COMPEKO BREZNO, s.r.o.,
Štúrova 8, 977 01 Brezno

SMERNICA
O SPRACOVANÍ OSOBNÝCH ÚDAJOV

Pre

OBEC ČUČMA

V Brezne, dňa 21.5.2018

Vypracoval: Mgr. Dušan Kusenda, projektový manažér

Obsah

1. Úvod 3
2. Cieľ a rozsah smernice 3
3. Základné pojmy 4
   3.1. Čo je osobný údaj? 4
   3.2. Čo je spracúvanie osobných údajov? 4
   3.3. Účel spracúvania osobných údajov 4
   3.4. Informačný systém 4
   3.5. Prevádzkovateľ 4
   3.6. Sprostredkovateľ 4
   3.7. Dotknutá osoba 4
   3.8. Oprávnená osoba 4
   3.9. Príjemca 5
   3.10. Tretia strana 5
   3.11. Súhlas dotknutej osoby 5
4. Informačné systémy 5
5. Subjekty pracujúce s informačnými systémami 5
6. Organizačné a technické opatrenia na zabezpečenie primeranej ochrany osobných údajov 5
   6.1. Práva oprávnenej osoby 5
   6.2. Povinnosti oprávnenej osoby 6
   6.3. Podmienky spracúvania osobných údajov 7
   6.4. Povinnosti vedúcich pracovníkov 8
   6.5. Povinnosti IT správcu 8
   6.6. Povinnosti zodpovednej osoby 9
7. Riešenie úniku osobných údajov 10
8. Zodpovednosť za porušenie práv a povinností 11
9. Prílohy 11

1. Úvod

Zákon o ochrane osobných údajov vychádza zo všeobecného nariadenia EU na ochranu osobných údajov (skratka GDPR). Týka sa všetkých, ktorí vlastnia alebo spracúvajú osobné údaje. Definuje práva občanov EU, ktorých sa údaje týkajú. Zároveň prevádzkovateľom a sprostredkovateľom týchto údajov stanovuje ich povinnosti.

Spracovaním osobných údajov sa rozumejú operácie alebo súbor operácií s osobnými údajmi. Môžu byť vykonávané ručne alebo pomocou automatizovaných postupov. Na spracovaní osobných údajov sa môžu podieľať dva subjekty: prevádzkovateľ a sprostredkovateľ. Prevádzkovateľ je ten, kto údaje získava, využíva a sám alebo spolu s ďalšími osobami určuje účel s spôsob spracovania. Sprostredkovateľom je ten, kto údaje v mene prevádzkovateľa spracúva, napr. účtovná spoločnosť.

Dôležité je, že prevádzkovateľ aj sprostredkovateľ sú povinní zrealizovať také technické a organizačné opatrenia, aby zabezpečili úroveň zabezpečenia zodpovedajúcu možnému riziku.

2. Cieľ a rozsah smernice

Spoločnosť vydáva túto smernicu s cieľom:

- zabezpečenia primeranej ochrany osobných údajov
- zamedzenia získavania osobných údajov fyzických osôb nad rozsah potrieb účelu ich spracúvania
- zabezpečenia záväzných pravidiel ich spracúvania a zabezpečenia ochrany pred zneužitím osobných údajov po skončení účelu, na ktorý boli získavané.

Táto smernica upravuje základné pravidlá pre zabezpečenie bezpečnej a spoľahlivej prevádzky automatizovaných a neautomatizovaných prostriedkov spracúvania osobných údajov v informačných systémoch prevádzkovateľa.

Smernica je záväzná pre všetkých zamestnancov prevádzkovateľa v rozsahu zodpovednosti vyplývajúcej z ich pracovného zaradenia alebo poverenia, pracovnej zmluvy, pracovnej náplne ako aj pre všetkých externých spolupracovníkov vykonávajúcich činnosť na základe iných právnych skutočností a zmlúv.

3. Základné pojmy

3.1. Čo je osobný údaj?

Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

3.2. Čo je spracúvanie osobných údajov?

Spracúvaním osobných údajov je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

3.3. Účel spracúvania osobných údajov

Účel spracúvania osobných údajov je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

3.4. Informačný systém

Informačný systém je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií.

3.5. Prevádzkovateľ

Prevádzkovateľ je ten, kto údaje získava a využíva. Určuje účel a spôsob spracovania.

3.6. Sprostredkovateľ

Sprostredkovateľom je ten, kto údaje v mene prevádzkovateľa spracúva, napr. účtovná spoločnosť.

