Směrnice k ochraně osobních údajů (GDPR)

Organizace - správce osobních údajů:

Ekodomov, z.s.
IČ: 26664488,
se sídlem V Podbabě 2602/29b, Dejvice, 160 00 Praha 6

(pro účely této směrnice dále jen „správce“)

Směrnice je platná ode dne: 15. 11. 2020

Čl. 1

Předmět a účel směrnice

1. Směrnice pro ochranu osobních údajů slouží k zajištění souladu činnosti správce s požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR“ nebo „nařízení“) a zákona č. 110/2019 Sb., o zpracování osobních údajů.
2. Tato směrnice je závazná pro všechny zaměstnance správce, kteří jsou povinni se s ní prokazatelně seznámit, a pro další osoby, které mají se správcem jiný právní vztah (smlouva o dílo, nájemní smlouva) a které se zavázaly postupovat podle této směrnice.
3. Účelem směrnice je zejména stanovení opatření a pravidel, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů a činnost správce odpovídala požadavkům GDPR a zákona o zpracování osobních údajů.

Čl. 2

Vymezení základních pojmů

1. Pro účely této směrnice se rozumí:
    (a) automatizovaným zpracováním zpracování, které zahrnuje operace:
        (i) ukládání informací na nosiče dat nebo jejich zpracování v databázích a programech,
        (ii) archivování informací jejich ukládáním na archivační paměťová média a v případě potřeby obnovování informací z archivních médií;
    (b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů (např. vzorek DNA, otisk prstu, obraz oční sítnice);
    (c) manuálním zpracováním jakékoliv zpracování s výjimkou zpracování automatizovaného (listinná podoba, kartotéky, spisy);

(d) oprávněnými osobami pracovníci správce, zejména učitelé, lektoři, průvodci (dále jen „zaměstnanci“), kteří v rámci plnění pracovních povinností mají přístup k osobním údajům a dále je zpracovávají,

(e) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za identifikovatelný, jestliže ho lze přímo či nepřímo identifikovat na základě konkrétních údajů nebo informací. Osobním údajem se rozumí zejména jméno a příjmení, identifikační číslo (např. rodné číslo), datum narození, adresa, fotografie, údaje o zdravotním stavu, biometrické údaje apod.;

(f) příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky nebo Evropské unie;

(g) subjektem osobních údajů fyzická osoba, k níž se konkrétní osobní údaje vztahují, zejména zaměstnanci, děti a jejich zákonní zástupci;

(h) vedoucím zaměstnancem ředitelka (dále jen „ředitelka“);

(i) zpracovatelem každý subjekt, který na základě smluvního vztahu se správcem zpracovává osobní údaje;

(j) zpracováním osobních údajů jakákoliv operace s osobními údaji, a to automatizovaně nebo manuálně. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče dat, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace;

(k) záznamem o činnostech zpracování záznamy vedené v souladu s článkem 30 GDPR;

(l) bezpečnostním incidentem jakékoliv porušení zabezpečení osobních údajů dle článku 33 GDPR;

(m) základními zásadami zpracování osobních údajů zásada zákonnosti, korektnosti a transparentnosti zpracováním, zásada účelového omezení zpracování na legitimní účely, zásada minimalizace údajů, zásada přesného zpracování, zásada aktuálnosti údajů a zásada zabezpečeného zpracování.

Čl. 3

Základní zásady a povinnosti při zpracování osobních údajů

1. Všichni zaměstnanci musí dodržovat základní zásady týkající se zpracování osobních údajů. Zaměstnanci jsou povinni dodržovat všechny zákonné normy a vnitřní předpisy správce.
2. Zaměstnanci hlásí každý bezpečnostní incident přímo vedoucímu zaměstnanci.
3. Zaměstnanci zpracovávají veškeré údaje přesně a v rozmezí nezbytně nutném, tyto údaje musí aktualizovat a zpracovávat způsobem zajišťujícím zabezpečení před neoprávněným či protiprávním zpracováním, náhodnou ztrátou, zničením nebo poškozením. Zpracování údajů je možné pouze na základě právních důvodů. Zpracování údajů je zákonné, pokud je prováděno na základě souhlasu, pokud je nezbytné pro plnění smlouvy nebo její uzavření (předsmluvní jednání), pokud je nezbytné pro plnění právní povinnosti správcem, pokud je nezbytné pro ochranu životně důležitých zájmů subjektů údajů, je nezbytné pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci anebo pokud je nezbytné pro účely oprávněných zájmů správce. Osobní údaje je možné shromažďovat pouze pro určité účely, které jsou výslovně vyjádřené a jsou legitimní. Subjekt má právo vědět, které údaje správce zpracovává a kdo

