ochrany osobních údajů nemůže spolehlivě fungovat.

Jednotlivé organizace si mohou procesy nadefinovat odlišně, s jinými formálními názvy, nicméně princip věci (zodpovědnost určitých osob a existence určitých evidencí) bude ve většině případů obdobný.

Registr zpracování osobních údajů

Organizace vede evidenci všech procesů a systémů, kde zpracovává osobní údaje. Základní evidence obsahuje údaje o zpracování (název, popis, účel, právní titul ...) a odkaz na podrobnější dokumentaci. Registr zpracování je základní informační zdroj pro všechny pracovníky zodpovědné za zpracování a ochranu osobních údajů.

Evidence žádostí subjektů

Pokud subjekt požádá organizaci o uplatnění svých práv, musí být tato žádost zpracována a evidována. Evidence musí obsahovat údaje žadatele, druh a rozsah žádosti a způsob vypořádání.

Evidence porušení ochrany osobních údajů

Agenda eviduje všechna porušení ochrany osobních údajů, která organizace sama zjistila nebo jí byla oznámena. Eviduje se přinejmenším kdy došlo k porušení, jakého druhu porušení bylo, klasifikace jeho závažnosti a zda, kdy a jak byl informován subjekt a dozorový orgán.

Registr souhlasů subjektu

Pokud subjekt vyjádří souhlas s textem pravidel či politiky služby a dá souhlas se zpracováním svých údajů, je potřebné tento souhlas zaznamenat. Evidence souhlasů může být buď samostatná, pro každé zpracování zvlášť (např. souhlasy uložené přímo v databázi konkrétní aplikace) nebo centrálně ve společném úložišti.

V každém případě musí být organizace schopna dohledat a doložit, kdy a s jakým textem subjekt vyslovil souhlas, a že tento souhlas splňoval všechny požadavky nařízení (např. že byl poskytnut skutečně svobodně, že byl subjekt údajů dostatečně informovaný, že byl souhlas dostatečně konkrétní a neslučoval více účelů apod.).

Každý souhlas by měl být omezen časem, na který je ze strany subjektu údajů udělen. Po uplynutí tohoto času by mělo být zpracování ukončeno, nebo souhlas obnoven.

Garant zpracování

Pracovník organizace, který v konkrétním případě zpracování osobních údajů zná účel zpracování osobních údajů, určuje pravidla jejich zpracování a dohlíží na související procesy. Je uveden v registru zpracování jako osoba zodpovědná za konkrétní zpracování osobních údajů.

V různých organizacích může být nazýván i odlišnými názvy, např. odpovědná osoba, zodpovědný pracovník, vlastník zpracování apod.; event. nemusí být tato zodpovědnost vyjádřená názvem, ale může být obecnou součástí zodpovědnosti vedoucích pracovníků.

Pověřený pracovník

Pracovník může být zaměstnanec, student, či jiná osoba pověřená konkrétním zpracováním osobních údajů. Pověření může vyplývat z pracovní náplně nebo z jednorázového úkolu. Pracovník musí být poučen o řádných postupech při zpracování osobních údajů.

Centrální místo

Kontaktní bod jak pro zaměstnance organizace, tak pro další osoby, které chtějí uplatnit žádost, informovat o porušení ochrany osobních údajů nebo získat obecnou informaci k danému tématu. Je žádoucí, aby všechny tyto požadavky byly vyřizovány nejlépe jedním vstupním bodem, který provede kvalifikované zhodnocení a rozhodne o dalším postupu řešení. U rozsáhlejších organizací lze předpokládat více takových míst (fakulty, větší složky organizace), ale i v takovém případě musí být činnost organizací koordinována a metodicky jednotně vedena. Centrální místo úzce spolupracuje s pověřencem na ochranu osobních údajů.

2 Zpracování osobních údajů podle GDPR

Každé zpracování osobních údajů by mělo splňovat několik základních náležitostí, aby bylo z pohledu Nařízení korektní.

2.1 Omezené účelem

Správce nesmí zpracovávat osobní údaje, které nejsou nezbytné s ohledem na stanovený účel. Mají-li se například zpracovávat e-mailové adresy za účelem odesílání elektronického newsletteru, není zapotřebí evidovat datum narození subjektu údajů.

