MINISTERSTVO
PRŮMYSLU A OBCHODU

PŘÍRUČKA PRO PŘÍPRAVU MALÝCH A STŘEDNÍCH FIREM NA GDPR

Obsah

Upozornění: Tato příručka je pouze základním a zjednodušeným souhrnem informací o obsahu obecného nařízení o ochraně osobních údajů (GDPR) a jeho dopadu na činnost malých a středních podniků (pozn.: Malý a střední podnik je podnik, který zaměstnává méně než 250 osob a jehož roční obrat nepřesahuje 50 mil. EUR nebo jehož bilanční suma roční rozvahy nepřesahuje 43 mil. EUR). Nemůže být brána jako komplexní nástroj nahrazující systematické vzdělávání všech řídících pracovníků i všech zaměstnanců firem na správnou práci s osobními údaji zaměstnanců a zákazníků či klientů, klade si za cíl pouze poskytnout základní vhled do nejdůležitějších oblastí problematiky, které se dotknou každé malé a střední firmy a v podrobnostech zejména firem, které se zaměřují na výrobu a obchod. Před započetím jejího čtení je třeba upozornit na to, že některá specifická pravidla, jejichž popis je nad možnosti rozsahu této příručky, se použijí například pro firmy zabývající se výzkumnou činností, statistickým zjišťováním, přímým marketingem nebo mezi jejichž hlavní činnosti patří podrobný monitoring osob například prostřednictvím mobilních aplikací nebo klientských věrnostních programů anebo zpracování osobních údajů dětí a mladistvých. I přesto, že jde o nástroj zjednodušený, snaží se příručka popisovat dopady GDPR a na ně promítnuté životní situace firem přesně a jasně, je však třeba počítat s tím, že ji v žádném případě nelze aplikovat na všechny obory podnikání. Pro podrobnější informace specificky se vztahující k vašemu oboru působení a způsobu zpracování osobních údajů doporučujeme dále konzultovat problematiku s Úřadem pro ochranu osobních údajů, nebo využít služeb specializovaných poradců.

1. ÚVOD DO PROBLEMATIKY

CO JE GDPR?

GDPR – anglicky General Data Protection Regulation neboli obecné nařízení o ochraně osobních údajů, celým názvem 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, je nový právní předpis EU, kterým je zaváděna evropská reforma ochrany osobních údajů. V celé EU nabude účinnosti dnem 25. května 2018, je přímo závazné a má přednost před vnitrostátními zákony.

- **CO JE JEHO CÍLEM:** cílem je posílit práva subjektů osobních údajů jako fyzických osob-nositelů osobních dat v celé EU i při pohybu jejich osobních dat mimo Unii.

- **JAKÉ K TOMU VOLÍ PROSTŘEDKY:** posiluje práva subjektů údajů na straně jedné a na straně druhé přitvrzuje na povinnostech správců a zpracovatelů údajů.

- **KOHO SE DOTKNE:** co do povinností dopadá na všechny firmy i orgány veřejné moci v EU i ty, které kdekoli ve světě zpracovávají osobní údaje osob nacházejících se v EU.

- **CO TO BUDE ZNAMENAT PRO FIRMY:** nutnost revize pravidel pro práci s osobními údaji vašich zaměstnanců, klientů i partnerů. Inventarizace dosud používaných údajů, způsobu práce s nimi, jejich správnosti, úplnosti, ochrany, zabezpečení a toho, zda je ještě potřebujete pro svou činnost, resp. zda je zpracováváte legitimně. Současně bude nutná revize vztahů s vašimi dodavateli, odběrateli, zpracovateli dat a všemi, kdo dosud s osobními daty procházejícími vaší firmou přišli nebo v budoucnosti budou přicházet do styku.

TIP: Jste si vědomi svých povinností správce údajů podle nyní platné legislativy (zákona č. 101/2000 Sb. o ochraně osobních údajů)? Plníte již nyní všechny své povinnosti správce osobních údajů? Pak pro vás zřejmě nebude problém pochopit logiku GDPR a ztotožnit se s jeho základními pravidly.

POZOR: GDPR je nařízení, nikoli směrnice. Platí tedy přímo a má přednost před zákonem. Ačkoli nový zákon o zpracování osobních údajů není k 1. březnu 2018 dosud schválen, není na místě čekat na nová vnitrostátní pravidla, protože GDPR a jeho principy jsou pro přípravu firem na novinky plně použitelné přímo. Nařízení nabývá účinnosti dnem 25. května 2018 a jeho odklad na úrovni EU ani opatřením národního zákonodárce není reálný. Není tedy na místě s přijetím opatření váhat.

KDO JE KDO DLE GDPR?

Před dalším výkladem je dobré označit si relevantní aktéry, tedy vymezit:

- **KDO JE DLE GDPR SUBJEKTEM ÚDAJŮ:** jakákoli identifikovaná nebo identifikovatelná fyzická osoba – nositel osobních údajů.

PŘÍKLAD: Subjektem údajů je váš zaměstnanec, klient – fyzická osoba podnikající i spotřebitel, jste jím i vy sami jako majitel nebo zaměstnanec firmy.

- **KDO JE SPRÁVCEM ÚDAJŮ:** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

PŘÍKLAD: Správcem údajů je vaše firma ve vztahu k vašim zaměstnancům či klientům a partnerům. Stává se jím v okamžiku převzetí údajů a zahájení jejich zpracování – formálně a ve strukturované podobě nebo i neformální cestou a nestrukturovaně, například formou uložení e-mailu či záznamu telefonního hovoru. Od tohoto okamžiku určuje účely a prostředky jejich zpracování.

KDO JE ZPRACOVATELEM ÚDAJŮ: fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

PŘÍKLAD: Zpracovatelem údajů může být firma, která pro vás externě zpracovává mzdovou agendu, poskytuje vašim zaměstnancům firemní benefity nebo například zajišťuje ostrahu vašeho závodu. Osobní údaje vašich zaměstnanců jí předáváte ke zpracování, avšak je to stále vaše firma jako správce údajů, kdo určuje účel zpracování údajů. Zpracovatelem je i firma likvidující osobní údaje ve vyřazené výpočetní technice.

KDO JSOU PŘÍJEMCI ÚDAJŮ: fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty. Pokud příjemce údaje dále o své vůli zpracovává, stává se dalším správcem, ale to je z pohledu původního správce irelevantní. Příjemcem však není orgán veřejné moci, který údaje může získávat v rámci své činnosti.

PŘÍKLAD: Příjemcem údajů může být správce sítě, který provádí vzdáleným přístupem údržbu nebo opravu vašeho počítače – získá přístup k osobním údajům, které máte v počítači uloženy, avšak dále s nimi nepracuje. Příjemcem mohou být i pracovníci správy budovy, kteří ověří totožnost příchozích osob podle občanského průkazu, avšak data z něj si nezaznamenávají ani s nimi dále nepracují – tito všichni mohou přijít do kontaktu s vašimi osobními údaji nebo s dokumenty, které je obsahují, avšak sami s daty v nich obsaženými obvykle dále nepracují.

KDO SI MUSÍ USTANOVIT ZÁSTUPCE SE SÍDLEM V EU: ten, kdo zpracovává osobní údaje občanů EU a/nebo provádí zpracování údajů na území EU, avšak není usazen (tj. nemá sídlo ani pobočku) v žádné ze členských zemí Unie.

PŘÍKLAD: Poskytovatel jakékoli online služby, která vyžaduje registraci uživatelů nebo e- shopu, který má sídlo mimo EU, avšak na území EU působí, má - byť by neměl v EU pobočku svého podniku - povinnost ustanovit si v EU svého zástupce, který bude k dispozici jako kontakt pro subjekty údajů a dozorové orgány.

KDO JE NÁRODNÍM DOZOROVÝM ÚŘADEM: nezávislý orgán veřejné moci zřízený členským státem EU; pro ČR je takovým dozorovým úřadem Úřad pro ochranu osobních údajů (dále jen ,,ÚOOÚ") - (www.uoou.cz), který přijímá stížnosti subjektů údajů a současně plní roli kontrolní a konzultační směrem ke správcům a zpracovatelům údajů.

CO JE TO EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ: ÚOOÚ, stejně jako dozorové úřady všech ostatních členských států EU, bude mít od účinnosti GDPR svého zástupce v Evropském sboru pro ochranu osobních údajů, který monitoruje naplňování GDPR na celém území EU a v celém rozsahu jeho působnosti, provádí výkladovou činnost, je poradním orgánem Evropské komise a v neposlední řadě může v rámci mechanismu jednotnosti i slaďovat postup dozorových orgánů členských států včetně ukládání pokut. Předchůdcem Sboru je Pracovní skupina podle článku 29 nyní platné Směrnice 95/46/ES (tzv. Article 29 Working Party neboli WP 29), která mimo jiné provádí i právně nezávazný výklad GDPR.

POZOR: Na úrovni ČR je sice Úřad pro ochranu osobních údajů národním dozorovým úřadem, avšak gesci za legislativu pro ochranu osobních údajů v rámci české vlády má Ministerstvo vnitra, ÚOOÚ je spolugestorem. V Česku tak na rozdíl od některých jiných evropských zemí, např. od Slovenska, neplní ÚOOÚ roli regulátora ochrany osobních údajů.

TIP: V rámci revize práce s osobními údaji ve vaší firmě si kromě dalšího pečlivě inventarizujte i své zpracovatele údajů a podívejte se na smlouvy o zpracování osobních údajů, které s nimi máte uzavřeny. Rozhodně by měly obsahovat klauzule o odpovědnosti zpracovatele, o zabezpečení samotného zpracování dat i jejich přenosu mezi vaší firmou a zpracovatelem a ohlašovací povinnost zpracovatele v případě porušení zabezpečení údajů. Dobré je také zamyslet se nad tím, jaká data poskytujete ke zpracování mimo vaši firmu a zda není možné objem takto přenášených osobních údajů snížit nebo pseudonymizovat (což si lze představit jako dočasnou anonymizaci údajů). Ušetří vám to mnoho budoucích starostí s řešením vztahů se zpracovateli.

POZOR: Vzhledem k subjektům údajů platí princip společné odpovědnosti správců a zpracovatelů za škodu způsobenou porušením GDPR – náhrady škody způsobené ztrátou, zničením, deformací nebo jiným pochybením při zpracování osobních údajů se tedy subjekt údajů může domáhat u kteréhokoli správce nebo zpracovatele údajů a je třeba prokázat, že k němu skutečně nedošlo právě ve vaší organizaci. Lze tedy důrazně doporučit, aby vztahy při zpracování údajů mezi správci a zpracovateli byly řešeny co nejpřesněji.

CO JE CO DLE GDPR?

GDPR neobsahuje přelomově novou definici osobních údajů oproti dosud platné české legislativě, za **osobní údaj** jsou totiž považovány dle GDPR veškeré informace o identifikované nebo identifikovatelné fyzické osobě; zákon o ochraně osobních údajů přitom hovoří o osobě určené nebo určitelné.

PŘÍKLAD: GDPR explicitně hovoří o tom, že osobním údajem je jméno, identifikační číslo, lokační údaje, síťový identifikátor anebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Může tedy jít např. i o IP adresu počítače či mobilního zařízení, e-mailovou adresu nebo lokalizační údaj, s nímž je ztotožnitelná konkrétní osoba, SPZ automobilu, která je přiřaditelná ke konkrétnímu uživateli-fyzické osobě, ale i nezaměnitelné znaky fyzické podoby člověka, jako je způsob chůze, mimika, barva duhovky oka, genetický údaj obsažený v lidské tkáni nebo otisk prstu.

Zvláštní ochrany pak zasluhují **tzv. zvláštní kategorie osobních údajů,** za které se považují **osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod fyzických osob.**

PŘÍKLAD: Citlivými osobními údaji jsou údaje o rasovém či etnickém původu, genetické a biometrické údaje, údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci, politické názory, náboženské vyznání, filosofické přesvědčení, ale i členství v odborech. Citlivým osobním údajem tedy může být například informace, že dotyčný subjekt údajů má fyzický handicap, hlásí se, byť veřejně, k jistému politickému přesvědčení nebo náboženskému vyznání, nebo náleží do určitého etnika nebo má určitý rasový původ.

Současně je na místě vymezit si, jaké nejdůležitější procesy dle GDPR přicházejí v úvahu a tedy:

CO JE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ: je to jakákoliv automatizovaná nebo manuálně prováděná operace nebo soubor operací s osobními údaji nebo soubory osobních údajů.

PŘÍKLAD: Může jít o: 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 údajů. Zpracováním údajů je tedy jakákoli operace s osobními údaji získanými systematicky nebo nahodile v písemné, ústní, nebo audiovizuální podobě.

CO JE EVIDENCÍ OSOBNÍCH ÚDAJŮ: jakýkoliv strukturovaný soubor osobních údajů přístupný podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný nebo rozdělený podle funkčního či zeměpisného hlediska.

PŘÍKLAD: Evidencí údajů je jakýkoli excelový soubor, soupiska účastníků či abecedně či jinak seřazená prezenční listina, sofistikovaná databáze klientů či jejich prostý abecední seznam.

NA KTERÉ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ SE GDPR VZTAHUJE: nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

PŘÍKLAD: Osobní údaje přijaté do vaší firmy prostřednictvím doručení vizitek vašich obchodních partnerů se stávají předmětem ochrany v okamžiku, kdy se tyto vizitky stávají součástí uspořádané evidence – lhostejno, zda se jedná o evidenci manuálně či elektronicky vedenou a lhostejno, zda se jedná o samostatnou evidenci jednotlivého zaměstnance (kontaktní seznam v telefonu či poštovní schránce) nebo evidenci sdílenou (firemní CRM – Customer relationship management – řízení vztahů se zákazníkem, nebo jiný evidenční systém). To neplatí pro obecné firemní emailové adresy nebo telefonní čísla na ústřednu.

NA KTERÉ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ SE GDPR NEVZTAHUJE: nařízení GDPR se nevztahuje zejména na zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností. Nevztahuje se dále ani na orgány činné v trestním řízení (jejichž činnost upravuje zvláštní právní úprava) a na zpracování v rámci obrany a zajištění bezpečnosti ČR.

PŘÍKLAD: Na vedení seznamu řemeslníků, které soukromě kontaktujete při potřebě služby v domácnosti ani na vaši soukromou evidenci poskytovatelů kosmetických služeb, servisu automobilů nebo domácích spotřebičů se GDPR nevztahuje. Předpokladem ovšem je, že uvedené kontakty slouží pouze pro vaši osobní, nikoli pro firemní potřebu a nejsou součástí žádné firemní evidence údajů.

