Magazín GDPR
číslo 2/2018

Vážení zákazníci,

přinášíme Vám druhé číslo našeho nepravidelného magazínu věnovaného tématice ochrany osobních údajů podle GDPR. Načerpali jsme další poznatky, které si myslíme, budou pro Vás v této hektické době přínosné. Věříme, že pro Vás informace, které získáte díky našemu dalšímu magazínu, budou užitečné při lepším zajištění procesů v ochraně osobních údajů ve Vaší organizaci podle GDPR.

Naďa Lukášková
pracovník zákaznické podpory

Obsah

Prohlášení o zpracování osobních údajů fyzických osob podle nařízení Evropského parlamentu a Rady (EU) číslo 2016/679

Podle článku 13 Nařízení Evropského parlamentu má každá organizace podle zásady transparentnosti a korektnosti informovat fyzické osoby o způsobech zpracování a ochrany osobních dat v její společnosti. K tomuto účelu jsme pro Vás připravili návrh prohlášení, které lze obecně použít v každé organizaci. Toto prohlášení je následně ideální umístit na webové stránky a odkazovat na něj v každém případě, kdy dochází k získávání osobních údajů od fyzické osoby.

Při aplikaci prohlášení pro Vaši společnost je důležité změnit:

- V článku 3 doplnit celý název včetně IČA Vaší společnosti (organizace)
- Pokud máte jmenovaného pověřence pro ochranu osobních dat, potom článek uveďte a změňte si jméno pověřence. Pokud je pověřenec externí pracovník či společnost, je třeba tam uvést i jméno organizace a její IČO. Pokud jste pověřence nejmenovali, potom článek 4 zcela vyřaďte
- V článku 5 můžete uvést typy osobních údajů, které zpracováváte, můžete i další doplnit či některé vypustit, pokud je nezpracováváte
- V článku 6 upravte oblasti či agendy, kde zpracováváte osobní údaje podle zaměření Vaší společnosti
- V článku 8 doplňte situace, kdy posíláte osobní údaje fyzických osob do třetích zemí
- U článku 9 upravte text v případě, že je jiný a v případě, že využíváte nějaké formy cíleného marketingu. Pokud ve Vaší společnosti nevyužíváte nějaké formy cíleného marketingu, potom uveďte třeba text „ Osobní údaje v naší společnosti nejsou využívány pro účely cíleného marketingu“
- U článku 11, aplikace práv fyzických osob, si upravte adresu firmy a kontaktní email
- U článku 10, předávání osobních údajů dalším příjemcům doplňte či upravte všechny společnosti, kam předáváte osobní údaje.

Budete-li chtít s tímto prohlášením pomoci, neváhejte nás kontaktovat. Rádi Vám pomůžeme.

Prohlášení GDPR - vzor

Cílem tohoto prohlášení je seznámit a ujistit všechny naše zákazníky, dodavatele, zaměstnance a další spolupracující fyzické osoby se zásadami a pravidly, kterými se naše společnost řídí při ochraně a zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) číslo 2016/679 ze dne 27. 4. 2016 (dále jen „GDPR“). Toto nařízení GDPR vstoupilo v platnost dnem 25. 5. 2018.

1. **Co jsou osobní údaje?**
   Osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě – subjektu osobních údajů, například její jméno, datum či místo narození, emailová adresa, telefonní číslo, bydliště, síťový identifikátor (cookies) apod.

2. **Co je zpracování osobních údajů?**
   Zpracování osobních údajů je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděná pomocí či bez pomoci automatizovaných postupů, jako je např. 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 osobních údajů.

3. **Správce**
   Správcem osobních údajů je společnost Softbit software s.r.o. Rychnov nad Kněžnou, IČO : 27473716.

4. **Pověřenec pro ochranu osobních údajů**
   Pro zajištění a dodržování všech pravidel pro ochranu osobních údajů jsme jmenovali pověřence pro ochranu osobních údajů Ing. Tomáše Nováka, programátora společnosti, email: softbit@softbit.cz .

5. **Kategorie zpracovávaných osobních údajů**
   Ve společnosti zpracováváme osobní údaje fyzických osob, jako jsou:
   - Jméno
   - Příjmení
   - Adresa bydliště
   - Telefonní číslo
   - Emailová adresa
     a další

   Osobní údaje včetně citlivých osobních údajů zpracováváme pouze v oblasti mezd a personální agendy. U osobních údajů, jakou je fotografie zaměstnance pro prezentaci na webových stránkách společnosti máme zajištěn svobodný souhlas podle zásad GDPR.

6. **Oblasti zpracovávaných osobních údajů**
   Zpracováváme osobní údaje fyzických osob zejména v oblastech a agendách:
   - Vedení účetnictví
   - Mzdová a personální agenda
   - Obchod
   - Oddělení péče o zákazníky
   - Webové stránky společnosti

7. **Dodržování zásad při zpracování osobních údajů**
   Při zpracování osobních údajů se důsledně řídíme zásadami, které jsou stanoveny nařízením GDPR.

   a) **Zákonnost**
   Zpracováváme osobní údaje jen v té míře, kde nám to ukládá příslušný zákon, na základě uzavření či plnění smlouvy, či na základě oprávněného zájmu, který však nepřiměřeně neomezuje ochranu soukromí a práv fyzické osoby. U ostatních činností si vždy získáváme svobodný, informovaný souhlas fyzické osoby podle zásad nařízení GDPR.

   b) **Korektnost a transparentnost**
   Veškeré osobní údaje zpracováváme korektně vůči každé fyzické osobě. Dodržujeme plně zásadu transparentnosti tak, aby každá fyzická osoba byla srozumitelně seznámena o způsobech zpracování svých osobních údajů v naší společnosti. K tomuto účelu bylo vytvořeno i toto prohlášení.

   c) **Účelové omezení**
   Zpracováváme osobní údaje fyzických osob jen k těm účelům, ke kterým nám byly tyto údaje svěřeny. Zásadně osobní údaje nepředáváme bez souhlasu a vědomí fyzických osob třetím stranám, pokud nám toto neukládá příslušný zákon či tuto činnost nám neukládá uzavřená smlouva.

   d) **Minimalizace údajů**

Při všech operacích s osobními údaji dodržujeme zásadu minimalizace, která nám určuje, že nemáme zpracovávat osobní údaje, které nepotřebujeme bezpodmínečně k dané činnosti. Údaje, které nepotřebujeme, vůbec nezpracováváme.

e) Přesnost
Zpracováváme pouze přesné a pravdivé osobní údaje. Přiměřenou formou si ověřujeme u našich zákazníků, zaměstnanců, obchodních partnerů a dalších spolupracujících fyzických osob aktuálnost a správnost jejich osobních údajů vedených v našich evidencích.

f) Omezení uložení
Osobní údaje vedeme jen po dobu, kterou nám ukládá zákon, doba uzavřené smlouvy nebo po dobu platnosti souhlasu fyzické osoby se zpracováním. V jasně definovaných případech vedeme osobní údaje rovněž na základě oprávněného zájmu, ale jen po nezbytně nutnou dobu, která neomezuje práva a svobody fyzické osoby.

g) Integrita a důvěrnost
Veškeré osobní údaje fyzických osob zabezpečujeme proti jejich zcizení, zničení či neoprávněnému zneužití. O všech skutečnostech a informacích ve zpracování osobních údajů našich zákazníků, dodavatelů, zaměstnanců a dalších spolupracujících fyzických osob zachovávají všichni pracovníci naší společnosti, kteří mají k těmto údajům přístup, bezpodmínečnou mlčenlivost. Máme zajištěno, aby se k osobním údajům nedostala v naší společnosti osoba, která nemá oprávnění tyto údaje zpracovávat podle nařízení GDPR.

h) Odpovědnost
Ke každému zpracování osobních údajů ve společnosti přistupujeme maximálně odpovědně. Všichni pracovníci společnosti jsou seznámeni se zásadami ochrany osobních údajů, právy fyzických osob. Ve společnosti máme vytvořenu vnitropodnikovou směrnici, která stanovuje všechna pravidla ochrany osobních údajů. Jmenovali jsme pro kontrolu všech činností pověřence pro ochranu osobních dat.

