Označení	**Ochrana osobních údajů**	
Výtisk číslo		
Platnost od	**1. 5. 2018**	
Vydání	**1**	
	jméno	datum
Zpracoval		**1. 5. 2018**
Schválil		**1. 5. 2018**

2 OBSAH

3 OCHRANA OSOBNÍCH ÚDAJŮ

3.1 Politika ochrany osobních údajů

Vedení úřadu obce Malá Štáhle chápe systém řízení ochrany osobních údajů jako nedílnou součást svého přístupu k podnikatelskému záměru úřadu a zahrnuje proces řízení a zlepšování ochrany osobních údajů do organizační struktury, plánování a veškerých dalších klíčových činností a procesů úřadu.

Politika ochrany osobních údajů je závazná pro všechny pracovníky úřadu obce Malá Štáhle a všechny další osoby zainteresovaných stran, jež jsou vázané k zajištění ochrany osobních údajů úřadu příslušnou smlouvou.

Vedoucí pracovníci jsou plně zodpovědní za seznámení všech svých podřízených s obsahem tohoto dokumentu.

3.1.1 Uplatňované principy

Vedení úřadu obce Malá Štáhle deklaruje v celém procesu řízení ochrany osobních údajů soulad činností úřadu a chování svých zaměstnanců s následujícími kriteriálními principy:

- adresné odpovědnosti, kdy budou vždy stanoveny konkrétní odpovědnosti vlastníků informačních aktiv a ostatních subjektů zajišťujících ochranu či zpracování osobních údajů;
- nezbytné znalosti, kdy všechny subjekty, participující na zajišťování ochrany osobních údajů, budou znát bezpečnostní dokumentaci a opatření v nich stanovena;
- integrity, kdy je zajištěno řízení celého životního cyklu osobních údajů;
- přiměřenosti opatření, kdy přijímána bezpečnostní opatření jsou vždy přímo úměrná aktuální míře rizik.

3.1.2 Základní pojmy

osobní údaje	…	veškeré informace o identifikované nebo identifikovatelné fyzické osobě (např. jméno, identifikační číslo, lokační údaje, podobizna, síťové identifikátory, prvky prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity)
citlivé OÚ	…	osobní údaje, které odhalují rasový nebo etnický původ osoby, její politické názory, náboženské přesvědčení, filozofické postoje, nebo členství v odborových organizacích; biometrické údaje (např. otisky prstů nebo rozpoznávání obličeje) nebo genetické informace; informace o zdraví, pohlavním životě nebo sexuální orientaci osoby; údaje o trestech nebo spáchaných trestných činech (včetně obvinění).
zpracování OÚ	…	jakákoliv operace prováděná s osobními údaji (např. shromáždění, zaznamenání, uložení, změna, vyhledání, použití, seznámení, zpřístupnění, výmaz, omezení zničení)
správce	…	subjekt, který určuje účely a prostředky zpracování OÚ
zpracovatel	…	subjekt, který zpracovává osobní údaje pro správce
příjemce	…	subjekt, kterému jsou OÚ poskytnuty
souhlas	…	jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým dává subjekt svolení ke zpracování OÚ
subjekt údajů	…	fyzická osoba, ke které se osobní údaje vztahují

3.1.3 Zkratky

CCTV	…	Closed Circuit Television (UzavřenýTV okruh – kamerový systém)
DPIA	…	Data Protection Impact Assessment (Posouzení vlivu na ochranu OÚ)
GDPR	…	General Data Protection Regulation (Nařízení o ochraně osobních údajů)
DPO	…	Data Protection Office (Pověřenec pro ochranu osobních údajů)
IT	…	Information Technology (Informační technologie)
OÚ	…	osobní údaj

ÚOOÚ … Úřad pro ochranu osobních údajů

3.2 Tým ochrany osobních údajů

Pro nastavení procesů řízení ochrany osobních údajů a zajištění řízení bezpečnostních opatření ochrany osobních údajů je v rámci úřadu ustanoven Tým ochrany osobních údajů ve složení:

- pověřenec pro ochranu osobních údajů
  - vlastníci zpracování osobních údajů

Tým ochrany osobních údajů:

- je podřízen vedení úřadu;
- podílí se na přípravě předpisů pro ochranu osobních údajů;
- stanovuje opatření ke zlepšení pro všechna zjištění z auditu ochrany osobních údajů;
- poskytuje metodickou pomoc všem pracovníkům úřadu v oblasti ochrany osobních údajů.

3.2.1 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (DPO) je definován v článku 38 GDPR. Pověřenec pro ochranu osobních údajů musí být zapojen do všech činností úřadu týkajících se zpracování osobních údajů.

Odpovědnosti:

- dohled na dodržování právních požadavků v oblasti ochrany osobních údajů;
- odpovědnost za vytvoření, zavedení a udržování procesů, pokynů a pravidel potřebných pro systém ochrany osobních údajů a zpracování osobních údajů;
- dohled nad procesy ochrany osobních údajů;
- zpracování Posouzení vlivu na ochranu osobních údajů (DPIA);
- komunikace a spolupráce se subjekty údajů;
- komunikace a spolupráce s ÚOOÚ;
- vedení evidence zpracování osobních údajů a záznamů o zpracování osobních údajů;
- organizace pravidelného monitorování zpracování osobních údajů (přezkoumání, audit);
- poskytování informací o zpracování osobních údajů vedení úřadu;
- zlepšování systému ochrany osobních údajů;
- zajištění školení pracovníků úřadu.

3.2.2 Vlastník zpracování osobních údajů

Vlastník zpracování osobních údajů odpovídá za provádění procesů zpracování v souladu s požadavky na ochranu osobních údajů.

Odpovědnosti:

- autorizace přístupových práv k osobním údajům;
- spolupráce na výkonu práv subjektů;
- spolupráce na zpracování analýzy rizik;
- spolupráce na tvorbě pravidel pro zpracování osobních údajů;
- identifikace nebezpečí a hodnocení rizik zpracování osobních údajů;
- zajištění implementace a dodržování stanovených opatření.

Vlastník zpracování osobních údajů je povinen:

- dodržovat všechny pokyny a opatření vydaná k podmínkám, rozsahu a způsobu jim prováděných zpracování osobních údajů;
- zúčastňovat se nařízených školení v oblasti ochrany osobních údajů;
- poskytovat potřebnou součinnost správci osobních údajů;
- bezprostředně oznámit pověřenci pro ochranu osobních údajů případy neoprávněného nebo nahodilého přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů;

- bezprostředně oznámit pověřenci pro ochranu osobních údajů jakákoliv zjištěná porušení bezpečnostních opatření k ochraně osobních údajů.

3.3 Zpracování osobních údajů

Každé zpracování osobních údajů prováděné úřadem musí zpracovávat přesné osobní údaje a musí být:

- zákonné, korektní a transparentní;
- pro určité, vyjádřené a legitimní účely;
- časově adekvátní požadavkům a účelům;
- bezpečné.

3.3.1 Zákonnost zpracování

Zpracování osobních údajů je zákonné, pouze pokud je to nezbytné pro:

- Plnění smlouvy či poskytnutí služby.
- Plnění požadavků právních předpisů.
- Účely oprávněných zájmů úřadu (pokud nebudou mít přednost zájmy nebo základní práva a svobody subjektu údajů).

V ostatních případech je nezbytné zajistit pro zpracování osobních údajů souhlas subjektu údajů a údaje zpracovávat pouze na základě tohoto souhlasu.

Souhlas se zpracováním osobních údajů musí být svobodný (nesmí být vynucený nebo součástí smluvních podmínek) a kdykoliv odvolatelný (odvolání nesmí být navázáno na jiná plnění nebo výhody či odepření služeb). V souhlasu musí být uveden účel zpracování, doba zpracování, identifikace správce. Souhlas může být zpracován v elektronické i fyzické podobě, ale úřad jej musí být schopen doložit.

> *Poznámka:*
> *U souhlasů je nezbytná pravidelná kontrola jejich platnosti a zajištění obnovy souhlasů nebo likvidace údajů po ukončení platnosti souhlasu.*

3.3.2 Webové prezentace

Zásady zpracování osobních údajů

Na webových prezentacích úřadu je vhodné zveřejnit zásady zpracování osobních údajů. Tyto zásady je vhodné zveřejnit na hlavním webu úřadu a z ostatních webů na tyto zásady odkazovat.

Vzor zásad je uveden v příloze Příloha č. 1 – Zásady zpracování osobních údajů.

> *Doporučení - adresa odkazu na stránku se zásadami zpracování osobních údajů by měla být smysluplná (např. domena.cz/zasady_zpracovani_ou, a ne domena.cz/page?id=28.)*

Cookies[1]

Veškeré weby s cookies (jakéhokoliv druhu) musí obsahovat informační panel (banner) s informacemi o používání souborů cookies. Součástí informačního banneru a webové prezentace musí být také zásady používání souborů cookies.

Vzor zásad je uveden v příloze Příloha č. 2 – Zásady používání cookies.

> *Doporučení - adresa odkazu na stránku se zásadami používání souborů cookies by měla být smysluplná (např. domena.cz/zasady_cookies, a ne domena.cz/page?id=29.)*

[1] Cookies jsou malé textové soubory obsahující zanedbatelné množství informací (písmena a číslice), které se ukládají do prohlížeče při návštěvě webové stránky. Webovým stránkám umožňují rozeznat webový prohlížeč nebo zařízení, které uživatel používá nebo slouží k ukládání různých nastavení.

Fotografie a videa osob

Umístění fotografií a videí osob na webových stránkách úřadu vždy podléhá souhlasům se zpracováním osobních údajů.

Pro všechny fotografie a videa zveřejněné na webové prezentaci je nezbytné mít k dispozici platný souhlas se zpracováním osobních údajů.

Výjimku tvoří fotografie a videa větších skupin osob pro ilustrační účely a fotografie a videa, kde není možné rozeznat jednotlivé osoby.

Vzor souhlasu pro zaměstnance je uveden v příloze Příloha č. 3 – Souhlas – Použití fotografií pro marketingové účely.

Kontaktní formuláře

V případě, že se na stránkách úřadu nacházejí jakékoliv kontaktní formuláře s možností zadat osobní údaje, je nezbytné doplnit tyto formuláře o informaci o účelu zpracování a způsobu nakládání s těmito osobními údaji.

Příklad:

Odesláním formuláře souhlasím se zpracováním zadaných osobních údajů za účelem reakce na odeslanou zprávu. Osobní údaje budou zpracovány v souladu se Zásadami zpracování osobních údajů.

