PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ V ORGANIZACI

(dále jako směrnice)

Tento dokument obsahuje pravidla pro ochranu osobních údajů v organizaci, a to v rámci požadavků, které jsou na organizaci, jakožto správce osobních údajů, kladeny NAŘÍZENÍM 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 (dále jen GDPR).

Tato směrnice stanovuje pravidla pro zpracování osobních údajů a také závazná pravidla a postupy pro zajištění jejich ochrany. Tato směrnice je zdrojem informací a závazných pravidel pro všechny zaměstnance organizace, a to tak, aby každá operace zpracování osobních údajů ve smyslu příslušných ustanovení GDPR a souvisejících právních předpisů, byla organizací, prostřednictvím jejích zaměstnanců, prováděna řádně a zákonným způsobem.

I. Definice

1. **Osobním údajem** je jakákoli informace, která dokáže žijící fyzickou osobu identifikovat přímo nebo je jejím účelem identifikace či dosažení takové osoby. Osobní údaje také někdy označujeme jako osobní data.

2. **Zvláštní kategorií osobních údajů** jsou údaje takového charakteru, které mohou subjekt údajů samy o sobě poškodit (např. ve společnosti, zaměstnání, škole) nebo mohou zapříčinit diskriminaci subjektů údajů. Pro zvláštní kategorii osobních údajů jsou stanoveny odlišné právní důvody jejich zpracování. Takovýmito osobními údaji jsou: biometrické údaje, informace o členství v odborové organizaci, členství v politické straně, etnický původ, filozofické vyznání, genetické údaje, informace o odsouzení, trestní delikty, náboženské vyznání, politické názory, rasový původ, sexuální orientace, sexuální život, zdravotní stav.

3. **Správcem osobních údajů** je taková osoba, která provádí zpracování osobních údajů. Správcem může být jak právnická, tak fyzická osoba. Správcem podle GDPR není fyzická osoba, která s osobními údaji nakládá pouze v rámci osobní nebo domácí činnosti.

4. **Zpracováním osobních údajů** je systematická činnost, kterou správce provádí s osobními údaji za určitým účelem. GDPR ve svém ustanovení čl. 4 odst. 1 stanoví neuzavřený výčet činností, které jsou zpracováním: shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

5. **Zpracovatelem** je osoba, která zpracovává osobní údaje pro správce. Může se jednat o fyzickou i právnickou osobu. O zpracovateli lze hovořit pouze ve vztahu k osobním údajům, které mu předal správce. Pokud tato osoba zpracovává údaje sama pro sebe, pak není zpracovatelem, ale správcem.

6. **Právním důvodem zpracování osobních údajů je** některý z typů oprávnění správce zpracovávat osobní údaje. Rovněž se používá pojem právní základ zpracování osobních údajů.

7. **Příjemcem** osobních údajů je osoba, které jsou osobní údaje poskytnuty, bez ohledu na to, zda s nimi nakládá jako správce nebo zpracovatel.

8. **Porušením zabezpečení** je taková situace, která vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

9. **Bezpečným heslem** se rozumí takové heslo, které se skládá nejméně z 10 znaků, přičemž musí obsahovat vždy nejméně jedno velké písmeno, jedno malé písmeno, jedno číslo a jeden speciální znak.

10. **Zpracovatelskou smlouvou** se rozumí právní vztah mezi správcem a zpracovatelem, při kterém dochází mj. ke zpracování osobních údajů. Nejedná se tedy o speciální smluvní typ

a platí, že každá smlouva uzavřená mezi organizací a externím subjektem, jejímž předmětem je zpracování osobních údajů tímto externím subjektem pro organizaci, je zpracovatelskou smlouvou (např. i smlouva o vedení účetnictví a mzdové agendy).

II. Zásady GDPR

1. Každý zaměstnanec, který při výkonu své práce přijde jakkoli do styku s osobními údaji, je povinen dodržovat níže popsané zásady ochrany osobních údajů, které plynou z příslušných ustanovení GDPR.

2. **Zákonnost**
   Správce, k tomu, aby mohl zpracovávat osobní údaje, potřebuje vždy nejméně jeden z právních důvodů (dále jsou také označovány jako právní základy zpracování osobních údajů). Pokud takový právní důvod neexistuje, pak nezpracovává osobní údaje v souladu s právním předpisem, tzn. zpracovává je nezákonně. Podrobnější informace k této zásadě jsou uvedeny v článcích 6 a 9 GDPR.

