GDPR PROCESY A POVINNOSTI

Kanceláře pro ochranu osobních údajů

Verze: 2.0
Datum: leden 2024
Vlastník: EZ

ŠKOENERGO

OBSAH

1 POVINNOSTI ZAMĚSTNANCŮ

Tento dokument je metodickou příručkou pro činnost Kanceláře pro ochranu osobních údajů a vlastníků procesů, která vyplývá z Nařízením Evropské unie 2016/679 (GDPR) a právních předpisů týkajících se oblasti ochrany osobních údajů. Cílem vyhotovení tohoto dokumentu je popsat povinnosti těchto činitelů, a s tím spojených aktivit a definování procesu řízení dokumentů v souvislosti se zpracováním osobních údajů za účelem naplnění uvedené legislativy.

1.1 Povinnosti kanceláře pro ochranu OÚ

Jedna z hlavních činností kanceláře pro ochranu osobních údajů je:

- **zajištění správného vyřízení přijatého požadavku na výkon práv od subjektu údajů**
- **činnosti související s řízením interní a externí dokumentace**, kterou je kancelář povinna vést a pravidelně aktualizovat

Mimo výše zmíněné činnosti, vyřizuje Kancelář zejména následující agendu:

- provádí **školení a vzdělávání zaměstnanců** v oblasti ochrany osobních údajů
- **poskytuje poradenství** zaměstnancům v oblasti ochrany osobních údajů
- zajišťuje **jednotný přístup** v aplikaci regulatorních požadavků napříč celou společností
- **kontroluje** efektivitu implementovaných **technických a organizačních opatření**
- **stanovuje a řídí metodiku** odborné problematiky a její **rozvoj**
- poskytuje podporu v uzavírání **smluv o zpracování osobních údajů**
- provádí pravidelný **monitoring** a kontrolu **aplikace příslušných zákonů** či jiných **právních předpisů** a dalších strategických dokumentů EU
- **vyhodnocuje rizika**, v této souvislosti vyhodnocuje i upozornění na protiprávní jednání a/nebo porušení interních předpisů v souvislosti s ochranou osobních údajů
- zajišťuje správné vyřízení a řídí komunikaci v případě **bezpečnostního incidentu**
- **komunikuje** s příslušnými **dozorovými úřady** a napomáhá při vyšetřování

Kancelář má povinnost spravovat především tyto dokumenty a implementovat změny, o kterých ji informují vlastníci procesů:

Záznamy o činnostech zpracování	Aktuální přehled všech činností v rámci ŠKO-ENERGO, při nichž dochází ke zpracování osobních údajů, společně se specifikací jednotlivých účelů zpracování, jakož i doplňující informace potřebné pro plnění povinností ŠKO-ENERGO jako správce osobních údajů.
DPIA (tzv. Data Protection Impact Assessment)	Nástroj sloužící k vyhodnocení rizikovosti jednotlivých procesů a okruhů, a zároveň pro sledování stavu nálezů, které tuto rizikovost ovlivňují.
Informační memorandum	Zajišťuje informační povinnost správce vůči subjektu údajů, který poskytuje své osobní údaje ke zpracování. Správce je povinen SÚ informovat před započetím zpracování, nebo při prvním kontaktu se SÚ, o rozsahu zpracovávaných osobních údajů, účelu zpracování, době uchování zpracovaných osobních údajů, případných dalších osobách, kterým budou osobní údaje předány, o právech, která náleží SÚ a dalších náležitostech zpracování.

1.2 Povinnosti zaměstnanců

Mezi povinnosti zaměstnanců patří především zajištění **spolupráce** u následujících činností:

- **Vyřizování požadavků subjektů údajů**
    - vyžaduje především spolupráci s kanceláří pro ochranu osobních údajů, která určuje způsob odbavení požadavku a zajišťuje komunikaci se žadatelem o uplatnění práv subjektů údajů.
- **Zajištění ochrany osobních údajů a hlášení bezpečnostních incidentů**
- **Ohlašování změny týkající se zpracování osobních údajů**
- **Správa záznamů o činnostech zpracování**
- **Provádění DPIA posouzení**
- **Interní audit jim svěřeného oddělení či procesu**
- **Posuzování nových projektů či činností**

Jednou z nejzásadnějších povinností zaměstnanců je **zabezpečení osobních údajů**. Jedná se o doposud nejčastěji a téměř nejpřísněji sankcionovanou povinnost ze strany ÚOOÚ.

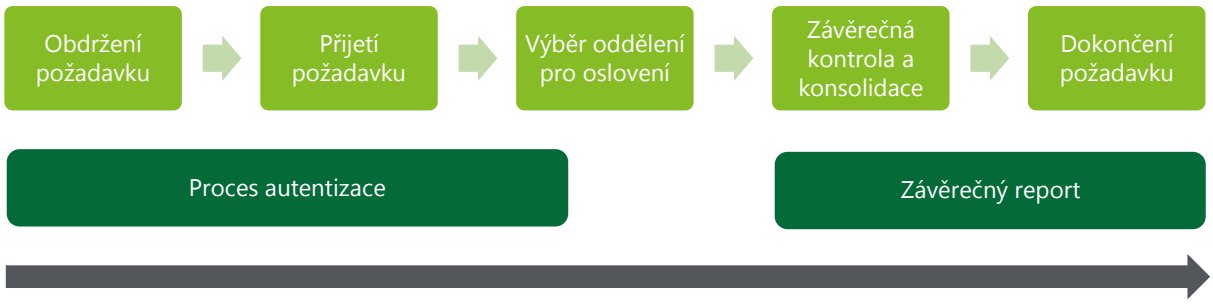
Zaměstnanec je povinen účastnit se pravidelných školení, zná interní směrnice či dokumenty týkající se ochrany osobních údajů, odpovídá za plnění všech výše uvedených povinností vyplývajících z GDPR a za dodržení zásad zpracování, přičemž jejich dodržení musí být schopen doložit relevantními interními dokumenty či jinými postupy, z nichž bude tato skutečnost jasně vyplývat.

2 PRÁCE S POŽADAVKY SUBJEKTŮ ÚDAJŮ DLE GDPR

Následující kapitola zaměřující se na proces práce s požadavky obsahuje podkapitoly s podrobným popisem kroků a procesů k vyřízení jednotlivých požadavků SÚ, a to:

- Specifikace kanálů pro příjem požadavku
- Formální náležitostí požadavku
- Výběr oddělení pro oslovení
- Dokončení požadavku

Postup práce s požadavky subjektů údajů dle GDPR (Fáze I.):



30denní lhůta

2.1 Specifikace kanálů pro příjem požadavků

Kancelář pro ochranu osobních údajů může obdržet požadavek na uplatnění práv GDPR skrze následující kanály:

- Telefonicky
- Poštou
- E-mailem
- Osobně
- Datovou schránkou
- Prostřednictvím zaměstnance ŠKO-ENERGO

Kancelář pro ochranu osobních údajů dále musí zajistit zaevidování všech požadavků přijatých těmito kanály a jejich následné zpracování.

Autentizace požadavku probíhá na základě porovnání e-mailu SÚ s evidovaným e-mailem nalezeným v interní databázi společnosti.

2.2 Formální náležitosti požadavku

Před přijetím požadavku kancelář pro ochranu osobních údajů musí posoudit, jestli je požadavek v souladu s nařízením GDPR.

Pracovník kanceláře pro ochranu osobních údajů projde požadavek a posoudí ho z hlediska kompletnosti a relevance. Kompletnost a relevance je v pořádku, pokud žádost splňuje následující 4 podmínky:

1. **Souvztažnost k problematice**
    - Souvisí požadavek s ochranou osobních údajů?
    - Pokud není relevantní, je potřeba žádost přeposlat na jiné adresní oddělení, které se předmětu žádosti týká.
2. **Jednoznačná kategorizace**
    - Obsahuje žádost dostatek informací k její jasné kategorizaci, tzn. lze jasně identifikovat, o jaký požadavek se jedná?
3. **Dostatek povinných údajů**
    - Jsou uvedeny všechny relevantní údaje o SÚ pro jeho jasnou identifikaci?
4. **Kontext žádosti**
    - Je zřejmé, o co přesně SÚ žádá, co si přeje a ideálně z jakého důvodu?

Po splnění všech čtyřech podmínek je požadavek předán k dalšímu vyřizování.

SÚ musí vždy poskytnout **minimálně tři povinné údaje**:

- Jméno
- Příjmení
- E-mailová adresa

a ideálně telefonní číslo z důvodu následné komunikace. **Čím více informací o sobě SÚ poskytne, tím efektivněji lze žádost vyřídit.**

2.2.1 Kategorizace žádostí

Kancelář pro ochranu osobních údajů může kategorizovat přijaté žádosti následujícím způsobem:

Výkon uplatněného práva + podkategorie

Žádost o **přístup k osobním údajům**

SÚ má zájem o informaci, zda a jaké osobní údaje o něm společnost ŠKO-ENERGO eviduje a za jakými účely jsou zpracovávány.

Žádost o **opravu osobních údajů**

SÚ má zájem o opravu osobních údajů, které o něm společnost ŠKO-ENERGO eviduje z důvodu nepřesnosti.

Např. může jít o změnu příjmení SÚ, či o změnu e-mailové adresy apod.

Žádost o **výmaz osobních dat**

SÚ má zájem o výmaz osobních údajů, které o něm společnost ŠKO-ENERGO eviduje, přičemž toto právo lze vykonat pouze za určitých podmínek.