k nim má přístup, a to po jakou dobu. Je možné zpracovávat pouze osobní údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu.

4. Zaměstnanci musí být schopni doložit oprávněnost jimi prováděných operací zpracování osobních údajů a zdroje, prostřednictvím kterých údaje získali (tj. zdrojem jsou buď samotné subjekty údajů nebo třetí osoba).
5. Při posuzování zákonnosti zpracování nesmí být opomenuto posouzení slučitelnosti účelů. Zpracování údajů pro jiný účel, než pro který byly získány, je možné pouze na základě souhlasu subjektů údajů nebo musí mít oporu v právu Unie nebo členského státu.
6. Správce odpovídá za dodržení výše uvedených zásad a musí být schopen toto dodržení souladu prokázat.

Čl. 4

Obecné postupy správce při nakládání s osobními údaji a jejich zpracováním

1. Všichni zaměstnanci, případně další osoby, jsou povinni zpracovávat osobní údaje v souladu se základními zásadami zpracování uvedenými v čl. 3 této směrnice.
2. Zaměstnanci jsou povinni dodržovat všechny zákonné normy, které se vztahují k výkonu jejich pracovních povinností, a dále vnitřní předpisy správce.
3. Zpracovávat osobní údaje je možné pouze na základě právních titulů uvedených v čl. 3 této směrnice. Osobní údaje je možné shromažďovat pouze pro určité účely, které jsou výslovně vyjádřené a jsou legitimní. Je možné zpracovávat pouze osobní údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování.
4. Správce vede záznamy o činnostech zpracování ve smyslu čl. 30 nařízení GDPR, které obsahují popis veškerých operací zpracování osobních údajů v rámci činnosti správce.
5. nepředává osobní údaje dětí, zaměstnanců nebo třetích osob jiným správcům, pokud není předání osobních údajů zákonným nebo smluvním požadavkem.
6. Správce nepředává osobní údaje do zemí mimo Evropskou unii nebo mezinárodním organizacím. Pokud by bylo nezbytné tak učinit, musí správce konzultovat podmínky předání s pověřencem.
7. Správce vede evidenci žádostí subjektů údajů v souvislosti s uplatňováním jejich práv podle čl. 10 až 16 této směrnice, a dále registr bezpečnostních incidentů podle čl. 14. této směrnice.
8. Zpracovávat citlivé údaje lze, ledaže lze aplikovat některou z výjimek uvedených v čl. 9 odst. 2 nařízení GDPR. Zpracování těchto osobních údajů správce konzultuje s pověřencem.
9. Datové soubory obsahující osobní údaje, jejichž ztráta nebo změna by mohly mít negativní důsledky pro subjekty údajů, musí být pravidelně, zálohovány.
10. Správce vede registr souhlasů v případě získávání souhlasů na dobu určitou a hlídá dobu trvání poskytnutého souhlasu tak, aby operace zpracování nebyly prováděny po uplynutí této doby.
11. Správce průběžně, dle momentální potřeby, aktualizuje technická a organizační opatření k zajištění ochrany osobních údajů.