8. Předávání osobních údajů do třetích zemí
Nezpracováváme a nepředáváme žádné získané osobní údaje do třetích zemí.

9. Cílený marketing
Naše společnost zasílá aktivně obchodní sdělení, firemní newslettery, pozvánky na školení a další informace pouze stávajícím zákazníkům, aktivním klientům společnosti. U nového zákazníka zasíláme obchodní sdělení pouze na základě jeho aktivní poptávky formou emailové korespondence nebo na základě poptávkového formuláře na webových stránkách společnosti. U ostatních činností, kde to není dáno příslušným zákonem, smlouvou nebo oprávněným zájmem nepřiměřeně poškozujícím práva fyzické osoby, si vždy vyžadujeme od fyzické osoby svobodný informovaný souhlas podle pravidel GDPR.

10. Předávání osobních údajů dalším příjemcům
Předáváme osobní údaje fyzických osob pouze příjemcům dle platných zákonů. Ostatním příjemcům předáváme pouze pro potřeby zajištění zasílání obchodní a ostatní korespondence, zboží a dalších využíváme služeb jiných společností, kterým předáváme na základě oprávněného zájmu osobní údaje fyzických osob.

Jsou to tyto společnosti:
a) Česká pošta s. p.

b) PPL a.s.

11. Aplikace práv fyzických osob

Jako společnost plně respektujeme a vycházíme vstříc všem právům fyzických osob, zejména potom práva na:

a) Přístup k osobním údajům (podle článku 15 nařízení GDPR)
b) Opravu (podle článku 16 nařízení GDPR)
c) Výmaz – být zapomenut (podle článku 17 nařízení GDPR)
d) Omezení zpracování (podle článku 18 nařízení GDPR)
e) Přenositelnost osobních dat (podle článku 20 nařízení GDPR)
f) Vznést námitku (podle článku 21 nařízení GDPR)

Všechny požadavky na práva fyzických osob přijímáme pouze formou písemného požadavku zaslaného na adresu společnosti Softbit software s.r.o., ul. Nad Dubinkou 1634, Rychnov nad Kněžnou, 516 01 nebo na e-mailovou adresu softbit@softbit.cz. Po ověření fyzické osoby, která požadavek zaslala, v zákonných termínech provádíme aplikaci jednotlivých práv. U práva na přístup k osobním údajům v podobě výpisu osobních údajů zasíláme formou datové zprávy službou datových schránek České pošty v případě, že příjemce vlastní datovou schránku. U ostatních předáváme výpisy osobních údajů formou osobního předání fyzické osobě po jejím ověření. V případech, kdy nelze použít ani jednu z předchozích variant, zasíláme výpis osobních údajů formou doporučeného psaní do vlastních rukou prostřednictvím České pošty s. p..

9) Závěrečné informace

Neustále sledujeme všechny změny a novinky v oblasti nařízení pro ochranu osobních údajů a aplikujeme je do svých vnitropodnikových procesů.

V Rychnově nad Kněžnou dne: 25. 5. 2018

Povinnost nahlášení „Pověřence pro ochranu osobních údajů“ na ÚOOÚ

Organizace, které mají povinnost jmenovat pověřence pro ochranu osobních údajů, musí tuto skutečnost nahlásit na Úřad pro ochranu osobních údajů. Ostatní organizace, které si jmenovali pověřence pro ochranu osobních údajů dobrovolně, toto mohou provést rovněž. V následujícím textu Vám přinášíme k tomuto tématu několik důležitých informací.

Povinnost pověřence jmenovat nastává v jedné z následujících situací:

1. Zpracování osobních údajů provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů (v jakémkoli rozsahu).

2. Hlavní činnosti správce nebo zpracovatele osobních údajů spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování osob.
3. Hlavní činnosti správce nebo zpracovatele osobních údajů spočívají v rozsáhlém zpracování zvláštních kategorií údajů, jako jsou genetické nebo biometrické údaje, nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Uvedený výčet je poněkud zjednodušený a ani se teď nemusíme zabývat rozlišováním mezi tzv. správcem a zpracovatelem osobních údajů, což mohou být dva rozdílné subjekty.

První uvedená kategorie se týká pouze **subjektů veřejného práva** a můžeme předpokládat, že ještě dojde k jejímu zpřesnění. Veřejný sektor bývá více či méně propojen se soukromou sférou, přičemž národní legislativy definují tyto kategorie rozdílně.

Podnikatelů se týkají především zbylé dvě kategorie, které ovšem také nejsou zcela jednoznačně vymezeny. Proto se dá očekávat, že definici ve finále vyjasní až praxe.

Odůvodnění GDPR a související text vytvořený pracovní skupinou WP29, tedy evropským poradním orgánem pověřeným výkladem nařízení, nabízí ale již nyní jasné znaky, které mohou podnikatelům pomoci určit, zda se na ně povinnost jmenovat DPO vztahuje.

1. Hlavní činnost

Aby byl správce či zpracovatel povinen pozici pověřence vytvořit, musí ke zpracovávání osobních údajů docházet v rámci jeho hlavní činnosti.

Od ní je třeba odlišit činnosti, při nichž sice rovněž dochází ke zpracovávání osobních dat, ale jedná se o činnosti podpůrného charakteru zajišťující samotný chod organizace a přímo nesouvisející s činností hlavní. Pro zjednodušení lze říci, že by se mělo jednat o ty činnosti, které musí vykonávat každá organizace nezávisle na tom, jaká je její hlavní činnost, například vyplácení mzdy zaměstnancům nebo zpracování obsahových, provozních či lokalizačních dat poskytovatelem telefonních a internetových služeb.

2. Rozsáhlost

Aby vznikla povinnost pověřence jmenovat, zpracovávání údajů musí být rozsáhlé.

Pracovní skupina WP29 doporučuje pro určení toho, zdali je prováděno rozsáhlé zpracování osobních údajů, zvážit zejména množství zpracovávaných osobních údajů (jak množství zpracovávaných údajů obecně, tak v poměru k relevantní populaci), různorodost zpracovávaných osobních údajů, dobu trvání zpracovávání osobních údajů či geografický rozsah území, z něhož pocházejí zpracovávané osobní údaje.

Jako příklad rozsáhlého zpracování lze uvést zpracovávání údajů o pacientech v rámci běžné činnosti nemocnice. Zpracování údajů o pacientech jednotlivým lékařem se však za rozsáhlé nepovažuje. Rozsáhlým zpracováním bude např. i zpracování osobních údajů vyhledávačem pro potřeby cílené reklamy či zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky.