Žádost o **omezení zpracování osobních údajů**

SÚ má právo na omezení zpracování osobních údajů, kdy je správce osobních údajů povinen zpracování omezit minimálně do doby vyřešení podnětu SÚ.

Např. OÚ jsou nepřesné, OÚ jsou zpracovány protiprávně a SÚ odmítá jejich výmaz apod.

Žádost o **přenos osobních údajů**

SÚ má zájem o získání osobních údajů a jejich předání jinému správci osobních údajů, než je společnost ŠKO-ENERGO.

Žádost o **odvolání souhlasu se zpracováním osobních údajů**

SÚ má zájem o odvolání dříve uděleného souhlasu se zpracováním osobních údajů.

Např. Odvolání marketingového souhlasu

Námitka proti zpracování osobních údajů

V případě námitky proti zpracování lze ukončit některá zpracování podmíněná oprávněným zájmem. SÚ může podat námitku i pokud je zpracování prováděno v rámci veřejného zájmu.

Např. SÚ vyjadřuje nesouhlas se způsobem, jakým je nakládáno s jeho osobními údaji.

Stížnost

SÚ vyjadřuje znepokojení či nesouhlas se způsobem, jakým je nakládáno s jeho osobními údaji.

Bezpečnostní incident

SÚ má podezření či obavy, že došlo k narušení bezpečnosti jeho osobních údajů.

Na požadavek subjektu údajů je nutné odpovědět nejpozději do 30 dnů ode dne přijetí této žádosti, a to i v případě neúspěšného přijetí žádosti.

2.2.2 Neúspěšné přijetí požadavku

K zamítnutí požadavku dochází v následujících případech:

- **Požadavek nesouvisející s ochranou osobních údajů**
  - kancelář pro ochranu osobních údajů předává požadavek na relevantní oddělení.
- **Nejednoznačná kategorizace žádosti**
  - kancelář pro ochranu osobních údajů může vyžadovat uvedení doplňujících informací k jeho jasné kategorizaci. V případě, že SÚ svou žádost neupřesní do 14 dnů, kancelář může tuto žádost zamítnout.
- **Nedostatek povinných údajů**
  - Pokud SÚ opomene jeden ze tří povinných údajů, může kancelář pro ochranu osobních údajů vyžadovat jejich doplnění. V případě, že SÚ neposkytne požadované údaje do 14 dnů, kancelář může tuto žádost zamítnout.
- **Nejednoznačný či nesmyslný předmět žádosti**
  - Požadavek může být v rámci procesu zamítnut nebo může být požadováno jeho objasnění.

2.3 Výběr oddělení pro oslovení

Oslovením oddělení se myslí oslovení jednotlivých vedoucích oddělení neboli vlastníků procesů, resp. jejich zástupců, kteří mohou osobní údaje daného subjektu údajů zpracovávat. Toto oddělení je vybráno na základě vyhodnocení obsahu žádosti subjektu údajů kanceláří pro ochranu osobních údajů.

Požadavek SÚ zašle kancelář ve formě dotazu na následující oddělení společnosti ŠKO-ENERGO:

- **Technická oblast (T)**
  - Teplárna (TT)
  - Služby a ostatní energie (TE)
  - Plánování a projektový management (TP)
- **Ekonomicko-obchodní oblast (E)**
  - Finance a energetické hospodářství (EE)
  - Nákup a skladové hospodářství (EN)
  - Personalistika, organizace a správa (EZ)

V rámci investigace jsou vlastníci povinni zkontrolovat požadavek a zjistit, zdali se v jejich evidenci (elektronické či papírové) vyskytuje záznam o daném SÚ a zdali dochází ke zpracování jejich osobních údajů. **Tento výskyt vlastníci procesu ověří pomocí shody jména, příjmení, emailu, telefonního čísla** či dalšího uvedeného osobního údaje.

❌ Pokud vlastník procesu v evidenci SÚ **nenalezne**, odesílá kanceláři negativní odpověď.

✔ Pokud vlastník procesu v evidenci SÚ **nalezne**, musí kancelář o nálezu informovat, společně s uvedením všech účelů zpracování a výčtem osobních údajů, které jsou u SÚ evidovány.

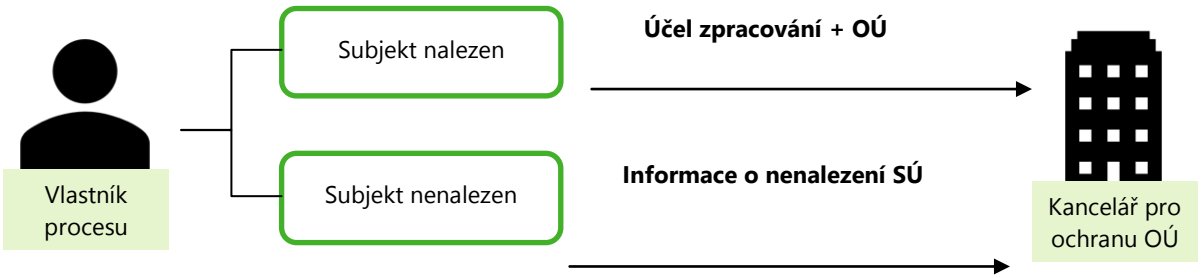
2.4 Dokončení požadavku

V následující podkapitole je definován postup pro kompletní dokončení požadavku, který navazuje na přijetí všech informací od vlastníků procesů, resp. jejich zástupců, kteří byli osloveni v rámci vyřízení požadavku.

Celkový proces vyřízení požadavku se dělí na dvě fáze, přičemž žádosti, které **nevyžadují autorizaci** (neboli potvrzení) **výkonu práva** ze strany SÚ a následnou realizaci výkonu práva v odděleních jsou dokončeny v rámci první fáze procesu.

2.4.1 Závěrečná kontrola a konsolidace

V rámci závěrečné kontroly kancelář pro ochranu osobních údajů ověřuje, jestli došlo ze stran vlastníků procesů k řádnému vyřízení všech rozeslaných požadavků.



Konsolidací odpovědí je myšleno zkompletování všech informací získaných z oslovení oddělení a pokračování v přípravě reportu pro SÚ.

Pokud některé informace v rámci vyřízení požadavku chybí, **musí kancelář kontaktovat odpovědného vlastníka procesu s výzvou o doplnění informace**.

2.4.2 Dokončení požadavku v rámci 1.fáze

Pracovník kanceláře pro ochranu osobních údajů připraví na základě shrnutí agregovaných údajů získaných od vlastníků procesů **report** neboli odpověď na žádosti SÚ.

Na základě těchto získaných odpovědí se může jednat o následující typy reportů:

- **Negativní report** – Připravuje kancelář v případě, pokud se nepodařilo na základě poskytnutých údajů v přijaté žádosti nalézt SÚ v žádném z oslovených oddělení
- **Pozitivní report** – Připravuje kancelář v případě, pokud se podařilo dohledat SÚ aspoň v jednom z oslovených oddělení. V reportu uvede výpis posbíraných účelů, na základě, kterých dochází ke zpracování osobních údajů žadatele

Požadavky, které vyžadují výkon práv neboli provedení požadované změny v relevantním oddělení, **postupují do druhé fáze.**

2.4.3 Dokončení požadavku v rámci 2.fáze

Mezi procesy, které spadají do druhé fáze, patří **autorizace požadavku SÚ, výkon práv, příprava a odeslání reportu spolu s potvrzením výkonu práva.**

Níže definovaný postup vyřízení požadavků se váže pouze na následující typy žádostí:

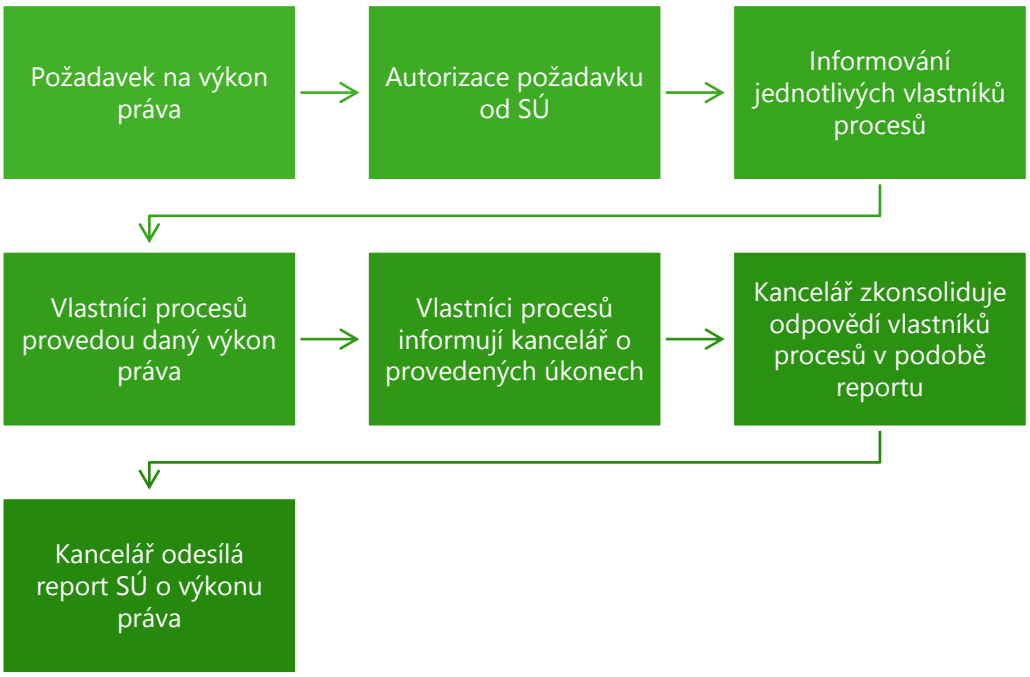
- **Žádost o opravu** osobních údajů
- **Žádost o výmaz** osobních dat
- **Žádost o omezení zpracování** osobních údajů
- **Žádost o odvolání souhlasu** se zpracováním osobních údajů

Námitka proti zpracování osobních údajů patří mezi specifické žádosti, jejichž vyřízení se odvíjí od podstaty a kontextu samotné žádosti. Pracovník kanceláře pro ochranu osobních údajů dle detailů žádosti stanoví, o jaký typ uplatněného práva se jedná a jak bude v případě námitky dále postupováno.