2.2 Časově omezené

Zpracování by nemělo být časově neomezené. Správce by neměl zpracovávat osobní údaje po dobu delší, než je nezbytné pro daný účel. Například:

- Mají-li se odesílat e-mailové informace o přijímacích řízení, není nutné e-mailové adresy zpracovávat po dobu deset let (pravděpodobně postačí do skončení přijímacího řízení).
- Při zpracování životopisů uchazečů o zaměstnání, kteří se přihlásili do výběrového řízení, by se tyto životopisy neměly zpracovávat po skončení výběrového řízení (a nebo by se měly zpracovávat na základě souhlasu s tímto dalším zpracováním).

2.3 Přesné

Při zpracování osobních údajů by se měly osobní údaje udržovat přesné a aktuální. Není povinností správce přesnost a správnost aktivně ověřovat, byť to za určitých okolností může být vhodné. Správce by měl každopádně údaje opravit, pokud jej subjekt údajů upozorní na nepřesnost.

2.4 Důvěrné

Správce by měl zajistit taková opatření, aby zpracovávané osobní údaje byly dostatečně zabezpečeny před neoprávněným či protiprávním zpracováním, náhodnou ztrátou, náhodným či neoprávněným zničením či poškozením. Například:

- V informačním systému, který zpracovává osobní údaje studentů, jsou implementována pravidla, která neumožní prohlížet informace studentů z jiných fakult (důvěrnost).
- Zdravotní dokumentace handicapovaných osob je uložená v uzamčené místnosti v samostatně uzamykatelné skříni; klíče mají k dispozici pouze pracovníci oprávněni k nakládání s těmito dokumenty (důvěrnost).
- Excel s evidencí kontaktních údajů pro určité společenské události je umístěn na síťovém úložišti s omezenými přístupy (důvěrnost). Toto síťové úložiště se pravidelně zálohuje (dostupnost).

2.5 Transparentní

Zpracování by nemělo probíhat „tajně“, subjekt údajů by měl mít dostatek informací o tom, za jakým účelem zpracování probíhá a jaké osobní údaje se zpracovávají. Subjekt údajů by měl být rovněž informován o totožnosti správce.

Například: účastníci semináře vyplňují své kontaktní údaje do přihlašovacího formuláře. Součástí formuláře je i informace o tom, kdo dané osobní údaje zpracovává, za jakým účelem je zpracovává a po jak dlouhou dobu je bude zpracovávat. Součástí je dále základní poučení o právech subjektu a odkaz na webové stránky, kde je možné získat více informací.

3 Práva subjektu údajů

Nařízení přisuzuje subjektům údajů řadu práv:

- Právo obdržet **informace** o zpracování, tedy jestli se osobní údaje subjektu zpracovávají a jakým způsobem správce zpracování provádí.
- Právo na **přístup** k osobním údajům. Jestliže se osobní údaje zpracovávají, má subjekt právo získat jejich kopii.
- Právo na **opravu** osobních údajů v případě, že správce má chybné nebo neaktuální osobní údaje.
- Právo na **výmaz** osobních údajů.
- Právo **vznést námitku** proti zpracování osobních údajů.
- Právo na **omezení zpracování** osobních údajů.
- Právo **odvolat souhlas**, který dříve udělil.

Práva získává subjekt údajů mj. proto, aby mohl správce účinně **kontrolovat**. Uplatnění práva nelze zpoplatnit. Výjimkou jsou zjevně nepřiměřené požadavky, zejména nepřiměřené opakování. Nelze však zpoplatnit uplatnění práva kvůli rozsahu.

Správce by měl uplatnění práv usnadňovat, např. tím, že nabídne více možných způsobů a forem uplatnění, zřídí centrální místo pro uplatnění, připraví proces pro jejich vypořádání či zpracuje souhrn náležitostí, které musí žádosti splňovat.

Správce může žádat subjekt o poskytnutí informací k potvrzení totožnosti. Pokud tyto informace nezíská, může poskytnutí informací odmítnout.

3.1 Právo na informace

Správce předává informace stručně, srozumitelně, jednoduše a snadno přístupným způsobem.

Vždy je třeba přihlédnout ke kategorii subjektu údajů. Tutéž informaci obdrží jinak děti, IT zaměstnanci, právníci aj.