3. **Korektnost a transparentnost**
   Podle článku 5 GDPR musí být správce ohledně zpracování osobních údajů velice otevřený, přičemž podrobnější povinnosti jsou pak stanoveny v článcích 12 – 14 GDPR. Subjekty údajů mají právo být informovány o tom, jak je s jejich osobními údaji nakládáno. Jinými slovy to znamená, že správce je povinen jim sdělit: jaká osobní data o nich sbírá, co s nimi dělá a s kým je sdílí.

4. **Přesnost**
   V souladu se zásadou přesnosti musí být osobní údaje, které správce zpracovává, přesné. Správce má rovněž povinnost aktivně se přičinit o to, aby byly tyto osobní údaje stále aktuální. Neznamená to, že by měl správce kontaktovat subjekt údajů primárně pouze proto, aby si ověřoval správnost zpracovávaných osobních dat, ale bude-li už se subjektem údajů z nějakého důvodu v kontaktu, tak by si měl ověřit jejich aktuálnost.

5. **Minimalizace údajů**
   Osobní údaje musí být relevantní a přiměřené ve vztahu k účelu, pro který jsou zpracovávány. Jinými slovy lze říci, že správce má zpracovávat pouze takové osobní údaje, které pro konkrétní účel nezbytně nutně potřebuje.

6. **Odpovědnost**
   Zásada odpovědnosti znamená, že správce odpovídá za dodržení všech povinností, které mu GDPR ukládá a zároveň musí být schopen prokázat, že všechny tyto povinnosti dodržuje.

7. **Omezení účelem**
   Osobní údaje mohou být shromažďovány pouze pro určité účely a nesmí být zpracovávány v rozporu s těmito účely. Pokud jsou údaje zpracovávány pro konkrétní účel, nelze je zpracovávat pro jiný účel, který není slučitelný s účelem původním.

8. **Omezení uložení**
   Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu a pro účely, pro které jsou zpracovávány. Zjednodušeně lze říct, že pokud správce osobní údaje už pro daný účel nepotřebuje, nesmí je dále zpracovávat. Samozřejmě to nemá vliv např. na archivační povinnost, kterou může správci stanovit některý právní předpis.

9. **Integrita a důvěrnost**
   Zásada integrity a důvěrnosti stanoví správci povinnosti přijmout taková organizační a technická opatření, aby zajistil minimalizaci rizika, že budou osobní údaje zpracovávány protiprávně nebo neoprávněně. Zároveň musí zajistit, že osobní údaje budou chráněny před zničením, poškozením nebo ztrátou.

III. Práva subjektů údajů

1. Subjektům údajů musí být umožněn výkon jejich níže uvedených práv, a to bezplatně. Úhradu za výkon práv lze vyžadovat pouze v případě, že subjekt údajů práva zneužívá nebo se chová šikanózním způsobem. Jedná se zejména o případy zjevného nadužívání výkonu práv ze strany subjektu údajů.

2. **Právo na přístup k osobním údajům**
   Subjekt údajů má právo na to, aby mu správce poskytl informace, zda zpracovává nebo nezpracovává jeho osobní údaje. V případě, že správce osobní údaje zpracovává, pak má právo na to, aby mu správce sdělil:
   - za jakým účelem jeho osobní údaje zpracovává,
   - v jakém rozsahu jsou tyto údaje zpracovávány,
   - jak dlouho budou uchovávány,
   - komu budou zpřístupněny,
   - zda dochází k automatickému rozhodování,
   - informaci o tom, že může podat stížnost u dozorového orgánu.

   Právo na přístup k osobním údajům je limitováno právem duševního vlastnictví organizace. To znamená, že pokud by organizace jakožto správce poskytnutím informací nutně sdělila i část svého know-how a tyto informace od sebe nejdou oddělit, pak není povinna subjektu údajů vyhovět. Právě uvedené v organizaci posuzuje osoba určená pro dohled nad ochranou osobních údajů, a to ve spolupráci s pověřencem pro ochranu osobních údajů, je-li jmenován.