- **Námitka proti zpracování** osobních údajů

Aby mohla následovat druhá fáze procesu vyřízení požadavku, pracovník kanceláře pro ochranu osobních údajů musí na základě získaného výstupu z první fáze jasně definovat platné účely zpracování osobních údajů, u kterých lze dle právního titulu požadované právo vykonat.

Postup výkonu práv v rámci 2.fáze



3 HLÁŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Povinností vlastníků procesů a zároveň všech zaměstnanců je nahlašování bezpečnostních incidentů (porušení zabezpečení osobních údajů dle čl. 32 GDPR).

Bezpečnostní incident představuje **jakýkoliv incident, který vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí či zpřístupnění** přenášených, uložených nebo jinak zpracovávaných **osobních údajů** (narušení důvěrnosti, dostupnosti a integrity osobních údajů).

3.1 Bezpečnostní incident

V níže uvedené tabulce jsou bezpečnostní incidenty rozděleny do pěti základních kategorií. V praxi však bezpečnostní incident, v závislosti na okolnostech, může spadat do několika nebo i všech kategorií.

Druh bezpečnostního incidentu	Kategorie	Charakteristika	Příklad
Náhodné nebo neoprávněné poskytnutí osobních údajů	Narušení důvěrnosti	Osobní údaje byly poskytnuty, nebo zpřístupněny subjektům, které nemají oprávnění osobní údaje získat, nebo mít k nim přístup.	**Dodavatel neoprávněně poskytne osobní údaje o klientech společnosti jiné společnosti za úplatu.**
Náhodné nebo neoprávněné zpřístupnění osobních údajů	Narušení důvěrnosti		**Zaměstnanec zapomene dokumenty obsahující osobní údaje v autobusu, kde se k nim dostane neoprávněná osoba.**
Náhodná nebo neoprávněná ztráta přístupu k osobním údajům	Narušení dostupnosti	Osobní údaje mohou stále existovat, avšak společnost nad nimi ztratila kontrolu, nebo přístup k nim, či je už nemá v držení.	**Ztráta přístupu způsobená výpadkem elektřiny nebo znemožnění uživatelského přístupu, díky tomu, že zaměstnanec spustil zavirovanou přílohu emailu, prostřednictvím webového prohlížeče nebo návštěvou webu, který je infikován malwarem.**
Náhodné nebo neoprávněné zničení osobních údajů	Narušení dostupnosti	Osobní údaje již neexistují vůbec, nebo přinejmenším ne v podobě, aby byly společnosti k užitku.	**Odcházející zaměstnanec z pomsty smaže soubory obsahující osobní údaje, které nelze obnovit ani ze zálohy.**
Náhodné nebo neoprávněné pozměnění osobních údajů	Narušení integrity	Osobní údaje byly pozměněny, nebo už nejsou úplné.	**Záměrná změna čísla bankovního účtu zaměstnance, za účelem získání finančního obnosu z osobního účtu.**

Za bezpečnostní incident **nelze** považovat zejména situace:

- Napadená zařízení/systémy, které **neobsahovaly žádné informace/data**.
- Dokument/systém **obsahoval informace/data, ale nejednalo se o osobní údaje** (např. údaje týkajících se pouze technických specifik).
- Nedostupnost (např. výpadek proudu) systému, který nemůže mít žádný dopad na subjekt údajů (např. nemožnost rozeslání newsletteru zákazníkům).

3.2 Přístup založený na hodnocení rizik

Přístup založený na hodnocení rizik je důležitý primárně v situacích připravovaného zpracování osobních údajů, kdy musí být vzata v úvahu všechna rizika pro práva a svobody fyzických osob, což by se mělo následně promítnout v úrovni technických a organizačních opatření.

V rámci bezpečnostního incidentu existuje ohlašovací povinnost v případech, **kdy je pravděpodobné**, že bezpečnostní incident má za následek riziko pro práva a svobody fyzických osob. Proto **je důležité stanovit závažnost bezpečnostního incidentu ve vztahu k ohrožení subjektu údajů.**

Bezpečnostní incident může mít celou řadu nežádoucích dopadů na SÚ, což může vyústit např. v tělesnou újmu, materiální, nebo nemateriální škodu, zejména:

- ztráta kontroly nad vlastními osobními údaji,
- krádež identity,
- podvod,
- společenské znevýhodnění,
- diskriminace,
- hospodářské znevýhodnění,
- omezení práv,
- poškození pověsti,
- finanční ztráta.

Určení úrovně dopadu je důležité z pohledu ohlašovací povinnosti. Tedy jestli existuje ohlašovací povinnost vůči SÚ a jak rychle a jakým způsobem jim má být ohlášení bezpečnostního incidentu komunikováno.

3.3 Plán reakce na bezpečnostní incident

Řízení bezpečnostních incidentů je proces, který se skládá z celkem 9 na sebe plynule navazujících kroků.

Níže je popsán detailní přehled jednotlivých kroků tak, aby došlo k včasnému odhalení, posouzení, ohlašování a přijetí nápravných opatření za účelem neustálého zdokonalování.

Krok 1. Zjištění a předání podnětu o podezření

Každý zaměstnanec a dodavatel je povinen oznámit podezření na bezpečnostní incident dispečinku, nebo kanceláři pro ochranu osobních údajů **bez zbytečného odkladu**, nejpozději do 24 hodin, od chvíle, kdy se **dozvěděl o možném narušení bezpečnosti osobních údajů** (identifikoval jak vlastní činností, tak získal podnět od třetích stran).

Za účelem přijímání podnětů o výskytu bezpečnostního incidentu jsou užívány níže uvedené komunikační kanály dispečinku společnosti ŠKO-ENERGO oblasti TE, který je k dispozici v režimu 24/7:

- Telefonní číslo: +420 326 8 17550
- Mobil: +420 734 264 505

Krok 2. Prvotní posouzení a neodkladná opatření

Je potřeba ověřit, zda došlo ke skutečnému bezpečnostnímu incidentu či nikoliv. Zodpovědná osoba v rámci prvotního posouzení:

a. Získá dostatek informací:
   - jakou kategorii bezpečnostního incidentu se jedná,
   - přibližný počet subjektů údajů, na které může bezpečnostní incident dopadnout,
   - kategorie osobních údajů,
   - počet a druh záznamů,
   - datum a čas zjištění,
   - jaká opatření již byla přijata

b. Zhodnotí potřebu a případně iniciuje neodkladná opatření zaměřená na odstranění, zastavení, nebo minimalizaci následků identifikovaného podezření na bezpečnostní incident (např. zajištění sběru dokumentů nalezených na veřejném místě, obnovení výpadku systému, odebrání přístupových oprávnění).

c. **Jedná-li se o bezpečnostní incident**, postupuje dále Krokem 3.

d. **Nejedná-li se o bezpečnostní incident**, zhodnotí potřebu iniciovat příslušná nápravná opatření.

Krok 3. Hodnocení pravděpodobnosti rizika pro práva a svobody

Zodpovědná osoba posoudí, jaká je pravděpodobnost, že bezpečnostní incident má za následek riziko pro práva a svobody subjektu údajů.

Pravděpodobnost rizika	Příklad
Nepravděpodobné	Zapomenutí pracovní aktovky v restauraci, ve které jsou pouze dokumenty, které neobsahují jakékoli osobní údaje.
Pravděpodobné	Několikahodinový výpadek proudu a nedostupnost systému, kdy se klienti nemohou dostat k osobním údajům, které jsou zde uloženy.
Vysoce pravděpodobné	Společnost zjistí, že nemá přístup k osobním údajům v konkrétním informačním systému, v době, kdy média upozorňují na masivní vlnu šíření nového typu ransomware.
Jisté	Na sociální síti uniklá citlivá fotografie zaměstnance z vánočního večírku společnosti.

Pro určení pravděpodobnosti rizika je potřeba vzít v úvahu:

- **zavedená bezpečnostní opatření**, která mohou následky eliminovat, nebo snížit (např. osobní údaje byly zašifrovány, systém je možné provozovat ze zálohy, kompromitovaná přístupová oprávnění byla okamžitě zablokována),
- **druh bezpečnostního incidentu dle** dle kapitoly č. 3.1,
- **snadnost identifikace subjektu údajů**, tedy jak snadné je identifikovat konkrétní fyzickou osobu,
- **doba**, za jakou se projeví negativní následky bezpečnostního incidentu.