Jedná-li se o formulář s možností zadání emailové adresy, která by mohla být mimo jiné zpracována za účelem zasílání marketingových sdělení, je nezbytné doplnit formulář o „zaškrtávací políčko“ souhlas se zpracováním osobních údajů pro marketingové účely.

Kontakt na pověřence pro ochranu osobních údajů

Na stránkách úřadu je nezbytné zveřejnit kontaktní údaje (jméno a příjmení, poštovní adresu, telefonní číslo a email) na pověřence pro ochranu osobních údajů, kterým vždy musí být konkrétní fyzická osoba.

Vhodným místem zveřejnění jsou obecné kontaktní údaje, úřední deska (elektronická i fyzická) a sekce povinně zveřejňovaných informací (dle zákona č. 106/1999 Sb.) a Zásady pro zpracování osobních údajů.

Kontakty na pracovníky

Kontakty na pracovníky úřadu mohou být na webových prezentacích uvedeny volně, pokud součástí kontaktů nejsou osobní emaily nebo telefony pracovníků nebo fotografie nebo údaje přímo nesouvisející s nezbytným kontaktem (životopisy, stav přítomnosti v práci, apod.)

V ostatních případech je nezbytné získání souhlasu.

Kontakty na osoby třetích stran

Kontakty na osoby jiných organizací mohou být na webových prezentacích uvedeny pouze na základě plnění smlouvy či poskytnutí služby nebo na základě získaného souhlasu dotyčné osoby.

3.3.3 Pracovníci

Pracovní smlouvy a dohody

Pracovní smlouvy a dohody s pracovníky je vhodné doplnit o informace nakládání s jejich osobními údaji pro naplnění informační povinnosti.

Informační povinnost je možné vyřešit také samostatným dokumentem, se kterým se pracovník seznámí a seznámení potvrdí svým podpisem.

Vzor informační doložky je uveden v příloze Příloha č. 4 – Doplněk do pracovních smluv a dohod.

Dohody o mlčenlivosti

S pracovníky, kteří zpracovávají osobní údaje v rámci své hlavní pracovní náplně (minimálně s pověřencem pro ochranu osobních údajů a vlastníky zpracování osobních údajů), je vhodné uzavřít dohodu o mlčenlivosti.

Vzor dohody o mlčenlivosti je uveden v příloze Příloha č. 5 – Dohoda o mlčenlivosti - zaměstnanec.

Seznámení s dokumentací

Všechny pracovníky je nezbytné seznámit s řídicí dokumentací. Seznámení provádí pracovníci zajišťující nábor nového pracovníka nebo vedoucí pracovníci v rámci revize řídicí dokumentace.

Seznámení je evidováno např. na formuláři Záznam o seznámení pracovníků.

Docházkový systém s otisky prstů

Zpracování otisků prstů (citlivých osobních údajů) pro potřeby přihlašování pracovníků k docházkovému systému vždy podléhá souhlasu se zpracováním osobních údajů. Pracovníci musí dostat také jinou možnost pro přihlášení k docházkovému systému.

Vzor souhlasu se zpracováním osobních údajů je v příloze Příloha č. 6 – Souhlas – biometrika.

3.3.4 Stanovení Týmu ochrany osobních údajů

Jmenování

Pověřenec pro ochranu osobních údajů je jmenován do funkce pověřovací listinou nebo jmenovacím dekretem, kde je uveden název funkce a rozsah pověření (může být formou odkazu na dokumentaci systému ochrany osobních údajů).

Vzor souhlasu se zpracováním osobních údajů je v příloze Příloha č. 11 – Jmenování – Pověřenec OOÚ.

Popisy pracovních míst

Členové týmu musí být seznámeni s popisem pracovního místa a s vymezenými odpovědnostmi a pravomocemi, což stvrzují podpisem.

Seznámení s dokumentací

Členy Týmu ochrany osobních údajů a všechny pracovníky, kteří manipulují s osobními údaji, je nezbytné prokazatelně seznámit s řídící dokumentací. Seznámení je evidováno např. na formuláři Záznam o seznámení pracovníků.

Dohody o mlčenlivosti

S pracovníky, kteří zpracovávají osobní údaje v rámci své hlavní pracovní náplně (minimálně s členy Týmu ochrany osobních údajů), je vhodné uzavřít dohodu o mlčenlivosti.

Vzor dohody o mlčenlivosti je uveden v příloze Příloha č. 5 – Dohoda o mlčenlivosti zaměstnanec.

3.3.5 Dodavatelé a odběratelé

Dodavatelé služeb

Externího dodavatele služeb (účetnictví, právní služby, audity, konzultace, IT služby, IT správa) je nezbytné zavázat k řízenému zpracování osobních údajů a poskytování záruk a nezbytné odpovědnosti za zpracování údajů.

Ke stávajícím smlouvám s dodavatelem je vhodné doplnit dodatky o ochraně osobních údajů, a pokud je součástí také přímo zpracování osobních údajů, pak také dodatky o zpracování osobních údajů.

Ochrana osobních údajů

Vzor dodatku o ochraně osobních údajů je uveden v příloze Příloha č. 7 – Dodatek ke smlouvě.

V případě, že s dodavatelem je uzavřeno smluv více nebo není vhodné řešit dodatek ke stávající smlouvě nebo správce údajů vyžaduje větší garance a jistoty, může být s dodavatelem uzavřena á zpracovatelská smlouva, která řeší pouze povinnosti zpracování osobních údajů. Samotná zpracovatelská smlouva nijak nenarušuje smluvená ujednání uzavřených kontraktů s dodavatelem.

Vzor zpracovatelské smlouvy je v příloze Příloha č. 8 – Zpracovatelská smlouva.

Odběratelé

Ke stávajícím smlouvám s odběratelem je vhodné doplnit dodatky o ochraně osobních údajů.

Vzor dodatku o ochraně osobních údajů je uveden v příloze Příloha č. 7 – Dodatek ke smlouvě.

3.3.6 Kamerové systémy

Kamerové systémy (CCTV)

Při monitorování prostor pomocí kamerového systému je nezbytné zajištění účelného monitorování prostor bez monitorování veřejného prostranství (mimo obecní kamerové systémy a systémy policie) a soukromých prostor.

Doba záznamu by neměla přesáhnout 14 dnů.

Všechny osoby v monitorovaném prostoru je nezbytné informovat o provozování kamerového systému – pracovníky pomocí informační doložky v pracovní smlouvě, nájemníky či vlastníky budov informací v nájemních smlouvách a ostatní výstražnou cedulí.

Monitorované prostory je nezbytné označit výstražnou cedulí s textem (např. „Prostor monitorován kamerovým systémem se záznamem“), piktogramem kamery a kontaktem na správce kamerového systému.

3.4 Pověřenec pro ochranu osobních údajů (DPO)

Pověřence pro ochranu osobních údajů je nezbytné jmenovat pokud:

- zpracování OÚ provádí orgán veřejné moci či veřejný subjekt;
- hlavní činnost zpracování spočívá v rozsáhlém pravidelném a systematickém monitorování subjektů;
- hlavní činnost zpracování spočívá v rozsáhlém zpracování citlivých osobních údajů.

3.4.1 Zveřejnění kontaktních údajů DPO

Kontaktní údaje na pověřence pro ochranu osobních údajů musí být zveřejněny (na webových stránkách, na úřední desce, apod.) a sděleny ÚOOÚ.

Sdělení ÚOOÚ lze provést elektronicky (na adresu posta@uoou.cz nebo do datové schránky qkbaa2n).

Obsahem sdělení je:

- předmět sdělení – „Oznámení pověřence“;
- text sdělení:
  - identifikace správce, který jmenuje pověřence;
  - jméno a příjmení pověřence;
  - kontaktní údaje (email a telefon) na pověřence.

3.5 Porušení zabezpečení osobních údajů

O každém porušení zabezpečení osobních údajů Pověřenec pro ochranu osobních údajů rozhodne, zda je nutné tohle porušení hlásit a zajistí případné hlášení na ÚOOÚ nebo hlášení subjektům údajů.

Každé porušení zabezpečení osobních údajů pověřenec pro ochranu OÚ zaeviduje v příslušné evidenci.

3.5.1 Hlášení na ÚOOÚ

Pověřenec pro ochranu osobních údajů je povinen nahlásit porušení zabezpečení osobních údajů ÚOOÚ vždy. Výjimkou jsou pouze porušení, kdy je nepravděpodobné, že porušení mělo za následek riziko pro práva a svobody fyzických svobod.

Nahlášení ÚOOÚ je třeba učinit do 72 hodin od okamžiku, kdy se úřad o porušení dozvěděl.

3.5.2 Hlášení subjektům údajů

Pověřenec pro ochranu OÚ je povinen oznámit porušení zabezpečení osobních údajů dotčeným subjektům údajů pokud je pravděpodobné, že bezpečnostní incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob

Oznámení je třeba učinit do 72 hodin od okamžiku, kdy se úřad o porušení dozvěděl, a to prostřednictvím přímého kontaktování dotčených subjektů údajů (emailem, telefonicky, apod.). Není-li přímé kontaktování dotčených subjektů údajů možné, zveřejní se oznámení na webových stránkách úřadu, případně se oznámení zveřejní jiným vhodným způsobem.

4 ZPŮSOBY ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

4.1 Personální zajištění ochrany osobních údajů

Dle obecného nařízení o ochraně osobních údajů je zodpovědnou osobou za zpracování osobních údajů statutární orgán - starosta.

Pro praktické a efektivní zajištění ochrany osobních údajů a splnění všech povinností, jsou povinnosti zodpovědné osoby rozčleněny na jednotlivé výkonné role.

Naplňování všech požadavků na ochranu osobních údajů zajišťuje tým ochrany osobních údajů.

4.2 Administrativní zajištění ochrany osobních údajů

- úřad má pro každé zpracování přijata a zdokumentována příslušná opatření a vede záznamy o zpracování;
- dále vede a průběžně aktualizuje:
  - záznamy o provedených školeních zaměstnanců v oblasti ochrany osobních údajů;
  - přehled o případných smluvních zpracovatelích osobních údajů;
  - záznamy řešení práv subjektů údajů;
  - záznamy o případné komunikaci s Úřadem pro ochranu osobních údajů;
- skartační řízení písemností s osobními údaji provádí v souladu s dokumentovaným postupem.

4.3 Fyzické zajištění ochrany osobních údajů

V rámci technické a objektové bezpečnosti ochrany osobních údajů je u úřadu zajištěno:

- stanovení objektů, míst, prostor a úschovných objektů, ve kterých se mohou osobní údaje zpracovávat a kde mohou být jejich nosiče uloženy;
- zdokumentování objektových a technických opatření k ochraně těchto objektů.