3. Pravidelné a systematické monitorování

Jedná se o další, nařízením přímo nedefinovaný pojem. Pravidelnost by se měla určovat na základě kombinace jedné nebo více následujících charakteristik:

průběžný nebo v pravidelných intervalech a po určitou dobu se opakující stále se opakující nebo opakovaný ve stanoveném čase neustále nebo pravidelně se vyskytující

Zda se jedná o systematické monitorování, by nám měly objasnit tyto kategorie:

- vyskytující se podle určitého systému, přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Jako praktické příklady „pravidelného a systematického monitorování“ uvádí pracovní skupina WP29 zejména provozování telekomunikačních sítí, poskytování telekomunikačních služeb, ale i tzv. email retargeting, věrnostní programy anebo reklamní sdělení cílená na základě chování osob při používání vyhledávacích nástrojů (angl. *behavioural advertising*).

Je třeba si uvědomit, že podle toho, kdo splňuje kritéria povinného jmenování, může být povinným subjektem pouze správce či pouze zpracovatel údajů, ale i oba zároveň.

Je také důležité vyzdvihnout, že pokud správce splňuje kritéria povinného jmenování DPO, ještě to neznamená, že ho musí jmenovat i smluvní zpracovatel údajů. A lze si představit i takovou situaci, kdy pověřenec jmenovaný zpracovatelem rovněž dohlíží na činnosti, které zpracovatelská organizace vykonává pro sebe jako správce.

Funkci pověřence může zvláště ve velkých organizacích zastávat více osob. Je však nutné, aby bylo navenek jasné, kdo je z funkce odpovědný a na koho se má případně dozorový orgán či občan obracet a to tak, aby příslušnou osobu bylo možné kontaktovat přímo a důvěrně. Jako vhodné se tak jeví zveřejnění poštovní adresy, telefonního čísla či e-mailové adresy, pro styk s veřejností dále pak například zpřístupnění kontaktního formuláře na webové stránce. Jako součást dobré praxe lze doporučit i zveřejnění jména pověřence, ač to nařízení přímo nevyžaduje.

GDPR umožňuje určit pro skupinu podniků pouze jednoho pověřence, a to za předpokladu, že bude dostupný v každém z podniků tak, aby stále dokázal efektivně plnit svěřené úkoly. To znamená především to, aby byla účinně zajištěna možnost okamžité komunikace s dozorovým orgánem, jednotlivými zaměstnanci každého z podniků a veřejností.

Příklad zprávy na ÚOOÚ o jmenování Pověřence DPO:

Jméno organizace (doplňte) v souladu s článkem 37 odst. 7 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) sděluje dozorovému úřadu, že jmenovalo pověřence pro ochranu osobních údajů, kterým je zástupce právnické osoby Softbit software s.r.o. Rychnov nad Kněžnou, IČO 27473716, pan Tomáš Urban, ul. Nad Dubinkou 1634, Rychnov nad Kněžnou email: tomas.urban@softbit.cz .
Organizace má k 25. 5. 2018 zajištěn výkon této funkce.

Zprávu zašlete prostřednictví datové schránky číslo: qkbaa2n.

GDPR a přímý elektronický marketing

V poslední době v souvislosti se aplikací zásad podle Nařízení GDPR se nám vyskytuje hodně dotazů z této oblasti. V pátek minulého týdne k tomuto tématu vyšel přímo na stránkách Úřadu pro ochranu osobních údajů konečně v oficiální podobě tento článek.
Přetiskujeme jej tedy v plném rozsahu:

1. 6. 2018 – Na základě četných dotazů veřejnosti uveřejňuje Úřad pro ochranu osobních údajů své vyjádření ohledně práv a povinností správce a zákazníka v přímém elektronickém marketingu po nabytí účinnosti obecného nařízení.

Zpracování osobních údajů (telefonních čísel, e-mailových adres apod.) zákazníků pro účely přímého marketingu (při rozesílce obchodních sdělení) je zpracování prováděné z důvodu oprávněného zájmu dle čl. 6 odst. 1 písm. f) obecného nařízení. Zákazník při nákupu výrobku či služby může odůvodněně očekávat, že mu obchodník zašle obdobnou nabídku. Zájem obchodníka převažující v tomto případě nad zájmem zákazníka je přitom korigován dalšími povinnostmi obchodníka jako správce osobních údajů. Správce musí splnit informační povinnost stanovenou v článku 13 obecného nařízení, jejíž součástí musí být též informace o právu subjektu údajů vznést námitku dle čl. 21 odst. 2 obecného nařízení proti zpracování osobních údajů pro účely přímého marketingu. Pokud subjekt údajů tuto námitku vznese, nesmějí již být osobní údaje pro tento účel zpracovány (jde tedy o tzv. princip opt-out).

Způsob realizace oprávněného zájmu správce při samotné rozesílce obchodních sdělení prostřednictvím elektronických prostředků je přesně dán ustanoveními zákona č. 480/2004 Sb., o některých službách informační společnosti. Na zasílání obchodních sdělení vůči zákazníkům se uplatní § 7 odst. 3 zákona č. 480/2004 Sb., kdy obchodní sdělení lze zákazníkům zaslat bez jejich předchozího souhlasu (princip opt-out), ovšem zákazník musí mít možnost toto zasílání odmítnout před odesláním takového obchodního sdělení (např. obchodník umožní zákazníkovi v rámci obchodních podmínek či při finálním potvrzení objednávky, aby zaškrtl políčko, že si nepřeje, aby mu byla obchodní sdělení zasílána). Pokud zákazník toto dopředu neodmítne, tak tato možnost musí být dána v každém dalším odeslaném obchodním sdělení. Současně je také zakázáno šířit obchodní sdělení, která by nebyla zřetelně a jasně označena jako obchodní sdělení; která by skrývala či utajovala totožnost odesílatele, jehož jménem se komunikace uskutečňuje; a která by byla zaslána bez platné adresy, na kterou lze přímo a účinně toto zasílání odmítnout.

Tato pravidla mají předejít obtěžování uživatelů elektronických kontaktů nevyžádanými obchodními sděleními, nehledě na to, zda je uživatelem fyzická či právnická osoba, ale zároveň i umožnit oprávněný obchodní styk, kde je to očekávatelné a není a priori obtěžující.

Z výše uvedeného textu vyplývá:

- Zákazníkovi či obchodnímu partnerovi (fyzické osobě) můžeme zasílat obchodní sdělení na obdobný okruh zboží či služeb, které od nás odebírá. Měli bychom mu ale dát vždy možnost zrušit souhlas se zasíláním obchodních sdělení na každém takovém sdělení.
- Zákazníkovi v případě, že nám zruší souhlas se zasíláním obchodních sdělení, žádné takové další mu již neposíláme.

- Při uzavírání objednávky na zboží či služby, registraci na webových stránkách správce atd. musí mít zákazník možnost odmítnout zasílání obchodních sdělení ze strany správce
- Souhlas se zasíláním obchodních sdělení nesmí být součástí žádné smlouvy. Musí být zcela zvlášť
- Před zasláním obchodní nabídky na zcela jinou oblast dodávky zboží či služeb musíme mít nejprve od zákazníka, kterého vedeme za jiným účelem, jeho souhlas.

Na tuto oblast marketingu upozorňujeme zejména z důvodu, že na webových stránkách úřadu pro ochranu osobních údajů je ihned na první straně v sekci „Nevyžádaná obchodní sdělení“ odkaz na podání stížnosti na zasílání obchodních sdělení.