POZOR: GDPR se vztahuje jak na elektronické, tak i na papírové či manuální kartotéční zpracování osobních údajů. Častým omylem bývá, že pravidla jsou vztahována pouze na jednu z forem zpracování, ale opak je pravdou – GDPR se použije na všechny, a to od okamžiku, kdy se údaje staly součástí jakékoli elektronické evidence nebo manuálně vedené uspořádané evidence.

POZOR: Častou nežádoucí praxí je mixování osobních údajů určených pro vlastní potřebu zaměstnanců – domácké zpracování – a pro potřebu firmy např. ve služebních telefonech nebo služebních noteboocích používaných i pro soukromou potřebu. Lze jen doporučit ukončení této praxe a striktní oddělení osobních údajů, které ke zpracování přijímá zaměstnavatel jako správce údajů a těch, které slouží výlučně pro osobní potřebu zaměstnance a GDPR se na ně tedy nevztahuje, nebo jasné nastavení pravidel pro zacházení s firemními údaji v mobilních IT zařízeních zaměstnanců, včetně jejich odpovídající odpovědnosti za zabezpečení takových údajů. Mimo jiné vám to ušetří spoustu administrativy při hlášení případů porušení zabezpečení údajů a možné důsledky uplatnění náhrady škody při zneužití údajů.

ZÁKLADNÍ ZÁSADY GDPR

GDPR stojí na několika základních zásadách, které je nutné jako obecné principy používat pro jakékoli zpracování údajů. Jedná se o tyto zásady:

ZÁKONNOST ZPRACOVÁNÍ, která ukládá zpracování osobních údajů výlučně zákonným způsobem a ze zákonných důvodů.

PŘÍKLAD: Důvody pro zákonnost zpracování mohou být plnění povinnosti vyplývající správci nebo zpracovateli ze zákona, plnění smlouvy, ochrana životně důležitých zájmů subjektu údajů nebo plnění úkolu ve veřejném zájmu, může jím být i oprávněný zájem správce údajů. Důvodem pro zákonné zpracování může být i souhlas udělený ke zpracování subjektem údajů, jeho podoba a náležitosti jsou ale podle GDPR poněkud odlišná a složitější oproti dosavadním zvyklostem a měl by optimálně jako podklad pro zákonnost zpracování sloužit pouze tam, kde se jiných důvodů pro zákonnost nedostává.

TIP: Lze jen doporučit revizi souhlasů ke zpracování osobních údajů, které vaše firma v minulosti získala od zaměstnanců a klientů. Ve velké většině případů nebude nutné zpracování údajů provádět „pod souhlasem“, ale pro zpracování údajů např. zaměstnanců budou ve velké míře jiné důvody, např. povinnosti uložené zaměstnavateli zákonem. Rozhodnete-li se využít souhlasu jako důvodu pro zákonnost zpracování, je nutné počítat s tím, že dříve dané souhlasy musí způsobem svého udělení odpovídat GDPR.

POZOR: Pokud se pro zpracování údajů rozhodnete využít souhlas jako právní titul, je třeba počítat s tím, že musí mít dle GDPR přesně stanovené parametry: musí jít o jednoznačný projev vůle, který je svobodný, konkrétní co do osobních údajů nebo jejich typů, kterých se týká, účelu jejich zpracování, informovaný – před jeho udělením tedy subjekt údajů musí mít k dispozici veškeré relevantní informace – oddělitelný a tedy de facto oddělený od ostatních smluvních ujednání, musí být aktivně projeven (minimálně např. zaškrtnutím políčka, nikoli formou odsouhlasení políčka předem zaškrtnutého). Udělením souhlasu není možné podmiňovat poskytnutí služby nebo uzavření smlouvy a nelze na něm postavit zpracování údajů tam, kde existuje principiálně nerovnovážný vztah mezi správcem a subjektem údajů – např. zpracovatel je orgánem veřejné moci a subjekt údajů občanem apod. Pro každý účel a na něj navázaný způsob zpracování, nejsou-li účely jednoznačně propojeny, musí být udělen samostatný souhlas. Souhlas také musí vždy obsahovat poučení o možnosti či právu jej odvolat.

KOREKTNOST A TRANSPARENTNOST ZPRACOVÁNÍ, která znamená, že všechny informace o zpracování musejí být bezúplatně, jednoduše a transparentně přístupné, při jejich publikaci musí být využit jasný a srozumitelný jazyk, optimálně by měly být publikovány v písemné podobě (ústně na vyžádání subjektu údajů) a tam, kde to je možné, elektronicky. Hmatatelným vyjádřením transparentnosti jsou mj. informační povinnosti správců vůči subjektům údajů.

PŘÍKLAD: Zásada transparentnosti se v praxi promítá ve firemní politice práce s osobními údaji (tzv. privacy policy), o jejíchž pravidlech by subjekty údajů měly být jednoduše, dostupným způsobem a bezplatně informovány – například na webové stránce správce údajů nebo ve zvláštní záložce či boxu v aplikaci. Informace by měly být jasné, srozumitelné a dávat subjektům údajů základní obecné informace o tom, jak bude s jejich osobními údaji při činnosti vaší firmy nakládáno.

ÚČELOVÉ OMEZENÍ SHROMAŽĎOVÁNÍ OSOBNÍCH ÚDAJŮ, která ukládá správcům zpracovávat osobní údaje výlučně k účelu, k němuž byly shromážděny a způsoby, které jsou s ním slučitelné.

PŘÍKLAD: Jsou-li osobní údaje shromážděny za účelem registrace subjektů údajů jako účastníků semináře pořádaného správcem údajů, je možné k nim obvykle jako účel dalšího použití přiřadit i rozesílání obchodních sdělení správce, protože tyto účely zpravidla nebudou neslučitelné. K tomuto dalšímu zpracování je zapotřebí zvláštního/dalšího právního titulu, kterým v tomto případě bude souhlas subjektu údajů se zasíláním obchodních sdělení na jeho kontaktní e-mailovou nebo poštovní adresu, nebo oprávněný zájem správce, ledaže je převážen zájmy subjektu údajů.

MINIMALIZACE ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ, v jejímž rámci mohou být osobní údaje shromažďovány pouze v přiměřené míře a v nezbytném rozsahu ve vztahu k danému účelu zpracování.

PŘÍKLAD: Praktickým vyjádřením této zásady je i tzv. standardní ochrana osobních údajů – tedy přístup, v jehož rámci má ochrana osobních údajů jednu z nejvyšších priorit při zpracování jakýchkoli dat o subjektech údajů. Zpracovávána by měla být pouze ta data, která jsou vzhledem k naplnění daného účelu nezbytná – například pro uzavření pracovního poměru se zaměstnancem, který nepřichází do styku s finanční hotovostí, zbraněmi či výbušninami a není tedy v zájmu zaměstnavatele bezpodmínečně nutné sledovat jeho trestní bezúhonnost, by nemělo být vyžadováno doložení výpisu z rejstříku trestů. Pro online nákup elektroniky pak například provozovatel e-shopu nepotřebuje znát datum narození zákazníka, počet a věk jeho dětí, to, zda zákazník nosí či nenosí brýle, jaké jsou jeho politické preference nebo náboženské cítění.

PŘESNOST OSOBNÍCH ÚDAJŮ v praxi znamená, že zpracovávány by měly být pouze přesné osobní údaje, které v případě potřeby budou aktualizovány a správce přijme veškerá opatření k opravě či výmazu údajů nepřesných.

PŘÍKLAD: Zaměstnankyně správce údajů změní po svatbě příjmení, tuto skutečnost nahlásí na personální oddělení svého zaměstnavatele. Automaticky by pak mělo dojít ke změně jejího příjmení ve všech evidencích (mzdové, docházkové, stravovací apod.) zaměstnavatele jako správce údajů i všech jeho zpracovatelů a zaměstnankyně by tak od hlášení změny neměla být nucena hlásit změnu na více místech. Obdobně tomu bude u změny bydliště či jakýchkoli jiných osobních údajů vedených o firemních zákaznících či zaměstnancích.

OMEZENÉ ULOŽENÍ OSOBNÍCH ÚDAJŮ, a to na dobu pouze nezbytně nutnou k dosažení daného účelu zpracování, po jejímž uplynutí by osobní údaje měly být automaticky vymazány.

PŘÍKLAD: Po realizaci jednorázového nákupu ve specializovaném e-shopu by osobní údaje zákazníka měly být uchovány pouze po dobu nezbytně nutnou pro uplatnění jeho případného nároku z vad zboží, maximálně pak na dobu, po kterou zákazník udělil svůj souhlas se zasíláním obchodních sdělení e-shopu. Přichází však v úvahu i oprávněný zájem na uchování osobních údajů i po delší dobu – tento oprávněný zájem je však třeba přesně identifikovat a zákazníka o něm informovat. Jeho příkladem může být dlouhodobé sledování situace na trhu. Stejně tak by měla být po uplynutí určité doby po jednorázové návštěvě ZOO, akvaparku, kulturní akce nebo využití jakékoli jiné služby smazána osobní data návštěvníků, kteří si

například zakoupili vstupenky online nebo svůj nákup platili kartou, anebo jejichž pohyb po areálu poskytovatele služby byl nějakým způsobem monitorován. Jiná je samozřejmě situace tam, kde je subjekt údajů pravidelným uživatelem služby, účastní se věrnostního návštěvnického programu nebo udělil svůj explicitní souhlas s dalším zasíláním obchodních sdělení poskytovatele služby.

POZOR: Automatický výmaz údajů poté, co jejich zpracování přestalo být nutné pro daný účel zpracování, dosud v českém prostředí není zvykem – data se (a to často duplicitně či vícenásobně v různých evidencích a informačních systémech) uchovávají pro eventuální budoucí potřebu, aniž by si firmy uvědomovaly, že tím porušují již nyní platné předpisy. Současně jde i o zbytečnou komplikaci - čím více dat a čím více evidencí, tím větší riziko nepřesnosti údajů, jejich nadbytečnosti ve vztahu k účelu jejich zpracování a tím vyšší pravděpodobnost porušení zabezpečení údajů spojené s povinností toto porušení hlásit a nést důsledky v podobě náhrady škody nebo sankcí.

INTEGRITA A DŮVĚRNOST ZPRACOVÁNÍ, která obnáší požadavek na odpovídající zabezpečení údajů a jejich ochranu pomocí vhodných technických nebo organizačních opatření vůči neoprávněnému a protiprávnímu zpracování, náhodné ztrátě a zničení či poškození.

PŘÍKLAD: Praktickou ukázkou naplnění zásady integrity a důvěrnosti zpracování může být praxe, v jejímž rámci správce údajů zpřístupňuje plný obsah zaměstnanecké databáze pouze pracovníkům, kteří tyto údaje nutně potřebují pro výkon zaměstnání na své pracovní pozici, nebo umožnění editačního práva pouze vybrané skupině uživatelů nebo i jen jedinému uživateli. Zaměstnavatel jako správce údajů tím zamezí jednak možnému úniku dat z databáze, a současně preventivně i nesprávnostem či neúplnostem v evidenci zaměstnaneckých osobních údajů.

ODPOVĚDNOST SPRÁVCE, která zahrnuje povinnost správce dodržet všechny povinnosti vyplývající ze zásad GDPR a současně i povinnost správce prokázat dodržení shody všech svých postupů a procesů zpracování údajů s těmito zásadami.

PŘÍKLAD: Dodržení všech povinností správce vyplývajících z GDPR může být zkoumáno v obecné i v konkrétní rovině, v oblasti nastavení procesů i v realizaci procesu zpracování v konkrétním případě. Současně by správce měl postupovat v obdobných případech zpracování vždy stejně nebo alespoň kompatibilním způsobem tak, aby shodu bylo možné prokázat u všech procesů zpracování obdobné povahy. Například pro všechny osobní údaje zaměstnanců by měly platit stejné obecné zásady, přístupy a metodiky, které se aplikují ve všech případech zaměstnanců konzistentně, a nemělo by se stát, že se praxe změní například s personální obměnou na postu vedoucího HR oddělení (human resources – oddělení lidských zdrojů).

TIP: Nestačí jen být s GDPR fakticky v souladu, ale musíte to i prokázat. K tomu vám při případné kontrole dozorového úřadu a/nebo i při interním auditu či kontrole ochrany osobních údajů napomůže vymezení obecných postupů a procesů ještě před tím, než zahájíte zpracování údajů podle nových pravidel GDPR, a následné striktní dodržování předem stanovených procesů a postupů ve všech relevantních případech zpracování osobních údajů. Každé konkrétní zpracování by mělo mít svůj obecný vzor v metodickém postupu, standardním procesu nebo schváleném systému workflow. Ještě před účinností GDPR je tedy dobré mít tyto procesy nastaveny a současně i upraveny interní předpisy, pracovní smlouvy, popisy práce atp. Do účinnosti GDPR je optimální i absolvovat pilotní provoz spojený s testováním (např. i na fiktivních případech) praktického naplňování vašich povinností správce údajů a realizace uplatňování práv subjektů údajů.

POZOR: Každý řádný správce údajů by si měl pro sběr a zpracování osobních údajů osvojit trojčlenku „pouze to, co je nutné - pouze k přesně stanovenému účelu - pouze po dobu ohraničenou naplněním tohoto účelu“ a současně vždy dbát na transparentnost, přesnost, důvěrnost a bezpečnost zpracování údajů. K datům včetně osobních údajů je třeba přistupovat jako ke vzácné komoditě, která je bohatstvím firmy, jehož nikdy nesmí být, byť ani nedbalostí nebo nevědomě, zneužito.

2. PRÁVA SUBJEKTŮ ÚDAJŮ

Nejdůležitější práva subjektů údajů lze rozdělit na dvě skupiny: na ta, na jejichž naplnění má subjekt údajů právo automaticky i bez vyžádání (a která na druhé straně tedy odpovídají automatické povinnosti správce údajů) a ta, která se uplatní pouze na žádost subjektu údajů. Dle tohoto členění tedy subjektům údajů náleží:

A) VE SKUPINĚ AUTOMATICKY SE UPLATŇUJÍCÍCH PRÁV:

- **PRÁVO NA INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ** má každý subjekt údajů, jehož osobní údaje přebírá správce ke zpracování od subjektu údajů přímo nebo zprostředkovaně od jiného správce. Automaticky pak musí správce subjekt údajů informovat o veškerých podstatných náležitostech tohoto získání a zpracování údajů jako jsou kontaktní údaje správce, jeho případného pověřence pro ochranu osobních údajů, rozsah získaných údajů, účel, ke kterému budou zpracovávány, důvod pro legitimitu zpracování i dobu, po kterou budou zpracovávány či u správce uloženy. Není nutné informovat o tom, co subjekt údajů ví. Pokud vyplňuje např. formulář, není nutné jej informovat o údajích, které právě vyplnil, ale jen o účelech zpracování, totožnosti správce a dalších náležitostech.