4.4 Informační a komunikační zajištění ochrany osobních údajů

Informační a komunikační bezpečnost zajišťuje úřad pomocí:

- stanovení struktury IT;
- ochrany dat a informací v IT;
- antivirové ochrany, omezení instalace aplikací;
- monitorováním a kontrolou provozu;
- dokumentace IT.
- řízením změn IT.
- periodických školeních pracovníků v oblasti používání IT.

4.5 Režimové zajištění ochrany osobních údajů

V rámci režimového zajištění ochrany osobních údajů úřadu zajišťuje:

- periodické proškolování zaměstnanců s problematikou ochrany osobních údajů, přijatými opatřeními a s jejich povinnostmi;
- stanovením režimových opatření při výkonu svých činností;
- zapracování přijímaných režimových opatření do příslušné bezpečnostní dokumentace;
- efektivní provádění monitorování stavu ochrany osobních údajů u úřadu.

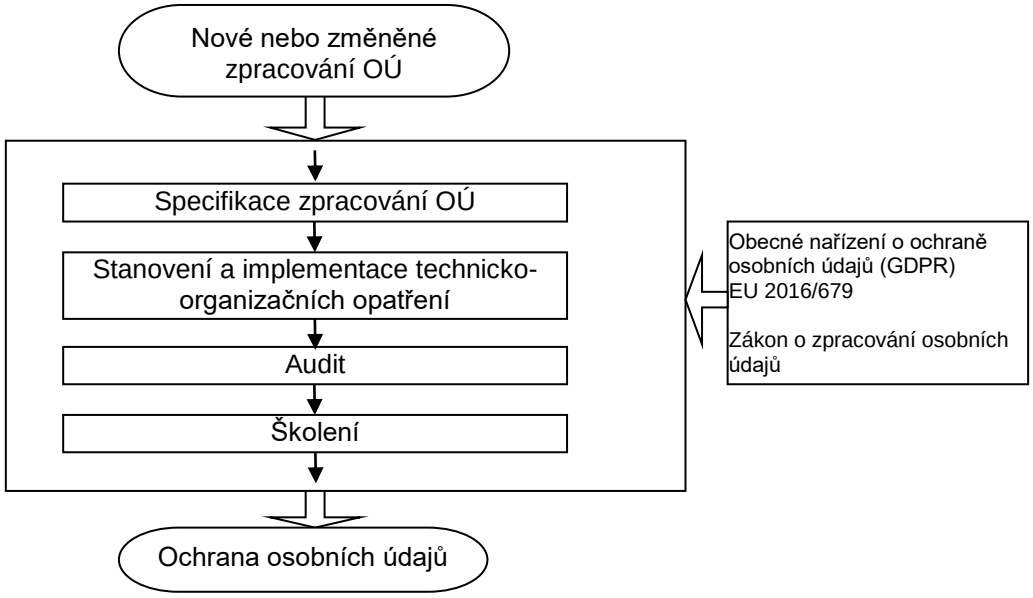
4.6 Procesy ochrany osobních údajů

Ochrana osobních údajů je zajišťována prostřednictvím implementace procesů ochrany osobních údajů. Jednotlivé procesy jsou integrovány do systému řízení úřadu.

- Řízení zpracování osobních údajů
- Řízení bezpečnostních incidentů
- Řešení práv subjektů.

5 ŘÍZENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

5.1 Proces řízení zpracování osobních údajů



Vlastníkem procesu je Pověřenec pro ochranu osobních údajů.

5.2 Specifikace zpracování OÚ

V rámci specifikace je vyhodnocen účel, zákonnost a právní základ pro zpracování osobních údajů.

O každém zpracování musí být definovány základní parametry (záznamy o zpracování):

- identifikace správce OÚ;
- kontakt na pověřence pro ochranu OÚ;
- způsob, jakým budou osobní údaje zpracovány;
- kdo je zpracovává, kde a jak;
- jaké jsou plánované lhůty pro výmaz OÚ.

Před samotným zpracování OÚ musí Pověřenec pro ochranu osobních údajů posoudit potřebu vypracování Posouzení vlivu na ochranu osobních údajů (DPIA).

V rámci specifikace je nezbytné provedení také analýzy rizik zpracování osobních údajů a jejich možných dopadů na subjekty údajů.

Celou specifikaci zpracování OÚ uvede Pověřenec pro ochranu osobních údajů do formuláře Záznamy a pravidla zpracování.

5.3 Stanovení a implementace techniko-organizačních opatření

Nastavení technicko-organizačních opatření nutných pro zajištění bezpečného zpracování osobních údajů.

Jednotlivá opatření jsou formulována v bezpečnostní politice úřadu, ochraně osobních údajů nebo jednotlivých postupech pro zpracování osobních údajů. Postupy pro zpracování osobních údajů nahrazují záznamy o zpracování OÚ.

Veškerá opatření musí respektovat provedenou analýzu rizik.

Bezpečnost zpracování osobních údajů musí být zajišťována v oblastech:

- personální bezpečnosti;
- fyzické bezpečnosti;
- administrativní bezpečnosti;
- informační a komunikační bezpečnosti;
- režimové bezpečnosti.

Veškerá stanovená technicko-organizační opatření uvede pověřenec pro ochranu osobních údajů do formuláře Záznamy a pravidla zpracování.

5.4 Audit

Audit ochrany osobních údajů je nezbytnou součástí zajištění ochrany osobních údajů. Audit je zaměřen na hodnocení souladu zpracování s právními požadavky.

Audit ochrany osobních údajů je u úřadu prováděn minimálně 1x ročně.

Hlavní cíle auditu:

- posouzení a zhodnocení zajištění ochrany osobních údajů;
- identifikace oblastí pro zlepšení;
- poskytování informací subjektům údajů;
- poskytování informací ÚOOÚ a externím subjektům.

Postup provádění auditu je stanoven v kapitole Audit ochrany osobních údajů.

Zjištění z auditu ochrany osobních údajů slouží pro zlepšování ochrany osobních údajů a zajištění neustálého souladu systému ochrany osobních údajů s požadavky GDPR

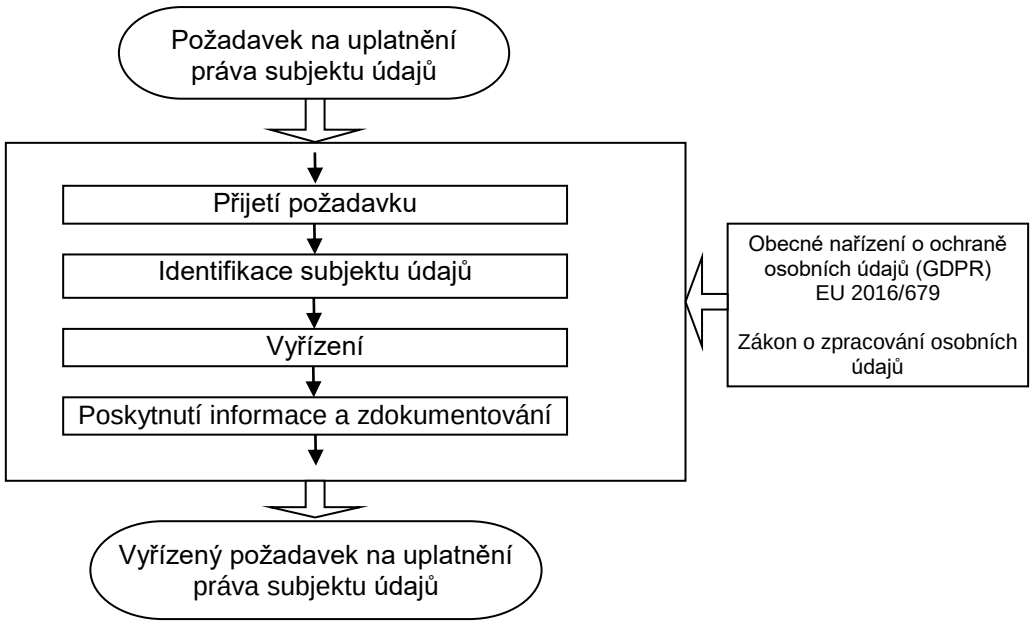
5.5 Školení

Školení oblasti ochrany osobních údajů, zpracování osobních údajů, bezpečnosti IT, změn souvisejících právních přepisů je u úřadu prováděno minimálně 1x ročně.

Při nástupu nových pracovníků je zajištěno povinné proškolení v oblasti ochrany osobních údajů a bezpečnosti IT.

Operativně jsou školení realizována po zjištění a nápravě bezpečnostních incidentů.

6 ŘEŠENÍ PRÁV SUBJEKTŮ ÚDAJŮ



Vlastníkem procesu je Pověřenec pro ochranu osobních údajů.

O každém požadavku subjektu údajů zajišťuje Pověřenec pro ochranu osobních údajů vedení evidence a dokumentaci celého procesu řešení požadavku.

6.1 Přijetí požadavku

Požadavky na uplatnění práva subjektu údajů přijímá pracovník úřadu. Pracovník má povinnost každý nahlášený požadavek ihned předat pověřenci pro ochranu osobních údajů (včetně identifikace subjektu údajů, typu požadavku, data a času jeho přijetí.).

Přijetí požadavku je subjektu údajů potvrzeno vyplněním formuláře Potvrzení přijetí žádosti subjektu údajů.

6.2 Identifikace subjektu údajů

Pověřenec pro ochranu osobních údajů musí zajistit ověření totožnosti subjektu údajů.

Identita všech subjektů musí být před vyřízením požadavku ověřena. Ověření může být realizováno osobně nebo vzdáleně. Ověření subjektu údajů musí vždy vycházet z údajů, které má úřad k dispozici. Pro ověření identity subjektu může Pověřenec pro ochranu osobních údajů využít všechny vlastníky zpracování osobních údajů.

Veškeré podklady mohou být zasílány jen ověřeným subjektům.

6.3 Vyřízení

V rámci vyřízení požadavku subjektů údajů Pověřenec pro ochranu osobních údajů spolupracuje s vlastníky zpracování osobních údajů, kteří zajistí samotné vyřízení požadavků.