Čl. 5

Konkrétní povinnosti zaměstnanců, případně dalších osob při nakládání s osobními údaji

1. Všichni zaměstnanci správce jsou povinni zejména:

1.1. dodržovat pravidla bezpečnosti práce včetně požárních a poplachových pravidel tak, aby nedošlo ke zničení uložených písemností a digitálních záznamových médií s osobními údaji v důsledku požáru, potopy nebo jiné havárie;

1.2. zabezpečit pracovní počítače a informační systémy prostřednictvím povinné autentizace (přihlášení do počítače po jeho zapnutí zadáním uživatelského jména a přiměřeného hesla a přihlášení do informačního systému po jeho spuštění zadáním uživatelského jména a hesla, zadání hesla do mobilního telefonu apod.);

1.3. nesdělovat nebo nezpřístupnit vlastní autentizační údaje (hesla) jakékoliv jiné osobě (a to ani osobě odpovědné za správu IT), ani je kamkoliv napsat nebo uložit;

1.4. používat k plnění pracovních úkolů výhradně služební výpočetní techniku (počítače, telefony)

1.5. při plnění pracovních povinností nepořizovat fotografie a videonahrávky dětí na své soukromé telefony, není-li to nezbytně nutné. V případě takového pořízení jsou zaměstnanci povinni tyto záznamy ze svých soukromých telefonů odstranit, jakmile to bude možné;

1.6. při dočasném opuštění pracoviště spustit spořič obrazovky chráněný heslem, uzamknout PC, apod;

1.7. po skončení pracovní činnosti vypnout PC nebo jej uvést do režimu spánku tak, aby nemohla být činnost obnovena bez zadání hesla, a dále zavřít okna a uzamknout dveře v místnosti. Nosiče obsahující osobní údaje vedené v listinné a elektronické podobě, nemůže-li zaměstnanec, byť jen dočasně vykonávat přímý dohled, uloží na náležitě zajištěná místa;

1.8. neponechávat při tisku, kopírování a skenování dokumentů obsahující osobní údaje tyto dokumenty v zařízeních bez dozoru;

1.9. nezpřístupňovat dokumenty obsahující osobní údaje a nepředávat je třetím osobám;

1.10. pořizovat kopie nosičů s osobními údaji jen v případech nezbytných pro výkon pracovní činnosti, po jejich využití je bezpečně zlikvidovat;

1.11. vynášet nosiče s osobními údaji z pracoviště mimo prostory správce;

1.12. ohlásit bezodkladně vedoucímu zaměstnanci a pověřenci jakékoliv porušení zabezpečení osobních údajů (např. ztráta služebního notebooku, služebního telefonu nebo dokumentu obsahujícího osobní údaje, odeslání e-mailu obsahujícího osobní údaje nesprávnému adresátovi, ztráta klíče k prostorám správce či jiným uzamykatelným prostorám, ve kterých se uchovávají osobní údaje), neoprávněné použití osobních údajů, zneužití osobních údajů nebo jiné neoprávněné jednání související s ochranou osobních údajů;

1.13. používat svěřené prostředky pouze k plnění svých pracovních povinností, a to v souladu s účelem, ke kterému byly určeny, neužívat osobní údaje subjektů údajů pro vlastní potřebu;

1.14. upozornit vedoucího zaměstnance a pověřence na případné nedostatky v zabezpečení, nejedná-li se přímo o bezpečnostní incident dle této směrnice;

1.15. při komunikaci s veřejností (bez ohledu na formu) dodržovat základní zásady ochrany osobních údajů uvedené v čl. 3 této směrnice. Osobní údaje je zakázáno sdělovat telefonicky a elektronickou poštou bez náležitého ověření totožnosti;

1.16. oznamovat vedoucímu zaměstnanci a pověřenci jakoukoliv skutečnost, jež by mohla být žádostí v souvislosti s uplatňováním jakýchkoliv práv podle čl. 10 až 16 této směrnice;

1.17. v případě získávání souhlasu subjektů údajů se zpracováním jsou zaměstnanci oprávněni využít pouze závazný vzor schválený pověřencem;

1.18. zamezit nahodilému a neoprávněnému přístupu k osobním údajům zaměstnanců, dětí, zákonných zástupců a dalších osob, které správce zpracovává;

1.19. obrátit se na pověřence v případě jakýchkoliv pochybností ohledně zpracování osobních údajů.