Z FIREMNÍHO ŽIVOTA: Okamžitě po získání osobních údajů od zákazníka, který si založil klientskou kartu, jsou mu v písemné podobě poskytnuty nebo na kontaktní e-mail zaslány informace o tom, které osobní údaje o něm řetězec, jehož věrnostní program se rozhodl zákazník využít, začal shromažďovat (krom vstupních informací se jedná i o sběr informací o jeho nákupech), co je účelem zpracování těchto údajů (nabídnout lépe na míru padnoucí služby a nabídky) a jaký je právní podklad pro tuto činnost (oprávněný zájem obchodního řetězce spočívající v marketingové strategii). Subjekt údajů je současně upozorněn na to, že proti sběru svých osobních údajů má právo podat námitku, anebo podat stížnost k Úřadu pro ochranu osobních údajů.

- **PRÁVO NEBÝT PŘEDMĚTEM AUTOMATIZOVANÉHO ROZHODNUTÍ ZALOŽENÉHO NA PROFILOVÁNÍ** znamená, že o právech subjektu údajů nemůže být rozhodováno automatickými prostředky, mj. na základě profilu subjektu údajů, pokud to pro subjekt údajů má právní účinky nebo se ho to dotýká obdobně významným způsobem – tedy podle automatizovaného zpracování osobních údajů například na základě pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se subjekt údajů nachází, nebo jeho pohybu. Výjimkou jsou případy, kdy s tím subjekt údajů souhlasí nebo kdy je to nezbytné k uzavření nebo plnění smlouvy (např. zřízení účtu na webu vyžaduje zadání nějakých nezbytných kontaktních údajů a bez toho bude automaticky přerušeno).

Z FIREMNÍHO ŽIVOTA: Podle GDPR tedy bude zakázáno automatické rozřazování klientů či zaměstnanců do skupin a následné automatické nabídnutí nebo přiznání diferencovaných nabídek či benefitů těmto subjektům údajů právě podle jejich příslušnosti k těmto skupinám – profilům. Normování práce, které by se odbývalo výlučně na základě automatizovaného sběru dat a následného automatického zařazení zaměstnance do stupně osobního ohodnocení založeného na výkonu bez individuálního posouzení situace zaměstnance jeho nadřízeným tedy bude napříště zapovězeno, neboť to má na zaměstnance přímý zásadní dopad. Stejně tak tomu bude například i při určování bonity klientů bank a následném automatickém přiřazování jednotlivých bonitních skupin k nabídkám produktů nebo míry úrokové sazby. Cílem je zamezit časté praxi, kdy je subjektům údajů často automaticky (bez lidské intervence) upírán přístup k výhodnějším nabídkám či lepší uplatnění práv jen proto, že se staly příslušníky méně preferované skupiny-profilu.

- **PRÁVO NA VÝMAZ („PRÁVO BÝT ZAPOMENUT“)** by se mělo uplatnit automaticky tam, kde již osobní údaje nejsou potřebné pro účel, ke kterému byly zpracovány, nebo pro další kompatibilní účel, nebo pokud například subjekt údajů odvolá svůj souhlas se zpracováním. Pokud by snad správce k výmazu nepřistoupil automaticky, má subjekt údajů právo si realizaci práva vyžádat. Právo na výmaz však není možné realizovat tam, kde jsou údaje dále uchovávány či zpracovávány z důvodu plnění právní povinnosti, ochrany veřejného zdraví, archivace nebo například pro výkon, určení či obhajobu právních nároků.

Z FIREMNÍHO ŽIVOTA: Pan P. ukončil svůj pracovní poměr u firmy Q. Zaměstnavatel s ukončením jeho pracovního poměru automaticky vymazal údaje o jeho rodinných příslušnících, které potřeboval pro účely poskytování zaměstnaneckých benefitů – podnikových rekreací, zneplatnil jeho pracovní e-mailovou adresu i mobilní telefonní číslo a zařídil, aby e-mailová schránka automaticky odesílala zprávu „Pan P. již u nás nepracuje, v případě potřeby, prosím, kontaktujte jeho kolegu pana Z." Z důvodu plnění svých právních povinností však prozatím firma Q zachovala mzdovou agendu pana P., veškeré údaje vztahující se k daňové povinnosti pana P. i firmy Q, účasti pana P. na systému sociálního zabezpečení i údaje o sledování jeho zdravotního stavu v průběhu zaměstnání pro účely eventuálních budoucích nároků z nemoci z povolání. O rozsahu vymazaných i dále uchovávaných údajů pana P. při ukončení pracovního poměru písemně informoval.

PRÁVO NA OPRAVU ČI AKTUALIZACI ÚDAJŮ náleží subjektu údajů automaticky, avšak lze je uplatnit i na žádost v případě, že by správce k opravě či aktualizaci údajů nepřistoupil z vlastní iniciativy. Správce je v rámci tohoto práva povinen bez zbytečného odkladu opravit nepřesné osobní údaje, které se jej týkají. Současně má právo na doplnění neúplných údajů, například formou poskytnutí dodatečného prohlášení.

Z FIREMNÍHO ŽIVOTA: Paní P. ještě pod svým dívčím příjmením pravidelně navštěvovala fitness centrum, po svatbě a narození dítěte však službu delší dobu nevyužila. Protože fitness centrum nabízelo svým klientům zajímavé podmínky věrnostního programu, po delší době paní P. požádala o aktualizaci svých kontaktních údajů a přiznání zákaznické slevy na další vstupy do fitness centra. To její žádosti vyhovělo, automaticky změnilo příjmení paní P. ve své databázi a přiznalo jí i zpětně slevu pro stálé zákazníky, protože si ověřilo, že byť paní P. fitness centrum navštěvovala pod dvěma různými příjmeními, jedná se o tutéž osobu.

B) VE SKUPINĚ PRÁV NA ŽÁDOST SUBJEKTU ÚDAJŮ:

PRÁVO ZÍSKAT OD SPRÁVCE OSOBNÍCH ÚDAJŮ potvrzení o zpracování údajů má každý subjekt údajů. Má možnost uplatnit jej prostřednictvím žádosti u kteréhokoli správce údajů a získat pak od správce potvrzení, zda jeho osobní údaje jsou či nejsou zpracovávány.

Z FIREMNÍHO ŽIVOTA: Pan S. pojal podezření, že je systematicky sledován kamerovým systémem společnosti U a dotázal se proto, zda společnost zpracovává jeho osobní údaje. V okamžiku vznesení dotazu o něm společnost žádná jeho osobní data nezpracovávala, to se nicméně změnilo v okamžiku, kdy pan S. položil svůj dotaz. Společnost U si pro vyhovění jeho žádosti musela ověřit jeho identitu i vizuální podobu a pro účely budoucí evidence zpracování a předejití eventuálním sporům o to, zda bylo právo řádně uplatněno, tak byla nucena osobní údaje pana S. zavést do své evidence. Pana S. pak informovala o tom, že doposud sice jeho osobní údaje nezpracovávala, avšak od nynějška již zahajuje zpracování údajů v nezbytném rozsahu nutných k dokumentaci naplnění práva pana S. na získání potvrzení o zpracování údajů.

PRÁVO NA PŘÍSTUP SUBJEKTU K OSOBNÍM ÚDAJŮM navazuje na právo předchozí – pokud totiž údaje o subjektu údajů jsou správcem zpracovávány, pak má subjekt údajů právo na přístup k těmto údajům a na informace zejména o rozsahu, účelu a době zpracování jeho osobních údajů včetně informace o tom, z jakého zdroje byly údaje získány. Pokud firma provádí takové zpracování, že není schopna identifikovat subjekt údajů, který právo využil (např. snímá SPZ aut na firemním parkovišti), nemusí jen pro splnění žádosti sama získávat další osobní údaje, ale je na subjektu údajů, aby jí s identifikací pomohl (přijel jsem s touto SPZ v určitý čas) za účelem výkonu svého práva.

Z FIREMNÍHO ŽIVOTA: Pan F. byl opakovaně telefonicky kontaktován společností M., která se specializuje na přímý marketing. V rámci telefonátu sice původně vyjádřil svůj souhlas s obchodními sděleními a sledováním svého zákaznického chování, s kterými jej společnost M. kontaktovala, avšak později již se cítil být neustálými nabídkami obtěžován. Požádal proto o informaci o tom, jaké osobní údaje a k jakému účelu o něm společnost M. zpracovává. Poté, co se dozvěděl, že sleduje jeho zákaznické chování a pocitové reakce na nově uváděné produkty za účelem zlepšování své marketingové strategie, svůj souhlas s doručováním obchodních sdělení odvolal a požádal si o výmaz všech svých osobních údajů z databáze společnosti M. Protože neexistoval jiný právní důvod pro zpracování údajů, společnost byla nucena mu vyhovět, údaje o jeho zákaznickém chování vymazala a již jej v budoucnosti nekontaktovala. Po dobu dvou let od žádosti o výmaz nicméně ještě uchovávala údaje o způsobu realizace tohoto práva tak, aby měla zdokumentováno jeho řádné naplnění a vyhnula se případné stížnosti pana F. na postup firmy.

PRÁVO ZÍSKAT KOPII ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ je další součástí práva na přístup k údajům, kterou lze uplatnit na žádost subjektu údajů. Správce je pak povinen poskytnout mu kopii zpracovávaných osobních údajů.

Z FIREMNÍHO ŽIVOTA: Paní A. měla zájem o získání výpisu ze svého klientského účtu vedeného v rámci věrnostního programu řetězce hypermarketů T. Požádala si proto v rámci práva o přístup k údajům o výpisy ze své zákaznické karty a současně i o výpis informace o tom, které nákupy byly hrazeny v hotovosti a které platební kartou. Zjistila tak, že za poslední dvě léta v několika hypermarketech tohoto řetězce utratila celkem 72.000 Kč. Mimo jiné se jí takto podařilo získat informace o běžící záruce ke kuchyňskému robotu, u kterého již vyhodila účet. Současně byla s to na svých vlastních nákupech zpětně zjistit, že vynecháním nákupů cukrovinek by mohla ušetřit více než 5000 Kč. Zajímavá pro ni byla i informace o tom, že více než 90 % svých nákupů uskutečnila bezhotovostně prostřednictvím platební karty.

PRÁVO NA OMEZENÍ ZPRACOVÁNÍ má subjekt údajů v některých zvláštních případech za předpokladu, že je zapotřebí ověřit přesnost zpracovávaných osobních údajů, nebo jsou dány důvody pro výmaz, který však nelze z různých důvodů realizovat, údaje jsou nutné pro obhajobu právních nároků nebo subjekt údajů vznesl proti jejich zpracování námitku.

Z FIREMNÍHO ŽIVOTA: Pan I. uplatnil u firmy Q. právo na výmaz svých osobních údajů, v žádosti uvedl, že u firmy naposledy jednorázově nakupoval před více než 3 lety a že tedy není právní důvod pro další zpracování jeho údajů. Prověřením na právním oddělení Q. bylo zjištěno, že firma vede proti panu I. soudní řízení o úhradu části kupní ceny. Obchodní oddělení prověřilo rozsah osobních údajů, které Q. o panu I. vedla a zjistilo, že krom údajů nutných pro vedení obchodního sporu s panem I. jako podnikající fyzickou osobou obchodní databáze obsahuje i řadu informací o starších, již úspěšně ukončených obchodních případech s panem I. Tyto údaje proto vymazala a omezila zpracování údajů pouze na data nutná k vedení sporu s panem I. ohledně posledního obchodního případu.

PRÁVO NA PŘENOSITELNOST ÚDAJŮ znamená právo subjektu údajů na získání osobních údajů, které se jej týkají, od správce, který je zpracovává a předání těchto údajů ke zpracování jinému správci. Údaje musejí být předány ve strukturovaném, běžně používaném a strojově čitelném formátu. Další podmínkou pro realizaci přenositelnosti je, že se jedná o zpracování založené na souhlasu nebo smlouvě a současně jde o zpracování automatizované. K předání údajů by mělo optimálně dojít přímo mezi správci údajů navzájem bez toho, aby subjekt údajů byl nucen se na přenosu dat sám podílet.

Z FIREMNÍHO ŽIVOTA: Paní B. měla oblíbenou službu pro online přehrávání hudby, ve které měla vytvořenu řadu playlistů pro využití při různých příležitostech jako zvukový podkres při práci, hudební doprovod k aerobicu nebo relaxační hudbu. Poté, co si koupila nový telefon, však zjistila, že aplikace není ke stažení v App Storu operačního systému, který používá výrobce jejího nového telefonu. Požádala si proto o přenos svých údajů spočívajících v playlistech sestavených pod jejím uživatelským jménem k nově vybranému poskytovateli audiovizuálního obsahu online, jehož aplikaci si nainstalovala na novém telefonu. Přenos proběhl zcela bez nutnosti jejího zásahu a paní B. pak měla možnost pokračovat v poslechu oblíbené hudby i z nového telefonu.

PRÁVO VZNÉST NÁMITKU proti zpracování údajů lze efektivně uplatnit zejména tehdy, pokud zpracování provádí správce na základě svých oprávněných zájmů, ve veřejném zájmu nebo při výkonu veřejné moci, včetně zpracování z obou těchto důvodů zahrnujícího profilování – tj. automatizované zařazení subjektu údajů do skupiny dle jeho výkonnosti, zdravotního stavu, ekonomické situace a podobně. Subjekt údajů musí argumentovat svou výjimečnou situací; to neplatí, pokud využívá možnost vznést námitku vůči zpracování údajů pro účely přímého marketingu. Od okamžiku vznesení námitky správce údaje nesmí dále zpracovávat, jedinou výjimku tvoří situace, kdy správce prokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy, právy a svobodami subjektu údajů nebo jsou nutné pro uplatnění právních nároků. Je však třeba upozornit, že tato výjimka neplatí pro oblast přímého marketingu.