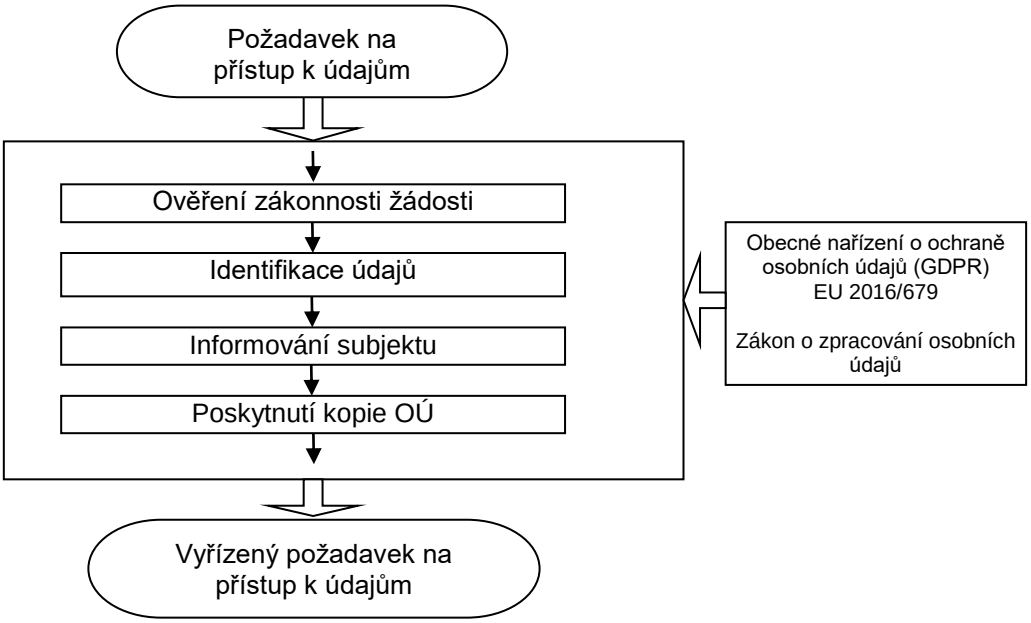
V případě potřeby je Pověřenec pro ochranu osobních údajů oprávněn svolat tým ochrany osobních údajů, případně rozšířit tým o další nezbytné pracovníky či externisty.

Požadavky na jednotlivé řešitele jsou předávány prostřednictvím elektronické pošty.

Průběh celého řečení požadavku subjektu údajů je dokumentován v rámci interních záznamů.

6.3.1 Právo na přístup k osobním údajům (přístup)

Subjekt má (v souladu s článkem 15 GDPR) právo získat potvrzení, zda jeho osobní údaje jsou či nejsou zpracovávány a má právo získat přístup ke svým osobním údajům a k informacím o účelu zpracování, kategorii dotčených údajů, příjemcích údajů, době zpracování údajů, existenci práva na opravu a výmaz údajů, existenci práva podat stížnost u dozorového úřadu, informacích o zdroji osobních údajů a skutečnostech o případném automatizovaném zpracování údajů.



6.3.1.1 Ověření zákonnosti žádosti

Každý požadavek na přístup k údajům musí být posouzen, zda je požadavek relevantní a zda existuje zákonný důvod k odepření přístupu k údajům.

6.3.1.2 Identifikace údajů

U zákonných a relevantních požadavků jsou identifikovány veškeré údaje vedené o subjektu. U údajů je ověřeno, zda mohou být spojeny s identifikovanou osobou.

Identifikace předávání údajů do třetí země nebo mezinárodní organizaci a identifikace souvisejících záruk, které se vztahuji na dané předávání osobních údajů.

V rámci identifikace údajů je nezbytná revize omezení týkajících se poskytnutých údajů (dopady na jiné subjekty údajů, omezení práv a svobod ostatních, apod.)

6.3.1.3 Informování subjektu

Sestavení informace o všech aspektech zpracování, zdrojích a předáních údajů.

Součástí informace musí být upozornění na existenci práva podat stížnost u ÚOOÚ a případně oznámení o existenci práva na výmaz či opravu údajů.

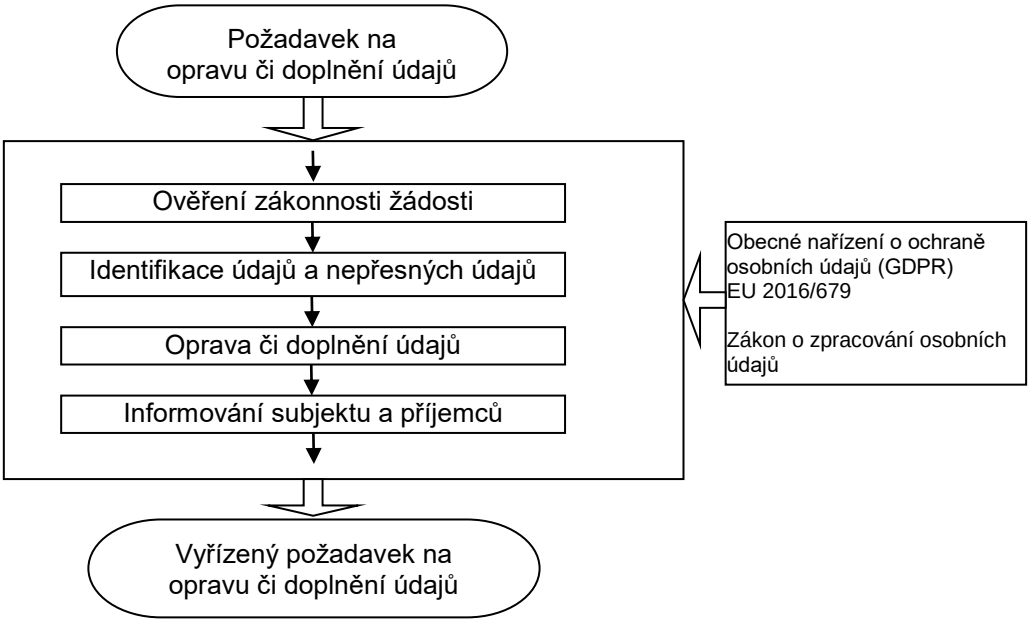
Informace jsou subjektům údajů poskytovány pouze zabezpečeným kanálem. Informace mohou být podávány v elektronické nebo fyzické podobě (dle požadavku).

6.3.1.4 Poskytnutí kopie OÚ

Úřad musí poskytnout kopie údajů. Tímto právem nesmí být dotčena práva jiných subjektů či jiná práva a předpisy. Veškeré poskytnuté údaje musí být zkontrolovány, zda neobsahují informace o jiných subjektech nebo chráněných skutečnostech.

6.3.2 Právo na opravu (oprava)

Subjekt má (v souladu s článkem 16 GDPR) právo, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje subjektu, případně tyto údaje doplnil.



6.3.2.1 Ověření zákonnosti žádosti

Každý požadavek na opravu údajů musí být posouzen, zda je požadavek relevantní a zda může být oprava či doplnění údajů provedena.

6.3.2.2 Identifikace údajů a nepřesných údajů

Vlastník zpracování musí zajistit identifikaci údajů subjektu a ověřit, zda jsou údaje o subjektu přesné a identifikuje nepřesně evidované údaje.

6.3.2.3 Oprava či doplnění údajů

Vlastník zpracování musí zajistit opravu všech nepřesných údajů ve svých zpracováních a případné doplnění osobních údajů.

O každé opravě či doplnění údajů musí vlastník zpracování vyhotovit záznam.

6.3.2.4 Informování subjektu údajů

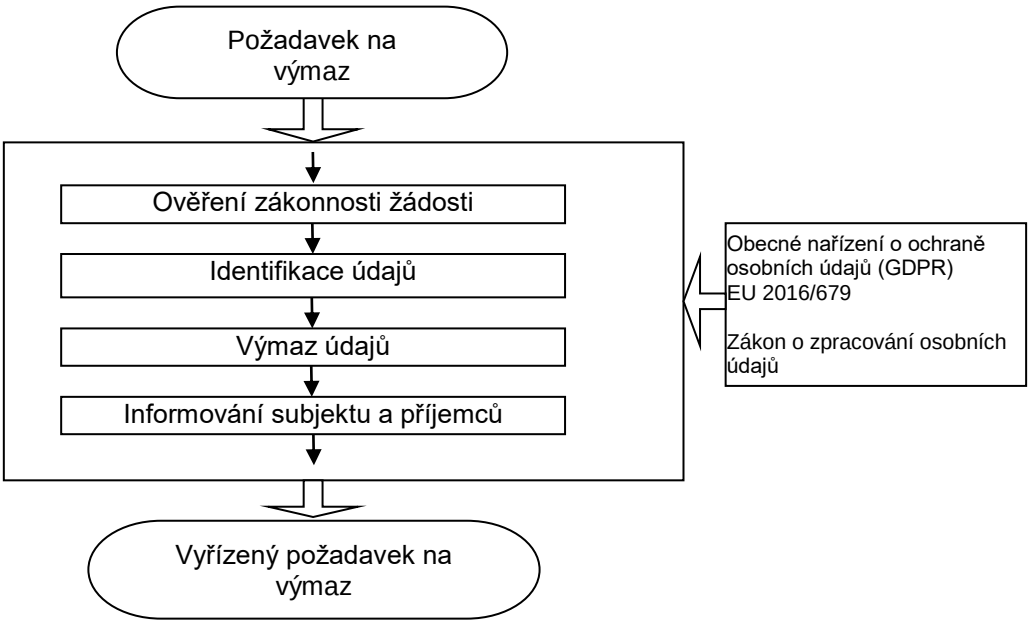
Za sestavení informace o vyřízení požadavku zodpovídá vlastník zpracování. Informace předává Pověřenci pro ochranu osobních údajů.

Součástí informace musí být upozornění na existenci práva podat stížnost u ÚOOÚ a případně oznámení o existenci práva na výmaz či opravu údajů.

Vlastník zpracování musí informovat o opravě či doplnění údajů všechny poskytovatele (správce) údajů, kterým byly osobní údaje subjektu předány, a všechny navazující příjemce (zpracovatele) údajů a musí zajistit opravu údajů jimi vedených.

6.3.3 Právo na výmaz („právo být zapomenut“)

Subjekt má (v souladu s článkem 17 GDPR) právo, aby správce bez zbytečného odkladu vymazal osobní údaje subjektu.



6.3.3.1 Ověření zákonnosti žádosti

Každý požadavek na výmaz musí být posouzen, zda je relevantní a zda existuje zákonná povinnost, jež by výmazu údajů bránila.

Osobní údaje není možné vymazat, pokud:

- je jejich zpracování nezbytné pro výkon práva na svobodu projevu a informace;
- jsou nezbytné pro naplnění právních povinností;
- jsou nezbytné pro účely povinné archivace;
- jsou nezbytné pro určení, výkon nebo obhajobu právních nároků.