3.7. Dotknutá osoba

Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

3.8. Oprávnená osoba

Podľa predchádzajúceho zákona O ochrane osobných údajov z r. 2013 budeme naďalej používať pojem „Oprávnená osoba". Je to zamestnanec prevádzkovateľa, ktorý prichádza do styku s osobnými údajmi.

3.9. Príjemca

Príjemcom je každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou. Za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu.

3.10. Tretia strana

Treťou stranou je každý, kto nie je dotknutou osobou, prevádzkovateľom, sprostredkovateľom alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

3.11. Súhlas dotknutej osoby

Súhlasom dotknutej osoby je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.

4. Informačné systémy

Spoločnosť je prevádzkovateľom viacerých informačných systémov, ich zoznam aj podrobné informácie o nich tvoria prílohu č. 1 tohto dokumentu.

5. Subjekty pracujúce s informačnými systémami

S informačnými systémami pracujú jednotlivé subjekty (oprávnené osoby prevádzkovateľa, sprostredkovatelia, tretie strany). Ich aktuálny stav je zachytený v prílohe č. 2 tohto dokumentu.

6. Organizačné a technické opatrenia na zabezpečenie primeranej ochrany osobných údajov

6.1. Práva oprávnenej osoby

Oprávnená osoba má právo vykonávať spracovateľské operácie s osobnými údajmi spracúvanými v informačných systémoch osobných údajov prevádzkovateľa výlučne v súlade s právnym základom, od ktorého prevádzkovateľ odvodzuje oprávnenie spracúvať osobné údaje, a to len v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo vymedzeného účelu spracúvania a je v súlade so

zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi predpismi a internými riadiacimi aktmi prevádzkovateľa.

Oprávnená osoba má právo na:

- pridelenie prístupových práv do určených informačných systémov osobných údajov prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej úloh,
- opätovné poučenie, ak došlo k podstatnej zmene jej pracovného zaradenia alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného zaradenia,
- porušenie povinnosti mlčanlivosti uloženej podľa, ak je to nevyhnutné na plnenie úloh súdov a orgánov činných v trestnom konaní alebo vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky pri plnení jeho úloh,
- vykonávanie spracovateľských operácií s osobnými údajmi v mene prevádzkovateľa v rozsahu nevyhnutnom na plnenie pracovných úloh určených pracovnou zmluvou,
- odmietnutie vykonať pokyn na spracúvanie osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
- ak je oprávnenou osobou štatutárny orgán, vyžadovať od kontrolného orgánu preukázať sa poverením na vykonanie kontroly a svojou príslušnosťou k úradu, oboznamovať sa s kontrolnými zisteniami a písomne sa k nim vyjadrovať, podávať písomné námietky po oboznámení sa s kontrolnými zisteniami, vyžadovať plnenie povinností kontrolného orgánu pri výkone kontroly

6.2. Povinnosti oprávnenej osoby

Oprávnená osoba je povinná:

- získavať na základe svojho pracovného zaradenia pre prevádzkovateľa len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel,
- vykonávať povolené spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
- pri získavaní osobných údajov od dotknutej osoby oboznámiť ju o jej právach, údajoch o prevádzkovateľovi, účele spracúvania osobných údajov, rozsahu spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov, pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú, podľa prílohy č. 4,
- zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov prevádzkovateľa, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby,
- zabezpečiť právo dotknutej osoby na opravu svojich osobných údajov, tj. nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť je povinná blokovať, kým sa rozhodne o ich likvidácii,

- získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania,
- vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov prevádzkovateľa,
- v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na vedúceho pracovníka,
- chrániť prijaté dokumenty a súbory pred stratou, poškodením a zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,
- dodržiavať mlčanlivosť o osobných údajoch, s ktorými oprávnená osoba v rámci svojho pracovného pomeru prichádza do styku,
- vo vzťahu ku kontrole je oprávnená osoba kontrolovaného prevádzkovateľa povinná najmä poskytnúť úradu potrebnú súčinnosť pri výkone jeho dozoru,
- ak je oprávnenou osobou štatutárny orgán, vo vzťahu ku kontrole, sa dostaviť na predvolanie úradu s cieľom podať vysvetlenia v určenom čase na určené miesto, umožniť kontrolnému orgánu výkon iných oprávnení, oboznámiť sa s obsahom protokolu a na požiadanie kontrolného orgánu dostaviť sa na jeho prerokovanie,
- oprávnená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, či potrebu inej osoby alebo na iné, ako služobné účely podľa tohto záznamu.