Krok 4. Hodnocení dopadu pro práva a svobody subjektu údajů

Zodpovědná osoba posoudí, jaká je úroveň možného dopadu (důsledku) bezpečnostního incidentu na práva a svobody subjektu údajů dle tabulky níže.

Hodnota dopadu	Charakteristika	Fyzický dopad	Materiální dopad	Psychický a morální dopad
Nízká	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům, které bude schopen bez větších obtíží překonat.	Nemožnost dostatečně pečovat o závislou osobu (dítě, důchodce). Bez fyzického onemocnění.	Ztráta času při opakování formálních činností nebo čekání na jejich vyřízení. Příjem nevyžádané pošty (spamy). Opětovné použití údajů zveřejněných na webových stránkách za účelem cílené reklamy.	Pocit (strach) z narušení soukromí bez skutečného nebo objektivního poškození. Ztráta času, např. při změně nastavení konfigurace systému.

Střední	Subjekt údajů bude vystaven značným nepříjemnostem, které bude schopen za cenu jistých potíží překonat.	Menší fyzické onemocnění. Nedostatek péče vedoucí k menšímu, ale skutečnému poškození (postižený)	Neočekávané platby (neoprávněně uložená pokuta), dodatečné náklady (právní poplatky). Ztráta možností (zrušení dovolené, ukončení online účtu). Příjem nevyžádaných cílených zásilek, které by mohly poškodit reputaci subjektu údajů. Zpracování neaktuálních osobních údajů vytvářejících účetní chyby. Nepřesné a nevhodné profilování.	Odmítnutí pokračovat v používání informačních systémů (sociální síť, linka důvěry). Pocit narušení soukromí bez neodvratných škod. Zastrašování na sociálních mediích.
Vysoká	Subjekt údajů bude vystaven vážným nepříjemnostem, které bude schopen překonat pouze se značnými obtížemi.	Změna fyzické integrity (po útoku, domácí nehodě).	Zneužití peněz, které není kompenzováno. Dlouhodobější finanční potíže. Cílené, jedinečné a neopakovatelné, ztracené příležitosti (povýšení, studijní pobyt, vzdělávání). Poškození zařízení. Ztráta zaměstnání. Rozvod nebo ztráta partnera.	Závažné psychické potíže (deprese, rozvoj fobie). Pocit narušení soukromí s nevratnými škodami. Pocit zranitelnosti po předvolání k soudu. Pocit porušení základních práv (diskriminace, svoboda projevu). Kyberšikana a obtěžování.
Kritická	Subjekt údajů bude vystaven extrémním nebo nezvratným důsledkům, které nemusí být schopen překonat.	Smrt, vražda, smrtelná nehoda. Trvalé narušení fyzické integrity.	Finanční krize. Výrazné dluhy Neschopnost práce Ztráta důkazu při obhajobě svých práv. Ztráta přístupu k životně důležité infrastruktuře (voda, elektřina).	Dlouhodobé nebo trvalé psychické potíže. Rozsudek o trestu. Únos. Ztráta rodinných vazeb. Neschopnost hájit se a žalovat.

Pro určení dopadu je potřeba posoudit dopady z pohledu:

- Kategorie a senzitivity osobních údajů
- Počtu subjektů údajů a počtu záznamů (rozsah)
- Zvláštní charakteristiky subjektu údajů s ohledem na citlivost (např. děti, důchodci)
- Již přijatá preventivní/neodkladná opatření a jejich způsobilost snížit úroveň dopadu
- Způsob zveřejnění, zájem médií apod.

Krok 5. Posouzení existence ohlašovací povinnosti

V rámci tohoto kroku zodpovědná osoba rozhodne:

- zda jsou či nejsou naplněny podmínky pro ohlašování;
- jakému subjektu je třeba ohlášení učinit, tj. správci, úřadu a/nebo subjektu údajů;

Tabulky níže uvádějí přehled, za jakých podmínek a komu je nezbytné bezpečnostní incident ohlásit v souladu s čl. 33 a 34 GDPR.

Výsledek hodnocení pravděpodobnosti rizika				
Úroveň	**Výjimka**	**GDPR pozice**	**Příjemce**	**Doba k ohlášení**
Pravděpodobná **Vysoce pravděpodobná**	N/A	Správce	Úřad	Bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy byl Bezpečnostní incident identifikován
Jistá	N/A	Zpracovatel	Správce	Okamžité ohlášení

Výsledek hodnocení dopadu na práva a svobody subjektu údajů				
Úroveň	**Výjimka**	**GDPR pozice**	**Příjemce**	**Doba k ohlášení**
Vysoká **Kritická**	Nejsou dány výjimky dle čl. 34/3 písm. a) a b) GDPR	Správce	SÚ osobně	Bez zbytečného odkladu, kdy byl bezpečnostní incident identifikován
	Je dána výjimka dle čl. 34/3 písm. c) GDPR	Správce	SÚ prostřednictvím veřejného oznámení	Bez zbytečného odkladu, kdy byl bezpečnostní incident identifikován

Výjimky, kdy není nezbytné ohlášení subjektu údajů:

- Společnost zavedla náležitá technická a organizační opatření ještě **před bezpečnostním incidentem**, zejména taková, která činí osobní údaje nesrozumitelnými (např. šifrování).

- Společnost **ihned po bezpečnostním incidentu** zajistila, že vysoké riziko pro práva a svobody subjektu údajů se pravděpodobně neprojeví (např. blokace přístupu k účtu, ke kterému byly přihlašovací údaje odcizeny).

Krok 6. Eskalace vedení společnosti

Jsou-li splněny podmínky pro ohlašování úřadu/správci, případně úřadu a subjektům údajů, zodpovědná osoba zajistí zasedání vedení společnosti.

Zodpovědná osoba pro zasedání vedení připraví popis bezpečnostního incidentu.

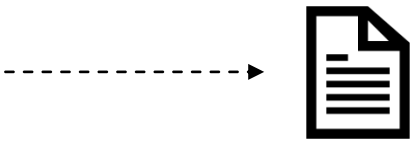
O ohlašování a případných nápravných opatřeních, včetně způsobu a prostředků k ohlášení subjektu údajů, rozhoduje vedení společnosti.

Krok 7. Ohlášení příjemcům

Zodpovědná osoba, po získání souhlasu vedení společnosti, zajistí ohlášení v souladu s níže uvedenými pravidly.

OHLÁŠENÍ ÚŘADU

Vyplnění a zaslání formuláře porušení zabezpečení osobních údajů



Bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy byl bezpečnostní incident identifikován.

- **Výjimky**
  a) Postupné ohlášení
    - V případě, kdy nejsou známy všechny požadované informace týkající se bezpečnostního incidentu během 72 hodin od identifikování (např. může být nutné komplexní forenzní šetření k úplnému stanovení povahy případu a rozsahu, v jakém jsou osobní údaje ohroženy). **Zodpovědná osoba provede ohlášení úřadu v rozsahu informací, které zná a sdělí mu, že další poskytne později**.

  b) Opožděné ohlášení
    - V případě, kdy nedošlo k ohlášení do 72 hodin, zodpovědná osoba provede ohlášení bezprostředně s patřičným zdůvodněním, proč k ohlášení nedošlo ve stanoveném časovém limitu.

  c) Hromadná ohlášení
    - V případě, kdy **společnost čelí několika podobným bezpečnostním incidentům stejného typu osobních údajů** v krátkém časovém období, která stejným způsobem postihují subjekt údajů, zodpovědná osoba provede hromadné ohlášení.

OHLÁŠENÍ SUBJEKTU ÚDAJŮ

Jasné a jednoduché jazykové prostředky

- prostřednictvím e-mailu, SMS, telefonického hovoru
- výrazné oznámení na webových stránkách, komunikace poštou
- případně nápadného oznámení v tištěných mediích

Bez zbytečného odkladu od identifikace bezpečnostního incidentu a **bezodkladně v mimořádných případech**, **kdy je nezbytné, aby subjekt údajů učinil kroky k zajištění vlastní ochrany / minimalizaci vysokého nebo kritického dopadu.**

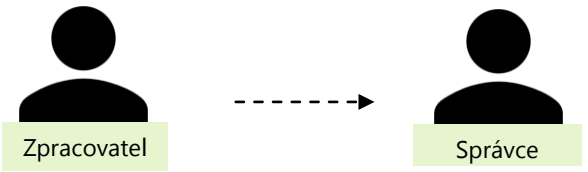
Sdělení musí obsahovat:

a) **jméno a kontaktní údaje**, nebo jiného kontaktního místa, **které může poskytnout bližší informace**

b) **popis pravděpodobných dopadů**

c) **popis opatření**, která společnost přijala nebo navrhla k přijetí s cílem vyřešit daný bezpečnostní incident, včetně případných opatření ke zmírnění možných nepříznivých dopadů

d) **kroky, které by měly učinit subjekty údajů** pro zajištění vlastní ochrany/minimalizaci dopadů



Ohlášení správci je prováděno přímo v nezbytném rozsahu, bez zbytečného odkladu od identifikace bezpečnostního incidentu

OHLAŠOVÁNÍ SPRÁVCI

Sdělení musí obsahovat:

e) **popis povahy daného případu** porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

f) **jméno a kontaktní údaje pověřence pro ochranu osobních údajů** nebo jiného kontaktního místa, které může poskytnout bližší informace;

g) **popis pravděpodobných důsledků**;

h) **popis opatření**, která byla přijata nebo navržena k přijetí s cílem vyřešit daný bezpečnostní incident, včetně případných opatření ke zmírněné možných nepříznivých dopadů.