Upozornění – výjimky z práva na výmaz neplatí paušálně pro všechny údaje zpracovávané v dané agendě a je nezbytné rozlišovat, na které konkrétní údaje je možné uplatnit výjimku z práva výmazu.

6.3.3.2 Identifikace údajů

Vlastník zpracování osobních údajů musí zajistit identifikaci všech údajů vedených o subjektu a rozhodnout, zda existují výjimky požadavku na výmaz.

6.3.3.3 Výmaz údajů

Vlastník zpracování musí zajistit výmaz osobních údajů subjektu, odkazů na ně a jejich kopií a replikací. Pokud není technicky možné údaje vymazat, musí zabránit jejich zpracování pomocí blokace.

6.3.3.4 Informování subjektu a příjemců

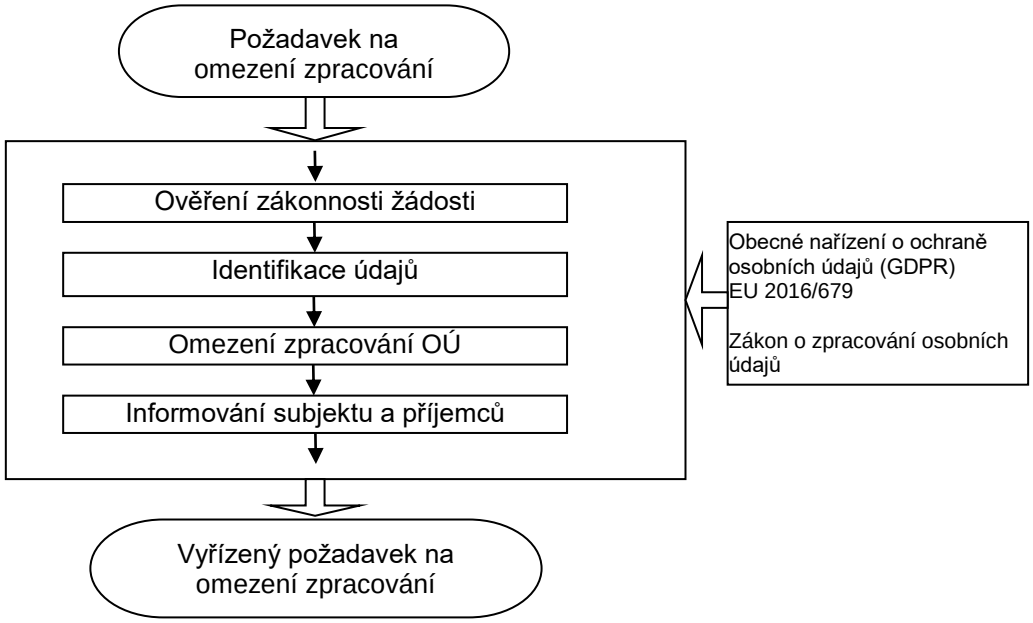
Za sestavení informace o vyřízení požadavku zodpovídá vlastník zpracování. Informace předává pověřenci pro ochranu osobních údajů.

Součástí informace musí být upozornění na existenci práva podat stížnost u ÚOOÚ.

Vlastník zpracování musí informovat všechny poskytovatele (správce) údajů a všechny navazující příjemce (zpracovatele) údajů, kterým byly osobní údaje subjektu předány, že jej subjekt údajů žádá o výmaz osobních údajů a odkazů na tyto osobní údaje.

6.3.4 Právo na omezení zpracování (omezení)

Subjekt má (v souladu s článkem 18 GDPR) právo, aby správce omezil zpracování osobních údajů subjektu.



6.3.4.1 Ověření zákonnosti žádosti

Každý požadavek na omezení zpracování musí být posouzen, zda je požadavek relevantní a zda existuje zákonná povinnost omezení zpracování.

Právo na omezení zpracování nastává pokud:

- subjekt údajů zpochybňuje přesnost vedených osobních údajů (do doby ověření);
- zpracování je nezákonné a subjekt požaduje omezení místo vymazání;
- pominul účel zpracování, ale subjekt údajů potřebuje údaje k určení, výkonu nebo obhajobě právních nároků;
- jsou nezbytné pro určení, výkon nebo obhajobu právních nároků.

Upozornění – výjimky z práva na výmaz neplatí paušálně pro všechny údaje zpracovávané v dané agendě a je nezbytné rozlišovat, na které konkrétní údaje je možné uplatnit výjimku z práva výmazu.

6.3.4.2 Identifikace údajů

Vlastník zpracování osobních údajů musí zajistit identifikaci všech údajů vedených o subjektu a rozhodnout, zda existují výjimky požadavku na omezení zpracování.

6.3.4.3 Omezení zpracování OÚ

Vlastník zpracování musí zajistit omezení zpracování OÚ pomocí jejich blokace.

6.3.4.4 Informování subjektu a příjemců

Za sestavení informace o vyřízení požadavku zodpovídá vlastník zpracování. Informace předává pověřenci pro ochranu osobních údajů.

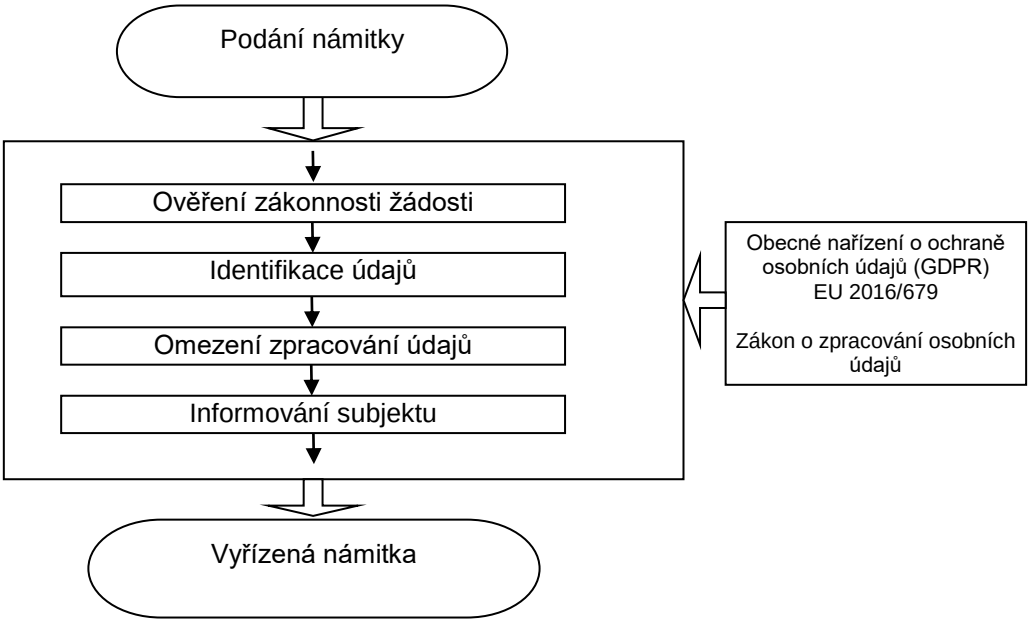
Součástí informace musí být upozornění na existenci práva podat stížnost u ÚOOÚ.

Vlastník zpracování musí informovat všechny poskytovatele (správce) údajů a všechny navazující příjemce (zpracovatele) údajů, že jej subjekt údajů žádá o výmaz osobních údajů a odkazů na tyto osobní údaje.

Informaci o předání požadavků ostatním zpracovatelům údajů, kterým byly osobní údaje subjektu předány, musí vlastník zpracování zaznamenat, včetně vyjmenování všech ostatních zpracovatelů údajů.

6.3.5 Právo na podání námitky (námitka)

Subjekt má (v souladu s článkem 21 GDPR) právo kdykoliv vznést námitku proti zpracování osobních údajů.



6.3.5.1 Ověření zákonnosti žádosti

Každé podání námitky musí být posouzeno, zda je relevantní a zda existují oprávněné důvody pro odmítnutí námitek.

Subjekt může podávat námitky proti:

- zpracování na základě oprávněného zájmu a plnění úkolu při výkonu veřejné moci;
- zpracování pro účely přímého marketingu;
- zpracování pro účely vědeckého či historického významu nebo pro statistické účely.

Námitky je nezbytné posuzovat vždy individuálně, zda individuální práva a svobody daného subjektu nepřevyšují nad oprávněný zájem správce.

Námitky proti zpracování OÚ pro účely přímého marketingu jsou vždy absolutní a vždy znamenají omezení zpracování OÚ subjektu.

6.3.5.2 Identifikace údajů

Vlastník zpracování osobních údajů musí zajistit identifikaci všech údajů vedených o subjektu a rozhodnout, zda je možno na ně aplikovat právo námitky.

6.3.5.3 Omezení zpracování údajů

Vlastník zpracování musí zajistit omezení zpracování OÚ pomocí jejich blokace.

6.3.5.4 Informování subjektu a příjemců

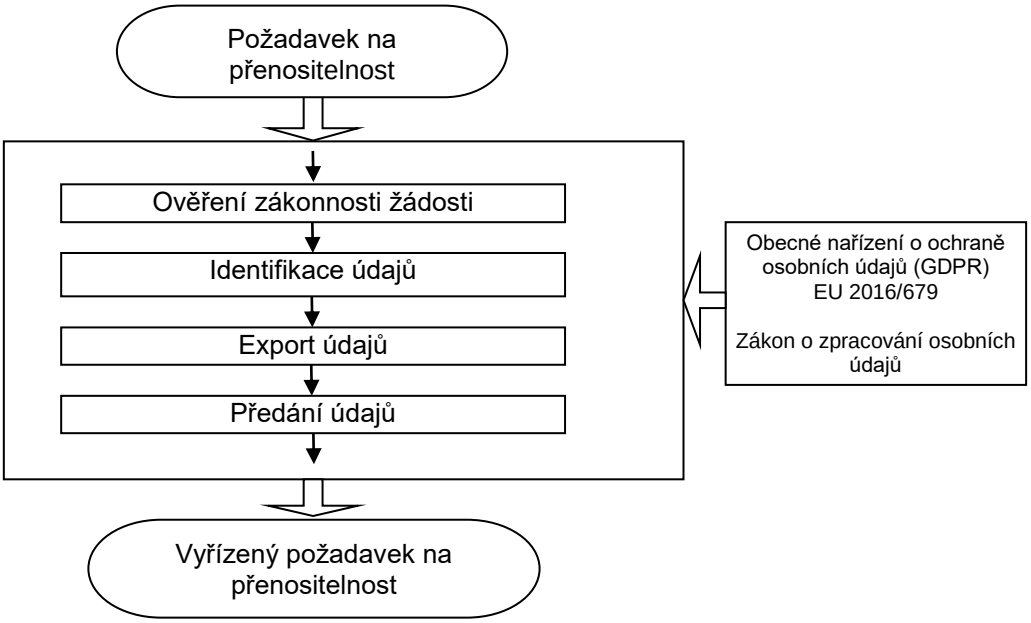
Za sestavení informace o vyřízení požadavku zodpovídá vlastník zpracování. Informace předává pověřenci pro ochranu osobních údajů.