Z FIREMNÍHO ŽIVOTA: Pan S. se cítil být obtěžován neustálými telefonáty pracovníků firmy U.T., kterými byly zjišťovány jeho zákaznické preference. Telefonáty sice neobsahovaly žádnou určitou obchodní nabídku a pracovník firmy mu při posledním rozhovoru, který pana S. vyrušil z obchodního jednání, vysvětlil, že ke sběru informací o situaci na trhu včetně chování zákazníků dochází z důvodu realizace průzkumu trhu, který je hlavním předmětem podnikání U.T., a telefonické dotazování vybraných vzorků zákazníků včetně pana S. je prováděno v rámci oprávněného zájmu firmy U.T., pan S. však přesto telefonicky formuloval svou námitku proti dalšímu svému kontaktování a vedení svých osobních údajů v databázi U.T. Firma námitku akceptovala, dále již pana U.T. v rámci průzkumů trhu nekontaktovala a ze své databáze vymazala všechny údaje kromě základních informací o námitce pana S. a způsobu jejího vyřízení včetně informace o tom, že osobní údaje pana S. včetně telefonního čísla byly z databáze U.T. vymazány.

TIP: Naplňování práv subjektů údajů může vaši firmu administrativně zatížit – obzvláště tam, kde nejste na zvýšenou možnost dotazování ze strany svých klientů či zaměstnanců dobře připraveni. Je zcela jistě na místě uvažovat o publikaci online formulářů pro realizaci práva na přístup k údajům a zpracovat si typizované formulářové informace určené pro subjekty údajů v okamžiku zahájení zpracování jejich osobních dat, do nichž vaši zaměstnanci vždy jen doplní potřebné náležitosti či relevantní pole. Pro snadný kontakt subjektů osobních údajů s vaší firmou je dobré mít jednu sběrnou e-mailovou adresu určenou výlučně pro vyřizování žádostí týkajících se zpracování osobních údajů ve vaší firmě nebo jednoho pracovníka/jeden útvar, který bude řešením těchto žádostí u vás ve firmě pověřen.

POZOR: Pokud nejste malá a střední firma s počtem zaměstnanců do 250 provádějící pouze příležitostné zpracování necitlivých osobních údajů s nízkým rizikem, a neplatí tedy pro vás výjimka z povinnosti vést evidenci o činnostech zpracování údajů, dohlédněte na to, aby způsob uplatňování a naplňování práv subjektů údajů byl evidován optimálně na jednom místě nebo v rámci jednoho systému ve vaší firmě tak, aby v případě kontroly bylo možné spolehlivě prokázat, jak jsou v obecné rovině nastaveny mechanismy pro naplňování práv subjektů údajů i jak naplňování práv běží v konkrétních případech.

3. POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ ÚDAJŮ

Naopak vaše firma jako správce údajů by si měla osvojit všechny své povinnosti, z nichž některé jsou v českém prostředí zcela nové. Jde zejména o:

- **POVINNOST VÉST ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ:** každý správce údajů má dle GDPR povinnost vést písemné záznamy o všech činnostech souvisejících se zpracováním údajů, které budou dostupné na vyžádání dozorovému úřadu. Takovými záznamy mohou být výstupy v obecné podobě ve formě schválených podnikových směrnic nebo politik, a dále pak vzorové procesy vedoucí k plnění úkolů a realizaci operací souvisejících se zpracováním údajů jako je automatizace procesů při likvidaci údajů, které mají být vymazány, změny v informačních systémech včetně jejich propojení, realizace potřebných změn smluvní dokumentace a inventarizace souhlasů udělených se zpracováním údajů včetně jejich zrušení tam, kde souhlasů dle GDPR nebude zapotřebí, a změn tam, kde dle GDPR budou zachovány, avšak musejí získat novou podobu. Takovým záznamem může být i popis předem nastaveného systému, který představuje soubor organizačních a technických opatření, které vaše firma jako správce údajů zavedla pro zajištění bezpečnosti a zákonnosti zpracování údajů. Z povinnosti vést záznamy o činnostech zpracování platí jediná výjimka – povinnost neplatí pro malé a střední podniky do 250 zaměstnanců provádějící pouze příležitostné zpracování necitlivých osobních údajů s nízkým rizikem.

Z FIREMNÍHO ŽIVOTA: O. jako výrobní firma se začala připravovat na aplikaci GDPR. Počet jejích zaměstnanců byl sice nižší než 250, ale zpracování údajů nebylo příležitostné a zahrnovalo i rizikové operace a nechtěla proto riskovat, že v době nabytí účinnosti GDPR nesplní svou povinnost vést záznamy o činnostech zpracování údajů. Nejprve inventarizovala všechna aktuální úložiště osobních údajů, zmapovala všechny procesy, v jejichž rámci byly ve firmě doposud přenášeny a zpracovávány osobní údaje a určila si osoby zodpovědné za jednotlivé fáze zpracování. Poté přistoupila ke zpracování projektu optimalizace objemu vedených osobních údajů, k racionalizaci procesů jejich zpracování a zúžení počtu osob, které s osobními údaji přicházejí do styku tak, aby co možná nejvíce snížila rizika z poškození, deformace, ztráty nebo jiného porušení zabezpečení údajů. Poté, co identifikovala způsob budoucí úpravy procesů zpracování, přepracovala svou interní dokumentaci, v které přesně vymezila role a odpovědnosti jednotlivých úseků a pracovníků, kteří s osobními údaji přicházeli do styku a věnovala pozornost i procesům, které povedou k úspěšnému naplnění práv subjektů údajů i O. jako správce údajů. Záznamy o veškerých provedených operacích zařadila do obecných informací o vedení záznamů o operacích zpracování.

Podařilo se také realizovat několik nových nástupů zaměstnanců a dodat první zakázky již v souladu s novými pravidly, na těchto prvních případech pak byly odladěny drobné nedostatky a nedorozumění při aplikaci nových pravidel. Všechny obchodní případy i zaměstnanecké složky byly zaneseny do hlavní evidence v informačním systému určeném pro vedení záznamů o zpracování osobních údajů, který si firma určila jako centrální úložiště informací o operacích zpracování. V tomto centrálním úložišti pak byla napříště shromažďována evidence o individuálních operacích zpracování osobních údajů a firma si tak byla jista, že plní svou evidenční povinnost.

- **POVINNOST ZAJISTIT ODPOVÍDAJÍCÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ:** Správce i zpracovatel údajů musejí dle GDPR přijmout s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, kontextu a rozsahu zpracování i k různě pravděpodobným a různě závažným rizikům všechna vhodná technická a organizační opatření k zajištění zabezpečení zpracování, kterými mohou být například šifrování, pseudonymizace (dočasná či přechodná anonymizace údajů pro účely určité fáze nebo určitého procesu jejich zpracování), zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb, schopnost obnovení údajů v případě bezpečnostních incidentů prostřednictvím racionálního systému jejich zálohování a automatizace procesů pro jejich obnovení a podobně.

Z FIREMNÍHO ŽIVOTA: Firma S., která podniká v oblasti energetiky, začala připravovat úpravu svých bezpečnostních opatření a jejich uvedení do souladu s GDPR. Zrevidovala své informační systémy, podívala se na existující rizikové matice a text své bezpečnostní směrnice. Zjistila, že veškeré své povinnosti správce osobních údajů v oblasti bezpečnosti plní, neb současně jako poskytovatel základní služby podléhá i přísným pravidlům pro kybernetickou bezpečnost. V souvislosti s účinností GDPR tedy v rámci svých procesů zpracování osobních údajů nastavila zejména racionální periodicitu pro přezkum míry rizikovosti všech firemních procesů pro zpracování osobních údajů a systém pro zjišťování a hlášení případů porušení zabezpečení údajů dle GDPR.

POZOR: Ani při vynaložení maximálních možných prostředků na zabezpečení údajů není možné nikdy dosáhnout nulového rizika, vždy je třeba pracovat s tzv. zbytkovým rizikem, které by optimálně mělo tvořit takové situace, které nastanou buď s minimální pravděpodobností, nebo závažnost hrozby bude velmi nízká. Proces zabezpečení a ošetřování rizik je procesem živým a neustále se opakujícím, kdykoli po bezpečnostním incidentu nebo významné změně rizikových faktorů je třeba jej znovu přehodnocovat a identifikovat přijatelnou míru zbytkového rizika i přijatelnou míru nákladů a kapacity na opatření směřující ke snížení bezpečnostních rizik.

POVINNOST OHLAŠOVAT BEZPEČNOSTNÍ INCIDENTY NA POLI OCHRANY OSOBNÍCH ÚDAJŮ: v případě jakéhokoli porušení zabezpečení údajů – tedy i v případech, kdy fyzicky nenastal únik dat, avšak pouze byla porušena jejich bezpečnost a je pravděpodobné riziko pro práva a svobody subjektu údajů – musí správce údajů bez zbytečného odkladu, nejpozději do 72 hodin, hlásit tento incident dozorovému orgánu a v případě, že je pravděpodobné, že tímto incidentem vznikne vysoké riziko pro práva a svobody fyzických osob-subjektů údajů, pak je nutné hlásit jej i dotčeným subjektům údajů.

Z FIREMNÍHO ŽIVOTA: V praxi jsou teoreticky chápaných „bezpečnostních incidentů" v životě každé firmy minimálně desítky denně: zapomenuté či bez dozoru ponechané pracovní flashdisky na konferencích či jednáních, bez dozoru ponechané papírové dokumenty, vyhazování dokumentů obsahujících osobní údaje do košů, ač by měly být skartovány, možné ztráty či zapomenutí služebních telefonů nebo počítačů. Hlásit ÚOOÚ se ale nemají incidenty, u kterých je vznik rizika nepravděpodobný (pokud někdo na chvíli opustí flashdisk v jednací místnosti nebo odejde od počítače na dobu kratší, než je opětovné zaheslování počítače). Je nanejvýš vhodné, aby vaše firma zavedla vzhledem k zaměstnancům, klientům i zpracovatelům údajů jasnou povinnost hlášení jakýchkoli relevantních bezpečnostních incidentů (ztráta pracovního notebooku, ztráta jiného nosiče nezašifrovaných dat apod.), a to nejlépe standardizovaným způsobem (online, ve formuláři) a nejlépe s povinností hlásit incident okamžitě poté, co nastane – jedině tak se totiž může vyhnout možnému postihu za nesplnění této své povinnosti. V praxi se sice může stát, že se správce údajů o porušení bezpečnosti dat vůbec nedozví (a nemůže jej tedy ohlásit dozorovému úřadu ani oznámit dotčeným subjektům údajů), pak to ale svědčí o tom, že mohl zanedbat některé své jiné povinnosti, zejména povinnost podniknout všechna organizační a technická opatření k zabezpečení údajů.

POVINNOST PROVÉST POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA): před započetím nových zpracování údajů, které obnášejí vysoké riziko pro práva subjektů údajů, má správce v rámci procesu hodnocení dopadů povinnost posoudit jejich vliv na ochranu údajů. Posouzení přitom není jednorázové, ale opakuje se kdykoli při zavedení nového procesu zpracování, který obnáší vysoké riziko, nebo při zvýšení míry rizika procesu již existujícího.

Z FIREMNÍHO ŽIVOTA: Tato povinnost je vyjádřením principu, který se prolíná celým GDPR a tím je přístup založený na riziku. V rámci procesní přípravy na GDPR lze tedy doporučit zpracování rizikové matice, která bude následně aplikována na všechny procesy zahrnující zpracování osobních údajů, a to podle pravděpodobnosti rizika a závažnosti jeho následku. Výsledkem hodnocení by měla být identifikace procesů s nízkým, středním a vysokým rizikem. U procesů s rizikem vysokým je pak zapotřebí dbát na konzultace s ÚOOÚ (viz níže). Je zapotřebí samozřejmě nezapomínat ani na průběžné hodnocení nových dopadů.

POVINNOST REALIZOVAT PŘEDCHOZÍ KONZULTACE S DOZOROVÝM ÚŘADEM: Tam, kde by mělo zpracování podle posouzení vlivů za následek vysoké riziko pro práva subjektů údajů, má správce povinnost přijmout opatření ke zmírnění tohoto rizika a tato opatření předběžně konzultovat s dozorovým orgánem. Tento konzultační proces má podle GDPR závazné lhůty a pravidla.

Z FIREMNÍHO ŽIVOTA: Firma Q. zpracovala rizikovou matici svých procesů zpracování osobních údajů a identifikovala tři stupně existujících rizik. U rizika nejnižšího stupně přijala pouze základní organizačně technická opatření k ochraně osobních údajů a jednotlivá rizika řešila jednotlivě podle jejich aktuální hrozby. U rizik středního stupně přijala systém opatření spočívající zejména ve vyšší míře zabezpečení údajů, při jejichž zpracování riziko vznikalo a současně využila systém přechodné anonymizace (pseudonymizace údajů) nebo jejich zašifrování. U druhů zpracování, která obnášela vysoké riziko, před přijetím opatření konzultovala své kroky s dozorovým úřadem. Mezi takové vysoce rizikové případy firma zařadila například databáze s velkým množstvím citlivých údajů nebo předávání velkého množství osobních údajů mimo EU nebo práci zaměstnanců z domova (homeoffice).

POVINNOST ZA URČITÝCH OKOLNOSTÍ JMENOVAT POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ: Tato povinnost platí pro všechny orgány veřejné moci a veřejné subjekty a dále pro všechny správce, jejichž hlavní činnost spočívá v rozsáhlém pravidelném a systematickém monitorování subjektů údajů a/nebo rozsáhlým způsobem zpracovávají citlivé osobní údaje a údaje týkající se rozsudků v trestních věcech. Vnitrostátní předpisy mohou stanovit požadavek na jmenování pověřence i v některých dalších případech, v českém právním prostředí se však s touto možností nepočítá. Pověřenec může ve firmě či organizaci figurovat jako její zaměstnanec nebo své služby poskytovat externě. Je však vždy zapotřebí, aby disponoval kombinací znalostí právních v oblasti ochrany osobních údajů, technických v oblasti bezpečnosti dat a informačních systémů a současně aby byl velmi podrobně zasvěcen do chodu firmy nebo organizace, které své služby pověřence poskytuje včetně znalosti o všech jejích agendách, procesním způsobu jejich realizace, využívaných informačních systémech a dalších úložištích osobních údajů. Současně musí být zařazen na pracovní pozici nejméně na stupni bezprostředně podřízeném hlavnímu řídicímu orgánu nebo osobě firmy. Pověřence si může firma nebo organizace jmenovat i dobrovolně, je však vždy třeba, aby jeho činnost naplňovala všechny znaky a povinnosti, které stanoví GDPR.