2. Všichni zaměstnanci správce a třetí osoby seznámené s touto směrnicí jsou dále povinni zachovávat mlčenlivost o zpracovávaných osobních údajích a o implementovaných

bezpečnostních opatřeních a zárukách k jejich ochraně. Povinnost mlčenlivosti trvá i po skončení pracovněprávního poměru či funkčního nebo smluvního vztahu se správcem.

Čl. 6

Pověřenec pro ochranu osobních údajů

1. Výkon funkce pověřence bude zajištěn externím dodavatelem na základě smluvního vztahu.
2. Správce zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. V případě pochybností musí zaměstnanci konzultovat jakékoliv otázky v souvislosti se zpracováním nebo ochranou osobních údajů. Dále správce zajistí, aby pověřenec nedostával žádné pokyny týkající se výkonu úkolů v oblasti zpracování osobních údajů.
3. V rámci činnosti správce plní pověřenec zejména následující úkoly:
   - poskytování informací a poradenství v souvislosti se zpracováním osobních údajů zaměstnancům správce,
   - monitorování souladu činností správce s touto směrnicí, GDPR a dalšími relevantními předpisy a s předpisy správce v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců zapojených do operací zpracování a souvisejících auditů;
   - v souvislosti se zpracováním osobních údajů vydává doporučení za účelem zajištění souladu s právními předpisy a zvýšení úrovně zabezpečení osobních údajů;
   - poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 GDPR;
   - spolupráce s dozorovým úřadem;
   - hlášení bezpečnostních incidentů dozorovému úřadu za podmínek uvedených v čl. 33 GDPR;
   - vyřizování žádostí subjektů údajů v souvislosti s uplatňováním jejich práv podle čl. 10 až 16 této směrnice
   - působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle článku 36 GDPR, a případně vedení konzultací v jakékoli jiné věci vztahující se k ochraně osobních údajů;
   - působení jako kontaktní místo pro subjekty údajů a dozorový úřad.
4. Správce zajistí vhodné zveřejnění informací o totožnosti pověřence, včetně jeho kontaktních údajů, způsobem umožňující dálkový přístup, zejména na svých internetových stránkách, a dále v listinné podobě, např. na školní nástěnce. Správce sdělí totožnost a kontaktní údaje pověřence dozorovému úřadu.
5. Zaměstnanci jsou povinni informovat pověřence o veškerých skutečnostech, které mohou být významné pro ochranu osobních údajů ze strany správce.

Čl. 7

Podmínky pro získání souhlasu subjektu údajů

1. Souhlas se získává v případě, že zpracování údajů není prováděno na základě jiného právního titulu. Zaměstnanci vždy konzultují s vedoucím zaměstnancem definici souhlasů a stanovení účelu, pro který se souhlas získává.
2. V případě, užití souhlasu jsou zaměstnanci oprávněni využít pouze závazný vzor poskytnutý správcem.

3. V případě získávání souhlasů na dobu určitou musí odpovědný zaměstnanec vést registr souhlasů a hlídat expirační doby tak, aby operace zpracování nebyly prováděny po expiraci souhlasu.
4. Souhlas musí být informovaný – text souhlasu musí obsahovat rovněž plnění informační povinnosti nebo musí na text informační povinnosti odkazovat, v takovém případě zaměstnanec ověří, zda se subjekt údajů poskytující souhlas s informační povinností seznámil.