Krok 8. Součinnost s úřadem

Zodpovědná osoba **aktivně spolupracuje s úřadem** v rámci řešení bezpečnostního incidentu, poskytuje mu dostatečné informace a **eskaluje na vedení společnosti rozhodnutí úřadu**.

Krok 9. Náprava a neustálé zlepšování

Určení zaměstnanci IT:

1. Obnoví systém, procesy, služby narušené bezpečnostním incidentem na akceptovatelnou úroveň
2. Ověří, že obnovení proběhlo v pořádku
3. Plánují testování obnovených systémů, procesů a služeb

Zodpovědná osoba:

1. Analyzuje příčinu bezpečnostního incidentu a rizik zranitelností.
2. Analyzuje problémy, které vznikly v průběhu realizace plánu reakce.
3. Navrhuje nápravná opatření na základě analýzy příčin a problémů za účelem předcházení bezpečnostnímu incidentu.
4. Poskytuje a přenáší načerpané znalosti do všech společností.

3.4 Zadokumentování a evidence

Zodpovědná osoba je odpovědná za archivaci veškeré dokumentace k předmětnému bezpečnostnímu incidentu, zejména:

- Formulář bezpečnostního incidentu
- Důkaz o ohlášení úřadu/subjektu údajů/správci, pokud bylo rozhodnuto vedením společnosti
- Analýzy a další dokumenty vzešlé z procesu řešení bezpečnostního incidentu

3.5 Reportování koncernu

Na základě odpovědnosti společnosti vůči koncernu je společnost povinna reportovat a dokumentovat případy bezpečnostních incidentů.

Zodpovědná osoba je povinna o podstatných případech bezpečnostních incidentů neprodleně informovat koncernového pověřence pro ochranu osobních údajů.

Tato povinnost nastává v případech, zejména:

- Neoprávněného předání osobních údajů třetím stranám
- Neoprávněného přístupu třetích osob k osobním údajům
- Při ztrátě osobních údajů

4 SPRÁVA ZÁZNAMŮ O ČINNOSTECH ZPRACOVÁNÍ

Klíčovým dokumentem k prokázání plnění povinností vlastníků procesů jsou Záznamy o činnostech zpracování (dále jen „**Záznamy o zpracování**“ či „**ZoZ**“), které má společnost povinnost vést.

Záznamy o činnostech zpracování jsou základní inventář zpracovávaných osobních údajů ve společnosti a jsou v něm přehledně vedeny ty nejdůležitější informace související se zpracováním osobních údajů.

Za vedení Záznamů o zpracování odpovídá kancelář pro ochranu osobních údajů a vlastníci procesů, kteří s osobními údaji v rámci jednotlivých procesů/činností přichází do styku.

Vlastníci procesů jsou povinni poskytovat informace o změnách ve zpracování osobních údajů a poskytnout tak kanceláři dostatečné podklady pro **aktualizaci záznamů o zpracování, která musí proběhnout minimálně jednou ročně**.

4.1 Kategorizace informací v ZoZ

Mezi povinné informace v záznamu o zpracování, které musí být uvedeny v dokumentu dle GDPR, patří:

- Právní postavení ŠKO-ENERGO
- Záznam
- Účel účelu
- Popis účelu (činnost zpracování)
- Kategorie SÚ
- Kategorie osobních údajů
- Právní základ zpracování (právní titul)
- Kategorie příjemců
- Plánované lhůty pro výmaz
- Předávání do třetích zemí nebo mezinárodních organizací
- Vhodné záruky při předávání

Informace uvedené v dokumentu ZoZ se propisují do **informačního memoranda**, a některé z nich i do **souhlasu** o zpracování osobních údajů, konkrétně:

- Účel zpracování
- Popis účelu (činnost zpracování)

4.2 Správa dokumentu ZoZ

Správa konkrétních záznamů probíhá především na listu *„Záznamy o činnostech zpracování“*, kde se jednotlivé záznamy rozpadají na jeden a vice účelů zpracování. Každý z účelů musí obsahovat dostatečné typy informací, přičemž **základ tvoří povinné informace uvedené v předchozí podkapitole**.

List „*Kategorie osobních údajů*“, má funkci kompletního přehledu daných kategorií a slouží jako master data pro odvozené informace na listu *„Záznamy o činnostech zpracování“*.

List „*Pomůcka pro tvorbu dokumentů*“, slouží jako pomocný nástroj při tvorbě informačních memorand.

V případě, že **vzniká nový účel či záznam**, správce dokumentu ZoZ přidá nový řádek na relevantní místo na listu *„Záznamy o činnostech zpracování“*, do kterého je nutné doplnit povinné informace k danému účelu či záznamu a aktualizovat ostatní listy dokumentu, pokud došlo k jejich změně či rozšíření.

5 SMLOUVA O ZPRACOVÁNÍ ÚDAJŮ

5.1 Technická a organizační opatření

Osobní údaje jsou náchylné ke zneužití nebo krádeži, proto musí správce přijmout vhodná **technická a organizační opatření** k zajištění dostatečné úrovně zabezpečení odpovídající riziku.

Příklady technických a organizačních opatření:

Technická opatření	Organizační opatření
Šifrování e-mailů při odesílání citlivých OÚ	Školení zaměstnanců na téma ochrany osobních údajů
Zamykání skříní s dokumenty s OÚ	Interní směrnice a pokyny týkající se ochrany OÚ
Nastavením přístupu ke sdíleným diskům s OÚ pouze oprávněných osobám	Pravidelný přezkum ZoZ
„Clean desk policy“ (zásada čistého stolu)	Zavedení procesů pro účinné řízení ochrany OÚ
Udržování operačního systému v aktualizovaném stavu	„Top Management Commitment“ (závazek nejvyššího vedení)
Spolehlivý anti-virový software	Jmenování odpovědných osob pro oblast ochrany OÚ

Všichni zaměstnanci by již měli být s většinou těchto opatření seznámeni, vzhledem ke skutečnosti, že se jedná o standardní bezpečnostní zásady, které jsou v souladu s Organizačním pravidlem OP 905 Ochrana osobních údajů.

Při definování technických a organizačních opatření je nutné zodpovědět následující:

- **Kde budu data ukládat?**
- **Jak budou data chráněna?**

Pro většinu činností zpracování lze použít již existující opatření.

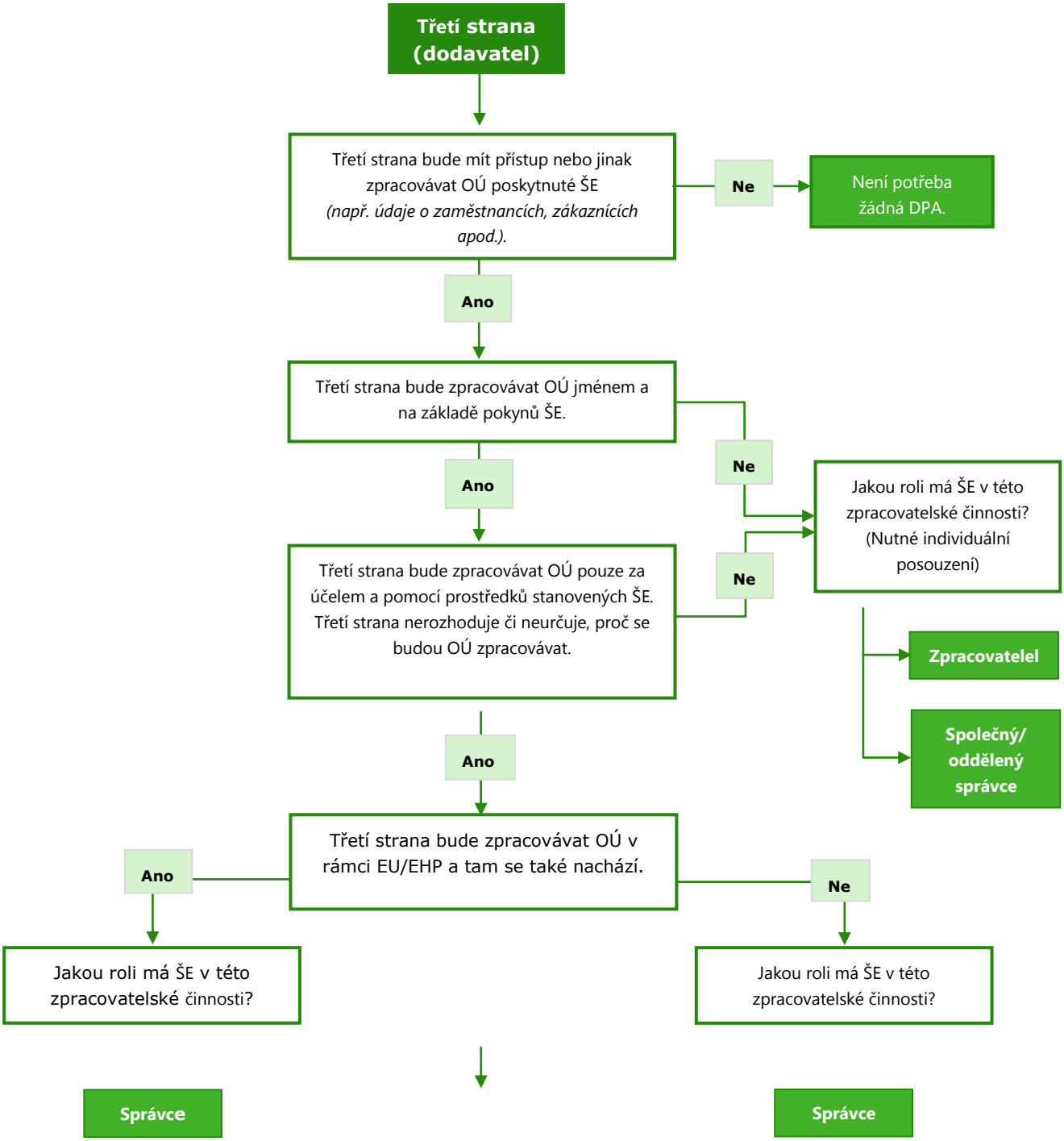
Neexistuje univerzální řešení, protože každá činnost zpracování vyžaduje jinou úroveň ochrany. Vždy je třeba posoudit rozsah, povahu údajů a možná rizika. Při rozhodování o vhodných a dostatečných opatření je třeba zvážit také náklady a složitost implementace.