POZOR: V praxi se často vyskytuje mylné přesvědčení, že pověřenec musí mít zvláštní vzdělání, kvalifikaci či certifikaci. Opak je pravdou – GDPR ani český právní řád s ničím takovým nepočítají a je tedy na zodpovědnosti každé firmy či organizace, aby si zajistila služby takového pověřence a v takovém rozsahu, který vyhoví jejím potřebám. Kvalifikace musí odpovídat rozsahu, citlivosti a intenzitě zpracování osobních údajů v dané organizaci. Může jít od minimalistického řešení formou zlomkového externího úvazku až po ustavení interního týmu několika pověřenců, závisí vždy na rozsahu a povaze zpracování údajů u daného správce. Je také potřeba dávat pozor na to, aby se pověřenec nedostal do střetu zájmů. Neměl by tedy své služby poskytovat více správcům, kteří jsou v potenciálně konkurenčním postavení, ani by sám neměl zpracovávat osobní údaje či se podílet na jejich zpracování. Pověřence si lze představit jako jakéhosi firemního „auditora ochrany osobních údajů“, který slouží primárně jako poradce, mentor a kouč pro ostatní pracovníky firmy a jako kontakt pro subjekty údajů i dozorový úřad.

TIP: Pokud jste dospěli k názoru, že vaše firma bude muset dle GDPR zřídit pověřence, vyhodnoťte si nejprve rozsah zpracování citlivých údajů nebo monitoringu subjektů údajů, který ve vaší firmě provádíte, a v návaznosti na to odhadněte pravděpodobný rozsah činnosti pověřence. To bude podkladem pro vaše rozhodnutí o tom, zda zvolíte externistu či zda se pověřencem stane některý z vašich zaměstnanců.

Pozor – externista se nesmí dostat do střetu zájmů tím, že by poskytoval své služby více správcům údajů v reálně či potenciálně konkurenčním postavení, je tedy vyloučeno např. sdílení jednoho pověřence mezi členy podnikatelské asociace, kteří poskytují stejné nebo obdobné služby.

Naopak u interních pověřenců je třeba dávat pozor, aby se pověřenec nedostal do střetu zájmů tím, že sám bude určovat účely zpracování osobních údajů (nebo rozhodovat o nich). Pověřencem by tedy neměl být šéf firemního IT (spravuje uživatelské přístupy zaměstnanců k firemním systémům), vedoucí personálního oddělení (pracuje se zaměstnaneckými osobními údaji) ani šéf obchodu (spravuje klientské databáze) nebo financí (nastavuje pravidla pro workflow účetních dokumentů apod.). Jako racionální postup při jmenování interního pověřence se jeví nikoli nábor nového člověka, který by musel být od začátku zasvěcen do všech firemních procesů a systémů, ale spíše identifikace některého z vašich zkušených zaměstnanců jako budoucího pověřence a zajištění podmínek pro to, aby nejpozději od účinnosti GDPR tento splnil všechny podmínky pro fungování pověřence včetně zákazu střetu zájmů, a tedy i bezprostřední práci s osobními údaji.

POZOR: I pokud dospějete k tomu, že vaše firma pověřence potřebovat nebude, je vhodné k tomu zpracovat odůvodnění a vyhodnocení rozsahu a způsobu zpracování údajů ve vaší firmě ve vztahu k požadavkům GDPR na jmenování pověřence. Obzvláště pokud je vaše firma hraničním případem (např. provádí zpracování citlivých údajů, avšak nikoli rozsáhlým způsobem, jako je tomu kupříkladu u soukromé ordinace s jedním lékařem) nebo provádí monitoring subjektů údajů (avšak ten není součástí vaší hlavní činnosti), pomůže vám toto předběžné vyhodnocení a záznam o něm při eventuální budoucí kontrole dozorového úřadu.

4. PROCESNÍ PŘÍPRAVA FIREM NA ÚČINNOST GDPR

Při přípravě vaší firmy na účinnost obecného nařízení o ochraně osobních údajů byste měli dodržovat logickou a na sebe navazující posloupnost jednotlivých kroků přípravy tak, aby přípravy pokračovaly konzistentně a plynule a nebylo nutné některé kroky opakovat či se k nim zpětně vracet. V souladu s ověřenou praxí je tak možné doporučit nejprve:

A) INVENTARIZACI EXISTUJÍCÍHO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ, která by měla zahrnovat:

a. **Určení rozsahu** zpracovávaných osobních údajů
b. **Vyhledání osobních údajů:**
   i. ve strukturovaných datech / v databázích a evidencích
   ii. v nestrukturovaných datech / mimo databáze
c. **Zachycení osobních údajů ve firemních procesech,** a to:
   i. v procesech manuálních
   ii. v procesech automatizovaných
d. **Revize aktuálních metodik a interní dokumentace** se vztahem ke zpracování údajů
e. **Revize kvality** dosud zpracovávaných dat / osobních údajů
f. **Revize způsobu zabezpečení** údajů
g. **Revize způsobu nastavení kontrolních mechanismů a reportingu**

B) V návaznosti na ni pak pečlivé **NAPLÁNOVÁNÍ PROJEKTU SMĚŘUJÍCÍHO K IMPLEMENTACI GDPR** ve vaší firmě, který bude zahrnovat:

a. **Návrh konkrétních opatření,** které firma musí podniknout, aby její provoz byl kompatibilní s GDPR,
b. **Transformace procesů** firmy tak, aby byly v souladu s těmito opatřeními,
c. **Uvedení upravených procesů do provozu**
d. **Zajištění souladu** těchto procesů s GDPR i mezi sebou navzájem – tedy nastavení zabezpečení, kontrolních mechanismů, systému řízení rizik i auditního systému.

Konkrétní kroky, týkající se procesu inventarizace zpracování osobních údajů ve vaší firmě, prvotního vyhodnocení aktuálního stavu, rozsahu a způsobu vedení agendy zpracování i plánování a realizace implementačního projektu, jsou blíže popsány v následujících kapitolách.

5. PERSONÁLNÍ A ZAMĚSTNANECKÁ AGENDA

Jednou z důležitých oblastí, kterou bude ve vztahu k GDPR řešit každá firma kromě osob samostatně výdělečně činných, je oblast zpracování zaměstnaneckých osobních údajů. Personální a mzdová agenda je pro tuto oblast základní oblastí zpracování údajů, ke které není třeba souhlasu se zpracováním, neboť se odbývá téměř výlučně na základě plnění zákonných povinností zaměstnavatele, nebo v rámci plnění pracovní smlouvy, eventuálně v rámci naplňování oprávněného zájmu zaměstnavatele. Zahrnuje v sobě činnosti:

A) **PŘED VZNIKEM PRACOVNÍHO POMĚRU V SOUVISLOSTI S NÁBOREM ZAMĚSTNANCŮ A JEDNÁNÍ O PRACOVNÍ SMLOUVĚ,** která zahrnuje práci s údaji uchazečů o zaměstnání, s jejich životopisy, citlivými údaji o zdravotním stavu apod. I toto zpracování lze zařadit pod personálně-mzdovou agendu a není tedy pro ně nutný souhlas subjektů údajů, je však vždy třeba myslet na povinnost poskytnout při zahájení zpracování úplné spektrum informací o zpracování uchazečům jako subjektům údajů v tom rozsahu, v jakém je již nemají.

POZOR: Po ukončení výběrového řízení je třeba pečlivě zvážit, zda, k jakému účelu a po jakou dobu hodláte dále osobní údaje neúspěšných uchazečů uchovávat a buď je o tom informovat již předem při zahájení zpracování, nebo po ukončení výběrového řízení. Jako dobrou praxi je možné hodnotit uchování těchto údajů pro eventuální budoucí nabídku zaměstnání, což je zpracování z důvodu oprávněného zájmu zaměstnavatele, proti kterému může subjekt údajů, není-li s ním srozuměn, podat námitku. K uchovávání údajů by rozhodně nemělo dojít na dobu delší, než je několik málo let.

B) **V PRŮBĚHU SAMOTNÉHO PRACOVNÍHO POMĚRU,** jehož nedílnou součástí je již nyní práce s osobními údaji zaměstnanců, bez níž si nelze realizaci pracovněprávního vztahu vůbec představit. Součástí je nejen evidence mezd, dalších odměn, dávek sociálního zabezpečení a sociálního pojištění, dovolené nebo evidence docházky zaměstnanců, jejich služebních cest a podobně, ale i činnosti jako je použití fotografií nebo biometrických prvků na průkazech zaměstnanců nebo v jejich přístupových údajích, evidence pracovní docházky anebo vstupů zaměstnanců do jednotlivých prostor organizace zaměstnavatele, evidence pracovních úrazů, nemocí z povolání, vyřizování stížností zaměstnanců nebo povinné uchovávání dokumentace po ukončení pracovněprávního vztahu. Zpravidla půjde o zpracování kvůli právní povinnosti, plnění smlouvy, nebo z důvodu oprávněného zájmu (ochrana majetku apod.).

TIP: Pro vedení zaměstnanecké agendy osobních údajů je dobré zavést si jednotnou evidenci nebo jednotný informační systém, který bude formou elektronické kartotéky zaměstnanců sledovat rovněž i práci s jejich osobními údaji, systém jejich zpracování, uplatňování práv zaměstnanců jako subjektů údajů vůči zaměstnavateli jako správci a stejně tak bude obsahovat i přiřazení zákonných důvodů pro zpracovávání konkrétních osobních údajů.

C) **PO UKONČENÍ PRACOVNÍHO POMĚRU,** kdy postupně odpadají důvody pro další zpracování jednotlivých druhů osobních údajů zaměstnanců: pro vstup již není nutné uchovávat údaje o podobě nebo biometrických identifikátorech zaměstnanců, není nutné vést údaje o rodinných příslušnících zaměstnanců (krom údajů bezpodmínečně nutných pro daňovou evidenci). Naopak po určitou dobu po skončení pracovního poměru je nutné dále uchovat údaje z evidence mezd, důchodového, nemocenského a zdravotního pojištění zaměstnanců, jejich služebních cest, evidenci docházky, nemocí z povolání, ale i vyřizování stížností, a to nejméně po dobu promlčecí doby. Postupně však odpadají i tyto důvody, posledními z povinně ze zákona vedených údajů obvykle bývá doba expozice škodlivým vlivům pro účely eventuálního zpětného prokazování vzniku nemoci z povolání.

Krom této agendy však mezi zaměstnanci a zaměstnavateli jako mezi subjekty osobních údajů a jejich správci vzniká i řada dalších akcesorických agend, které zasluhují hlubší pozornosti při hledání jejich optimálního nastavení tak, aby byly plně v souladu s GDPR. Je zejména vhodné zaměřit se na zpracování údajů vznikajících při:

- Vedení databáze zájemců o práci (životopisy, shromažďování databáze uchazečů či potenciálních uchazečů i po výběrovém řízení nebo ještě před jeho zahájením)

- Užití fotografie zaměstnanců na internetu/intranetu anebo v PR materiálech firmy
- Správě personálních záležitostí mateřskou společností v rámci skupiny firem
- Politika whistleblowingu a její kolize s povinností mlčenlivosti zaměstnanců
- Uchovávání jiných než povinných osobních údajů bývalých zaměstnanců
- Provozu kamerového systému s uchováváním záznamu
- Permanentním monitoringu e-mailů nebo pohybu zaměstnanců na internetu
- Monitoringu obsahu počítačů
- Nahrávání telefonních hovorů
- GPS monitoringu služebních vozidel anebo dalšího vybavení svěřeného zaměstnanci
- Vedení databáze zaměstnanců jako zákazníků firmy
- Nakládání s kontaktními údaji rodinných příslušníků zaměstnanců.

POZOR: Citlivou a často v praxi nesprávně uchopenou otázkou je monitoring zaměstnanců a nastavení hranice mezi tím, kde jde ještě o oprávněný zájem zaměstnavatele na kontrole způsobu ekonomického využití prostředků, které svěřuje zaměstnanci k výkonu práce, a tím, kde jde již o nepřípustný permanentní monitoring zaměstnanců. Tuto otázku částečně řeší již nyní (a po účinnosti GDPR se na tom nic nezmění) zákoník práce, dle kterého je přiměřená (nepermanentní) kontrola možná, může ji realizovat každý zaměstnavatel. V souladu se zákoníkem práce i s GDPR je nicméně nutné o příležitostném monitoringu zaměstnance informovat, a to buď adresně a přímo nebo minimálně v rámci obecné politiky zaměstnavatele zakazující zneužití firemního vybavení. Vždy přitom platí, že kontrola by měla být příležitostná, časově omezená a decentní a jako takovou je pak možné považovat ji za součást personálně-mzdové agendy jako základního účelu zpracování.

Jiná by však situace byla u monitoringu permanentního – ať už se jedná o monitoring elektronické komunikace, telefonních hovorů nebo lokace zaměstnanců (včetně GPS lokátorů ve služebních automobilech). Zde si lze v určitých případech představit, že monitoring lze ještě odůvodnit oprávněnými zájmy zaměstnavatele, avšak v řadě případů již půjde o sledování za jeho hranou a nepostačilo by o něm zaměstnance informovat, nýbrž by bylo nutné k němu mít explicitní souhlas zaměstnance. V případě pochybností o oprávněnosti takového sledování zaměstnanců konzultujte dozorový úřad nebo se obraťte na specializovaného odborníka.

V rámci pracovněprávních vztahů je pak třeba klást zejména důraz na přípravu zaměstnavatelů na naplňování práv zaměstnanců na:

- **INFORMACE,** jejichž poskytnutí by mělo následovat bezprostředně po zahájení zpracování osobních údajů.
- **PŘÍSTUP K ÚDAJŮM,** v jehož rámci mohou zaměstnanci požadovat informace o celém spektru činností zaměstnavatele, které zahrnují zpracování jejich osobních údajů i o tom, které údaje, k jakému účelu a po jakou dobu jsou o nich shromažďovány i kdo jsou jejich další zpracovatelé. Obdobně jako doposud, bude i po zrušení zákona č. 101/2000 Sb. dále díky GDPR platit právo na přístup každého subjektu údajů k jeho vlastním údajům zpracovávaným u kteréhokoli správce včetně zaměstnavatele.
- **ZÁKAZ AUTOMATIZOVANÉHO ROZHODOVÁNÍ ZALOŽENÉHO NA PROFILOVÁNÍ ZAMĚSTNANCŮ,** například dle jejich pracovní výkonnosti, dovedností apod. O právech zaměstnanců nesmí být v těchto případech rozhodováno automaticky, tedy bez využití lidského faktoru v rozhodovacích procesech.