3. **Právo na přesnost**
   Subjekt údajů, pokud se domnívá, že správce zpracovává jeho nepřesné osobní údaje, má právo na jejich opravu. To znamená, že v případě, kdy subjekt údajů nepřesnost zjistí a upozorní na to správce, má správce povinnost údaje opravit.

4. **Právo být zapomenut (právo na výmaz)**
   K právu na výmaz osobních údajů se váže povinnost správce bez zbytečného odkladu zlikvidovat zejména takové údaje, které:
   - správce již pro konkrétní účel nepotřebuje,
   - jsou zpracovávány bez relevantního právního základu,
   - jsou zpracovávány protiprávně,
   - proti jejichž zpracování byly vzneseny námitky a neexistují převažující oprávněné důvody pro jejich zpracování,
   - musí být ze zákona likvidovány povinně.

5. **Právo na přenositelnost údajů**
   V případě, že správce zpracovává osobní údaje automatizovaně (tj. strojově čitelně a strukturovaně - jedná se o výstupy databázových souborů např. .json, .csv apod.), má subjekt údajů právo správce požádat, aby osobní údaje byly předány jinému správci. Musí se jednat o osobní údaje, které splňují následující:
   - údaje aktivně poskytl správci sám subjekt údajů
     a
   - zpracování je založeno na těchto právních důvodech: souhlas nebo smlouva.

6. **Právo nebýt předmětem automatizovaného rozhodování**
   Subjekt údajů má právo na to, aby o něm nebylo rozhodováno automatizovaně, tedy bez lidského prvku.

7. **Právo na omezení zpracování**
   Po dobu, než správce rozhodne o námitce subjektu údajů (tedy ve sporných případech), má subjekt údajů právo na to, aby byly jeho osobní údaje v režimu omezeného zpracování.

8. Zaměstnanci jsou povinni zajistit, že pro případ, kdy subjekt údajů uplatní některé ze svých práv, bude na toto uplatnění práva zareagováno nejpozději do 1 měsíce. Tuto lhůtu je možné v závažných případech prodloužit až o 2 měsíce, ale platí, že o tomto je třeba v jednoměsíční lhůtě informovat subjekt údajů a zároveň je nutné subjektu údajů sdělit odůvodnění takového prodloužení lhůty.

IV. Právní základy zpracování osobních údajů

1. Aby byl splněn požadavek GDPR na zákonnost každého zpracování osobních údajů vyjádřený v článku 5 odst. 1 písm. a), jsou zaměstnanci povinni zajistit, aby, ke každé operaci zpracování osobních údajů, organizace disponovala vždy nejméně jedním z právních základů zpracování. Pokud organizace žádným takovým právním důvodem

nedisponuje, pak nejsou v rámci dané operace zpracování osobní údaje zpracovávány zákonně a je nutné tyto osobní údaje dále nezpracovávat, případně provést jejich likvidaci.

2. Právní základy zpracování osobních údajů pro obecné osobní údaje jsou: souhlas, plnění smlouvy, plnění právní povinnosti, životně důležitý zájem, úkol ve veřejném zájmu nebo výkon veřejné moci, oprávněný zájem. Podrobnosti pro jednotlivé dílčí právní důvody stanoví GDPR v článku 6.

3. Právními základy zpracování osobních údajů pro zvláštní kategorii osobních údajů jsou: výslovný souhlas, plnění povinností a výkon práv v oblasti sociálního zabezpečení a sociálního práva, ochrana životně důležitých zájmů subjektů údajů nebo jiných fyzických osob, oprávněné činnosti nadací, sdružení či jiných neziskových organizací sledujících politické, odborové, filozofické nebo náboženské cíle, údaje zjevně zveřejněné subjektem údajů, určení, výkon nebo obhajoba právních nároků a výkon soudních pravomocí, významný veřejný zájem na základě unijního nebo vnitrostátního práva, zdravotní a sociální péče, veřejný zájem v oblasti veřejného zdraví, archivace, vědecký nebo historický výzkum a statistika. Podrobnosti pro jednotlivé dílčí právní důvody stanoví GDPR v článku 9.