Dále doporučujeme na všechny webové stránky, kde získáváte od návštěvníků osobních údaje v podobě kontaktních a poptávkových formulářů, registrací apod. uvést text, kterým návštěvníka informujete o účelu a pravidlech zpracování jeho osobních údajů.

Tento text může vypadat například takto:

Společnost Softbit software s.r.o. Rychnov nad Kněžnou, IČO: 27473716 prohlašuje, že bude osobní údaje vyplněné v poptávkovém formuláři zpracovávat pouze za účelem vyhotovení obchodní nabídky a pro zajištění služeb souvisejících s charakterem poptávky a to po dobu nezbytně nutnou. Tyto údaje nebudou předávány třetím osobám a společnost je bude chránit v souladu s nařízením Evropského parlamentu a Rady (EU) číslo 2016/679 o ochraně osobních údajů.

Ohlašování případů porušení zabezpečení osobních údajů

Jedním z pravidel podle nového Nařízení GDPR je i povinnost nahlašování tzv. bezpečnostních incidentů na Úřad pro ochranu osobních údajů. V následujícím článku Vám přinášíme některé odpovědi na dotazy, které vydal úřad v minulém týdnu.

Jaké případy je třeba ohlašovat?

Je třeba ohlašovat jakékoliv porušení zabezpečení osobních údajů, které může mít za následek riziko pro práva a svobody fyzických osob.

Může jít například o útok proti počítači, ve kterém jsou osobní údaje zpracovávány, jehož důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití. Může jít také např. o ztrátu listinných dokumentů obsahujících osobní údaje, které byly součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byly vytištěny z počítače, ve kterém je taková evidence vedena a obsah těchto dokumentů zakládá riziko pro dotčené osoby (např. ztráta zdravotnické dokumentace).

Jaké případy není třeba ohlašovat?

Ohlašovat není třeba případy, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby.

Může jít např. o momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byl vytištěn z počítače, ve kterém je taková evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení.

Co musí ohlášení obsahovat?

Ohlášení musí obsahovat:

a) 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;

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

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Byl-li správcem nebo zpracovatelem jmenován pověřenec, k jehož úkolům patří spolupráce s dozorovým úřadem, může být vypracování ohlášení úkolem tohoto pověřence.

Komu se ohlášení zasílá?

Správce osobních údajů ohlašuje případ dozorovému úřadu, kterým je Úřad pro ochranu osobních údajů se sídlem Pplk. Sochora 27, Praha 7. Zpracovatel ohlašuje případ příslušnému správci.

Do kdy je třeba ohlášení učinit a jak?

Správce i zpracovatel ohlašují případ bez zbytečného odkladu. Správce případ ohlásí Úřadu pokud možno do 72 hodin od okamžiku, kdy se o něm dověděl. Pokud není ohlášení Úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Správce zasílá Úřadu ohlášení na adresu elektronické pošty, e-mail: posta@uoou.cz nebo do datové schránky: qkbaa2n.

Zpracovatel zasílá ohlášení správci na dohodnuté kontaktní údaje správce.

Kdy je třeba případ oznámit lidem, u nichž k porušení zabezpečení jejich osobních údajů došlo?

Je to třeba, když je pravděpodobné, že případ bude mít za následek vysoké riziko pro práva a svobody dotčených osob.

Může jít např. o případ porušení zabezpečení osobních údajů v bankovním systému, v jehož důsledku by mohlo dojít k majetkové újmě klientů banky.

Jaké jsou výjimky z povinnosti oznámit takový případ těmto lidem?

Oznámení dotčeným osobám se nevyžaduje, jestliže:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;

b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek pod shora uvedenými písm. a), b) a c).

Více informací k této oblasti nabízí schválená vodítka Pracovní skupiny WP29, nynějšího Evropského sboru pro ochranu osobních údajů.

Návrh vzoru dodatku ke smlouvě mezi správcem a zpracovatelem.

Řada z Vás se na nás obracíte s žádostí o poskytnutí nějakého vzoru smlouvy mezi správcem a zpracovatelem podle zásad GDPR. Na tomto místě chci uvést, že každá taková smlouva či dodatek může být hodně individuální, a proto nelze obecně takovou smlouvu specifikovat.

Doplňuji, že správcem je vždy společnost, která má povinnost zpracovávat osobní údaje a zpracovatel je společnost, která pro správce zajišťuje některé činnosti v oblasti zpracování osobních údajů, které správce z personálních nebo finančních důvodů neprovádí sám. Je to například outsourcing zpracování mzdové agendy nebo účetnictví atd. V následujícím textu Vám tedy přinášíme jednoduchý návrh, který si sami můžete upravit.

Hlavní body v takové smlouvy by neměly v takové smlouvě chybět:

- Povinnosti zpracovatele vůči správci v oblasti zabezpečení zpracování osobních údajů podle zásad GDPR
- Povinnosti zpracovatele zachovávat mlčenlivost o všech skutečnostech v oblasti zpracování osobních údajů
- Nepředávat bez vědomí správce žádné osobní údaje třetím stranám
- Informovat správce o všech porušení zásad ochrany, ke kterým došlo u zpracovatele

Jednoduchý vzor dodatku ke smlouvě uvádíme v dalším textu:

Správce:

Společnost X

a

Zpracovatel:

Společnost Y

uzavírají

Dodatek ke smlouvě číslo

o zpracování osobních údajů na základě Nařízení Evropského parlamentu a Rady (EU) číslo 2016/679, dále jen nařízení GDPR

I. Závazky zpracovatele

Zpracovatel se zavazuje, že bude veškeré osobní údaje fyzických osob, které bude zpracovávat podle požadavků správce, chránit podle zásad nařízení GDPR.
Ve své společnosti přijme zpracovatel taková opatření, aby nedošlo ke zcizení, zničení či neoprávněnému zneužití těchto údajů.
Bude osobní údaje zpracovávat jen k těm účelům, ke kterým má od správce pověření.
Osobní údaje bude předávat správci jen v takové zabezpečené podobě a formě, na jaké jsou se správcem dohodnuti v článku III této smlouvy.
O všech skutečnostech týkajících se osobních údajů fyzických osob zachová mlčenlivost a nebude je předávat třetím stranám bez vědomí správce.
O jakýchkoli skutečnostech v souvislosti s únikem či neoprávněným zpracováním osobních dat ve společnosti bude zpracovatel neodkladně informovat správce.

II. Závazky správce

Správce bude osobní údaje předávat zpracovateli jen v takové zabezpečené podobě a formě, na jaké jsou se zpracovatelem dohodnuti v článku III této smlouvy.

III. Formy předávání osobních dat

Správce předává zpracovateli osobní údaje v listinné podobě osobně pouze do rukou odpovědné osoby stanovené zpracovatelem.
Zpracovatel předává správci osobní údaje v listinné podobě osobně pouze do rukou odpovědné osoby stanované správcem.
V jiných případech jsou osobní údaje zasílány listinnou zásilkou formou doporučeného psaní do vlastních rukou.
Elektronické dokumenty mezi zpracovatelem a správcem jsou zasílány formou datové zprávy přes služby Datové schránky České pošty.
V jiných případech mohou být elektronické dokumenty zasílány mezi správcem a zpracovatelem formou e-mailové zprávy, ale pouze za předpokladu, že budou osobní data uvedena pouze v zabezpečené příloze opatřené heslem nebo zašifrované. Heslo bude vždy sděleno mezi správcem a zpracovatelem jinou cestou.