Správce předává informace v okamžiku získání osobních údajů nebo zahájení jejich zpracování, případně ve chvíli, kdy o to subjekt údajů požádá.

Rozlišuje se, zda správce získal osobní údaje přímo od subjektu údajů nebo od někoho jiného.

Vždy je zapotřebí uvést alespoň:

- **Kdo je správcem** a jaké jsou jeho kontaktní informace. Byl-li jmenován pověřenec pro ochranu osobních údajů, uvádí se také jeho kontaktní údaje.

- **Proč se osobní údaje zpracovávají**, tedy jaký je účel zpracování a jaké jsou právní základy. V relevantním případě, např. u oprávněných zájmů, se uvádí upřesnění.

- **Zda a komu lze osobní údaje předat**, což se určuje jmenovitě nebo jen kategoriemi.

- Vymezení doby zpracování osobních údajů.

- Poučení o právech, která subjekt údajů má, včetně práva podat stížnost dozorovému orgánu.

- Od koho byly osobní údaje získány, nebyl-li jejich zdrojem sám subjekt.

3.2 Právo na přístup

Subjekt údajů má právo na informaci zda správce zpracovává nějaké jeho osobní údaje a na případné podrobnosti tohoto zpracování.

V případě, že zpracování probíhá, má subjekt údajů právo na přístup ke svým údajům a na bezplatné získání jejich kopie.

Kopie osobních údajů se poskytuje přednostně v elektronické podobě, pokud subjekt nepožaduje jinou formu či pokud forma není konkrétně specifikována. V každém případě by se však mělo jednat o formu běžně používanou a dostupnou. Vhodný je formát PDF, který je standardizovaný normou ISO, existují pro něj bezplatné prohlížeče a soubory v něm se snadno vytváří přímo z aplikací anebo i skenováním papírových podkladů přímo do formátu PDF. Výhodou je i fakt, že dokumenty ve formátu PDF lze zabezpečit, opatřit elektronickým podpisem apod.

Při uplatnění tohoto práva je nutné pamatovat na to, že informace a kopie by měly být poskytnuty skutečně dotyčnému subjektu údajů (ověření identity), a také na to, že kopie mohou obsahovat osobní údaje i jiných subjektů, na něž by zpřístupnění mohlo mít nepříznivý dopad. V takovém případě by měly být osobní údaje dalších subjektů odstraněny.

3.3 Právo na opravu

Správce nemusí aktivně ověřovat správnost a přesnost osobních údajů, nemusí aktivně vyhledávat nepřesné údaje. Pokud však subjekt údajů zjistí, že osobní údaje zpracovávané správcem jsou nepřesné či neúplné, může jej o tom informovat. Správce pak musí tyto osobní údaje na základě žádosti subjektu opravit či doplnit.

3.4 Právo na výmaz

Subjekt údajů má právo žádat výmaz osobních údajů. Nejde však o absolutní právo, byť tak bývá někdy prezentováno. Pokud existují jiné zákonné důvody pro zpracování, nemusí být výmaz proveden. Mezi takové důvody patří:

- Právní povinnosti správce.
- Zpracování osobních údajů nezbytné pro výkon nebo obhajobu právních nároků správce.
- Zpracování osobních údajů nezbytné pro ochranu veřejného zájmu (veřejné zdraví, archivace).

Správce má však i bez vyžádání **povinnost osobní údaje automaticky likvidovat** ve chvíli, kdy pominul účel jejich zpracování, nebo byl odvolán souhlas, na jehož základě zpracování probíhalo. Osobní údaje je taktéž třeba vymazat, jestliže byly zpracovávány protiprávně nebo subjekt údajů podal oprávněnou námitku proti zpracování.

Jestliže správce v těchto případech zpracování přesto provádí, musí žádosti subjektu o vymazání údajů vyhovět.

Po obdržení žádosti by správce měl subjekt údajů informovat o tom, že osobní údaje vymazal, případně mu sdělit důvod, proč tak neučinil. Správce by měl o výmazu informovat také příjemce, kterým smazané osobní údaje dříve poskytl.

Výmaz může být někdy technicky neproveditelný, např. u osobních údajů v zálohách databází apod. Potom je vhodné provést vymazání z produkčních dat a informovat subjekt údajů o existenci záloh a o době, po kterou se budou tyto zálohy udržovat. Vedle toho je vhodné přijmout taková opatření, která zabrání případné obnově osobních údajů vymazaných z produkční databáze.