V. Bezpečnost zpracovávaných osobních údajů

1. Osobní údaje, které organizace zpracovává a ukládá na technických či jiných prostředcích, musí být chráněny takovým způsobem, který odpovídá jejich povaze.

2. Osobní údaje v listinné podobě jsou uchovávány v uzamykatelných skříních (případně v trezorech) v prostorách, jejichž ochrana odpovídá povaze uchovávaných osobních údajů.

3. Nezašifrovaná datová média obsahující osobní údaje jsou uchovávána v uzamykatelných skříních (případně v trezorech) v prostorách, jejichž ochrana odpovídá povaze uchovávaných osobních údajů.

4. Osobní údaje v elektronické podobě mohou být na pracovních počítačích a serverech, přičemž je zvolena různá kategorizace přístupových práv (toto je zabezpečeno uživatelským jménem a heslem, přičemž tyto údaje jsou nepřenositelné), je používán firewall a antivirový program. V případě, že se na pracovních počítačích a serverech nacházejí citlivé osobní údaje, pak tyto zařízení musí být šifrovány.

5. Všichni zaměstnanci organizace musí dodržovat tzv. zásadu prázdného stolu a prázdné obrazovky, které znamenají, že osobní údaje v listinné podobě budou ihned po vytištění odebrány z tiskárny a uchovávány v souladu ust. čl. V. odst. 2 této směrnice; nepoužívaná datová média obsahující osobní údaje budou uchovávány v souladu s ust. čl. V. odst. 3 této směrnice; nepoužívané zapnuté pracovní počítače nesmí být ponechány bez dozoru a zaměstnanci jsou při odchodu z pracoviště povinni tyto počítače chránit heslem.

6. Jakákoli zařízení obsahující osobní údaje, která jsou v majetku organizace musí být při vynášení z prostor organizace evidována. Evidenci provádí pověřený zaměstnanec,

přičemž tato evidence obsahuje alespoň: specifikaci zařízení; specifikaci osoby, která zařízení převzala; datum a podpis osoby, která zařízení převzala.

VI. Bezpečnost předávání a přenášení osobních údajů

1. Jsou-li osobní údaje předávány interní elektronickou poštou organizace, pak nemusí být šifrovány nebo jinak zabezpečeny, to však pouze za předpokladu, že je zamezeno automatickému přesměrování uživatelských schránek na e-mailové adresy mimo organizaci.

2. Jsou-li osobní údaje předávány elektronickou poštou mimo organizaci, pak musí být šifrovány nebo alespoň zabezpečeny bezpečným heslem.

3. Elektronický přenos osobních údajů by měl být zabezpečen uznávanými kryptografickými prostředky (např. protokoly SSH, FTPS, HTTPS apod).

4. Přenáší-li zaměstnanec organizace osobní údaje v listinné podobě nebo na nezašifrovaných elektronických zařízeních (datových médiích), pak platí, že tyto nosiče osobních údajů nesmí nechat volně ležet bez dozoru (např. v zaparkovaném automobilu apod.).

VII. Organizační opatření

1. Všichni zaměstnanci organizace berou na vědomí, že jsou přijata následující organizační opatření, přičemž každý zaměstnanec je povinen se jimi řídit, tj. dodržovat povinnosti, která jsou v nich stanovena.

2. Přijatá organizační opatření:
    - Vnitro-organizační dokumenty:
        - Zásady ochrany osobních údajů (pro splnění povinnosti informovat subjekty údajů vně organizace o rozsahu zpracování osobních údajů);
        - Tato směrnice;
        - Archivační a skartační řád (vychází z těchto předpisů: Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, Zákon č. 496/2004 Sb., o elektronických podatelnách, ve znění pozdějších předpisů, Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, Zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů);
    - Ustanovení o mlčenlivosti v pracovních smlouvách;
    - Smlouvy se zpracovateli splňují minimální požadovaný standard předpokládaný ust. čl. 28 an. GDPR;
    - Pravidelná školení klíčových zaměstnanců, kteří při výkonu své práce přijdou do styku s osobními údaji subjektů údajů;

- Metodika pro provádění vnitřních auditů ve vztahu k ochraně osobních údajů.

VIII. Technická opatření

1. Všichni zaměstnanci organizace berou na vědomí, že jsou přijata následující technická opatření, přičemž každý zaměstnanec je povinen je dodržovat.