5.2 Smlouva o zpracování údajů

V některých případech ŠKO-ENERGO využívá externích partnerů či dodavatelů, kteří mají v rámci svých služeb přístup k osobním údajům poskytnutých ŠKO-ENERGO. V takovém případě je nezbytné před zahájením poskytování služeb uzavřít **smlouvu o zpracování údajů (DPA)**, která bude v souladu s čl. 28 GDPR.

DPA může být součástí komplexní smlouvy o poskytování služeb, nebo může být uzavřena jako samostatná smlouva.

V závislosti na lokaci poskytovatele služeb a roli ŠKO-ENERGO mohou nastat následující situace, jak znázorňuje tento rozhodovací strom:



Rozlišujeme 4 situace dle lokace třetí strany a identifikace zpracovatelské role, jelikož je nutné aplikovat odpovídající vzor smlouvy o zpracování osobních údajů:

Poskytovatel služeb se nachází v EU:

- ŠE jako správce > Smlouva_SE_správce [vzor]
- ŠE jako zpracovatel > Smlouva_SE_zpracovatel

Poskytovatel služeb se nachází mimo EU:

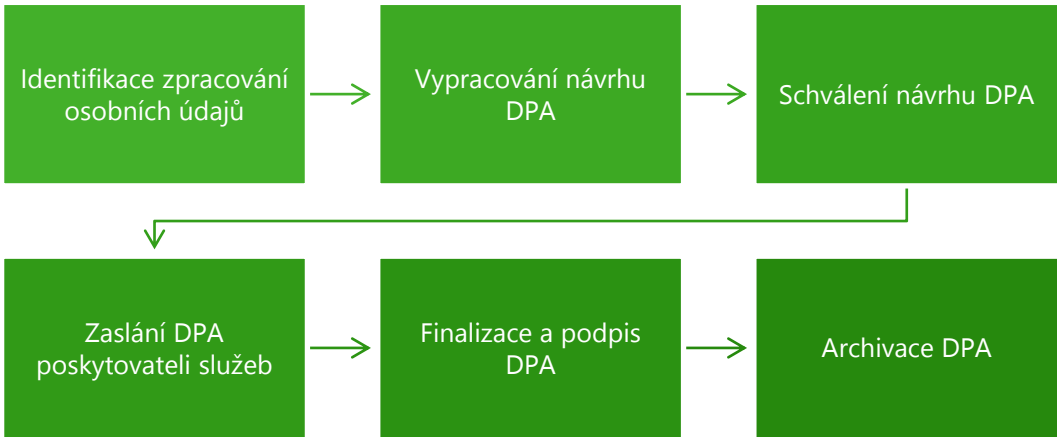
- ŠE jako správce mimo EU

Rozhodovací strom se používá pomocná návodka k určení, zda je nezbytné **uzavřít DPA,** a popřípadě jakou šablonu smlouvy použít.

- ŠE jako zpracovatel mimo EU

V rámci uzavírání DPA je nejdříve nezbytné určit, zda bude mít poskytovatel služeb přístup k osobním údajům a v jakém rozsahu. Dle povahy zpracování a odpovědností jednotlivých stran je nutné stanovit zpracovatelskou roli, přičemž společnosti ŠKO-ENERGO se může jednat v roli správce nebo zpracovatele. Na tomto základě je vypracován návrh, který je odeslán poskytovateli služeb k revizi a následnému podpisu. Posledním krokem procesu je archivace uzavřené DPA.

Celý proces uzavírání DPA je znázorněn níže:



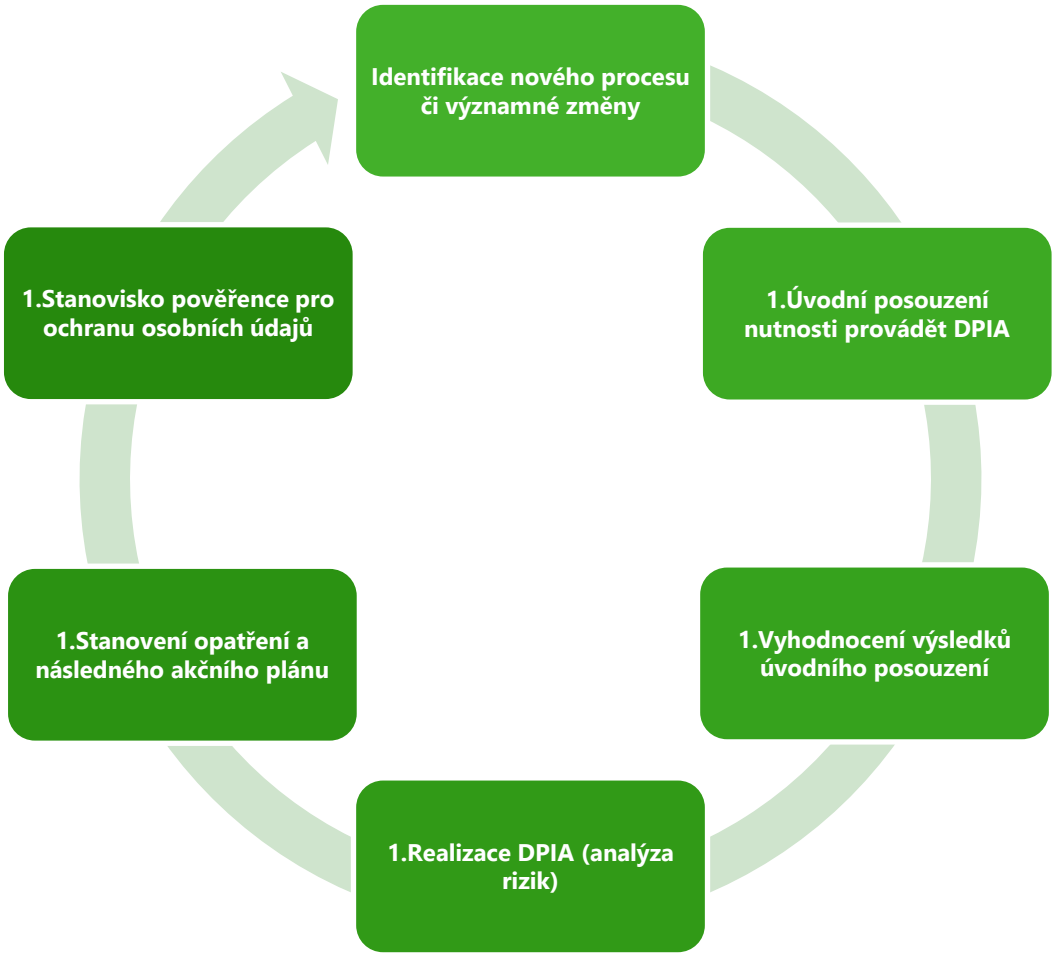
6 VÝKON DPIA

Z požadavků legislativy dále vyplývá, že se vlastníci procesu musí podílet na vypracování posouzení vlivu na ochranu osobních údajů, tzv. Data Protection Impact Assessment (ve zkratce DPIA) ve spolupráci s kanceláří pro ochranu osobních údajů.

DPIA musí být vykonána, pokud má zpracování za následek vysoké riziko pro práva a svobody subjektů údajů. To může být způsobeno například **zpracováním zvláštních kategorií osobních údajů nebo používáním nových technologií.**

Z toho důvodu mezi další povinnost vlastníků procesů patří spolupráce s kanceláří pro ochranu osobních údajů při vyhotovení takového posouzení, aby byla zajištěna dostatečná opatření v případě provádění organizační, procesní, či systémové změny. Pokud má připravovaná změna dopad na rozsah, význam a bezpečnost zpracování osobních údajů a může představovat vysoké riziko pro práva a svobody SÚ, následuje bezpodmínečně proces výkonu DPIA.

PROCES VYHOTOVENÍ DPIA



1. Identifikace nového procesu či významné změny

U každé **významné organizační, procesní, či systémové změny** či u **nově zavedeného procesu** je nutné **posoudit**, zda má **dopad na zpracování a ochranu osobních údajů**. Vlastník procesu je povinen o této plánované změně informovat kancelář pro ochranu osobních údajů, která iniciuje realizaci úvodního posouzení.

2. Úvodní posouzení nutnosti provádět DPIA

V rámci první fáze výkonu DPIA kancelář odešle **dotazník s úvodním posouzením**, umístěným na listu „*Fáze 1 - Dotazník*" v DPIA nástroji na odpovědnou osobu za daný proces s žádostí o vyplnění.