Informaci o předání požadavků ostatním příjemcům údajů musí vlastník zpracování zaznamenat, včetně vyjmenování všech ostatních příjemců údajů.

6.3.6 Právo na přenositelnost (přenositelnost)

Subjekt má (v souladu s článkem 20 GDPR) právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, strojově čitelném formátu.

Subjekt má také právo, aby správce předal osobní údaje na jeho žádost jinému správci.



6.3.6.1 Ověření zákonnosti žádosti

Každý požadavek na přenositelnost musí být posouzen, zda je legitimní a zda existuje důvod, proč by údaje neměly být subjektu předány.

Právo na přenositelnost údajů lze uplatnit pouze, pokud je prováděno automatizovaně a zároveň je založeno na:

- souhlasu subjektu údajů;
- plnění smlouvy.

Správce může umožnit přenos také jiných údajů ze své vůle.

6.3.6.2 Identifikace údajů

Vlastník zpracování osobních údajů musí zajistit identifikaci všech údajů vedených o subjektu a rozhodnout, zda je možno je poskytnout.

Poskytnout lze jen údaje, které se týkají subjektu a které subjekt údajů poskytl správci.

V rámci identifikace údajů je nezbytná revize omezení týkající se poskytnutých údajů (dopady na jiné subjekty údajů, omezení práv a svobod ostatních, apod.)

6.3.6.3 Export údajů

Vlastník zpracování musí zajistit export údajů ve strukturovaném, strojově čitelném formátu (XLS, CSV, XML).

Exportované osobní údaje musí být zkontrolovány z hlediska úplnosti, a zda neobsahují osobní údaje jiných subjektů.

6.3.6.4 Předání údajů

Exportované údaje musí být předány subjektu údajů nebo jinému správci prostřednictvím zabezpečeného komunikačního kanálu.

Předání údajů zajišťuje Pověřenec pro ochranu osobních údajů.

6.4 Poskytnutí informace a zdokumentování

Pověřenec pro ochranu osobních údajů zajišťuje kontrolu plnění požadavků jednotlivých vlastníků zpracování. Z uzavřených požadavků a jejich řešení sestavuje následné vyrozumění pro subjekt údajů.

Pověřenec pro ochranu osobních údajů má povinnost každou poskytnutou informaci předat subjektu stejnou cestou, kterou získal prvotní požadavek subjektu (pokud subjekt nepožaduje jinak).

Pověřenec pro ochranu osobních údajů musí celé řešení požadavku včetně data a času odeslání odpovědi, formy zaslání odpovědi a předmětu poskytnutých informací a případných přijatých opatření zaznamenat.

7 PROVOZ IT

7.1 Politika řízení přístupů

Přístupy jsou u úřadu zajištěny standardně definovanými přístupovými právy k jednotlivým částem IT.

Přístupová práva jsou přidělována jednotlivým uživatelským účtům nebo jejich skupinám tak, aby bylo uživatelům umožněno používat prostředky IT v souladu s rozsahem jejich pracovních povinností.

Uživatelské účty mají stanoven životní cyklus, který počíná vyplněním údajů o uživateli do IT a nastavením účtu administrátorem IT, konče jeho zablokováním dnem ukončení pracovního poměru u úřadu.

7.2 Zásady pro zřizování a užívání přístupových práv

- za nastavení přístupových práv jsou zodpovědní administrátoři IT;
- uživatelské jméno nesmí mít možnost měnit sám uživatel;
- uživatel nesmí zpřístupnit svůj uživatelský účet jiným uživatelům;
- uživatel nesmí zneužít nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, aby v IT pracoval pod cizí identitou;
- pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programu, chybným nastavením administrátorem nebo chybou technického vybavení), je povinen tento bezpečnostní incident bez zbytečného prodlení hlásit dle postupu Řízení bezpečnostních incidentů.

7.2.1 Hesla a jejich správa

U úřadu jsou pro práci s hesly stanoveny následující zásady a pokyny:

- hesla jsou složena minimálně ze 7 znaků;
- hesla jsou náhodného charakteru;
- je vyžadována pravidelná změna hesla minimálně jednou za rok;
- prvotní generované heslo uživateli přiděluje utajeným způsobem administrátor IT;
- uživatel má povinnost toto heslo udržovat před všemi ostatními osobami v tajnosti a nikomu ho nesdělovat;
- uživatel je oprávněn měnit vlastní heslo kdykoliv je to zapotřebí, ke změně hesla musí znát vždy stávající;
- uživatel IT je povinen provést změnu hesla bezprostředně v případě jeho vyzrazení nebo podezření z vyzrazení a tento bezpečnostní incident neprodleně hlásit dle postupu Řízení bezpečnostních incidentů.

7.3 Používání emailu a Internetu

7.3.1 Email

Pro používání elektronické pošty jsou stanovena následující pravidla a zásady:

- konečná celková velikost jedné odesílané zprávy včetně příloh nesmí přesáhnout 15 *MB*;
- veškerá emailová komunikace musí probíhat výhradně prostřednictvím emailu úřadu;
- je zakázáno rozesílat spam, řetězové dopisy a hoaxy (poplašné zprávy);
- je zakázáno používat e-mail pro šíření a výměnu komerčních informací;
- je zakázáno používat síť pro politickou, náboženskou a rasovou agitaci a k šíření materiálů, které jsou v rozporu s právními předpisy;
- je zakázáno obtěžování ostatních uživatelů hromadnými zprávami a zprávami, které svým charakterem nesouvisí přímo s pracovním zařazením a povinnostmi;
- je zakázáno používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům (elektronické diskusní skupiny, news...);
- je zakázáno zneužívat e-mail k reklamním a jiným účelům, sloužícím k získání osobního prospěchu;
- je zakázáno využívat elektronických prostředků (především elektronické pošty) k obtěžování nebo zastrašování jiných uživatelů (spadá sem i rozesílání řetězových dopisů či dopisů na náhodně vybrané adresy v síti);
- je zakázáno používat e-mail a vůbec prostředky a zařízení IT k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím počítačové sítě;

je zakázáno využívat IT k páchání trestných činů.

7.3.2 Internet

Pro používání Internetu jsou u úřadu stanoveny následující zásady:

- uživatel nesmí prostřednictvím Internetu šířit nelegální SW, popřípadě jej z Internetu vědomě stahovat a používat;
- uživatel nesmí na pracovišti využívat služeb Internetu k soukromým komerčním záležitostem (za účelem zisku);
- uživatel nesmí na IT přes Internet stahovat, instalovat a spouštět jakýkoliv neschválený SW
- uživatel nesmí využívat Internet ke hraní on-line her;
- uživatel nesmí stahovat a sledovat videoklipy, filmy a podobné multimediální soubory včetně sledování streamovaného (on-line vysílaného) zvuku a videa nad rámec svých pracovních povinností; (pokud takto není vyžadováno k výkonu jeho pracovní činnosti);
- uživatel nesmí komunikovat přes Internet s jinými osobami mimo rámec svých pracovních povinností, jedná se zejména o používání chatů a audio a video rozhovorů v reálném čase;
- uživatel nesmí prohlížet stránky a stahovat materiály s nežádoucím obsahem, zejména:
  - erotické, pornografické, sexuální a vulgární;
  - propagující nenávist, politickou, náboženskou a rasovou agitaci;
  - související s poškozováním autorských práv (cracky, warez apod.).

Provoz Internetu může být z bezpečnostních důvodů (napadení sítě atd.) průběžně **monitorován**. Lze tedy v případě potřeby vyhledat důkazy o činnosti uživatelů až na úroveň lokálních PC, na kterém se tato činnost vykonávala. Uživatel je seznámen s tím, že k tomuto monitorování dochází.

Opakované porušování podmínek provozu Internetu může být důvodem k dočasnému odebrání přístupu a zahájení disciplinárního řízení.

7.4 Antivirová ochrana

Na všech stanicích a serverech je nainstalován antivirový program.

Program zabezpečuje nejen ochranu proti virům, ale i proti trojským koňům, červům a dalším druhům škodlivého SW. Program vytváří na každém počítači po spuštění rezidentní štít, který kontroluje všechny používané soubory a kontroluje síťový provoz, čímž brání vniknutí a šíření škodlivých programů do počítače. Program kontroluje soubory na lokálních discích počítače a výměnných médiích, data přijímaná ze sítě a zprávy elektronické pošty včetně jejich příloh.

Veškerá nastavení antivirového programu, řízení aktualizací a automatické spouštění testů je řízeno administrátory IT a uživatelé nesmí tato nastavení měnit.

V rámci antivirové bezpečnosti jsou uživatelé povinní dodržovat následující základní pravidla antivirové prevence:

- neukončovat běh antivirového programu ani žádné jeho části (rezidentní štít)
- nepřerušovat aktualizaci antivirového prostředku a řídit se pokyny antivirového programu, především pokynu pro opětovné spuštění (restart) počítače;
- neukončovat časově spuštěné testování;
- nepoužívat počítač podezřelý z infikování virem do jeho odborného prověření administrátory IT;
- nespouštět SW s nejasným či neznámým původem;
- neotevírat a nespouštět podezřelé soubory s neznámým původem, podezřelé přílohy e-mailů
- kontrolovat na přítomnost virů všechny přijaté soubory a to včetně souborů na výměnných médiích, stažených z internetu nebo připojených k e-mailu před jejich použitím, otevřením nebo zkopírováním do IT.

V rámci prováděných opatření při podezření na aktivity zlomyslného SW mají administrátoři IT právo na:

- odstavení pracovní stanice PC;
- odpojení Internetového připojení;
- vyžadování součinnosti uživatele po nezbytně nutnou dobu;
- omezení nebo přerušení provozu počítačové sítě;

- vypnutí serverů.

7.5 Instalace aplikací

Instalaci jakéhokoliv SW provádí výhradě administrátoři IT, kteří vedou také jeho přesnou evidenci. Ve výjimečných případech mohou po předchozím souhlasu nebo výzvě administrátora IT některé instalace provádět uživatelé. V této souvislosti je administrátory IT periodicky prováděna kontrola nainstalovaného SW (SW audit) na lokálních stanicích PC uživatelů.