- **VÝMAZ ÚDAJŮ** tam, kde jich již není zapotřebí pro naplnění daného účelu zpracování.

TIP: Na osobní údaje zaměstnanců v rámci pracovněprávních vztahů nelze uplatnit právo na přenositelnost u těch údajů, které jsou zpracovávány na základě zákona, což je převážná většina zaměstnaneckých dat. Zaměstnanec tedy nemůže požádat o vyfiltrování všech nebo některých svých osobních údajů jednoho zaměstnavatele a požádat o jejich automatický přenos k jinému zaměstnavateli – mohlo by tím dojít jak k porušení zákonných povinností zaměstnavatele, tak i k narušení jeho oprávněných zájmů.

Naopak zaměstnavatelé se musejí připravit na naplňování svých nových povinností, pokud se týče:

- **OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ DOZOROVÝM ÚŘADŮM,** a to zejména v případech, kdy porušení zabezpečení způsobí vědomě, nevědomě nebo z nedbalosti jejich vlastní zaměstnanci.

- **OZNAMOVÁNÍ OBZVLÁŠTĚ ZÁVAŽNÉHO PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ VŠEM OSTATNÍM ZAMĚSTNANCŮM,** ať už k incidentu došlo zaviněním zaměstnavatele, některého ze zaměstnanců, zpracovatelů údajů nebo z důvodu externích vlivů.

- **VEDENÍ EVIDENCE O ČINNOSTECH TÝKAJÍCÍCH SE ZPRACOVÁNÍ ÚDAJŮ ZAMĚSTNANCŮ,** která zahrnuje jak obecné nastavení procesů a postupů, tak i informace o jejich realizaci v konkrétních případech. Z povinnosti vést záznamy o činnostech zpracování platí jediná výjimka – povinnost neplatí pro malé a střední podniky do 250 zaměstnanců provádějící pouze příležitostné zpracování necitlivých osobních údajů s nízkým rizikem.

Co do procesu přípravy zaměstnavatelů, lze zcela jistě doporučit:

- **REVIZI STÁVAJÍCÍHO PROSTŘEDÍ ZPRACOVÁNÍ ZAMĚSTNANECKÝCH OSOBNÍCH ÚDAJŮ** – jak jsou nastaveny kanály sběru údajů o zaměstnancích, kdo k nim má v průběhu zpracování přístup, jak jsou údaje uchovávány (úložiště papírových dokumentů nebo elektronických dat), zabezpečeny, jaký je cyklus jejich zpracování včetně toho, kdo je jejich zpracovateli mimo organizaci zaměstnavatele, jak je prováděna aktualizace údajů a kdy jsou naplněny podmínky pro výmaz údajů a jak k němu fakticky dochází.

- **REVIZI UDĚLENÝCH SOUHLASŮ SE ZPRACOVÁNÍM ÚDAJŮ** – v převážné většině případů bude možné souhlas se zpracováním údajů vypustit, je však o tom třeba informovat zaměstnance a současně mu poskytnout i všechny ostatní informace, jejichž poskytnutí ukládá zaměstnavatelům jako správcům údajů GDPR.

POZOR: Problematickým může v praxi být používání biometrických údajů zaměstnanců – například otisků prstu, snímku nebo videozáznamu obličeje apod. pro přístup do firemních prostor nebo systémů. Jde sice o praxi stále více se rozšiřující, v souladu s GDPR však k ní rozhodně nepostačí plnění smlouvy nebo oprávněný zájem zaměstnavatele jako právní titul pro zpracování údajů a je zapotřebí si od dotčených zaměstnanců vyžádat souhlas s použitím jejich biometrických dat.

- **REVIZE SMLUVNÍ DOKUMENTACE PRO ZAMĚSTNANCE** – od pracovních smluv až po předávací protokoly upravující používání služební techniky apod. Vzhledem k tomu, že řada účelů zpracování v pracovněprávních vztazích vyplývá přímo ze zákona, není nutné jejich zahrnutí do smlouvy. Rozšíření smluvních ujednání naopak lze doporučit tam, kde dochází ke zpracování údajů na základě oprávněného zájmu zaměstnavatele.

- **REVIZI METODICKÝCH POSTUPŮ, SMĚRNIC A JINÝCH INTERNÍCH PŘEDPISŮ ZAMĚSTNAVATELE** – ať už těch, které přímo upravují práci s osobními údaji, nebo těch, které se týkají dalších firemních procesů zahrnujících i zpracování osobních dat.

REVIZI SMLUV O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ S EXTERNÍMI SUBJEKTY – například se zpracovateli mzdové agendy, agenturami práce nebo náborovými agenturami, smluvními pracovními lékaři, firmami poskytujícími zaměstnanecké benefity jako jsou stravenky nebo programy výhod pro zaměstnance apod. V řadě případů ve smlouvách dosud není ochraně osobních údajů zaměstnanců věnována odpovídající pozornost, což se může stát zaměstnavateli fatálním například v případech, kdy by například zpracovatel nehlásil včas porušení zabezpečení osobních údajů – za porušení ohlašovací povinnosti směrem k dozorovému úřadu totiž odpovídá vždy správce, a to i v případech, kdy bezpečnostní incident vznikl při činnosti externího zpracovatele údajů.

REVIZI ZPŮSOBU VYSÍLÁNÍ ZAMĚSTNANCŮ K VÝKONU PRÁCE DO ZAHRANIČÍ – jednodušší situace bude sice při vysílání pracovníků v rámci Evropské unie, protože GDPR platí pro všechny členské země EU a navíc i pro země EHP (tedy Norsko, Lichtenštejnsko a Island), komplikovanější ale naopak při vysílání do třetích zemí. U těch GDPR rozlišuje země „bezpečné" (jejichž výčet – whitelist, aktuálně zahrnující 12 zemí nebo jejich částí, vydává svým rozhodnutím o adekvátní ochraně Evropská komise) a „nebezpečné" (jejichž výčet – blacklist - dosud nebyl publikován, avšak publikaci lze očekávat nejpozději s účinností GDPR). Do zemí bezpečných lze osobní údaje zaměstnanců přenášet bez dalšího, pro ty další však platí přísná omezení. Pro bližší informace o této problematice doporučujeme konzultaci s Úřadem pro ochranu osobních údajů nebo se specializovaným poradcem.

Z FIREMNÍHO ŽIVOTA: VÝBĚROVÉ ŘÍZENÍ NA NOVOU FUNKCI

Společnost S. se rozhodla vypsat výběrové řízení na nového vedoucího IT oddělení. Inzerát publikovala na svém webu a současně si vyhledání vhodného kandidáta zadala u externí personální agentury. Do výběrového řízení se přihlásilo 12 kandidátů, z nichž 7 postoupilo do užšího kola. Vhodný kandidát na volnou pozici byl skutečně nalezen a byla s ním uzavřena pracovní smlouva. Životopisy a další údaje 7 uchazečů, kteří se dostali do užšího výběru, si firma chtěla ponechat pro budoucí možné použití.

☹ Osobní údaje neúspěšných uchazečů zůstaly po realizaci výběrového řízení nekoordinovaně roztroušeny jak v personální agentuře, tak i na úsecích pracovníků, kteří se podíleli na výběru pracovníka (personální oddělení, úsek ředitele, právník). Špatně – není zajištěna odpovídající bezpečnost údajů.

☹ Životopisy všech neúspěšných uchazečů zůstaly zaarchivovány na personálním oddělení, ostatní úseky byly požádány o jejich skartaci. Neúspěšní uchazeči, kteří postoupili do druhého kola, nicméně nebyli informováni o tom, že jejich údaje jsou u zaměstnavatele uchovány pro eventuální potřebu budoucích výběrových řízení. Pro uchování údajů neúspěšných uchazečů, kteří do druhého kola nepostoupili, nezbyl žádný právní důvod. Špatně – nedošlo k výmazu nepotřebných údajů a žádný z neúspěšných uchazečů neobdržel informace o způsobu dalšího zpracování svých údajů.

☺ Všechny osobní údaje úspěšného uchazeče se staly součástí jeho osobního spisu. Osobní údaje neúspěšných uchazečů, kteří nepostoupili do dalšího kola, byly na všech dotčených úsecích skartovány. Životopisy uchazečů, kteří postoupili do druhého kola, byly skartovány na všech úsecích kromě personálního oddělení, které je převedlo do elektronické podoby a zařadilo do databáze potenciálních zájemců o zaměstnání ve firmě a informovalo o tom dotčené uchazeče. Správně – došlo k výmazu nepotřebných údajů, všechny dotčené subjekty údajů obdržely informace o dalším zpracování svých údajů a současně je i zajištěna odpovídající úroveň zabezpečení údajů.

HODNOCENÍ PRACOVNÍKŮ PODLE VÝKONU

Výrobní firma U.P. má zaveden systém normování práce, který obnáší i sledování výkonu zaměstnanců. Vzhledem k napjatému harmonogramu plnění firemních zakázek se nabízí i navázání systému odměňování zaměstnanců na plnění norem. Firma řeší, jak tento systém nadále provozovat v souladu s GDPR.

☹ Zaměstnanci jsou informováni o tom, že ve firmě probíhá systém sledování výkonnosti zaměstnanců a že budou odměňováni v návaznosti na svůj pracovní výkon, neobdrží už však informaci o tom, že sledován není jen počet vyrobených výrobků, ale i prostoje, resp. inaktivita zaměstnanců v pracovní době. Špatně – probíhá monitorování zaměstnanců, o kterém zaměstnanci neobdrželi úplné informace.

☹ Sledováno je několik indikátorů výkonnosti zaměstnanců, ti jsou o svém monitoringu řádně informováni. Všechny systémy sběru dat jsou automatické a zaměstnanci jsou hodnoceni dle pracovních výkonů na základě předem stanoveného klíče. O odměnách nerozhoduje nadřízený pracovník, ale zaměstnancům je přiděluje na základě jejich zařazení do výkonnostních stupňů automaticky mzdový systém. Špatně – do-

chází k nepřípustnému automatizovanému rozhodování o právech zaměstnanců na základě jejich profilování.

Zaměstnanci jsou informováni o tom, které indikátory jejich výkonnosti jsou sledovány. Sběr dat o výkonnosti zajišťuje systém pro sledování efektivity výroby, o odměnách zaměstnanců dle jejich výkonnosti pak (na návrh mzdového informačního systému, který čerpá data o výkonnosti jednotlivých zaměstnanců ze systému pro sledování výroby) rozhoduje jejich nadřízený pracovník. Správně – zaměstnanci mají všechny potřebné informace o svém monitoringu a současně nedochází ani k porušení zákazu automatizovaného rozhodnutí o jejich právech a povinnostech.

GPS VE SLUŽEBNÍCH AUTOMOBILECH

Jelikož opakovaně docházelo ke zneužívání osobních automobilů pro soukromé účely, rozhodla se firma S. umístit do nich GPS lokátory. Zaměstnance o této novince informovala s tím, že se jedná o opatření zahrnující novou formu zpracování osobních údajů zaměstnanců, které bylo zavedeno v zájmu zaměstnavatele.

GPS lokátory byly v provozu nepřetržitě a monitorovaly každé použití služebního automobilu kterýmkoli zaměstnancem firmy S. Špatně – jednalo se o nepřípustný permanentní monitoring subjektů údajů.

Záznamy z GPS lokátorů, které byly v provozu nepřetržitě, byly navíc zařazovány jako trvalá součást evidence služebních cest - knihy jízd. Tento požadavek dokonce vznesl na společnost S. při daňové kontrole místně příslušný správce daně. Špatně – kromě toho, že šlo o permanentní monitoring subjektu údajů, jednalo se dále i o zpracování osobních údajů bez právního důvodu: výpis z GPS lokátorů není nutné archivovat z důvodu plnění zákonné povinnosti, smlouvy a neobstojí ani hledisko oprávněného zájmu. Správce daně zde evidentně překročil svou pravomoc a požadoval průkaznost daňové evidence v rozsahu, který byl v kolizi s ochranou osobních údajů zaměstnanců společnosti S.

Provoz GPS lokátorů byl spouštěn pouze nahodile, a to dle klíče, který zaměstnancům nebyl znám. Jeho prostřednictvím byla zajišťována nepermanentní, avšak přesto efektivní kontrola využívání prostředků svěřených zaměstnavatelem zaměstnanci. Po období, za něž byly vyúčtovány služební cesty a pracovník správy vozového parku vše ověřil, byl proveden výmaz těchto údajů. Správně, jednalo se o nepermanentní kontrolu způsobu využívání pracovních prostředků svěřených zaměstnavatelem a současně byl zajištěn výmaz údajů, jejichž zpracování již nebylo nutné pro naplnění daného účelu, tedy oprávněného zájmu zaměstnavatele na kontrole ekonomického využívání služebních automobilů.

6. KLIENTSKÁ A OBCHODNÍ AGENDA

Podnikání jako činnost postavená na dosahování zisku samozřejmě nemůže být realizováno bez kontaktu se zákazníkem, resp. klientem, který, je-li fyzickou osobou (lhostejno, zda podnikající či nepodnikající), je sám subjektem osobních údajů, a nebo může být kontakt s osobními údaji jeho představitelů nedílnou součástí kontaktu s ním (je-li právnickou osobou, za kterou ve výsledku jednají fyzické osoby jako subjekty údajů). Je třeba při tom mít na paměti, že osobní údaje všech dotčených subjektů údajů je třeba chránit po celou dobu životního cyklu obchodního případu, tedy:

A) V RÁMCI JEDNÁNÍ S KLIENTEM PŘED UZAVŘENÍM SMLOUVY, kdy je třeba pečlivě hlídat, aby byly shromažďovány skutečně pouze údaje nezbytně nutné pro daný účel, kterým je uzavření smlouvy. Na tomto účelu je také postaven právní titul zpracování – oprávněný zájem na zpracování osobních údajů během jednání o budoucí smlouvě – a je nutné o něm informovat subjekt údajů.