IV. Sankce

Zpracovatel si je vědom toho, že odpovídá u sebe za ochranu osobních dat správce.
V případě pochybení z viny zpracovatele může být tento postižen vymáháním škody od správce, která vznikne správci při úniku či neoprávněnému zpracování předaných osobních dat.

V. Závěrečná ustanovení

Správce a zpracovatel uzavřeli tuto smlouvu svobodně a zavazují se, že jí budou plnit. V případě ukončení smluvního vztahu je ukončena platnost i tohoto dodatku.
Zpracovatel se zavazuje, že po ukončení smluvního vztahu předá veškerá osobní data fyzických osob zpracovateli.
O veškerých osobních datech, se kterými přišel do styku v průběhu trvání smlouvy, však zpracovatel zachová nadále mlčenlivost a bude i nadále chránit osobní data,

která bude mít i po ukončení smluvního vztahu povinnost zpracovávat na základě zákona.
Dodatek ke smlouvě je vyhotoven ve dvou originálech, z nichž jeden si ponechá správce a jeden zpracovatel.
Dodatek ke smlouvě nabývá platnosti dnem podpisu obou smluvních stran.

V …….. dne: ……..

---------- ----------
-

Správce Zpracovatel

Upozorňujeme, že odkazujeme na Nařízení Evropského parlamentu číslo 2016/679. Je ale pravděpodobné, že v letošním roce na podzim začne platit Český zákon, který bude na toto nařízení navazovat. V tom případě bychom měli smluvní vztah následně aktualizovat na nové číslo zákona. O tomto vás budeme ale ještě včas informovat.

Doporučené činnosti správce IT při zajišťování ochrany osobních údajů

Tento dokument obsahuje základní doporučené činnosti související se zajištěním ochrany nejen osobních údajů fyzických osob na počítačových zařízeních v organizaci správce. Dokument není nedílnou součástí směrnice pro nakládání a ochranu osobních údajů, přesto je vhodné se řídit základními poučkami uvedenými v tomto dokumentu.

Obsah:

A. Pravidla práce s výpočetní technikou

A. 1. Rozdělení uživatelů počítačové sítě, zabezpečení uživatelských účtů

Uživatelé počítačové sítě v rámci organizace jsou rozděleni s ohledem na své pracovní zařazení, pracovní náplň a také na zastávanou pozici v organizační struktuře organizace. Na základě tohoto rozdělení získávají uživatelé přístup do jednotlivých informačních systémů a příslušných pracovních adresářů na síťových discích. Správu uživatelských přístupů do informačních systémů a mapování složek pro ukládání dokumentů má za povinnost správce IT. Povinností každého uživatele je však smazat takové soubory, které vytvořil, ale již je nepotřebuje ke své činnosti a nadále je tedy nepoužívá (vyjma souborů, které jsou neoddělitelné od povinností tvořit takové soubory v rámci organizačních předpisů nebo na základě právního nároku správce). Uživatel má dále povinnost ukládat soubory obsahující osobní údaje pouze do složek, které k tomuto účelu jsou zřízeny správcem IT (jsou to zpravidla složky na datovém serveru organizace, pokud jej organizace vlastní).

A. 2. Pravidla pro uživatelská jména a přístupová hesla

Všichni uživatelé mají přiděleno jednoznačné/jedinečné uživatelské jméno a musí dodržovat následující pravidla pro uživatelské heslo:

- Nesdělovat žádné osobě své heslo a udržovat jej v maximální tajnosti
- Heslo nezaznamenávat na žádné médium tak, aby se k němu mohla dostat jiná osoba (zejména ne potom na viditelná místa)
- Měnit jej kdykoliv pokud dojde k jeho odtajnění nebo je alespoň podezření, že heslo zná jiná osoba
- Nesmí být založeno na skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních údajů (jména, data narození, rodné číslo, telefonní číslo apod.)
- Heslo nedoplňovat do jakýchkoliv automatizovaných přihlášení
- Nesdílet hesla, která byla individuálně přidělena konkrétnímu uživateli
- Po počtu dní, které jsou uvedeny ve směrnici pravidelně měnit heslo za nové (pokud toto směrnice nařizuje)
- Nepoužívat uživatelské heslo v blízkosti jiné osoby tak, aby bylo možné odezírat toto heslo touto osobou
- Pracoviště v kanceláři mít vytvořeno tak, aby nebylo možné nahlížet na zpracovávané informace cizí osobám, které nejsou oprávněny tyto informace vidět (v praxi mít obrazovku počítače natočenu tak, aby cizí osoba nemohla vidět na údaje zobrazené na monitoru)

V případě, že uživatel své heslo ztratí nebo získá podezření, že by mohlo být zneužito, je povinen heslo neprodleně změnit, případně (není-li to možné) tuto skutečnost neprodleně ohlásit správci IT a požádat jej o zablokování daného hesla. Prozrazení hesla představuje bezpečnostní incident.

A. 3. Administrátorský účet

Administrátorský účet nesmí být využíván pro běžnou pracovní činnost, heslo pro tento účet musí být stanoveno podle pravidel uvedených výše.

Názvy hlavních administrátorských účtů musí být spolu s hesly sepsány a uloženy v zapečetěné obálce u určené odpovědné osoby. Je-li nezbytně nutný zásah na serveru v nepřítomnosti

správce IT, může po schválení tohoto zásahu odpovědnou osobou (ředitel/ka zařízení) provést pomocí příslušného názvu administrátorského účtu a hesla pověřená osoba. O této skutečnosti musí být sepsán záznam. Po každém mimořádném použití administrátorského účtu i hesla k němu, musí být toto heslo změněno/vytvořeno nové.

B. Přístupová práva k souborům a adresářům na síťových discích

B. 1. Zřízení přístupových oprávnění

Při zřizování přístupových oprávnění vždy o vytvoření uživatelského přístupu do počítačové sítě, informačních systémů a na datová úložiště žádá vedoucí pracovník správce IT. Přístup je zřizován vždy pro konkrétního podřízeného pracovníka s ohledem na jeho pracovní zařazení a pozici v organizační struktuře. Žádost by měla mít písemnou podobu, vedoucí pracovník zodpovídá za to, aby byl rozsah poskytnutého oprávnění v souladu s pracovním zařazením konkrétního zaměstnance. Správce IT následně na základě žádosti zajistí zřízení přístupů a předání uživatelských oprávnění konkrétnímu uživateli. Pokyny ke zřízení přístupových oprávnění musí být archivovány pro pozdější kontrolu.

B. 2. Změny v přístupových právech

Požadavky na změny v přístupových oprávněních k adresářům, souborům nebo aplikacím opět schvaluje příslušný vedoucí pracovník, obvykle na základě žádosti uživatele. Schválené požadavky (písemná podoba, změny se evidují a archivují) následně k realizaci obdrží správce IT.

B. 3. Odebrání přístupových práv

Při změně pracovního zařazení, ukončení pracovního poměru či nástupu na mateřskou dovolenou apod. jsou všechna přístupová oprávnění a uživatelské účty zablokovány. O provedení blokace se provádí záznam. Při zablokování účtů z důvodu ukončení pracovního poměru jsou účty zachovány pouze po dobu nezbytně nutnou, následně jsou správcem IT ze serveru zcela odstraněny. Data umístěna ve složkách, kam měl přístup uživatel, který již ukončil pracovní poměr, jsou po schválení vedoucím pracovníkem přesunuty novému pracovníkovi, který nastoupil na pracovní pozici po pracovníkovi, který pracovní poměr ukončil.