Čl. 8

Transparentní informace, sdělení a postupy pro výkon práv subjektů údajů

1. Za plnění informační povinnosti dle článku 12 GDPR je odpovědný vedoucí zaměstnanec.
2. Všeobecná informační povinnost je plněna zveřejněním na webových stránkách správce. Minimální požadavky jsou stanoveny v článku č. 9 této směrnice.
3. Soulad rozsahu a obsahu informační povinnosti kontroluje průběžně vedoucí zaměstnanec.
4. Při výkonu práv subjektů údajů musí být vždy relevantně ověřena totožnost žadatele, aby bylo jednoznačně prokázáno, že má vztah ke zpracovávaným osobním údajům. Totožnost při vyřizování žádosti ověřuje vedoucí zaměstnanec následovně:
    (a) žádost v listinné podobě musí být doručena osobně a totožnost žadatele ověřena z platného dokladu;
    (b) žádost v listinné podobě může být opatřena úředním ověřením pravosti podpisu, což nahrazuje osobní ověření identity žadatele;
    (c) žádost zaslaná ve formě e-mailové zprávy musí být opatřena zaručeným elektronickým podpisem žadatele;
    (d) žádost zaslaná datovou schránkou musí být odeslána výhradně z datové schránky žadatele, což nahrazuje osobní ověření identity žadatele.
5. Na žádost se odpovídá primárně ve stejné formě, v jaké byla podána. Je-li vyhověno žádosti o přístup, vyřídí se výhradně poštou do vlastních rukou subjektu údajů nebo jeho zástupce.
6. Při pochybnosti o identitě žadatele nemůže být žádost vyřízena. Žadatel musí být o tomto vyrozuměn a musí mu být umožněno dodatečné prokázání totožnosti.
7. Při podání žádosti zmocněncem subjektu údajů musí zmocnění odpovídat obecným požadavkům právních předpisů (§ 441 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů) s tím, že ověřena musí být jak totožnost zmocněnce, tak totožnost zmocnitele. Při ověření totožnosti se postupuje analogicky k odst. 4. tohoto článku.
8. Žádosti se vyřizují bez zbytečného odkladu, nejpozději ve lhůtě stanovené článkem 12 odst. 3 GDPR.
9. V případě uplatnění práva na přístup se poskytované informace zasílají výhradně prostřednictvím provozovatele poštovních služeb do vlastních rukou subjektu údajů (nebo jeho zástupce), aby bylo zabráněno zpřístupnění osobních údajů neoprávněné osobě.
10. Veškeré žádosti se evidují v registru žádostí subjektů údajů, a to včetně popisu způsobu jejich řešení. Za evidenci je odpovědný vedoucí zaměstnanec.

Čl. 9

Informace poskytované v případě, že osobní údaje jsou získány od subjektů údajů

1. Za řádné plnění informační povinnosti směrem k subjektům údajů odpovídá vedoucí zaměstnanec. V případě získání údajů jinak než od subjektů údajů, je nutné posoudit uplatnění výjimek pro situace, kdy je získávání nebo zpřístupnění osobních údajů výslovně stanoveno

právem EU nebo členského státu nebo pokud poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí. Není-li možné některé z výjimek uplatnit, je nutné splnit informační povinnost vůči subjektu údajů dle čl. 14 GDPR.

Základní náležitosti informační povinnosti dle článku 13 GDPR tvoří nejméně:

(a) Identifikační a kontaktní údaje správce;

(b) účely zpracování a právní základ zpracování;

(c) oprávněné zájmy správce nebo třetí strany;

(d) údaje o případných příjemcích nebo kategorie příjemců;

(e) případný úmysl předat údaje do třetí země nebo mezinárodní organizaci;

(f) doba uložení údajů nebo kritéria pro její stanovení;

(g) poučení o jednotlivých právech subjektů údajů včetně poučení o možnosti obrátit se na dozorový orgán;

(h) poučení o možnosti odvolat kdykoliv souhlas;

(i) skutečnost, zda je poskytnutí údajů zákonným nebo smluvním požadavkem.

Čl. 10

Právo subjektu údajů na přístup k osobním údajům

1. Za plnění povinnosti vyplývající z uplatnění práva subjektů údajů na přístup dle článku 15 GDPR odpovídá vedoucí zaměstnanec. Vedoucí zaměstnanec je povinen vyhotovit a zaslat žadateli vyjádření, zda jsou správcem zpracovávány jeho osobní údaje.
2. V případě existence zpracování osobních údajů žadatele správce poskytne vedoucí zaměstnanec tomuto žadateli zpracovávané osobní údaje a informace o zpracování. Na žádost budou rovněž poskytnuty kopie zpracovávaných údajů. Byla-li žádost podána elektronicky, poskytnou se informace primárně v elektronické formě.
3. V případě zpracování většího množství osobních údajů o subjektu bude žadatel vyzván k upřesnění, jaké informace konkrétně požaduje.
4. Žádosti subjektů údajů vyřizuje vedoucí zaměstnanec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.
5. Právo na přístup nesmí být odepřeno ani omezeno. Omezení je možné pouze z důvodu ochrany obchodního tajemství, duševního vlastnictví, know-how nebo z důvodu ochrany osobních údajů třetích osob. Rovněž v případech, kdy by byl přístup žadatele k údajům omezen zvláštním právním předpisem.