Taková opatření mohou být organizační – např. evidence informací o vymazaných datech (seznam identifikátorů datových vět, příslušné skripty v případě ručního výmazu, apod.). Podle této evidence pak lze provést výmaz (např. i ručně) dotčených osobních údajů v případě obnovy systému ze zálohy.

3.5 Právo na omezení zpracování

Jedná se o omezení zpracování na **pouhé uložení**. Správce musí omezit zpracování v případě, že:

- Subjekt popírá přesnost osobních údajů a správce potřebuje delší dobu na jejich ověření.
- Osobní údaje zpracovává protiprávně a subjekt odmítá jejich výmaz.

- Subjekt odmítá výmaz, přestože správce již zpracování nepotřebuje provádět.
- Subjekt vznesl námitku proti zpracování založenému na základě oprávněného zájmu správce.

3.6 Právo na přenositelnost

Právo na přenositelnost je možné uplatnit tehdy, když zpracování probíhá automatizovaně a zároveň je založeno na souhlasu či smlouvě. Např. při přechodu z jedné banky do druhé si obě banky předávají informace o nastavení trvalých příkazů klienta.

Správce musí osobní údaje poskytnout ve strukturovaném, běžně používaném elektronickém formátu. Musí je poskytnout přímo subjektu nebo jiném správci, kterého subjekt údajů určí.

Nařízení nespecifikuje konkrétní formát ani nepožaduje kompatibilitu formátů napříč různými správci. Požadavku vyhoví např. formáty CSV, XML, JSON ale i soubory MS Excel.

3.7 Právo na přezkum automatizovaného rozhodnutí

Pokud subjekt údajů podléhá rozhodnutí založenému výhradně na automatizovaném zpracování, má právo na přezkum a případný lidský zásah ze strany správce.

3.8 Právo na stížnost či ochranu

Subjekt údajů má právo podat stížnost na zpracování osobních údajů u dozorového orgánu (v České republice se jedná o ÚOOÚ – Úřad pro ochranu osobních údajů). V případě potřeby může žádat o soudní ochranu vůči dozorovému orgánu stejně tak jako vůči správci či zpracovateli.

Subjekt údajů může svým zastupováním při podání stížnosti pověřit neziskový subjekt. Stanoví-li tak národní legislativa, je zastupování možné i bez pověření.

4 Podpůrné procesy

4.1 Vyřízení žádostí subjektu

Jednou z oblastí, kterou GDPR rozšiřuje, je oblast práv subjektu údajů. Organizace by měla zajistit jednotný postup při zpracování žádostí subjektu. Především jde o následující kroky:

- **Přijetí žádosti subjektu**: Každý zaměstnanec by měl být poučen, kam případnou žádost subjektu směrovat. Je účelné, pokud má organizace jeden nebo několik málo vstupních bodů (centrální místo), které žádost kvalifikovaně přijmou, zaevidují a zpracují.
- **Prvotní zpracování žádosti**: Do tohoto spadá posouzení žádosti z hlediska úplnosti, komunikace se subjektem z hlediska doplnění informací v žádosti, ověření totožnosti žadatele a vyžádání si součinnosti od osob, které dané zpracování v rámci organizace provádí. Pokud je zpracování realizováno prostřednictvím informačního systému, který umožňuje automatizované provedení žádosti subjektu (třeba export všech uživatelských dat), subjekt může být odkázán přímo na konkrétní funkci systému.
- **Technické vyřízení žádosti**: Pokud není možné akci provést automaticky žadatelem, osoba provádějící zpracování by měla patřičné kroky provádět pouze na základě autorizované žádosti ze strany pracovníků centrálního místa. Provedení daných kroků ohlásí a případná související data předá zpět pracovníkovi centrálního místa, který zajistí další komunikaci se žadatelem. Osoba provádějící zpracování by obvykle neměla v dané věci komunikovat přímo se subjektem.
- **Uzavření žádosti**: Odpověď subjektu údajů nebo předání dat a uzavření záležitosti (včetně pořízení dokumentačního záznamu o průběhu vyřízení žádosti).