B. 4. Pravidla elektronické výměny dat a informací

Jsou zavedeny funkce pro ochranu výměny informací (elektronická komunikace, použití hlasových, faxových a video komunikačních zařízení, případně též FTP) při splnění následujících bezpečnostních požadavků:

- Všichni uživatelé jsou poučeni o možnostech kopírování, modifikací a zničení sdílených informací, případně o možnosti odposlechu neveřejných informací;

- Všichni uživatelé jsou obeznámeni s postupy a nástroji pro detekci a ochranu před škodlivými kódy, které mohou být přenášeny elektronickou komunikací (antivirové programy);
- Uživatelé, osoby smluvních a třetích stran mají zodpovědnost (často smluvně garantovanou), že nezneužijí data, která si se zařízením vyměňují například zasíláním reklamních sdělení, řetězovým zasíláním e-mailových zpráv apod.;
- Dokumenty, které obsahují osobní údaje, musí být bezprostředně po tisku odebírány z tiskárny či kopírky uživatelem, který tyto dokumenty zaslal do tohoto zařízení
- Uživatelé jsou poučeni, aby v nezabezpečených webech nezadávali žádné osobní údaje, neveřejné informace a podobně.

B. 5. Pravidla pro používání e-mailové komunikace

Přidělené schránky elektronické pošty (e-mailové schránky) smí být používány výhradně pro emailovou komunikaci související s výkonem práce.

Uvedené e-mailové schránky nesmí být používány pro odesílání nebezpečně (nešifrovaně) zabezpečených citlivých informací. Tyto elektronické zprávy lze odesílat jen s obsahem, který je řádně zašifrován (zaheslován). Dále nesmí být služební e-mail využíván pro odesílání nelegálního obsahu (videa, hudba apod.) a soukromou korespondenci.

B. 6. Pravidla pro používání informačních systémů

Práce s informačními systémy organizace a v nich obsaženými osobními údaji se řídí zejména pokyny a nařízeními ředitele/ředitelky zařízení, případně správce IT. Uživatelé těchto informačních systémů a aplikací musí dbát především na dodržování následujících pravidel:

- Používat informační systémy výhradně k pracovním účelům
- Používat přístupová hesla do informačních systémů a aplikací zařízení v souladu s pokyny pro používání hesel (viz výše)
- Používat informační systémy jen v souladu s uživatelským manuálem poskytovaným jako součást dodávaného software
- Používat pokud možno jen informační systémy od dodavatelů, kteří zajistí soulad s ochranou osobních údajů podle nového nařízení

B. 7. Pravidla pro využívání Internetu

Veřejnou celosvětovou síť Internet lze používat pouze k plnění pracovních úkolů, je třeba dbát zvýšené obezřetnosti (výskyt škodlivých programů). Je zakázáno stahování a instalace jakéhokoliv SW přístupného z internetu na pracovní stanici, toto může výhradně v odůvodněných případech provést správce IT (po schválení písemné žádosti nadřízeným).

C. Bezpečnost práce v síti

Cílem a smyslem níže uvedených opatření je zamezit neúmyslnému i úmyslnému poškození dat, jejich zničení či odcizení nebo vyzrazení neoprávněným osobám. Z pohledu uživatele se tato opatření projevují žádostí o zadání uživatelského jména a hesla při přihlašování se a také omezeným přístupem do příslušných adresářů.

Bezpečnostní opatření jsou zajištěna pomocí:

- Uživatelského jméno a heslo
- Data, která jsou uložená na síťových discích, není povoleno poskytovat osobám, které nejsou k organizaci v pracovním či jiném právním vztahu bez souhlasu nadřízeného nebo pokud to neukládá zákon či jiné nařízení o předávání dat jiným příjemcům či zpracovatelům
- Data v jakékoliv formě a podobě nesmí být vynášeny z prostor zařízení bez souhlasu nadřízeného
- Veškerá data z cizích zdrojů a vyměnitelná záznamová média (především přepisovatelná: CD, DVD, flash disk) musí být pře použitím prověřena antivirovým programem, zda neobsahují viry. Nastavení antivirového programu tak, aby toto kontroloval automaticky bez ovlivnění této funkce uživatelem, má na starost správce IT

C. 1. Antivirová ochrana, ochrana před škodlivými programy

Ochrana před počítačovými viry a škodlivými programy je v zařízení realizována prostřednictvím antivirového programu, který je nastaven tak, že probíhá automatická aktualizace a detekce infikovaných souborů. Za nastaven antivirového programu zodpovídá IT správce.

Uživatelům PC stanic a dalších prostředků IT je zakázáno jakkoliv měnit chod a nastavení antivirového programu. Pokud je nalezen vir, který není možné pomocí instalovaného antivirového programu běžně odstranit, je uživatel zařízení povinen na tuto skutečnost bezprostředně po zjištění, upozornit správce IT.

Všichni uživatelé PC jsou povinni při používání přenosných přepisovatelných médií před tím, než otevřou soubor uložený na takovém médiu, spustit antivirovou kontrolu daného média. Antivirový program doporučujeme nastavit tak, aby pokud možno uživatel nemohl ovlivnit jeho činnost.

Každý PC v organizaci a to i včetně přenosných musí být osazen vhodným antivirovým programem

Přenosný PC, kde je pravděpodobné, že bude připojován i do jiných sítí, než je lokální počítačová síť v sídle správce, musí mít nastavenu vhodnou ochranu před hrozbami z internetu (Firewall atd.)

D. Bezpečnost dat sítě

Přístup k datům v prostředí sítě je zajištěn prostřednictvím přístupových práv přiřazených jednotlivým uživatelským účtům.

D. 1. Zabezpečení rozhraní sítě internetu

Síť je před hrozícím externím nebezpečím chráněna prostřednictvím instalace bezpečnostní brány na rozhraní internetu a vnitřní PC sítě. Smysl bezpečnostní brány spočívá v tom, že

umožní přístup pouze bezpečných a podporovaných komunikačních protokolů. Zároveň musí být zajištěno pravidelné vyhledávání zranitelností daného rozhraní.

D. 2. Zabezpečení neobsluhovaných stanic

Každý uživatel počítačové stanice je povinen, se při jejím opouštění, byť jen na krátký časový úsek, odhlásit nebo stanici uzamknout, aby bylo zamezeno neoprávněnému přístupu k datům. Dále jsou na všech stanicích nainstalovány spořiče obrazovky, které se spouští po časovém úseku nečinnosti, který je uveden ve směrnici GDPR. Při opětovném zahájení činnosti spořiče vyžadují opětovné přihlášení.

D. 3. Externí přístupy do počítačové sítě

Přístupy externích zpracovatelů a servisních techniků k dodávanému software musí být zabezpečeny tak, aby nedošlo k neoprávněnému vniknutí do počítačové sítě jinou osobou. Externí přístupy lze zřídit vybraným uživatelům či dodavatelům pouze na základě schválení ředitelem/ředitelkou zařízení.