Čl. 11

Právo na opravu

1. Za plnění povinností vyplývajících z uplatnění práva subjektu údajů na opravu údajů dle článku 16 GDPR odpovídá vedoucí zaměstnanec.
2. Při doručení žádosti o opravu vedoucí zaměstnanec neprodleně zajistí aktualizaci nebo doplnění zpracovávaných údajů.
3. Žadatel bude vedoucím zaměstnancem vyrozuměn o provedení opravy nebo doplnění osobních údajů.
4. Žádosti subjektů údajů vyřizuje vedoucí zaměstnanec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.

Čl. 12

Právo na výmaz (právo být zapomenut)

1. Za plnění povinností vyplývajících z uplatnění práva subjektů údajů na výmaz (právo být zapomenut) dle článku 17 GDPR odpovídá vedoucí zaměstnanec.
2. Vedoucí zaměstnanec neprodleně po doručení žádosti o výmaz posoudí, zda je požadavek oprávněný nebo zda existuje důvod k odmítnutí provedení výmazu dle článku 17 odst. 3 GDPR.
3. Vedoucí zaměstnanec vyrozumí žadatele o tom, zda bylo žádosti vyhověno nebo zda byla odmítnuta. V případě odmítnutí musí být rozhodnutí náležitě odůvodněno.
4. Právo na výmaz se provede v listinné podobě fyzickou skartací všech dokumentů, v elektronické podobě pak výmazem ze všech databází a datových nosičů.
5. Žádosti subjektů údajů vyřizuje vedoucí zaměstnanec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.

Čl. 13

Právo na omezení zpracování

1. Za plnění povinností vyplývajících z uplatnění práva subjektů údajů na omezení zpracování dle článku 18 GDPR odpovídá vedoucí zaměstnanec.
2. Vedoucí zaměstnanec posoudí oprávněnost obdrženého podání a vyrozumí žadatele o tom, zda bylo žádosti vyhověno nebo zda byla odmítnuta.
3. V případě oprávněnosti žádosti vedoucí zaměstnanec vhodným způsobem zajistí omezení zpracování.
4. V případě odmítnutí žádosti musí být takové rozhodnutí náležitě odůvodněno, a v případě, že bylo zpracování po dobu vyřizování žádosti subjektu omezeno, musí být subjekt údajů předem upozorněn na to, že bude omezení zpracování zrušeno.
5. Omezení zpracování musí být vyznačeno v databázi, ve které jsou údaje vedeny. V případě vedení údajů v listinné podobě musí být upozorněním na omezení zpracování označen příslušný spisový materiál.
6. Žádosti subjektů údajů vyřizuje vedoucí zaměstnanec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.

Čl. 14

Registr žádostí subjektů údajů a registr bezpečnostních incidentů

1. Vedoucí zaměstnanec vede registr žádostí subjektů údajů a registru bezpečnostních incidentů. Registry slouží pro vnitřní kontrolu správce a pro účely prokázání náležitého plnění povinností vyplývajících z nařízení dozorových orgánů.
2. V registru incidentů musí být uvedeny veškeré dostupné informace o incidentu, zejména pak popis jeho průběhu, datum a čas zjištění, způsob ohlášení, účinky a přijatá nápravná opatření.
3. V případě, že nebyl bezpečnostní incident hlášen dozorovému úřadu, bude v registru rovněž uvedeno odůvodnění tohoto postupu.
4. V případě nedodržení lhůty pro ohlášení bude v registru rovněž uvedeno náležité odůvodnění.