Cílem prvotního posouzení je **určit povahu, rozsah, kontext a účel zpracování osobních údajů** tak, aby bylo možné zhodnotit soulad zpracování osobních údajů s GDPR, stanovit dopady do nastavení zpracování osobních údajů a následně zhodnotit potřebu provedení DPIA.

3. Vyhodnocení výsledků úvodního posouzení

Na základě **vyhodnocení výsledků úvodního posouzení** na listu *„Fáze 2 – Výsledková listina"* kancelář určí, zda zpracování osobních údajů představuje určité riziko pro práva a svobody SÚ.

V případě, že:

- se **jedná o rizikové zpracování**, přičemž zpracování podléhá nutnosti provést DPIA, následuje druhá fáze DPIA analyzující výši rizikovosti zpracování osobních údajů.
- se **nejedná o rizikové zpracování**, proces posouzení je uzavřen vyhodnocením úvodního posouzení.

4. Realizace DPIA (analýza rizik)

Kancelář provede samotné **posouzení DPIA** neboli interní audit **se zaměřením na kontrolu organizačních a technických opatření** sloužící k zabezpečení zpracování osobních údajů během daného procesu.

Cílem je:

- **identifikovat jednotlivé hrozby** pro riziko narušení dostupnosti, důvěrnosti a integrity osobních údajů,
- **provést analýzu příčin a následků** těchto hrozeb, a
- **posoudit celkovou rizikovost zpracování** (závažnost a pravděpodobnost ohrožení subjektů osobních údajů) pro jednotlivé hrozby.

Výstup výkonu DPIA představuje kompletní analýzu rizik s vyhodnocením závažnosti dopadu rizika a pravděpodobnosti jeho výskytu umístěnou na listu *„Fáze 3 – Hodnocení rizik"*.

5. Stanovení opatření a následného akčního plánu

Na základě vyhodnocení výsledného rizika kancelář **stanoví akční plán a naplánuje implementaci bezpečnostních kontrol a opatření** pro vysoká rizika za účelem jejich zmírnění.

Seznam stanovených opatření se nachází na listu *„Fáze 3 – Opatření > Akční plán"*.

6. Stanovisko pověřence pro ochranu osobních údajů

Správce je dle GDPR povinen si při provádění posouzení vlivu na ochranu osobních údajů **„vyžádat posudek" pověřence pro ochranu osobních údajů** umístěný na listu „*Stanovisko pověřence*".

Cílem je uvést stanovisko pověřence, zda posouzení vlivu na ochranu osobních údajů bylo či nebylo provedeno správně a zda jsou závěry (tedy zda přistoupit ke zpracování či nikoliv a jaké záruky uplatnit) v souladu s GDPR.

7 POSUZOVÁNÍ NOVÝCH PROJEKTŮ

Nový projekt lze vnímat jako organizační, procesní, či systémovou změnu ve společnosti, u niž je zapotřebí posouzení z hlediska dopadu do rozsahu, významu a bezpečnosti zpracování OÚ. V případě, že připravovaná změna má dopad na zpracování osobních údajů, je nutné okolnosti blíže specifikovat, jak je uvedeno v následující kapitole. Následně při implementaci změny je potřeba dopad detailněji popsat, posoudit a zajistit soulad s principy zpracování osobních údajů, přičemž je aplikován stejný postup jako u výkonu DPIA, viz *kapitola 6*. Celý tento proces je zapotřebí konzultovat s kanceláří pro ochranu osobních údajů, která zodpovídá za realizaci posouzení projektu a aktualizaci ZoZ.

V případě, že je plánována implementace nových IT systémů sloužících ke zpracování osobních údajů, musí být ověřeny jejich funkcionality, které musí respektovat IT požadavky vyplývající z GDPR legislativy.

7.1 Úvodní posouzení

V případě, že se v rámci připravovaného projektu zpracovávají osobní údaje (např. zákazníka, zaměstnance, brigádníka atd.), je třeba získat stanovisko od kanceláře pro ochranu osobních údajů. Před kontaktováním kanceláře za účelem projednání detailů projektu a stanovení závazných podmínek pro zpracování osobních údajů je vhodné, aby si vlastník procesu připravil odpovědi na následující otázky:

1. Dochází ke zpracování osobních údajů fyzických osob?
2. Které konkrétní osobní údaje se zpracovávají? (např. jméno, email, adresa, fotografie, CV, ...)
3. Je opravdu nutné zpracovávat tyto osobní údaje, nelze je zpracovávat anonymně?
4. Proč jsou osobní údaje zpracovávány? (účel zpracování)
5. Jakých fyzických osob jsou osobní údaje zpracovávány? (např. zaměstnanec, vlastník vozu, zákazník, ...)
6. Kde, v jaké formě a na jak dlouhou dobu budou osobní údaje uloženy?
7. Jsou pro zpracování osobních údajů využívány jiné subjekty jako zpracovatelé? (např. marketingová a personální agentura nebo poskytovatelé cloudových služeb)
8. Dochází k předání osobních údajů do třetích zemí nebo mezinárodních organizací? (v rámci EU, mimo EU – konkrétní stát)

7.2 Začlenění nového záznamu

Pokud kancelář pro ochranu osobních údajů schválí zavedení nového projektu, musí zajistit začlenění nového procesu či změny do interní evidence záznamů prostřednictvím následujících úkonů:

1. **Definování právního titulu, na základě kterého dochází k zamýšlenému zpracování:**
    a. Plnění právních povinností
    b. Nezbytnost pro uzavření a plnění smlouvy
    c. Souhlas
    d. Oprávněný zájem (analyzovaný pomocí balančního testu)
2. **Vyhodnocení nutnosti provedení DPIA**
3. **Zavedení nového záznamu**
4. **Implementace do Informačního memoranda a Záznamu o činnostech zpracování**
5. **Revize smlouvy o zpracování osobních údajů**

7.3 IT požadavky na začleněné systémy

Aby mohly implementované IT systémy pracovat s osobními údaji, musí být nejprve schopny pracovat s těmito údaji v souladu s GDPR legislativou a respektovat její IT požadavky. První podkapitola pojednává o povinnosti kanceláře pro ochranu osobních údajů zajistit provedení mapování účelů zpracování v daných systémech a posoudit rozsah osobních údajů z důvodu jejich minimalizace a účelového omezení. Systémy musí být dále schopny realizovat práva SÚ a zajistit přístup k těmto údajům pouze povolaným osobám. Metody pro dosažení této funkcionality jsou vysvětleny v následujících kapitolách.

7.3.1 Minimalizace a výmaz OÚ

V systému musí být nejprve provedeno mapování účelů zpracování všech osobních údajů, a to s ohledem na cíl **minimalizovat osobní údaje** v dotčených systémech a odděleních.

Osobní údaje musí mít:

- přiřazený účel a/nebo právní základ ke zpracování,
- platnou lhůtu pro zpracování osobních údajů,

V opačném případě musí být zajištěn výmaz či anonymizace.

V případě, že výmaz není možný, vlastník procesu:

- důsledně **zamezí jakémukoliv** zpracování těchto osobních údajů;
- zajistí bezpečnost osobních údajů proti neoprávněnému přístupu;
- vykoná důkladnou analýzu příčin nemožnosti výmazu.

Provedenou analýzu a zavedená opatření dokumentuje a s dokumentací obeznámí svůj tým, odpovědného za dotčený systém a kancelář pro ochranu osobních údajů.

Výmaz osobních údajů lze zajisti prostřednictvím následujících metod:

- **Zneplatnění osobních údajů na základě smazání identifikačních údajů**

Nezvratné **odmazání základních identifikačních údajů** (například jméno, příjmení, rodné číslo), tím pádem budou ostatní osobní údaje, které nebude možné spojit se skutečnou fyzickou osobou, anonymizované.

- **Zneplatnění osobních údajů na základě šifrování nebo anonymizace osobních údajů nebo jejích části**

V případě, kdy systém neumožňuje jednoduchý výmaz, se provede zneplatnění formou nezvratného **znečitelnění předmětných osobních údajů anonymizací**.

Forma samotné anonymizace může být provedena:

- **záměnou dat podle klíče** (pseudonymizace, šifrování),
- použitím **hash algoritmů** s následným nezvratným výmazem klíčů použitých k anonymizaci.

V některých systémech lze provést výměnu písmen za některý zvolený znak, například hvězdičky. Technologicky bude zachována kontinuita digitálního záznamu, avšak již se nebude jednat o osobní údaj, protože znaky budou nezvratně nahrazeny hvězdičkami nebo jinými substitučními znaky tak, aby z toho **nebylo možné zpětně odvodit skutečné vlastnictví osobních údajů**, nebo příslušnost k fyzické osobě.

- **Zneplatnění osobních údajů na základě použití rolí**

Méně preferovaná varianta je „schování OÚ“ na základě použití rolí, tj. osobní údaje nebudou přístupné uživatelům nebo jinému systému na základě úpravy práv rolí. Je nutné nastavit opatření, která minimalizují rizika přístupu administrátorů k těmto osobním údajům.

Tato metoda není v souladu s GDPR, tudíž je nutné její použití konzultovat s kanceláří pro ochranu osobních údajů.

- **Výmazy z logů, auditních záznamů, archivů a záloh**

V případě logů, sekvenčních archivů nebo záloh systémů **musí být nastavena retenční doba**.