V určitých případech (např. jde-li o zjevně nepřiměřenou či nedůvodnou žádost, nebylo-li možné spolehlivě ověřit identitu žadatele apod.) může být žádost i odmítnuta. V takovém případě je nutné odmítnutí náležitě zdůvodnit. Subjekt údajů má právo podat stížnost k dozorovému orgánu.

4.2 Zpracování případů porušení ochrany osobních údajů

Porušením ochrany osobních údajů se rozumí narušení důvěrnosti, dostupnosti nebo integrity osobních údajů. Proces zpracování porušení ochrany osobních údajů by měl obsahovat:

- **Rozpoznání** incidentu (pracovníkem organizace) nebo jeho **přijetí** (při nahlášení externí osobou). Informace o incidentu by měla být směrována opět na jeden kontaktní bod, který zajistí kvalifikované zpracování, evidenci a pro řádné vyřešení incidentu si vyžádá součinnost osob provádějících dané zpracování.
- **Úvodní klasifikace** incidentu (i hrubým odhadem), zda se jedná o porušení zabezpečení osobních údajů, určení jeho závažnosti, podle závažnosti

informování dozorového orgánu a případně i subjektu údajů. Od zjištění porušení zabezpečení osobních údajů běží 72hodinová lhůta k nahlášení incidentu, je tedy zapotřebí co nejdříve provést alespoň základní hlášení s tím, že později je možné hlášení upřesňovat. Nedodržení této lhůty je za určitých okolností možné, je však nutné zpoždění zdůvodnit.

- **Zpracování** incidentu: plné zvládnutí hrozby, provedení nápravných opatření, podle závažnosti porušení případně také informování dozorového orgánu či subjektu údajů.
- **Uzavření** incidentu: Dokončení prací na zvládnutí případu porušení zabezpečení osobních údajů, je-li potřeba, tak závěrečná informace zúčastněným osobám (subjekt, dozorový orgán, zodpovědné osoby v rámci organizace). Dále pak zpracování návrhu na preventivní opatření.

Zpracování porušení ochrany osobních údajů úzce souvisí se stávající strukturou pro řízení incidentů v oblasti bezpečnosti IT (tedy nejen ochrany osobních údajů). Proces by měl zahrnovat kooperaci bezpečnostního týmu, bezpečnostního manažera a dalších rolí, které už organizace má v této oblasti z minulosti k dispozici.

4.3 Evidence nového zpracování osobních údajů

Při zavádění nové agendy nebo informačního systému, který zpracovává osobní údaje, nebo při jejich změnách je zapotřebí nejprve provést posouzení. Pro toto posouzení je zapotřebí shrnout řadu informací, zejména účel a legitimnost zpracování, jeho nezbytnost, rizikovost, způsoby zabezpečení, apod. Tyto informace by typicky měla uvést osoba, která je za dané zpracování odpovědná. Samotné posouzení může mít v závislosti na vnitřních předpisech různý průběh (kdo posuzuje, zda je nezbytná nějaká forma schválení, apod.). Zpracování by mělo být po posouzení a schválení zařazeno do *Registru zpracování osobních údajů*. Teprve poté by mělo být zpracování osobních údajů zahájeno.

5 Vlastnosti informačních systémů

GDPR klade na procesy a informační systémy zpracovávající osobní údaje poměrně vysoké nároky. V následujícím textu jsou popsány vlastnosti, které zajišťují kvalitní ochranu osobních údajů. Je iluzorní předpokládat, že by všechny informační systémy organizace splnily všechny potřebné požadavky. Uplatnění alespoň některých níže uvedených zásad (ať už při revizi vlastností stávajících systémů nebo při návrhu a implementaci systémů nových) povede k lepšímu souladu s Nařízením.

5.1 Systémové vlastnosti

Data v systému a jejich struktura

- V systému jsou pouze nezbytně nutné osobní údaje.
- Významové nebo veřejné identifikátory (rodné číslo, zaměstnanecké číslo, studijní číslo) se nepoužívají jako vazební uvnitř datové struktury.
- Osobní údaje jsou odděleny v samostatných tabulkách (z důvodu oddělení přístupu dle rolí nebo pro snadnou anonymizaci dat).
- Citlivá data (osobní údaje zvláštní kategorie) jsou v databázi chráněna šifrováním.
- Data mohou mít definovaný životní cyklus (především minimální a maximální dobu uchování).