5. V případě, že nebyl bezpečnostní incident hlášen subjektům údajů, bude v registru rovněž uvedeno náležité odůvodnění tohoto postupu.
6. V registru žádostí subjektů se uvede, kdy byla žádost doručena, k uplatnění jakého práva směřovala a způsob a lhůty jejího vyřízení. U každé žádosti musí být rovněž uvedeno náležité odůvodnění způsobu vyřízení. Každá operace se žádostí subjektu bude označena datem, kdy byla provedena, aby bylo možné prokázat splnění jednotlivých lhůt.

Čl. 15

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

1. Za splnění oznamovací povinnosti dle článku 19 GDPR odpovídá vedoucí zaměstnanec.
2. Všechny postupy dle čl. 16 (právo na opravu), čl. 17 (právo na výmaz) a čl. 18 (právo na omezení zpracování) GDPR oznamuje vedoucí zaměstnanec všem příjemcům, jímž byly správcem dotčené osobní údaje poskytnuty.

Čl. 16

Právo vznést námitku

1. Za plnění povinností vyplývajících z uplatnění práva subjektů údajů na podání námitky dle čl. 21 GDPR odpovídá vedoucí zaměstnanec.
2. Vedoucí zaměstnanec neprodleně po doručení námitky posoudí její přiměřenost a důvodnost. Během tohoto hodnocení musí být zpracování omezeno na rozsah odpovídající účelu určení, výkonu nebo obhajoby právních nároků.
3. V případě vyhovění námitce bude zpracování údajů neprodleně ukončeno.
4. Žádosti subjektů údajů vyřizuje vedoucí zaměstnanec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.

Čl. 17

Odpovědnost správce

1. Správce odpovídá za zpracování údajů v souladu se základními zásadami dle článku 5 GDPR, dalšími právními předpisy a touto směrnicí. Kromě této směrnice může být bezpečnost zpracování osobních údajů a informací všeobecně upravena v ostatních interních předpisech správce.
2. Odpovědnost správce dle předchozího odstavce vykonává vedoucí zaměstnanec. Pravidelně monitoruje soulad této směrnice a dalších vnitřních předpisů správce s platnými předpisy a je povinen sledovat aktuální změny právní úpravy, rozhodovací praxi a proces tvorby nové právní úpravy v oblasti ochrany osobních údajů.

Čl. 18

Záměrná a standardní ochrana osobních údajů

1. Správce průběžně, dle momentální potřeby, aktualizuje technická a organizační opatření k zajištění ochrany osobních údajů.

2. Záměrnou ochranou se rozumí zohlednění a zapracování ochrany osobních údajů do přípravy nových postupů a opatření. Postupy ochrany osobních údajů začleňuje vedoucí zaměstnanec do přípravy všech procesů, v rámci kterých by mohly být zpracovávány osobní údaje.
3. Standardní ochranou osobních údajů se rozumí udržování zavedeného standardu ochrany, kdy zaměstnanci uplatňují zásady a principy ochrany osobních údajů při všech prováděných operacích zpracování. Tím se rozumí zejména dodržování povinností stanovených nejen touto směrnicí, ale rovněž GDPR a dalšími právními předpisy.

Čl. 19

Záznamy o činnostech zpracování

1. Správce vede záznamy o činnostech zpracování dle článku 30 GDPR. Záznamy o činnostech se vedou jednotlivě každým zaměstnancem pro agendu jím zpracovávanou. Záznamy o činnostech jsou dle potřeby aktualizovány vedoucím zaměstnancem.

Čl. 20

Zabezpečení zpracování

1. Zabezpečení zpracování údajů dle článku 32 GDPR kontroluje vedoucí zaměstnanec.
2. Vedoucí zaměstnanec dohlíží na aktuálnost organizačních a technických opatření k zabezpečení zpracování a uložení/archivace osobních údajů.
3. Pravidelně, nejméně však 1x do roka, kontroluje vedoucí zaměstnanec dodržování této směrnice, dalších vnitřních předpisů, GDPR a souvisejících předpisů.
4. Pravidelně, nejméně však 1x do roka, kontroluje vedoucí zaměstnanec aktuálnost této směrnice a dalších vnitřních předpisů, zejména s přihlédnutím k prováděným operacím zpracování, stavu techniky a možným rizikům pro práva a svobody subjektů údajů.