Zřízení přístupu probíhá na základě formálního schválení. Přístupy jsou přidělovány vždy na základě žádosti příslušného vedoucího pracovníka po schválení ředitelem/ředitelkou zařízení. Odpovědnost za zřízení a přidělení přístupu nese správce IT.

Externí přístupy by měly být přiděleny pouze osobám (společnostem), se kterými je sepsána smlouva o mlčenlivosti nebo smlouva se zpracovatelem. Součástí smlouvy musí být zajištěna maximální garance ochrany osobních údajů minimálně v takové výši, jakou má nastavenu správce osobních dat.

E. Pravidla používání přenosných prostředků mimo prostory zařízení

Pokud je uživateli z řad zaměstnanců zařízení přidělen přenosný prostředek (flash disk, notebook, paměťová karta apod.), který plánuje používat mimo zařízení, je povinen dodržovat následující pravidla:

- Prostředek nesmí předat třetí osobě, pokud to nevyplývá z pracovní povinnosti
- Pracovat tak, aby bylo zabráněno případné možnosti odezírat informace z displeje notebooku/PC neoprávněnými osobami
- Provést všechna opatření, která povedou k zabránění případné ztráty či odcizení daného prostředku (nenechat bez dozoru, zabezpečení v dopravních prostředcích, hotelech apod.)
- Hlásit okamžitě nadřízenému případnou ztrátu či odcizení prostředku

Datové nosiče přenosných prostředků, které obsahují osobní údaje, musí využívat šifrovací SW (např. komprimovaný soubor, zip či rar s ochranou pomocí hesla), za dodržování tohoto pravidla je zodpovědný uživatel prostředku.

Doporučujeme provést i šifrování datového disku v přenosném notebooku, který může či obsahuje osobní data. Odpovědnost za nastavení takového šifrování má správce IT.

F. Správa, obnova a údržba výpočetní techniky

Smyslem údržby a obnovy výpočetní techniky je uchovat ji v bezproblémovém a bezporuchovém chodu a také zajištění dostatečného výkonu prostředků výpočetní techniky ve vztahu k počtu používaných aplikací.

F. 1. Údržba osobních PC

Správce IT zodpovídá za plánování a provádění údržby hardware osobních PC, dojde-li k nekorektnímu chování počítače, je uživatel povinen o tom informovat správce IT.

F. 2. Údržba LAN sítě

Údržbu počítačové sítě (HW i SW) zajišťuje správce IT dle pokynů, které pro jednotlivé produkty (síťové komponenty) dodávají jejich výrobci či dodavatelé.

F. 3. Zálohování dat na serverech

Data uložená na síťových úložištích jsou zabezpečena před jejich ztrátou prostřednictvím zálohování na záložní média, zálohování dat provádí správce IT (inkrementální a plné zálohování ve stanoveném časovém intervalu), proto se na něj také obracejí uživatelé v případě, že potřebují, aby byla určitá data obnovena. Pokud dojde k obnově zálohovaných dat, informuje o tomto kroku správce IT předem ředitele (ku) organizace. Po provedené obnově dat všichni uživatelé, kterých se obnovená data týkají, provedou nejprve aktualizaci stavu osobních i jiných údajů na současný stav a následně teprve zahájí další zpracování. K provedeným zálohám dat má přístup pouze správce IT.

Systém provádění četnosti záloh a jejich zabezpečení je zaznamenáno ve vnitropodnikové směrnici k GDPR.

F. 4. Likvidace datových nosičů, bezpečné mazání dat

Datové nosiče, které obsahují informace s osobními údaji a jiné neveřejné informace organizace (diskety, CD-ROM, flash disky, HDD apod.) určené k vyřazení musí být odevzdány správci IT, který zajistí jejich bezpečné smazání či fyzickou likvidaci nosiče, aby byla minimalizována možnost obnovy dat z takového nosiče. Bezpečné smazání/fyzická likvidace je prováděna následujícím způsobem:

- CD-ROM, DVD-ROM, CD-RW, DVD-RW: rozřezáno pomocí skartovacího stroje nebo manuálně znehodnoceno tak, aby nebylo možné jeho další použití (např. manuálním rozlomením)
- Flash disky: funkční disky budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních bude fyzicky zlikvidován paměťový čip;

- HDD: funkční disky budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních proběhne provrtání v oblasti ploten disků, nebo rozebrání a fyzická likvidace magnetické vrstvy;
- Zálohovací kazety: funkční kazety budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních kazet proběhne rozebrání a páska bude rozstříhána.

Nepoužívaná datová media nikdy nelikvidujeme prostým vyhozením do komunálního odpadu před jejich fyzickou likvidací popsanou v předchozích bodech!

O likvidaci dat bude sepsán příslušný záznam/protokol.

Mzdy a personalistika – doby pro uchovávání osobních údajů podle zákona

V tomto článku Vám přinášíme podrobnější seznámení s dobami právního nároku u jednotlivých tiskopisů a osobních údajů v rámci mzdové a personální agendy. Tyto informace jsou důležité zejména pro dodržení zásady „Omezení uložení“ dle nařízení GDPR.

Dobu uschovávání zpracovávaných osobních údajů z mezd a personalistiky pro jednotlivé zákony určuje právní nárok. Správce osobních údajů však může zvýšit délku této doby nad právní nárok daný zákonem na základě oprávněného zájmu, který však musí náležitě zdůvodnit.

Délka doby uschovávání zpracovávaných údajů dle právního nároku

Zákon číslo	Název		Právní nárok	Dokumenty
262/2006Sb.	Zákoník práce	Výpočet mezd	4 roky	
582/1991Sb., (§37)	Zákon o organizaci a provádění soc. zabezpečení	Důchodové pojištění	30 let	Mzdové listy
582/1991Sb., (§35a, odst. 4 písm. d)		Důchodové pojištění	10 let	Mzdové listy pro poživatele starobního důchodu
582/1991Sb., (§35a, odst. 4 písm. a)		Evidenční listy důchod. poj.	3 roky	Stejnopisy ELDP
589/1992Sb.	Zákon o pojistném na sociální zabezpečení		10 let	Přehledy, oznamovací povinnost, kontroly
187/2006Sb.,(§95)	Zákon o nemocenském pojištění	Nemocenské pojištění	10 let	Doba doč. prac. neschop., doba karantény, doba ošetřování, doba mateřské a rodičovské

				dovolené, doba otcovské, atd.
48/1997Sb., (§10)	Zákon o veřejném zdravotním pojištění		10 let	Oznamovací povinnost
592/1992Sb.,(§22,25)	Zákon o pojistném na veřejné zdravotní pojištění		10 let	Kontrola, přehledy
586/1992Sb.	Zákon o daních z příjmu	Daň ze závislé činnosti	10 let	
563/1991Sb.	Zákon o účetnictví	vazba na účetnictví, identifikační osobní údaje, statistické údaje	4 roky 30 let 4 roky	Veškerá mzdová legislativa

Nový modul GDPR v rámci informačního systému SQL Ekonom

Pro všechny naše zákazníky jsme připravili zcela nový modul GDPR v rámci informačního systému SQL Ekonom. Modul vychází vstříc všem zákazníkům, kteří budou potřebovat jednoduše a přehledně evidovat požadavky a práva fyzických osob (subjektu údajů).

Všechny fyzické osoby z řad zaměstnanců, zákazníků, dodavatelů, klientů organizací budou mít od 25. 5. 2018 řadu nových práv. Každá organizace musí o těchto požadavcích vést přehlednou evidenci, kterou doloží případné kontrole soulad s GDPR.