POZOR: V případě neuzavření smlouvy je třeba vyhodnotit, zda existuje oprávněný zájem – např. eventuální budoucí obnovení jednání o smlouvě – na dalším uchovávání osobních údajů potenciálního klienta. Po určitou dobu po ukončení jednání o smlouvě je možné zpracovávat, resp. dále uchovávat tato data z titulu oprávněného zájmu na zpracování osobních údajů pro účely budoucího obchodního využití, toto uchování by však nemělo být neomezené a rámcově by nemělo přesáhnout dobu několika málo let.

B) V PRŮBĚHU REALIZACE SMLUVNÍHO VZTAHU je hlavním právním titulem pro zpracování údajů plnění smlouvy, které může dále kromě explicitně ve smlouvě ujednaného způsobu zpracování údajů zahrnovat i související účetní a daňovou agendu, oboustranný monitoring plnění smlouvy a jeho vyhodnocování, komunikaci se subjektem údajů týkající se plnění smlouvy nebo zajištění plnění ze smlouvy.

POZOR: Monitoring plnění ze smlouvy je účel zpracování, který lze navázat na plnění smlouvy jako zákonný důvod, tím však už není monitoring subjektu údajů, který využívá plnění, resp. produkt nebo službu, která je plněním ze smlouvy. Pro tento druh monitoringu je třeba získat explicitní souhlas subjektu údajů.

POZOR: Zpracování osobních údajů za účelem marketingu a propagačních akcí má vedle GDPR i speciální právní úpravu obsaženou v zákoně o ochraně spotřebitele a zákoně o některých službách informační společnosti. Podmínkou pro jakékoli zaslání obchodního sdělení je přitom fakt, že v minulosti proběhl aktivní kontakt správce se subjektem údajů, resp. nabízející firmy se zákazníkem, a současně dal subjekt údajů (zákazník) explicitní souhlas se zasíláním obchodních sdělení. Pozor tedy na jakékoli koupené či jinak převzaté databáze – oslovovat v rámci přímého marketingu subjekty údajů, které k tomu nedaly svůj souhlas, je praktika již nyní nezákonná a nejinak tomu bude i po nabytí účinnosti GDPR.

C) PO UKONČENÍ PLATNOSTI SMLOUVY ČI REALIZACE PLNĚNÍ, kdy po uplynutí lhůt pro možné uplatnění nároků z vad dodaného zboží a služeb (tedy dvou let pro náhradu škody a tří let pro promlčení dalších práv) lze uvažovat o povinnosti osobní údaje dále vést snad jen pouze z důvodu daňové evidence. Po expiraci i tohoto právního titulu pro zpracování by osobní údaje měly být bez dalšího vymazány, neboť odpadají všechny právní důvody pro jejich další zpracování – leda by důvodem byl oprávněný zájem vaší firmy na eventuálním budoucím obnovení obchodního vztahu.

V rámci obchodních vztahů je pak třeba klást zejména důraz na přípravu vaší firmy na naplňování práv vašich zákazníků na:

- **ZÍSKÁNÍ POTVRZENÍ O ZPRACOVÁNÍ ÚDAJŮ A PŘÍSTUPU K ÚDAJŮM,** tedy na to, zda je konkrétní osoba součástí vaší klientské databáze; v kladném případě pak i na přístup k těmto údajům a na informace o rozsahu zpracovávaných údajů, účelu zpracování, době, po kterou jsou údaje zpracovávány a informace o tom, z jakého zdroje pocházejí.

- **OPRAVU ČI AKTUALIZACI ÚDAJŮ,** tedy opravu nepřesností a neúplností, které by se snad vyskytly ve vašich klientských databázích.

- **PŘENOSITELNOST ÚDAJŮ** ze svého zákaznického účtu, pokud se týká historie nákupů, sledování preferencí nebo zákaznického chování na internetu.

- **ZÁKAZ AUTOMATIZOVANÉHO ROZHODOVÁNÍ ZALOŽENÉHO NA PROFILOVÁNÍ ZÁKAZNÍKŮ ČI KLIENTŮ,** například dle jejich preferencí, hodnoty nákupů, opakovanosti nákupů, spolehlivosti nebo objemu reklamací zboží apod. O právech zákazníků nesmí být v těchto případech rozhodováno automaticky, tedy bez využití lidského faktoru v rozhodovacích procesech.

- **VÝMAZ ÚDAJŮ** tam, kde jich již není zapotřebí pro naplnění daného účelu zpracování.

POZOR: Na rozdíl od pracovněprávních vztahů bude v obchodních vztazích zcela jistě právo na přenositelnost údajů hojně využíváno. Čím více si hýčkáte své zákaznické databáze, historie nákupů a seznamy preferencí svých klientů, tím více se vystavujete i riziku, že si výpisy z vaší evidence týkající se těchto projevů osobní povahy může klient vyžádat a nechat si je přenést k jinému správci údajů – vaší konkurenci – čímž odkryjete karty a konkurenční výhodu znalosti svých zákazníků tak budete nuceni dát k dispozici i jinému poskytovateli podobných služeb či produktů.

Co do plnění povinností správce údajů ve vztahu k obchodní agendě si lze představit jako velmi častou realizaci všech výše popsaných povinností vyplývajících z GDPR, zejména však opět:

- **OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ DOZOROVÉMU ÚŘADU,** přičemž znovu je třeba zdůraznit, že v převážné většině případů bývají původci incidentů (z nedbalosti nebo nevědomě) insideři v organizaci správce.

- **OZNAMOVÁNÍ OBZVLÁŠTĚ ZÁVAŽNÉHO PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ VŠEM KLIENTŮM, JEJICHŽ PRÁV BY SE INCIDENT MOHL ZÁVAŽNĚ DOTKNOUT,** na které je třeba klást obzvláštní důraz. Pokud k oznámení nedojde nebo pokud se o bezpečnostním incidentu vůbec nedozvíte, může dojít k uložení daleko citelnější sankce, než pokud incident (z důvodu spuštění funkčních mechanismů informování o bezpečnostních událostech uvnitř vaší firmy) odhalíte, pečlivě vyhodnotíte, splníte svou ohlašovací povinnost a následně podniknete všechny dostupné kroky k tomu, aby se situace již neopakovala.

- **VEDENÍ EVIDENCE O OPERACÍCH TÝKAJÍCÍCH SE ZPRACOVÁNÍ ÚDAJŮ ZÁKAZNÍKŮ A KLIENTŮ,** která zahrnuje jak obecné nastavení procesů a postupů, tak i informace o jejich realizaci v konkrétních případech. Tato povinnost neplatí pro malé a střední podniky do 250 zaměstnanců provádějící pouze příležitostné zpracování necitlivých osobních údajů s nízkým rizikem.

V rámci procesní přípravy vaší firmy na zpracovávání osobních údajů v obchodní agendě v souladu s GDPR lze zcela jistě doporučit:

- **REVIZI STÁVAJÍCÍHO PROSTŘEDÍ ZPRACOVÁNÍ ZÁKAZNICKÝCH A KLIENTSKÝCH OSOBNÍCH ÚDAJŮ** – jak jsou nastaveny kanály sběru údajů o klientech, kdo k nim má v průběhu zpracování přístup, jak jsou údaje uchovávány (úložiště papírových dokumentů nebo elektronických dat), zabezpečeny, jaký je cyklus jejich zpracování včetně toho, kdo je jejich zpracovatelem mimo vaši organizaci jako organizaci správce, jak je prováděna aktualizace údajů, kdy jsou naplněny podmínky pro výmaz údajů a jak k němu fakticky dochází.

- **PŘÍPRAVU NOVÝCH PROCESŮ, KTERÉ BUDOU PLNĚ V SOULADU S GDPR** – bude zcela jistě zapotřebí sladit klientské databáze a optimálně z nich identifikovat jedinou, která bude sloužit jako hlavní databáze pro zpracování zákaznických osobních údajů. Může jí být některá z databází již existujících, nebo databáze nadstavbová, která bude sloužit jako spojnice a současně rozcestník pro práci s osobními údaji vašich klientů.

- **REVIZE SMLUV S FIREMNÍMI ZÁKAZNÍKY I SPOTŘEBITELI** – oba typy smluv totiž obsahují osobní údaje, ať už jsou to údaje vašich zákazníků jako konečných spotřebitelů vámi obchodovaných výrobků nebo služeb, nebo zákazníků firemních, jejichž reprezentanti jsou fyzickými osobami a tedy subjekty údajů.

Vzhledem k tomu, že v obchodních vztazích bude minimum údajů zpracováváno ze zákona, je smlouva nejčastějším a nejsilnějším právním titulem pro zpracování osobních údajů v obchodních vztazích. Řadu účelů zpracování pak bude možné pokrýt oprávněným (obchodním, marketingovým) zájmem vaší firmy, ale stejně tak řadu údajů (zejména údaje citlivé) budete muset i nadále zpracovávat pouze pod souhlasem vašich klientů nebo osob, které je zastupují, jako subjektů údajů.

- **REVIZI METODICKÝCH POSTUPŮ, SMĚRNIC A JINÝCH INTERNÍCH PŘEDPISŮ UPRAVUJÍCÍCH OBCHODNÍ PRAKTIKY VAŠÍ FIRMY** – ať už těch, které přímo upravují práci s osobními údaji, nebo těch, které se týkají dalších firemních procesů, jako jsou práva a povinnosti zaměstnanců, obchod, marketing a práce s klientskými a zaměstnaneckými daty zahrnujících i zpracování osobních dat.

- **REVIZI SMLUV O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ S EXTERNÍMI SUBJEKTY** – například se zpracovateli průzkumů trhu, rozesilateli marketingových sdělení, agenturami zaměřenými na získávání podkladů pro marketingovou komunikaci apod. V řadě případů ve smlouvách dosud není ochraně osobních údajů zaměstnanců věnována odpovídající pozornost, což může způsobit velké problémy například při včasnosti hlášení porušení zabezpečení osobních údajů ze strany vašeho zpracovatele. I zde platí, že za porušení ohlašovací povinnosti směrem k dozorovému úřadu totiž odpovídá vždy správce, a to i v případech, kdy bezpečnostní incident vznikl při činnosti externího zpracovatele údajů.

- **REVIZI ZPŮSOBU PŘENOSU ÚDAJŮ VAŠICH ZÁKAZNÍKŮ A KLIENTŮ DO ZAHRANIČÍ** – v rámci EU i v EHP platí volný pohyb dat na jednotném vnitřním trhu EU, komplikace však zcela jistě nastanou při přenosu klientských dat do třetích zemí. U těch GDPR rozlišuje země „bezpečné“ (jejichž výčet – whitelist, aktuálně zahrnující 12 zemí nebo jejich částí, vydává svým rozhodnutím o adekvátní ochraně Evropská komise) a „nebezpečné“ (jejichž výčet – blacklist - dosud nebyl publikován, avšak publikaci lze očekávat nejpozději s účinností GDPR). Do zemí bezpečných lze osobní údaje zákazníků a klientů přenášet bez dalšího, pro ty další však platí velmi přísná omezení. Pro bližší informace o této problematice doporučujeme konzultaci s Úřadem pro ochranu osobních údajů nebo se specializovaným poradcem.

Z FIREMNÍHO ŽIVOTA: ZAVEDENÍ NOVÉHO SYSTÉMU EVIDENCE ZÁKAZNÍKŮ

Firma Z-Y, která se zabývá truhlářskou výrobou, se v rámci přípravy na GDPR kvůli zjednodušení naplňování svých povinností správce rozhodla přejít od primárně papírové evidence svých zákaznických spisů na konsolidovanou evidenci elektronickou. Doposud ke každému obchodnímu případu vedla papírový spis, který obsahoval všechny kontakty klienta, jeho objednávku, všechny informace o realizaci zakázky a konečnou fakturu včetně případných nároků z vad výrobků či jiných reklamací. Současně jednotliví pracovníci na prodejně, kteří přijímali objednávky, a na účetním oddělení, kteří realizovali fakturaci, vedli evidenci zákazníků ve svých počítačích. Evidence dokumentů o realizaci zakázky byla vedena pouze papírově. Firma se rozhodla pořídit si nový informační systém pro správu zákaznických dat, kterým by nahradila dosavadní roztříštěnou evidenci. Od jeho zavedení si mj. slibovala zjednodušení sledování obchodních případů a zamezení duplicitám při vedení evidence.

- Pracovníci přijímající objednávky i účetní si vedle databáze klientů i nadále vedli evidence objednávek a faktur ve svých počítačích. Špatně – nebylo možné zajistit naplňování zásady přesnosti osobních údajů a multiplicita evidencí fakticky pokračovala.
- Do počítače, v němž byla nainstalována nová klientská databáze, měl přístup neomezený okruh pracovníků, kteří se střídali na směnách. Špatně – osobní údaje nebyly odpovídajícím způsobem zabezpečeny.
- Nový klientský systém byl k dispozici na základě uživatelského jména a hesla pouze přesně vymezenému okruhu zaměstnanců, a to jak v počítačích, tak i v dalších firemních zařízeních jako mobilní telefony. Všichni zaměstnanci pohybující se v terénu navíc měli k dispozici tablety, na kterých zaznamenávali do systému informace o realizované dodávce a montáži výrobků. V rámci implementace nově přijaté interní směrnice se žádné osobní údaje zákazníků nepohybovaly v papírové ani elektronické podobě mimo klientský systém. Pokud takové duplicity byly zjištěny, informace byly okamžitě zaneseny do systému a duplicitní evidence skartována. Správně – je zajištěna jednotnost evidence zpracovávaných osobních údajů, jejich správnost a úplnost a současně i odpovídající míra zabezpečení.

ZPRACOVÁNÍ DOKUMENTACE SOUVISEJÍCÍ S USPOŘÁDÁNÍM VZDĚLÁVACÍ AKCE

Vzdělávací agentura J&P byla dosud zvyklá ostražitě nakládat s osobními údaji frekventantů svých vzdělávacích kursů v rámci zákona o ochraně osobních údajů. V souvislosti s účinností GDPR si však nebyla jista, zda jí nepřibývají nové povinnosti související se zpracováním osobních údajů obsažených na vizitkách posluchačů jejich vzdělávacích kurzů, v prezenčních listinách, testech účastníků kursů a v certifikátech o absolvování školení.

☹ Nechala si proto provést externí analýzu a doporučení ke zpracování osobních údajů při své činnosti. Vstupní informace do analýzy poskytovala externímu poradci vzdělávací pracovnice, která absolvovala teprve několik vzdělávacích akcí a nebyla tedy informována o tom, že krom evidence osobních údajů posluchačů kurzů společnosti J&P existuje i papírový archiv výsledků závěrečných testů a vydaných osvědčení. Zpracovatel analýzy se tak věnoval pouze elektronicky vedeným údajům a opomenul formulovat doporučení pro zabezpečení osobních údajů v papírové evidenci. Špatně – v rámci inventury způsobů zpracování údajů byla opomenuta část agendy a výsledné metodické doporučení se proto opíralo o nesprávná vstupní data.