2. Přijatá technická opatření:
   - Možnost likvidace všech dat v elektronických zařízeních (notebook, tablet, telefon) dálkově, a to pro případ ztráty či odcizení takového zařízení;
   - Využívání vlastního serveru (lokálního) při použití bezpečnostních záloh;
   - Pro informační systém je zvolena různá kategorizace přístupových práv (zabezpečeno uživatelským jménem a heslem, přičemž tyto údaje jsou nepřenositelné);
   - Firewall a antivirový program;
   - Šifrování používaných elektronických zařízení (je-li to z jejich povahy možné).

IX. Pravidla pro uzavírání zpracovatelských smluv

1. Uzavírá-li zaměstnanec za organizaci smlouvu se zpracovatelem a/nebo se účastní procesu kontraktace v kterékoli jeho fázi, tak je povinen zajistit, aby zpracovatelská smlouva obsahovala alespoň ustanovení o tom, že:
   a. Zpracovatel je povinen jednat výhradně v souladu s pokyny správce (pokud mu určité jednání nestanoví zvláštní právní předpis).

   b. Zpracovatel přijme veškerá nezbytná technická a organizační opatření k tomu, aby zajistil minimalizaci rizika, resp. zajistil, že budou osobní údaje chráněny před zničením, poškozením, zneužitím nebo ztrátou. Toto ustanovení bude obsahovat rovněž výčet použitých organizačních a technických opatření, která zpracovatel použije.

   c. Zpracovatel zapojí do zpracování pouze takové osoby (další zpracovatele nebo zaměstnance), které se zavázaly k mlčenlivosti nebo na které se vztahuje zákonná mlčenlivost.

   d. Zpracovatel je oprávněn zapojit do zpracování další zpracovatele (tj. subzpracovatele) pouze za předpokladu, že mu k tomu dá správce písemný souhlas a zároveň tento vztah (zpracovatele a subzpracovatele) bude založen smlouvou v písemné podobě.

   e. Zpracovatel je povinen poskytnout správci veškerou nezbytnou součinnost k tomu, aby bylo možné zajistit subjektům údajů nerušený výkon jejich práv dle příslušných ustanovení GDPR.

   f. Zpracovatel je povinen poskytnout správci veškerou nezbytnou součinnost při plnění povinnosti ohlašovat případy porušení zabezpečení osobních údajů Úřadu

na ochranu osobních údajů a povinnost oznamování případů porušení zabezpečení osobních údajů subjektům údajů, tak aby byla splněna lhůta požadovaná v článku 33 GDPR.

g. Zpracovatel je povinen, po zániku smluvního vztahu mezi ním a správcem, zlikvidovat osobní údaje, které mu byly předány ke zpracování, samozřejmě za předpokladu, že právní předpis nestanoví něco jiného.

h. Zajištění splnění povinností zpracovatele smluvní pokutou.

i. Stanovení možnosti správce, aby si ověřil, že zpracovatel postupuje v souladu se svými povinnostmi, které mu stanoví GDPR a zpracovatelská smlouva. Pro tento případ lze sjednat povinnost zpracovatele umožnit správci provést v jeho organizaci audit procesu nakládání s osobními údaji, které mu byly správcem svěřeny.

X. Pravidla pro bezpečnou archivaci a skartaci osobních údajů

1. Jsou-li osobní údaje archivovány v elektronické podobě, musí být pro archivaci využita taková technologie, která zajistí nezbytnou dobu trvanlivosti.

2. V případě, že jsou osobní údaje archivovány v souladu s předchozím odstavcem, avšak v zašifrované podobě, pak musí být rovněž zajištěna dostupnost hesla nebo dešifrovacího klíče.

3. Likvidace osobních údajů uložených v listinné podobě nebo na médiích typu CD, DVD, HDD, musí být provedena mechanicky (např. využitím speciálního skartovacího stroje), a to takovým způsobem, aby byla znemožněna jakákoli obnova zlikvidovaných osobních údajů.