Řízení přístupu k datům

- Komunikace při přístupu k datům je chráněna šifrováním nebo jinými prostředky.
- Systém má technicky řádně řešena přístupová práva (role).
- Probíhá pravidelná revize přidělených přístupových práv.
- Přístupy do systému jsou centrálně spravovány (myšleno napojení na centrální autentizační infrastrukturu a systém správy identit a přístupů).
- Je dořešen životní cyklus uživatele včetně změny jeho pozice v organizaci nebo ukončení platnosti uživatele.
- Přístupy k datům jsou nebo mohou být auditovány (nejen čtení a změny, ale třeba i tisk nebo tvorba sestav).

Zálohování

- Data jsou pravidelně zálohována.
- Zálohy jsou zabezpečeny proti přístupu neoprávněných osob.
- Provádí se testy obnovení dat ze záloh.
- Při obnovení ze zálohy je možné odmazat údaje, které již byly odmazány a obnovou ze zálohy došlo k jejich „návratu“.
- Existuje formální politika zálohování a kontroluje se její provádění.
- Vyřazená zálohovací média se bezpečně likvidují.

5.2 Podpora souvisejících procesů

Řešení souhlasu se zpracováním osobních údajů

- Informační systém podporuje prvotní komunikaci s uživatelem (zobrazení pravidel, získání souhlasu, evidence udělení souhlasu, ...).

Reakce na žádosti subjektu

- Informační systém umožňuje vytvořit jednoduchý výpis všech osobních údajů pro konkrétní osobu.
- Ve vybraných případech systém umožňuje exportovat data subjektu v přenositelném formátu.
- Systém umožňuje bezproblémové vymazání nebo anonymizaci dat subjektu (automatizovaně po uplynutí životního cyklu nebo manuálně).
- Systém umí likvidaci dat zaprotokolovat, aby ji mohl doložit subjektu údajů nebo dozorovému orgánu či zohlednit při obnově ze zálohy.

6 Bezpečné nakládání s osobními údaji

6.1 Uchování osobních údajů

Osobní údaje se mohou uchovávat dvěma způsoby, a to v listinné nebo v elektronické podobě. Listinnou podobu mají např. vytištěné osobní údaje, údaje na vizitkách a přístupových kartách. V elektronické podobě se mohou data uchovávat na CD/DVD, USB flash disku, pevném disku počítače, paměťové kartě, síťovém úložišti, magnetické pásce, disketě a dalších médiích.

6.2 Bezpečné nakládání s nosiči osobních údajů

V případě listinné podoby je uchování jednodušší, přestože jsou údaje hmatatelné. Zpravidla postačí jen ochránit nosné médium (potištěný papír, vizitky atd.) před ztrátou, zničením a neoprávněným přístupem. Tím je například uložení na nepřístupném místě, jakým může být uzamykatelná skříň či zásuvka nebo trezor.

Je třeba pamatovat na to, že uzamčené dveře do místnosti nemusí vždy zajistit bezpečné uchování osobních údajů, protože často existují tzv. generální klíče např. pro uklízečku.

U elektronické podoby to již tak snadné není, protože existuje celá řada způsobů, jak může k narušení dostupnosti, důvěrnosti a integrity osobních údajů

dojít. Stejně jako v případě listinné podoby může dojít k neoprávněnému zpřístupnění, například při neuzamčení počítače heslem, když od něj odcházíte. Ale především existuje i hrozba neoprávněného přístupu skrze počítačovou síť. Jak správně zabezpečit počítač najdete v dalších kapitolách.

6.3 Zabezpečení počítačů

Porušením zabezpečení osobních údajů z hlediska GDPR je narušení dostupnosti, důvěrnosti nebo integrity osobních údajů. V těchto odstavcích se nebudeme zabývat narušením dostupnosti. Nejsou-li údaje dostupné, nejsou v tu chvíli zneužitelné. Naproti tomu porušení důvěrnosti (tzn. zpřístupnění osobních údajů osobě, která k tomu nemá oprávnění) či integrity (tzn. neoprávněné změně dat) je třeba aktivně bránit. K oběma druhům narušení může dojít, není-li počítač dostatečně zabezpečen.