Logy a data z archivů a záloh nesmí být dále použity pro zpracování osobních údajů nebo předávány k dalšímu zpracování osobních údajů nebo k dalšímu zpracování osobních údajů.

Výmaz osobních údajů se musí provést z archivů s „random" přístupy zápisů. V případě, že byla provedena obnova systému nebo dat, vlastník procesu nebo správce systému je povinen uplatnit všechny výmazy, které byly aplikovány v primárním systému, ale nejsou obsaženy v záloze, ze které byla obnova provedena.

- **Zneplatnění osobních údajů v nestrukturovaných datech**

Zneplatnění osobních údajů v nestrukturovaných datech může být nepřiměřeně obtížné a nákladné.

Nejprve je nutné přistoupit k zneplatnění omezenou *„best effort"* formou, například vykonat prohledání existujících souborů standardními prostředky dostupnými pro pracovníky, např. interní search aplikace, file search, apod.

Kromě standardních aplikací lze zvážit nasazení některého z enterprise vyhledávacích systémů určeného pro fulltextová vyhledávání, např. Lucene, Solr, Elastic Search, apod.

V systémech, kde je úschova dokumentů s osobními údaji základní vlastností fungování systému, například dokumenty HR útvaru (životopisy apod.), je nutné vést evidenci formou metadat k nestrukturované formě osobních údajů. Strukturovaná forma metadat tak v podstatě vytvoří strukturu nad osobními údaji a zneplatnění se podstatně zjednoduší.

V případě, že nelze mít systém s metadaty nad nestrukturovanými osobními údaji, ani nelze rozumně použít fulltext vyhledávače, nebo jsou osobní údaje uloženy na sekvenčním médiu, pak je zapotřebí zavést expiraci nad datovým setem.

7.3.2 Realizace práv subjektu údajů

Nově začleněné systémy musí být schopny pracovat s osobními údaji SÚ, a vykonávat tak práva těchto subjektů. Mezi tyto práva patří:

1. Právo na přístup k osobním údajům
2. Právo na výmaz osobních údajů
3. Právo na omezení zpracování
4. Právo na opravu osobních údajů
5. Právo na přenositelnost osobních údajů

1) Naplnění práva na přístup k osobním údajům

Naplnění práva na přístup k osobním údajům vyžaduje po technické stránce možnost vyhledat konkrétní subjekt osobních údajů a všechny osobní údaje, které jsou k němu v daném systému zpracovávány.

Formát, ve kterém kancelář pro ochranu osobních údajů obdrží ze systému osobní údaje, není předem daný, respektive kancelář má plně v gesci rozhodnutí o akceptaci konkrétního formátu. Subjektu údajů se osobní údaje předávají ve formátu .docx.

2) Naplnění práva na výmaz osobních údajů

Kancelář prověří náležitosti související s výmazem, jako například návaznosti na další právní důvody zpracování. Vlastník nebo správce systému následně provede požadovaný výmaz nebo provede opatření, kterým se osobní údaje znečitelní a zamezí dalšímu zpracování.

3) Naplnění práva na omezení zpracování

V případě vznesení požadavku pro omezení zpracování je nutné pozastavit veškeré zpracování konkrétních OÚ konkrétního subjektu (např. zamezit synchronizaci těchto dat do dalších systémů).

Z technického hlediska je zapotřebí mít v systémech u osobních údajů označení, například „flag“, že osobní údaje subjektu se nesmí zpracovávat. Na tento „flag“ bude navázaná systémová logika, která pak tyto osobní údaje vynechá ze zpracování. Takto jsou osobní údaje subjektu evidovány, ale žádná systémová logika tyto údaje dál nezpracovává.

Přístup k osobním údajům s omezeným zpracováním je tak možné jenom za účelem aplikace jiného práva subjektu údajů (právo na přenositelnost, právo na informovanost apod.).

4) Naplnění práva na opravu osobních údajů

Naplnění tohoto práva z pohledu technologií je realizováno přes kancelář pro ochranu osobních údajů, která vznese požadavek na vlastníka procesu nebo správce systému. Vlastník procesu nebo správce systému následně provede požadovanou opravu, tj. editaci příslušných záznamů.

Naplnění práva na opravu osobních údajů vyžaduje po technické stránce možnost editovat údaje konkrétního subjektu údajů.

5) Naplnění práva na přenositelnost osobních údajů

Konkrétní subjekt údajů může zažádat o přenesení osobních údajů, které se ho týkají a jež poskytl správci, k jinému správci (například při změně zaměstnavatele, přenesení údajů jinému poskytovateli zákonného ručení, přenos nastavení komfortních funkcí vozidla apod.). V takovém případě musí správce poskytnout a předat tyto údaje ve strukturovaném, běžně používaném a strojově čitelném formátu.

Právo lze uplatnit, jen pokud je zpracování založeno na souhlasu nebo smlouvě a současně se jedná o automatizované zpracování, tedy takové zpracování, které probíhá výlučně prostřednictvím technických prostředků na základě předem určeného algoritmu a bez jakéhokoliv zásahu člověka.

Právo se na technologie aplikuje tak, že dotčené systémy budou mít vytvořený mechanismus, který vyexportuje osobní údaje pro daný subjekt údajů do souboru, který bude mít strojově čitelný formát. Sice GDPR nepředepisuje konkrétní formáty, ale je zde vhodné použít formát JSON, CSV nebo podobný. Export se uloží do souboru, který se bezpečnou cestou předá kanceláři pro ochranu osobních údajů, která jej následně předá SÚ

7.3.3 Další povinnosti pro systémy

Aby byla práce s osobními údaji v systémech bezpečnější, měly by systémy splňovat i následující požadavky:

- **Zprostředkování logových záznamů DPO**
- **Zneplatnění osobních údajů pro neprodukční systémy**
- **Autentizace uživatelů**

Díky těmto krokům budou mít k systémům přístup **pouze povolané osoby.**

Zprostředkování logových záznamů DPO

Na základě analýzy nedochází k přenášení logů do centrálního úložiště a tyto logy nejsou zpřístupněny DPO. Dále je nezbytné, aby logování v systému bylo v souladu s interní směrnicí OP 701 Bezpečnosti informací, která je k dispozici na intranetu ŠKO-ENERGO/Organizace/Řízené dokumenty.

V systému musí být zavedeno **logování aktivit s osobními údaji**, které bude obsahovat provedené změny osobních údajů a informaci o přístupech k osobním údajům.

Logování přístupů bude logované minimálně v rozsahu **login-logout** nebo **connect-disconnect** uživatele nebo služby. V případě, že to prostředky (výkon serveru, diskový prostor, …) umožňují, bude logován i každý přístup ke konkrétním osobním údajům subjektu. **Mimořádný důraz je nutné klást na logování exportů větších objemů osobních údajů.**

Logování konkrétních výstupů vyplývajících z přístupů k osobním údajům nebude vhodné logovat, protože by se generovalo neúměrné množství záznamů, a navíc takové záznamy by obsahovaly další kopie osobních údajů.

Je doporučeno logy ukládat do centrálního úložiště logů, čímž budou zajištěny proti modifikacím. DPO útvar musí mít přístup k logům pro čtení (read-only). Tento přístup lze realizovat přes centrální systém úložiště logů nebo přímo přístupem do dotčeného systému. Ideální je mít pro DPO útvar oba druhy přístupů.

Je třeba využít již existující možnosti systémů a sladit se s existujícími možnostmi a nastaveními. Například servery můžou mít aktivní „access log“, kde se potřebné informace již pravděpodobně zaznamenávají. Tento přístup je rovněž užitečný k **zajištění kybernetické bezpečnosti.**

Logování aktivit v dotčených systémech slouží pro účel forenzních aktivit v případě bezpečnostního incidentu nebo podezření na bezpečnostní incident.

Zneplatnění osobních údajů pro neprodukční systémy

Dotčený systém bude mít implementovaný mechanismus, který provede **výmaz, anonymizaci nebo pseudonymizaci** osobních údajů pro ne-produkční systémy. Mechanismus bude aplikovaný při přenosu dat z produkčního systému do neprodukčního.

Cílem je nemít osobní údaje v neprodukčních systémech. Tím se výrazně zmenší rozsah aplikovaných opatření, protože v těchto systémech nebudou osobní údaje (například testovací, vývojové, předváděcí nebo podobné systémy).

Osobní údaje potřebné pro identifikaci přihlašujícího se uživatele do neprodukčního systému není nutné anonymizovat. Zde je to případ uživatelského jména, a případně souvisejícího identifikačního popisu, pokud má charakter osobního údaje.

Autentizace uživatelů

Dotčený systém bude mít implementovaný **autentizační mechanismus, který jednoznačně ověří uživatele u přihlášení do systému.**

Pro autentizaci je vhodné integrovat dotčený systém na systém řízení identit a přístupů (Identity and Access Management, IAM). Součástí takového systému je i centrální registr uživatelů, například LDAP, Active Directory, nebo podobně. Samotná autentizace pak může probíhat přes standardní protokoly LDAP, Kerberos, Active Directory, SAML V2, WSAuth, nebo podobně. V případě, že dotčený systém neumožňuje využití standardizovaných protokolů, pak je nutné mít lokální správu uživatelů a udržet synchronní data s centrálním systémem řízení identit a přístupů. Vzhledem k citlivosti systému se v takovém případě doporučuje **zavedení vícefaktorové autentizace.**