6.3. Podmienky spracúvania osobných údajov

Pri spracúvaní osobných údajov neautomatizovaným spôsobom (listová forma spracúvaných osobných údajov) oprávnená osoba najmä:

- zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
- neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
- odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
- zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
- pri skončení pracovného pomeru je oprávnená osoba povinná odovzdať vedúcemu pracovníkovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje,
- v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlače neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť

ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním,
- uzamyká kanceláriu pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa,

Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania oprávnená osoba najmä:

- využíva služby Internetu za účelom plnenia pracovných úloh,
- nepoužíva verejné komunikačné systémy na rýchly prenos správ (ICQ, AOL, IRC a pod.),
- umiestňuje informačnú techniku (počítače, notebooky, USB kľúč, a pod.) iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode oprávnenej osoby uzamknutá a po skončení pracovnej doby je oprávnená osoba povinná vypnúť počítač a uzamknúť skrine s materiálmi obsahujúcimi osobné údaje,
- dbá na antivírusovú ochranu pracovných staníc,
- berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,
- dôsledne dodržiava pravidlá ochrany prístupových práv.

6.4. Povinnosti vedúcich pracovníkov

Vedúci pracovník je povinný:

- pri zmene zákona, nástupe nového pracovníka do pracovného pomeru, pri zmene pracovného zaradenia oboznámiť pracovníka s touto smernicou. O oboznámení pracovníka so smernicou vyhotoviť písomný zápis,
- primerane zabezpečiť objekt a prideliť kľúče od vstupu do objektu,
- pri zmene zaradenia pracovníka dať požiadavku na správcu IT na aktualizáciu prístupových práv a v prípade ukončenia pracovného pomeru rozhodnúť o naložení s údajmi na PC,
- dbať o trvalú úroveň vedomostí oprávnených osôb potrebných pre bezpečnú a spoľahlivú prácu s osobnými údajmi,
- zabezpečiť údržbu a upratovanie chránených priestorov (priestor, kde sa nachádza server),
- zabezpečiť pravidelnú kontrolu bezpečnostných opatrení, o kontrole vykonať písomný záznam,
- zmluvne zabezpečiť prístupy mimo lokálnej siete pre tretie strany, napr. pri servise IT.

6.5. Povinnosti IT správcu

IT správca je povinný:

- prideľovať prístupové práva pracovníkom podľa ich zaradenia, pre prípad núdze sú heslá uložené v zalepenej obálke na bezpečnom mieste, sú určené pravidlá práce s heslami (na pracovných staniciach, doménach, mailových účtoch, IS, ...),
- zabezpečovať zálohy IS, ideálne fyzicky na inom mieste,
- primerane zabezpečiť prepojenia IS s verejnou sieťou, sieťovú bezpečnosť (firewall), pravidlá prístupu do verejnej siete, sťahovanie súborov z verejnej počítačovej siete, ochranu proti iným hrozbám z verejnej siete (hackeri), a pod.,
- mať pripravený postup pri výpadku/poruche servera,
- v prípade používania prenosných zariadení (napr. notebooky, ktoré obsahujú osobné údaje), zvážiť šifrovanie údajov na týchto zariadeniach,
- zabezpečiť ochranu pred nevyžiadanou elektronickou poštou, používanie legálneho softvéru, aplikáciu antivírusov, aplikáciu aktualizácií softvérov,
- na základe písomnej požiadavky dotknutej osoby zabezpečiť jej právo na prístup k svojim osobným údajom,
- na základe písomnej požiadavky dotknutej osoby zabezpečiť jej právo na výmaz svojich osobných údajov, ak sú splnené podmienky GDPR,
- na základe písomnej požiadavky dotknutej osoby zabezpečiť jej právo na obmedzenie spracúvania svojich osobných údajov, ak sú splnené podmienky GDPR.

6.6. Povinnosti zodpovednej osoby

Úlohou zodpovednej osoby je monitorovanie súladu spracovania osobných údajov s povinnosťami vyplývajúcimi z GDPR.

Úlohy zodpovednej osoby:

- poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov,
- monitoruje súlad s GDPR, tj.
    - zhromažďuje informácie za účelom vytvorenia a aktualizácie dokumentácie GDPR,
    - analyzuje a preveruje právny súlad spracovateľských činností,
- spolupracuje s úradom na ochranu osobných údajov pri plnení svojich úloh,
- Poskytuje poradenstvo pri posudzovaní vplyvu na ochranu osobných údajov a monitoruje jeho uplatnenia.

Zodpovedná osoba musí byť nahlásená na úrad na ochranu osobných údajov a musí byť vrátane kontaktných údajov zverejnená, napr. na webovej stránke.