Zabezpečení počítačů je možné v několika úrovních. Ty si můžeme představit jako opevnění hradu – hradby, příkopy, stráže. Čím více překážek útočníkovi postavíme do cesty, tím složitější průnik jej čeká. Důležité je především:

- Silné heslo pro přihlášení a zamykání nebo odhlašování v nepřítomnosti.
- Podporovaný a aktualizovaný operační systém.
- Podporované a aktualizované programové vybavení.
- Minimálně nasazené antivirové řešení a firewall.

Další možnosti obrany představují například nástroje pro kontrolu spamu (nevyžádané pošty) a phishingu (pokusů o ovlivnění adresáta podvodným emailem) nebo šifrování, které zabraňuje neautorizovanému přečtení obsahu elektronických médií.

K úniku osobních údajů z počítače může tedy dojít:

- Podceněním zabezpečení – slabé heslo, nedbalost, zastaralý operační systém atd.
- Spuštěním škodlivého kódu např. z přílohy podvodného emailu.

V obou případech může dojít ke kompromitaci zařízení a případnému úniku osobních údajů.

6.4 Likvidace osobních údajů

Podstatou bezpečné likvidace osobních údajů je jejich znečitelnění.

V případě listinných podob se tím rozumí znečitelnění například pomocí skartovačky, případně předání firmě zabývající se skartací na základě smlouvy.

V případě elektronických podob lze likvidaci rozdělit na dva způsoby. V prvním případě se jedná o likvidaci média, které již nelze nebo není potřeba znovu použít. V takovém případě se médium musí fyzicky zničit. Druhou možností je recyklace média, které se použije k jinému účelu, případně jej bude ke svému účelu využívat jiný uživatel. V takovém případě je třeba médium bezpečně smazat. Při tom je třeba mít na paměti, že:

- Data nestačí vyhodit do koše, neboť odtamtud se dají obnovit.
- Data nestačí smazat, jelikož se dají za určitých podmínek obnovit.
- Médium nestačí zformátovat, protože i pak lze data za určitých podmínek obnovit.

Je nutné použít nástroje určené k bezpečnému smazání informací, které zajistí několikanásobné přepsání náhodnými daty, díky čemuž nezůstanou ani torza původních dat, která by bylo možné obnovit.

6.5 Opatrnost především

Všechny výše uvedené případy byly spíše technického rázu, ale je třeba si uvědomit, že k úniku osobních údajů může dojít i lidskou chybou nebo nedbalostí. Uvažme například situaci, kdy vám někdo zavolá, představí se jako nějaká autorita (např. rektor, vedoucí pracoviště a podobně), a bude pod pohrůžkou nějaké ztráty požadovat zaslání osobních údajů. Tato technika se nazývá „sociální inženýrství“. V takovém případě je potřeba se držet určitých zásad:

- Neposkytovat osobní údaje bezhlavě.
- Nezávislým kanálem ověřit, že je požadavek oprávněný.
- Pokud dojde k odeslání dat, musí se osobní údaje (zvláště citlivé) posílat zašifrovaně.

Odkazy pro další studium

- Směrnice v češtině *http://www.privacy-regulation.eu/cs/*
- Metodická pomůcka MŠMT k aplikaci GDPR *http://www.msmt.cz/file/44592/*
- Stanoviska ÚOOÚ ke GDPR *http://www.mvcr.cz/gdpr/*
- Hlavní stránky projektu *http://gdprcrp.ics.muni.cz*
- CRP YouTube kanál *http://crp-gdpr.zcu.cz*

Obsah

Jiří Bořík, Jiří Čepák, Jiří Šafra
CRP-GDPR – Příručka pro zaměstnance

Text Jiří Bořík, Jiří Čepák, Jiří Šafra
Obálka Šárka Zuzjaková
Sazba písmem TEX Gyre Pagella v typografickém systému LATEX 2ε Zdeněk Šustr
Publikace neprošla jazykovou ani redakční úpravou
Vydal Zdeněk Šustr v Praze
Vytiskl Typos, tiskařské závody, s.r.o., Plzeň
1. vydání, 2018

Publikace byla vytvořena v rámci CRP projektu MŠMT 2018 „Komplexní řešení ochrany osobních údajů v prostředí vysokých škol“.

ISBN 978-80-905464-3-1


CRP-GDPR
2018