Cílem je zajistit užívání počítačových programů výlučně oprávněnými uživateli na základě licenčních smluv a zajistit důsledný soulad užívání počítačových programů s platnými právními předpisy a příslušnými licenčními ujednáními a respektovat zákonná práva nositelů autorských a průmyslových práv k jednotlivým softwarovým produktům.

V případech mobilních výpočetních prostředků (zejména smartphony a komunikátory) nesou za instalaci dalšího SW a případné změny v konfiguraci SW i HW plnou zodpovědnost jejich autorizovaní uživatelé.

7.6 Ukládání, zálohování, archivace a obnova dat

7.6.1 Ukládání dat

Uživatelé musí ukládat veškeré soubory obsahující chráněná data úřadu na servery do jim určených složek a adresářů.

Je zakázáno ukládat soubory s chráněnými daty na lokální disky počítačů, neboť tyto disky nejsou centrálně zálohovány a data na nich uložená nejsou chráněna proti poruše disku.

7.6.2 Zálohování dat

Filozofií zálohovací politiky úřadu je řízená, průběžná a systematická činnost zajišťující jak vlastní zálohování dat, tak i jejich zpětnou obnovu (restore) při obnově systému.

Zálohování je prováděno v souladu se zálohovacím plánem a je zajišťováno administrátory IT.

Zálohována jsou však pouze data uložena na serverech v adresářích přiřazených jednotlivým uživatelům, tzn., že data uživatelů (dokumenty, soubory) ukládána v jimi vytvořených složkách a adresářích na lokálních discích jejich počítačů zálohována nejsou

Za zálohování dat uložených na lokálních discích počítačů uživatelů zodpovídají sami uživatelé!

7.6.3 Obnova dat

V případě potřeby obnovy dat uživatelům ji provede na základě jejich žádosti administrátor IT.

7.7 Manipulace s přenosnými počítačovými médii

Uživatel je povinen veškerá přenosná počítačová média uchovávat takovým způsobem, aby k nim nebyl umožněn fyzický přístup neoprávněných osob. V době jeho nepřítomnosti na pracovišti se média obsahující chráněné informace nesmí nacházet v mechanikách a portech počítačů, ležet volně přístupná na pracovních stolech, monitorech, parapetech, skříních apod.

Média obsahující chráněné informace musí být ukládána vždy do uzamykatelných úschovných objektů.

Všechna média musí být uchovávána a musí být s nimi manipulováno takovým způsobem, aby se zabránilo jejich zničení nebo poškození na nich zaznamenaných dat. Jedná se zejména o mechanické poškození, znečištění prachem a jinými nečistotami a pevnými částicemi, poškození teplem (intenzivní přímý sluneční svit, zdroje tepla v kancelářích), poškození elektromagnetickým polem apod.

7.8 Prostředky a zařízení pro zpracování informací

V rámci celého úřadu, bez ohledu na dislokaci pracovišť, jsou uplatňována následující opatření, principy a zásady používání prostředků pro zpracování informací.

7.8.1 Notebooky

- notebooky smí používat pouze ten uživatel, který je seznámen se způsobem jeho obsluhy a při používání se těmito pokyny musí řídit;
- notebooky mohou být uživateli v pracovní době používány výhradně k činnosti přímo spojené s plněním pracovních úkolů nebo v jejich souvislosti;
- instalace a používání jakéhokoliv jiného SW, než byl instalován při předání zařízení uživateli, je v plné odpovědnosti, včetně případných následků, na jeho uživateli;
- uživatel je povinen:
  - dodržovat předepsané pokyny údržby notebooku;
  - účinně chránit notebook před neautorizovaným přístupem a před jeho zcizením;
  - při používání notebooku dodržovat „pravidlo omezené komunikace“ a zejména dbát na to, aby nemohlo dojít k neoprávněnému nakládání s chráněnými informacemi zpracovávanými a uloženými v tomto zřízení;
  - mít v notebooku uloženy pouze ty nezbytné chráněné informace, které potřebuje pro plnění aktuálních pracovních úkolů a nevytvářet zde „archivy“ starších dat;
  - při jakékoliv závadě nebo poruše HW a SW notebooku tento stav bez prodlení oznámit svému přímému nadřízenému a administrátorovi IT a řídit se jimi vydanými pokyny, uživatel má zakázáno závadu sám odstraňovat;
- **uživateli je zakázáno**:
  - nechávat bez dozoru přenosná zařízení (NB, PDA, projektory, apod.) v zaparkovaném automobilu, v hotelu, ubytovně, na nezabezpečeném pracovišti, ve společenských, zdravotních, servisních, zákaznických apod. prostorech;
  - přenechávat notebook k používání neautorizovaným a cizím osobám včetně rodinných příslušníků;
  - servisování a upgrade notebooku provádět jiným způsobem než cestou administrátorů IT;

7.8.2 Mobilní telefony

Pro provoz firemních i soukromých mobilních telefonů jsou pro pracovníky stanoveny následující bezpečností pokyny:

- pracovníci jsou povinni při uskutečňování telefonních hovorů dodržovat „pravidlo omezené komunikace“ a dbát na to, aby touto cestou nikomu nesdělovali chráněné informace, údaje o provozu a činnosti úřadu, prováděné činnosti apod.; tento zákaz se nevztahuje na tísňové hovory;
- pracovníci jsou povinni tam, kde to plnění úkolů zvláštních zakázek vyžaduje, mít po dobu jejich provádění mobilní telefony vypnuty, a v místech, kde je používání mobilních telefonů režimově řízeno, jsou povinni je před vstupem do objektů odevzdat;
- pracovníci berou na vědomí, že charakter provozu mobilních telefonů umožňuje jejich relativně přesnou lokalizaci a že v podstatě všechny uskutečněné hovory a přenosy informací mohou být dlouhodobě a efektivně monitorovány;
- pracovníci nesmějí v mobilních telefonech uchovávat přístupová hesla a další chráněné informace, aby při ztrátě nebo odcizení mobilního telefonu mohla být přístupná neautorizovaným osobám.

7.8.3 Telefony - pevná linka

Pro provoz firemních telefonů připojených na pevnou linku (dále jen „telefony“) jsou u úřadu stanoveny následující pokyny a bezpečnostní zásady:

- pracovníci používající telefonní přístroje musí být seznámení administrátory IT se způsobem jejich obsluhy a při používání telefonů se těmito pokyny musí řídit;
- pracovníci používají telefony výhradně k hovorům v souvislosti s výkonem pracovní činnosti a v rozsahu nezbytném k zajištění úkolů;
- pracovníci mohou v odůvodněných případech a v přiměřeném rozsahu využít pevnou telefonní linku a k soukromým účelům;

- přestože by telefonní hovory měly být věcné, stručné a srozumitelné, musí při nich pracovníci zachovávat zásady společenského chování, být korektní a mít na paměti, že i jimi uskutečňované hovory jsou součástí kultury úřadu a mají vliv na její image;
- pracovníci berou na vědomí, že jejich hovory mohou být ze strany administrátorů IT kontrolními záznamy monitorovány co se doby trvání hovoru a identifikace čísla volaného nebo volajícího týká;
- pracovníci jsou při uskutečňování telefonních hovorů povinni dodržovat „pravidlo omezené komunikace“ a dbát na to, aby touto cestou nikomu nesdělovali chráněné informace; tento zákaz se nevztahuje na tísňové hovory;
- pracovníci mají kromě běžné obsluhy zakázáno zasahovat do přístrojů, souvisejících zařízení a telefonních rozvodů;
- pracovníci jsou povinni při jakékoliv závadě nebo poruše telefonu a telefonního spojení tento stav bez prodlení oznámit administrátorům IT či správcům PC a nesmějí poruchu nebo závadu sami odstraňovat.

7.9 Monitorování přístupu a používání IT

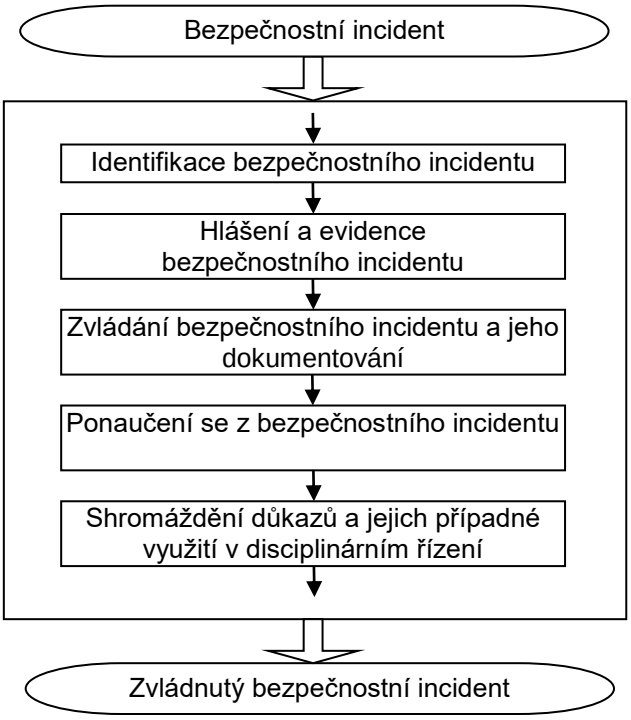
Cílem monitorování je odhalit neoprávněné činnosti a zajištění případných důkazů pro případ bezpečnostního incidentu.

Sledování přístupů (informací o všech operacích s IT, autorizovaných i neautorizovaných přístupech, pokusech o překonání bezpečnostních konfigurací, změnách v nastavení, modifikacích dat, podezřelých činnostech, pokusech o prolomení hesel apod.) může být analyzováno a výsledky mohou být v rámci prováděného přezkoumání předkládány jednateli.

Pravidelně jsou monitorovány také vzdálené přístupy do počítačové sítě.

8 ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

8.1 Procesní schéma



Vlastníkem procesu je pověřenec pro ochranu osobních údajů.

8.2 Všeobecně

Základním principem řízení bezpečnostních událostí a bezpečnostních incidentů (dále také jen „událostí“ a „incidentů“) je nastavení mechanismu jejich bezprostřední detekce, způsobu jejich nahlášení, zdokumentování, eliminace nebo odstranění a vyšetření (přezkoumání) s ohledem na příčiny, které je vyvolaly, aby mohlo být dosaženo efektivní nápravy (opatření k nápravě, preventivních opatření a ponaučení (přímý odraz v budování bezpečnostního povědomí a zvyšování informovanosti).

Obecným cílem řízení bezpečnostních událostí a incidentů je minimalizovat škody způsobené bezpečnostními incidenty a selháními, sledovat je a učit se z nich.