7. Riešenie úniku osobných údajov

Ak dôjde k porušeniu zabezpečenia osobných údajov, je prevádzkovateľ alebo sprostredkovateľ povinný túto situáciu bezodkladne riešiť. Ako porušenie zabezpečenia je podľa GDPR chápané porušenie zabezpečenia, ktoré vedie k náhodnému alebo protiprávnemu zničeniu, strate alebo neoprávnenému sprístupneniu prenášaných, uložených alebo inak spracúvaných osobných údajov. Riešenie situácie závisí od charakteru porušenia zabezpečenia. Prípady porušenia zabezpečenia môžu byť rôzne, všeobecne sa môžu členiť na:

- porušenie dôvernosti - neautorizované alebo náhodné prezradenie osobných údajov alebo neautorizovaný prístup k nim;
- porušenie dostupnosti - náhodná alebo neautorizovaná (neplánovaná) strata alebo zničenie osobných údajov;
- porušenie integrity - nežiadúca alebo neautorizovaná zmena osobných údajov.

Ak u prevádzkovateľa nastane prípad porušenia zabezpečenia, musí prevádzkovateľ okrem prijatia adekvátnych opatrení taktiež posúdiť riziko daného prípadu. Vždy sa musí porovnávať, aký dopad môže mať porušenie zabezpečenia na subjekty údajov, hlavne vo vzťahu ku strate kontroly nad ich údajmi, škode na reputácii, možnosti obmedzenia ich práv, atď. Veľkú úlohu pri hodnotení rizika porušenia zabezpečenia bude mať aj miera zavinenia, tj. či išlo o nedbanlivosť alebo úmysel, pretože pri úmysle možno predpokladať väčšie riziko pre osobné údaje subjektu údajov, pretože ich získanie bolo cieľom útoku.

Ak porušenie zabezpečenia predstavuje riziko pre práva a slobody fyzických osôb, je prevádzkovateľ povinný oznámiť ho dozornému orgánu – a to bez zbytočného odkladu, pokiaľ je to možné do 72 hodín od okamžiku, kedy sa o incidente dozvedel. Dozorným orgánom je Úrad na ochranu osobných údajov. Pokiaľ nastane porušenie zabezpečenia osobných údajov u sprostredkovateľa, oznamuje ho bez zbytočného odkladu prevádzkovateľovi, resp. všetkým dotknutým prevádzkovateľom. Prevádzkovateľ následne posúdi skutočnosti oznámené sprostredkovateľom a rozhodne, či oznámené porušenie zabezpečenia predstavuje riziká pre práva a slobody fyzických osôb. Ak je pravdepodobné, že určitý prípad porušenia zabezpečenia osobných údajov bude mať za následok vysoké riziko pre práva a slobody fyzických osôb, je prevádzkovateľ povinný oznámiť prípad porušenia aj subjektu údajov. Oznámenie subjektu údajov nie je potrebné vykonať, ak síce došlo k porušeniu zabezpečenia osobných údajov, avšak prevádzkovateľ vykonal predbežné opatrenia, ktoré zapríčinili, že vysoké riziko, ktoré by bez použitia týchto prostriedkov nastalo, nenastane. Medzi tieto "predbežné" opatrenia možno zaradiť napr. šifrovanie či pseudonymizáciu.

Ohlásenie musí obsahovať minimálne:

- popis povahy daného prípadu porušenia zabezpečenia osobných údajov (napr. hackerský útok na internetové bankovníctvo);
- meno a kontaktné údaje zodpovednej osoby na ochranu osobných údajov alebo iného kontaktného miesta;
- popis pravdepodobných dôsledkov porušenia zabezpečenia osobných údajov (napr. pravdepodobnosť neoprávneného prístupu k bankovým účtom);

- popis opatrení, ktoré prevádzkovateľ prijal alebo navrhol prijať s cieľom vyriešiť dané porušenie zabezpečenia osobných údajov (napr. dočasné zablokovanie internetového bankovníctva a výzva klientom na bezodkladnú zmenu hesiel).

8. Zodpovednosť za porušenie práv a povinností

Porušenie tejto smernice bude posudzované ako závažné porušenie pracovnej disciplíny zamestnancom. Prevádzkovateľ môže uplatniť svoje oprávnenie a vyvodiť pracovnoprávne dôsledky, čo môže viesť až ku skončeniu pracovnoprávneho vzťahu.

9. Prílohy

Príloha č.1: Zoznam IS

Príloha č.2: Zoznam subjektov pracujúcich s osobnými údajmi prevádzkovateľa

Príloha č.3: Vzor sprostredkovateľskej zmluvy, aj s pokynmi na vyplnenie

Príloha č.4: Informácie dotknutej osobe

.....
Pečiatka prevádzkovateľa

.....
meno a priezvisko
podpis štatutárneho orgánu prevádzkovateľa