4. O provedené archivaci nebo likvidaci osobních údajů bude pověřeným zaměstnancem sepsán protokolární záznam.

XI. Řešení porušení zabezpečení zpracování osobních údajů

1. V případě, že v organizaci dojde k situaci, z jejíchž okolností zaměstnanec dovozuje, že se jedná o porušení zabezpečení osobních údajů, je tento zaměstnanec povinen uvědomit svého vedoucího a zaměstnance, jehož náplní práce je mj. i problematika ochrany osobních údajů (dále odpovědný zaměstnanec). O této skutečnosti bude rovněž informován pověřenec pro ochranu osobních údajů, je-li jmenován.

2. Odpovědný zaměstnanec (ve spolupráci s pověřencem pro ochranu osobních údajů) vyhodnotí, zda se skutečně jedná o porušení zabezpečení osobních údajů. Následně posuzuje intenzitu rizika případného porušení zabezpečení pro práva a svobody fyzických osob.

3. V souladu s čl. 33 odst. 1 GDPR odpovědný zaměstnanec bez zbytečného odkladu (nejpozději do 72 hodin od chvíle, co se o porušení zabezpečení dozvěděl kterýkoli ze

zaměstnanců), ohlásí Úřadu na ochranu osobních údajů jakékoli porušení zabezpečení zpracování osobních údajů. Ohlášení dle předchozí věty nemusí učinit pouze v případě, kdy je nepravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob (např. ztracené elektronické zařízení je šifrováno). Předpřipravený (vzorový) dokument ohlášení porušení zabezpečení dle čl. 33 GDPR je součástí této směrnice a je označen jako Příloha 1.

4. V souladu s čl. 34 GDPR je odpovědný zaměstnanec povinen oznámit porušení zabezpečení osobních údajů dotčeným subjektům údajů, a to za předpokladu, že případné porušení zabezpečení může mít za následek vysoké riziko pro práva a svobody fyzických osob. Pro případ posouzení míry rizika bude odpovědný zaměstnanec vycházet z připravené analýzy rizik. Předpřipravený (vzorový) dokument pro oznámení porušení zabezpečení dle čl. 34 GDPR je součástí této směrnice a je označen jako Příloha 2.

5. Bez ohledu na to, zda bude třeba učinit nějaké z opatření dle čl. 33 a/nebo čl. 34 GDPR, je odpovědný zaměstnanec povinen provést záznam takové bezpečnostní události v interním registru porušení zabezpečení zpracování osobních údajů. Šablona interního registru porušení zabezpečení je součástí této směrnice a je označena jako Příloha 3.

XII. Pravidla vzdělávání v oblasti ochrany osobních údajů

1. Organizace pro své zaměstnance (kteří při výkonu své práce přijdou do styku s osobními údaji) zajišťuje, nejméně jednou ročně, školení v oblasti problematiky ochrany osobních údajů, a to na svůj vlastní náklad.

2. Každý zaměstnanec je tedy povinen každoročně absolvovat školení v rozsahu nejméně 5 hodin.

3. Organizace jakožto zaměstnavatel vede záznamy o proškolení toho kterého zaměstnance, který má povinnost školení absolvovat, a to především s ohledem na druh jím vykonávané práce.

XIII. Závěrečná ustanovení

1. Tato směrnice je závazná pro všechny zaměstnance organizace.

2. Tato směrnice nabývá účinnosti dnem [uvést datum].

PŘÍLOHA 1

[Specifikace správce]

_____

Úřad na ochranu osobních údajů
Pplk. Sochora 727/27
170 00 Praha 7 – Holešovice

[Vybrat: Doporučeně / datovou zprávou]

V [město] dne [datum]

Ohlášení případu porušení zabezpečení osobních údajů podle článku 33 obecného nařízení o ochraně osobních údajů

Tímto dáváme shora nadepsanému dozorovému orgánu na vědomí, že v naší organizaci došlo k případu porušení zabezpečení osobních údajů dle článku 33 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).

Porušení zabezpečení osobních údajů spočívalo v tomto:
[Co možná nejpodrobněji, s ohledem na okamžik, kdy tuto skutečnost dáváte na vědomí, specifikujte porušení zabezpečení. Pokud možno uveďte i konkrétní časy.]

Výše specifikované porušení zabezpečení osobních údajů se týkalo [uvést počet subjektů údajů, jichž se toto porušení zabezpečení týká] subjektů údajů, přičemž předmětné zpracování osobních údajů [Vybrat: zahrnovalo / nezahrnovalo] zvláštní kategorii osobních údajů.