8.2.1 Bezpečnostní události a bezpečnostní incidenty

Za bezpečnostní událost a bezpečnostní incident je považována jakékoliv nechtěná událost, která vede nebo by mohla vést k narušení bezpečnosti IT nebo jeho části, včetně stanovených bezpečnostních pravidel a opatření, což vede nebo by mohlo vést ke škodě jak materiální tak i abstraktní, kompromitaci činností úřadu a ohrožení bezpečnosti informací.

8.3 Identifikace bezpečnostního incidentu

Bezpečnostní události a incidenty mohou být kdykoliv zjištěny**:**

- pracovníkem úřadu;
- zákazníkem;
- třetí stranou;
- inspekčním (kontrolním) orgánem.

8.4 Hlášení bezpečnostního incidentu

Každý, kdo zjistí bezpečnostní událost nebo incident, nebo se domnívá, že bezpečnostní událost či incident existuje, zejména pak pracovník - uživatel IT, je povinen ihned tuto skutečnost (vzniklou situaci) předepsaným způsobem hlásit. Povinnost hlášení se vztahuje i na vznik bezprostřední hrozby vzniku bezpečnostní události nebo incidentu.

Oznámení (hlášení) o zjištění bezpečnostní události nebo incidentu nebo hrozbě jejich vzniku se provádí bezprostředním informováním pověřence pro ochranu osobních údajů.

Zároveň tuto informaci předává pracovník i svému přímému nadřízenému.

V případě spolupracujících osob, např. třetí strany, je tato informace předána pracovníkovi pověřenému realizovat příslušný smluvní vztah nebo spolupráci.

Za seznámení třetích stran se způsobem hlášení bezpečnostních incidentů je zodpovědný ten vedoucí pracovník, jež smluvní vztah oficiálně uzavřel nebo uzavírá.

Pověřenec pro ochranu osobních údajů má povinnost každý nahlášený bezpečnostní incident ihned zaznamenat do příslušné evidence.

Pracovníkům je zakázáno podávat jakékoliv informace o zjištěných slabinách a nedostatcích, bezpečnostních událostech nebo bezpečnostních incidentech, včetně přijatých opatřeních komukoliv mimo prostředí úřadu.

8.4.1 Okamžitá reakce

Uživatelé informačních služeb nesmí za žádných okolností podezřelé slabiny prověřovat a to z důvodu své vlastní ochrany před disciplinárním řízením, protože testování bezpečnostních slabin je interpretováno jako potenciální zneužití systému.

Obecný postup každého uživatele IT při identifikaci bezpečnostního incidentu:

- zaznamenat příznaky problému a jakékoliv zprávy objevující se na monitoru PC (jiného prostředku nebo zařízení pro zpracování informací);
- přestat používat PC (jiný prostředek nebo zařízení pro zpracování informací), a pokud je to možné, izolovat je od dalšího provozu, popř. ukončit pracovní činnost na jiném zařízení;
- ohlásit stanoveným způsobem bezpečnostní incident;
- zamezit přístup osob neautorizovaných k řešení incidentu k prostředkům a zařízení;
- vyjmout z PC veškerá výměnná média, vhodným způsobem je označit a předat administrátorovi, popř. evakuovat;
- nepřenášet diskety ani jiné nosiče informací používané před a po zaznamenání selhání programového vybavení, do jiných PC;
- neprovádět žádné pokusy o odstranění podezřelého programového vybavení ani žádné jiné opravy prostředků a zařízení IT;
- informovat o události svého přímého nadřízeného;
- postupovat dle pokynů pověřence pro ochranu osobních údajů nebo a svého přímého nadřízeného.

8.5 Zvládání bezpečnostních incidentů

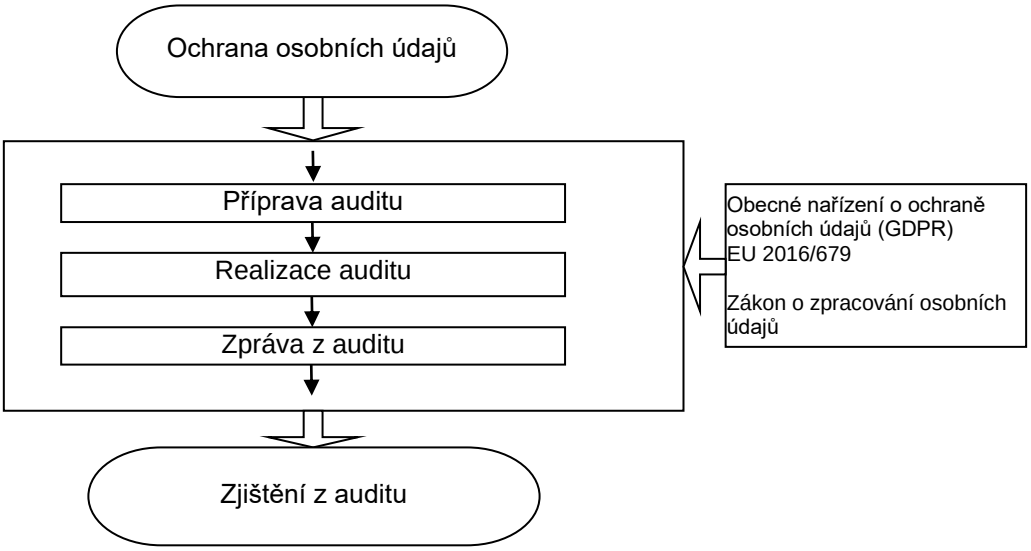
Zodpovědnost za zvládnutí bezpečnostního incidentu má pověřenec pro ochranu osobních údajů, popř. jiné osoby, jež byly pověřeny nadřízeným k jeho vypořádání.

Pověřenec pro ochranu osobních údajů rozhodne, zda je nutné bezpečnostní incident hlásit jako ohrožení zpracování osobních údajů a zajistí případné hlášení na ÚOOÚ.

9 AUDIT OCHRANY OSOBNÍCH ÚDAJŮ

Cílem procesu Audit ochrany osobních údajů je zajištění provádění interních auditů za účelem průběžného zjišťování funkčnosti a efektivity systému ochrany osobních údajů.

Postup stanovuje zásady pro plánování, přípravu, realizaci a vyhodnocení auditů ochrany osobních údajů.



Vlastníkem procesu je pověřenec pro ochranu osobních údajů.

9.1 Všeobecně

Proces auditu ochrany osobních údajů je u úřadu nástrojem pro nezávislé posuzování procesu ochrany osobních údajů nebo činnosti úřadu související se zpracováním osobních údajů. Proces auditu ochrany osobních údajů poskytuje nezávislý nástroj pro získávání důkazů o tom, že jsou splněny existující požadavky. Audity jsou prováděny kompetentními auditory, kteří nemají přímou odpovědnost za auditovaný proces.

Interní audit není chápán jako ověřování konkrétních činností, ale jako ověření, zda činnosti, které jsou součástí ochrany osobních údajů, jsou prováděny ve shodě s definovanými požadavky a zda jsou prováděny účinně a efektivně. V případě zjištění nedostatků jsou prováděny kroky na jejich odstranění. Neustálé opakování těchto činností je základem pro kontinuální zlepšování.

9.2 Příprava auditu

V rámci přípravy auditu zpracuje stanovený vedoucí auditor plán auditu.

Plán auditu obsahuje:

- předmět auditu:
- specifikaci týmu auditorů;
- specifikaci osob auditovaného útvaru;
- cíl auditu.

Vedoucí auditor kontaktuje minimálně 2 týdny před plánovaným auditem odpovědnou osobu auditovaného útvaru a sdělí mu základní informace o průběhu plánovaného auditu.

Po dokončení plánu auditu vedoucí auditor informuje o plánu členy týmu auditorů.

9.3 Realizace auditu

Vedoucí auditor postupuje dle stanoveného plánu auditu tak, aby zajistil dostatečné množství informací a důkazů pro následné stanovení zjištění z auditu. Podrobný postup při auditu závisí na celé řadě faktorů, zejména na cíli auditu, kritériích auditu, sledu činností v auditovaném procesu, na zvyklostech v auditovaném útvaru apod.

Jako základní zdroje informací z auditu slouží interní dokumentace ochrany osobních údajů, především vyplněné plány a záznamy, dále zprávy z předchozích auditů, záznamy o zjištěných incidentech a požadavcích subjektů, záznamy o kontrole apod.

Součástí každého auditu je hodnocení plnění opatření z předchozích auditů.

Pro zajištění potřebných informací o dané činnosti je třeba kontaktovat pracovníka, který tuto činnost vykonává. Množství, kvalitu a rychlost získání informací při rozhovorech auditora s pracovníky zásadním způsobem ovlivňuje formulace a způsob kladení otázek. Při vlastním kladení otázek auditor formuluje otázky tak, aby dostal odpovědi na:

JAK, CO, PROČ, KDY, KDE, KDO, CO KDYŽ

a odpovědi následně doplní požadavkem **UKAŽ**!

Shromážděné informace by měl auditor ověřit a jejich platnost doložit objektivními důkazy, které musí získat z jiných nezávislých zdrojů (tj. rozhovory s jinými pracovníky, fyzické zjišťování, měření, výsledky testů, ostatní záznamy apod.). Pokud se objeví v odpovědích rozpor, je třeba dalšího prověření a získání objektivních důkazů. Součástí auditu je také prosté pozorování činností jednotlivých pracovníků a srovnání prováděných činností s dokumentací ochrany osobních údajů.

Vedoucí auditor zaznamenává zjištěné důkazy.

9.4 Zpráva z auditu

Po provedení auditu musí vedoucí auditor zpracovat zprávu z auditu.

Zpráva z auditu musí být jasná, stručná a musí důkazy úplně dokumentovat a musí vyhodnotit a porovnat zjištění vzhledem ke kritériím auditu.

Součástí zjištění může být specifikace neshod a případně podnětů pro přijetí nápravného opatření, případně dalších doporučení.

Závěrečná zpráva z auditu musí být předložena auditovaným stranám.

PŘÍLOHY

Seznam příloh:

1) Zásady zpracování osobních údajů
2) Zásady používání cookies
3) Souhlas – Použití fotografií pro marketingové účely
4) Doplněk do pracovních smluv a dohod
5) Dohoda o mlčenlivosti
6) Souhlas - biometrika
7) Dodatek ke smlouvě
8) Zpracovatelská smlouva
9) Vzor výstražné cedule kamerového systému
10) Souhlas – uchování životopisu uchazeče
11) Jmenování – Pověřenec OOÚ