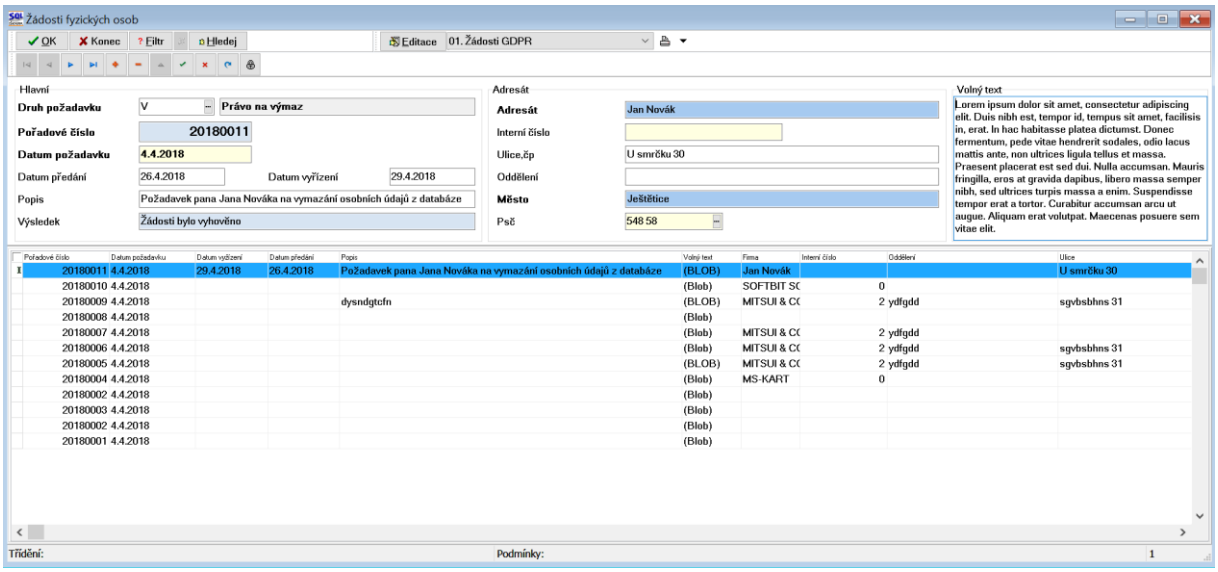
Jedná se hlavně o tato práva:

- Práva na přístup k osobním údajům
- Právo na výmaz (být zapomenut)
- Právo vznést námitku
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo na omezení automatického rozhodování

Dále každá organizace, která zpracovává osobní údaje na základě souhlasu, bude muset vést evidenci těchto souhlasů s datem od kdy, do kdy a k jakému účelu je souhlas platný.

Nový modul umí:

- Evidovat požadavky fyzických osob v rozsahu nových práv
- Evidovat souhlasy ke zpracování osobních údajů podle jednotlivých účelů
- Uchovávat veškerou dokumentaci k právům fyzických osob a jejich souhlasům
- Sledovat, zda požadavky jsou řešeny v zákonem stanovené lhůtě
- Zobrazovat podklady pro kontrolní orgán
- a další



Obrázek: Formulář žádostí o práva fyzických osob

Cenu nového modulu jsme stanovili podle součtu počtu fyzických osob, které každá společnost zpracovává, tj. počet zaměstnanců, počet dodavatelů a odběratelů z řad fyzických osob, počet klientů, dětí atd.

Ceník, uživatelé IS SQL Ekonom:

	Do 500 FO	Do 1000 FO	Do 3000 FO	Do 5000
Cena do 25. 5. 2018	1000,- Kč	2000,- Kč	3000,- Kč	4000,- Kč
Cena po 25. 5. 2018	1600,- Kč	3000,- Kč	4600,- Kč	5600,- Kč

Ceník, zákazníci, kteří nevlastní IS SQL Ekonom

	Do 500 FO	Do 1000 FO	Do 3000 FO	Do 5000
Cena do 25. 5. 2018	1700,- Kč	2700,- Kč	3700,- Kč	4700,- Kč
Cena po 25. 5. 2018	2300,- Kč	3700,- Kč	5300,- Kč	6300,- Kč

Modul si můžeme objednat přímo formou zaslání emailové objednávky na email softbit@softbit.cz. Při objednávce sdělte, prosíme, do počtu fyzických osob, které Vaše organizace spravuje a dále zda jste uživateli IS SQL Ekonom či ne.

Na základě objednávky Vám vystavíme licenční smlouvu a dodáme software pro evidenci požadavků a práv fyzických osob podle GDPR.

Nabídka služeb GDPR

Naší prioritou je dodávat našim zákazníkům kompletní služby. Z tohoto důvodu Vám nabízíme poskytování služeb pro řešení GDPR.
Rádi Vám umíme nabídnout:

- Zpracování úvodního **vnitřního auditu** k evidenci, uchovávání a zabezpečení veškerých informací o fyzických osobách, a to jak v elektronické, tak i v listinné podobě
- na základě tohoto auditu je zpracována **vnitropodniková směrnice** k nakládání s osobními údaji podle nařízení GDPR, která popisuje jednotlivé části v informačních systémech a evidenci dokumentů ve Vaší společnosti a navrhujeme taková řešení, která povedou k zajištění vyšší bezpečnosti dat o fyzických osobách
- toto by měl být začátek naší spolupráce. Doporučuji revizi vnitropodnikové směrnice vždy za určité období (rok asi ideální), kdy se provedou inventarizace změn proti předchozímu období a vyhodnotí se provedené změny
- **školení** všech pracovníků společnosti, kteří přicházejí do styku s osobními údaji subjektu údajů
- s každým klientem k tomuto uzavíráme smlouvu pro služby „**Pověřence pro ochranu osobních údajů“**, kde Vám garantujeme zajištění komplexního servisu k GDPR včetně metodické podpory. Tato služba je standardně bez žádného paušálního poplatku.
- v případě, že by ve Vaší společnosti došlo k incidentu se ztrátou osobních dat a byli jste za tuto chybu vyšetřování, nabízíme i spolupráci při řešení těchto situací. Nejsme však právníci tak, abychom Vás zastupovali u případného soudu. Věřím, že s naší pomocí se těmto událostem však vyhnete.

Ceník nabízených služeb

GDPR – vnitropodniková směrnice	7,000,00 Kč
Práce spojené s lokalizací směrnice na podmínky Vaší společnosti	900,00 Kč
Odborné školení pracovníků společnosti v oblasti ochrany osobních dat	1.200,00 Kč
Cestovní výdaje při osobních návštěvách	9,00 Kč/km + 450,00 Kč/hod strávený čas na cestě
Služby „Pověřence pro ochranu osobních dat“	Bez paušálního poplatku hodinovou sazbou

NA ZÁVĚR

Pevně věříme, že informace, které jsme Vám poskytli v tomto našem novém magazínu, jsou pro Vás užitečné a praktické.
Za celý kolektiv pracovníků firmy Vám přeji krásné prožití letních měsíců a dovolených.

Tomáš Urban
ředitel společnosti

Softbit software, s.r.o.
Nad Dubinkou1634
516 01 Rychnov nad Kněžnou
Tel.: 494 532 202, 494 534 354; fax: 494 377 63
e-mail: softbit@softbit.cz
www.softbit.cz