Je pravděpodobné, že uvedené porušení zabezpečení osobních údajů může pro dotčené subjekty údajů znamenat tyto důsledky:
[Specifikovat možná rizika a jejich dopady na subjekty údajů].

Abychom minimalizovali riziko obdobného porušení zabezpečení osobních údajů do budoucna, přijali jsme následující organizační a technická opatření:
[Specifikovat organizační a technická opatření].

Bližší informace stran tohoto bezpečnostního incidentu vám poskytne náš pověřenec pro ochranu osobních údajů /*není-li v organizaci pověřenec jmenován, pak uveďte kontaktní místo, které může poskytnout bližší informace:

[Uvést kontaktní údaje na pověřence/jinou osobu – e-mailovou adresu, telefonní číslo, korespondenční adresu].

Za [specifikovat správce]:
[jméno a příjemní]
[role ve společnosti]
[kontaktní informace]

PŘÍLOHA 2

Vzor oznámení případu porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 GDPR

Vážený/a [Specifikovat subjekt údajů],

bohužel, Vás touto cestou musíme informovat o tom, že v naší organizaci došlo k porušení zabezpečení zpracování osobních údajů, které obsahovalo rovněž Vaše osobní údaje.

O tomto jsme samozřejmě neprodleně informovali Úřad na ochranu osobních údajů a aktuálně pracujeme na nápravě, přičemž činíme vše pro to, abychom jakékoli další porušení zabezpečení do budoucna minimalizovali.

Co se stalo?
Došlo k následující události: [Popsat, co se stalo]

V dotčeném okruhu zpracování osobních údajů byly zahrnuty tyto Vaše osobní údaje: [specifikovat typy dotčených osobních údajů: např. jméno a příjmení, rodné číslo, podobizna, kopie občanského průkazu apod.]

Co to pro Vás znamená?
S ohledem na povahu porušení zabezpečení zpracování, a kategorii osobních údajů, které byly v rámci dotčeného zpracování zpracovávány se domníváme, že tento incident pro Vás může mít tyto následky: [Pokuste se popsat následky, které pro subjekt údajů připadají v úvahu. Rovněž připište doporučení, co by měl subjekt údajů udělat – např. změnit heslo, vyhledat právní pomoc apod.]

Jak obdobným incidentům předejdeme do budoucna?
Abychom zabránili opakovanému narušení zabezpečení zpracování a minimalizovali dopad na naše [vybrat dotčený subjekt údajů: klienty/zákazníky, dodavatele, zaměstnance], přijali jsme tato technická a organizační opatření a provedli následující kroky: [popsat použitá opatření, včetně toho, co organizace zatím pro prevenci učinila].

Pro úplnost upozorňujeme, že Vám v této věci již nebudeme zasílat další zprávy. Aktuální informace o řešeném bezpečnostním incidentu naleznete na našich webových stránkách pod tímto odkazem [Doplnit odkaz na web].

Bližší informace stran tohoto bezpečnostního incidentu vám poskytne náš pověřenec pro ochranu osobních údajů /*není-li v organizaci pověřenec jmenován, pak uveďte kontaktní místo, které může poskytnout bližší informace:

[Uvést kontaktní údaje na pověřence/jinou osobu – e-mailovou adresu, telefonní číslo, korespondenční adresu].

Závěrem se Vám velice omlouváme za způsobené potíže. Vězte prosím, že uděláme vše, co bude v našich silách, abychom zajistili, že se podobná situace v budoucnu nebude opakovat.

Za [specifikovat správce]:
[jméno a příjemní]
[role ve společnosti]
[kontaktní informace]

PŘÍLOHA 3

INTERNÍ REGISTR PORUŠENÍ ZABEZPEČENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pořadové číslo	**Datum vzniku**	**Popis události**	**Pověřenec pro ochranu osobních údajů/pověřená osoba (včetně e-mailu)**	**Popis pravděpodobných následků porušení**	**Vyhodnocení události (*zda jde o porušení zabezpečení a jaká je míra rizika pro práva a svobody subjektů údajů*)**	**Nápravná opatření (včetně informací o oznámení/ohlášení)**