Čl. 21

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Vedoucí zaměstnanec provádí hlášení případů porušení zabezpečení osobních údajů (tzv. bezpečnostních incidentů) dozorovému úřadu dle článku 33 GDPR.
2. V případě vzniku bezpečnostního incidentu o něm zaměstnanec nebo zpracovatel, který incident zaznamená, neprodleně informuje vedoucího zaměstnance a sdělí mu veškeré potřebné informace.
3. Vedoucí zaměstnanec vyhodnotí, zda bezpečnostní incident může mít za následek riziko pro práva a svobody fyzických osob. V případě podezření na takové riziko ohlásí incident dozorovému úřadu v rozsahu stanoveném GDPR.
4. Pokud vedoucí zaměstnanec neprovede hlášení bezpečnostního incidentu dozorovému orgánu, řádně odůvodní, proč tento incident vyhodnotil jako nikoliv rizikový pro práva a svobody subjektů údajů.
5. Vedoucí zaměstnanec dbá na to, aby byla dodržena lhůta 72 hodin pro nahlášení. Lhůta se počítá od okamžiku zjištění bezpečnostního incidentu správcem. V případě, že hlášení nebude provedeno do 72 hodin, vedoucí zaměstnanec odůvodní důvody zpoždění.

Čl. 22

Ohlašování případů porušení zabezpečení osobních údajů subjektům údajů

1. Vedoucí zaměstnanec provádí hlášení bezpečnostních incidentů subjektům údajů dle článku 34 GDPR.
2. Vedoucí zaměstnanec v případě bezpečnostního incidentu vyhodnotí okolnosti tohoto incidentu a jeho možný vliv na práva a svobody subjektů údajů. V případě vysoké rizikovosti vyhodnotí rovněž aplikovatelnost výjimky dle článku 34 odst. 3 GDPR. Výjimky se uplatní v případě, že správce zavedl náležitá technická a organizační opatření ve vztahu k údajům dotčeným porušením zabezpečení, zavedl následné opatření k vyloučení možného rizika pro subjekty údajů, při nepřiměřeném úsilí apod. Aplikaci výjimky je vedoucí zaměstnanec povinen pečlivě zvážit a náležitě odůvodnit.

Čl. 23

Obnova dat ze záloh

1. Při obnově dat ze záloh je nutné provést aktualizaci osobních údajů podle aktuálního stavu. Při obnově zálohy nesmí dojít k obnovení osobních údajů, které byly dříve vymazány.

Čl. 24

Spolupráce se zpracovatelem osobních údajů

1. V případě uzavření smluvního vztahu se zpracovatelem musí být splněny požadavky článku 28 GDPR.
2. Smlouva se zpracovatelem musí být písemná a obsahovat předmět a dobu trvání zpracování, povahu a účel zpracování, typ osobních údajů a kategorie subjektů údajů, práva a povinnosti správce. Zpracovatel musí mít povinnost zpracovávat údaje výhradně na základě pokynů správce a musí mít povinnost zajistit, aby osoby údaje zpracovávající byly vázány smluvní nebo zákonnou mlčenlivostí. Zpracovatel musí být smluvně zavázán přijmout opatření k zabezpečení údajů dle čl. 32 GDPR, k dodržování podmínek pro zapojení dalšího zpracovatele, zohledňovat povahu zpracování a být správcei nápomocen při plnění povinností při uplatňování práv subjektů údajů. Zpracovatel musí být smluvně zavázán k provedení všech požadovaných operací, zejména pak k realizaci práva na opravu, výmaz, přístup či omezení zpracování. Zpracovatel musí být rovněž smluvně zavázán k umožnění auditů a inspekcí prováděných správcem.
3. Pokud již smluvní vztah se zpracovatelem existuje, kontroluje namátkově vedoucí zaměstnanec dodržování podmínek ochrany osobních údajů ze strany zpracovatele.