☹ Agentura J&P si analýzu způsobů zpracování provedla interně, následně si objednala externí expertní doporučení k zajištění kompatibility způsobu své práce s osobními údaji. V předaném soupisu však opomněla uvést, že kromě elektronického systému obsahujícího evidenci realizovaného vzdělávání i výsledků zkoušek, papírové evidence certifikátů o absolvování kurzů a elektronické kontaktní databáze účastníků, vede současně i podrobnou abecední evidenci vizitek získaných jak od účastníků svých kurzů, tak i od dalších obchodních partnerů a poskytovatelů různých služeb jako jsou správa IT nebo dodávky tonerů do tiskáren. Externí doporučení proto opět vycházelo z nepřesných vstupních informací. Špatně – svou klientskou databázi agentura nepřístojně smísila s databází dodavatelskou, přičemž důvod a účel zpracování se u jednotlivých subjektů údajů lišil, ačkoli osobní údaje byly součástí jedné evidence. Současně nebyla zaručena správnost a aktuálnost zpracovávaných osobních údajů.

☺ Agentura z nedostatku časového prostoru zbývajícího do účinnosti GDPR a současně i prostředků přistoupila k interní inventarizaci způsobu zpracování osobních údajů. V jejím rámci zjistila, že zpracovává osobní údaje svých zaměstnanců, frekventantů svých kurzů a současně i dodavatelů-fyzických osob nebo zástupců dodavatelů-osob právnických. Současně identifikovala, že existuje několik duplicitních úložišť, v nichž se pohybují ne vždy zcela zabezpečené osobní údaje – např. skříně se spisy obsahujícími kopie vydaných certifikátů nemají zámky. Rozhodla se proto sjednotit všechny dokumenty vztahující se k realizovanému vzdělávání včetně vydaných certifikátů do jednotného elektronického systému a v papírové podobě (a to v uzamčené skříni) nadále vedla pouze účetní a daňové doklady vztahující se k jednotlivým účetním případům, které byly číselně provázány s evidencí klientů v elektronickém systému. Současně zavedla systém elektronické evidence kontaktů všech dodavatelů, ze kterého navíc periodicky vyřazovala nepoužívané kontakty, aby dodržela svou povinnost vymazat údaje, které nejsou potřebné k plnění účelu zpracování. Zjistila také, že od svých klientů nepotřebuje již nadále souhlasy se zpracováním údajů, neboť neshromažďuje jejich citlivé údaje a zpracování jejich osobních údajů je nutné výlučně ke splnění zákonných povinností agentury J&T a nebo ke splnění smlouvy o realizaci vzdělávání s klienty. Ještě před účinností GDPR tedy všechny své klienty informovala jednotným hromadným e-mailem o tom, že jejich souhlasu již není ke zpracování osobních údajů zapotřebí a současně neopomněla přidat informace o tom, které osobní údaje, z jakého právního titulu a po jakou dobu o svých klientech vede a eventuálně komu je předává k dalšímu zpracování. Od dodavatelů nikdy souhlasy ke zpracování osobních údajů nevyžadovala, proto jen zavedla s účinností GDPR nový systém – odkaz do svých e-mailových podpisů, informující o obecných zásadách ochrany soukromí při činnosti agentury, které publikovala na svém webu. Správně – bylo zamezeno duplicitám a nepřesnostem v evidenci, současně byla přijata všechna technická a organizační opatření k ochraně osobních údajů. Byly odděleny jednotlivé evidence osobních údajů podle účelu jejich zpracování a subjekty údajů, jejichž souhlasu ke zpracování již nebylo nadále zapotřebí, byly o tom odpovídajícím způsobem informovány. Současně se agentura i připravila na GDPR tím, že na svém webu publikovala zásady ochrany soukromí, které aplikuje a informovala o nich všechny klienty i jiné partnery prostřednictvím odkazu v e-mailových podpisech všech svých pracovníků.

SPRÁVA NOVÉHO OBCHODNÍHO PŘÍPADU

Společnost V., která vyrábí a dodává plastová okna, kontaktoval nový zákazník, který měl zájem o uzavření smlouvy o dodání a výměně oken. Operátorka zákaznického servisu poptávku zaevidovala do klientské databáze a předala ji obchodnímu úseku k dalšímu zpracování.

Případ si převzal specialista servisu a z databáze si pořídil výpis, do kterého pak dále doplňoval údaje, které o obchodním případu zjistil – upřesnění požadavku zákazníka, termín sjednané výměny oken, kompletní kontakt na zákazníka apod. Bezprostředně po provedení tohoto kroku v péči o zákazníka však dlouhodobě onemocněl a zjištěné údaje zapomněl zaznamenat do elektronické klientské databáze. Zápisník s jeho údaji navíc zůstal dlouhodobě na jeho stole, a když se servisní pracovník vrátil z nemocenské, nenašel jej tam. Špatně – údaje nebyly v databázi aktualizovány, navíc nebyly ani odpovídajícím způsobem zabezpečeny a došlo k porušení jejich zabezpečení, aniž by se společnost V. jako správce údajů o tomto porušení dozvěděla a mohla je tedy hlásit.

Na případu postupně pracovali servisní pracovník, následně oddělení zakázkové výroby oken a nakonec pracovní četa pro realizaci zakázek, resp. výměny oken, žádný z nich však prvotní údaje zapsané v zákaznické databázi operátorkou klientského servisu neaktualizoval, a ač úspěšně proběhlo plnění a fakturace, úspěšná realizace zakázky ani nebyla z databáze patrná. Při zpětné revizi databáze tedy nebylo bez získání údajů od fakturačního oddělení ani zřejmé, zda a kdy má dojít k výmazu údajů. Špatně – zpracovávané osobní údaje nebyly vedeny přesně a konzistentně, nebyl proveden výmaz údajů v okamžiku, kdy odpadl právní důvod pro zpracování údajů, kterým v tomto případě bylo plnění (a splnění) smlouvy a následné uplynutí lhůty pro uplatnění eventuálního nároku z vad výrobku.

Celý obchodní případ od jeho zahájení až po úspěšné skončení (realizaci výměny oken) byl jednotlivými dotčenými úseky postupně konzistentně zaznamenáván do klientské databáze, jednotliví pracovníci si nevytvářeli paralelní evidence. Po úspěšném ukončení obchodního případu a uplynutí záruční doby byl profil zákazníka z databáze vymazán, protože zákazník si nepřál být kontaktován s dalšími obchodními nabídkami firmy. Po dobu povinné archivace daňových dokladů ještě údaje o zákazníkovi vedlo fakturační oddělení, po jejím uplynutí byly vymazány i z jeho evidence. Správně – údaje o zákazníkovi byly vždy úplné a aktuální, navíc byly odpovídajícím způsobem zabezpečeny. Poté, co odpadly důvody zpracování údajů – plnění smlouvy a zákonné povinnosti vést průkaznou daňovou evidenci – došlo k bezodkladnému vymazání osobních údajů.

NEOPRÁVNĚNÉ POŘÍZENÍ KOPIE KLIENTSKÉ DATABÁZE

Paní S. pracovala v klientském servisu společnosti F. Při ukončení svého působení ve společnosti si pro potřeby budoucího vlastního podnikání pořídila bez vědomí zaměstnavatele kopii kompletní klientské databáze společnosti F. Databázi měla na oblíbeném flashdisku, který při jednom semináři zapomněla v PC jeho organizátora a k databázi se tak mohl dostat blíže neurčený okruh dalších osob.

Společnost F. jako bývalý zaměstnavatel paní S. vůbec nezjistila, že kopie databáze byla pořízena. Špatně – společnost F. měla mít nastaven takový systém zabezpečení údajů, aby údaje z klientské databáze nebylo možné jednotlivě ani jako celkovou evidenci kopírovat bez povolení příslušného pracovníka společnosti F.

Společnost F. při neoprávněném pořízení kopie údajů z databáze ani paní S. při ztrátě flashdisku obsahujícího kopii databáze nehlásili tyto události jako porušení zabezpečení údajů dozorovému úřadu ani neoznámili tyto skutečnosti subjektům údajů, jejichž údaje byly součástí databáze. Společnost F. to neučinila, neboť se o neoprávněném okopírování databáze vůbec nedozvěděla, paní S. proto, že si byla vědoma toho, že s databází disponuje neoprávněně. Pracovník, který nalezl ztracený flashdisk, si však byl vědom povinností při zacházení s osobními údaji a protože zjistil, že je na flashdisku celá databáze klientů společnosti F., ohlásil to společnosti a současně uvědomil dozorový úřad. Špatně – společnost F. si pro porušení své povinnosti odpovídajícím způsobem zabezpečit údaje ani nevšimla, že byla databáze neautorizovaně kopírována a nemohla tedy ani tušit, že došlo k jejímu zpřístupnění neomezenému okruhu osob. To ji však nevyvinilo ze škodlivého následku, kterým bylo porušení zabezpečení údajů a z uložení vysoké sankce dozorovým úřadem. Na paní S. pak společnost F. vymáhala škodu způsobenou takovým jednáním, a to v rámci občanskoprávního nároku na náhradu škody. Paní S., ač si byla vědoma neoprávněnosti zkopírování databáze, měla přece porušení zabezpečení hlásit dozorovému úřadu, protože by se tak možná vyhnula uplatnění vysokého nároku na náhradu škody společnosti F.

Při pokusu o zkopírování databáze si paní S. nevšimla, že databázi sice bylo možné zkopírovat, avšak data se na jejím flashdisku objevila jako zašifrovaná a nebylo tedy možné je dále použít ani nemohlo nastat ohrožení práv subjektů údajů. Správně – společnost F. jako řádný správce údajů použila odpovídajících prostředků zabezpečení své databáze a ztrátou flashdisku tedy nemohla být způsobena ve výsledku žádná škoda pro práva a svobody subjektů údajů.

SLEDOVÁNÍ VÝROBKŮ PO CELOU DOBU JEJICH ŽIVOTNOSTI

V rámci inovace své obchodní strategie přistoupila společnost E. k zabudování čipů do všech svých výrobků. Čipy obsahovaly nejen data o výrobním procesu, ale byly do nich ukládány i údaje ohledně způsobu distribuce, aktuální lokace výrobku a způsobu zacházení s ním (vystavení teplotním vlivům, otřesům, frekvence jejich používání).

☹ Zákazníci nebyli o umístění čipů ve výrobcích ani o sběru údajů o způsobu zacházení s výrobky po jejich zakoupení informováni. Špatně – nebylo naplněno ani právo subjektů údajů na informace o tom, že jimi zakoupené výrobky jsou sledovány výrobcem.

☹ Výrobce nedosledoval způsob práce s výrobky a tím i s čipy v nich umístěnými při ukončování životnosti výrobků. Výrobky, které byly postupně vyhazovány a likvidovány tak obsahovaly cenné nosiče údajů (čipy) a k údajům v nim obsaženým se mohl při použití odpovídající čtecí technologie dostat blíže neurčený okruh osob. Špatně – zpracovávané osobní údaje nebyly odpovídajícím způsobem zabezpečeny proti zneužití. Výrobce buď mohl využít systém pro šifrování dat, nebo zajistit sběr všech výrobků při ukončování jejich životnosti tak, aby měl možnost ovlivnit způsob likvidace čipů a zamezil jejich možnému zneužití.

☺ Zákazníci byli informováni o umístění čipů v jimi zakoupených výrobcích, ale výrobce si k tomu nevyžádal jejich souhlas, sledování výrobků a tím i spotřebitelského chování jejich uživatelů odůvodnil svým oprávněným zájmem na zlepšování kvality výrobků a jejich přizpůsobování potřebám trhu a spotřebitelů. Správně – k monitorování výrobků a s nimi i subjektů údajů, které jsou jejich uživateli, není zapotřebí souhlasu uživatelů, postačí, jsou-li o tom informováni a je-li dán oprávněný zájem správce údajů, který informace o výrobcích shromažďuje. Proti oprávněnosti zájmu samozřejmě může subjektů údajů vždy vznést námitku a požadovat omezení zpracování údajů. Současně je důležité, aby údaje byly odpovídajícím způsobem zabezpečeny proti zneužití, a to i po ukončení životnosti výrobků.

VYUŽÍVÁNÍ PERSONALIZOVANÉ REKLAMY PŘI ČINNOSTI E-SHOPU

E-shop A měl na svých stránkách nainstalovány soubory cookies, které po odsouhlasení možnosti jejich využití uživatelem e-shopu mapovaly jeho pohyb na webových stránkách. Tímto způsobem e-shop získával cenné informace o preferenci svých klientů a mohl tak přizpůsobovat svou nabídku požadavkům trhu. Současně uživatele podle jejich preferencí automaticky rozřazoval do skupin, kterým pak byla zasílána individualizovaná reklama, ale i akční nabídky zboží. V souvislosti s nabytím účinnosti GDPR se rozhodl tuto svou marketingovou strategii přehodnotit.

☹ Klienti byli v obecných informacích o způsobu zpracování osobních údajů publikovaných na webové stránce e-shopu informováni, že prostřednictvím souborů cookies jsou sledovány jejich zákaznické preference a e-shop této aktivity využívá ke zkvalitňování svých služeb poskytovaných spotřebitelů, což je jeho oprávněným zájmem. Privacy policy obsahovala i informaci o možnosti podat námitku proti takovému způsobu zpracování údajů, neobsahovala již však informace o tom, že na základě vyhodnocení pohybu zákazníků na webu dochází k jejich profilování a následnému rozhodování o jejich právech formou zasílání různorodě strukturovaných nabídek akčních cen, které platí jen pro určitou skupinu zákazníků. Špatně – e-shop neinformoval své zákazníky o tom, že dochází k jejich profilování a současně si nevyžádal jejich souhlas s automatickým rozhodováním (s automatickou rozesílkou nabídek akčního zboží), které je založeno na tomto profilování.

☺ Prostřednictvím publikace své politiky ochrany osobních údajů na webu zajistil e-shop zveřejnění informací o zpracování osobních údajů i o realizovaném profilování a na ně navázaném automatickém rozhodování o právech a povinnostech zákazníků. Současně si ode všech zákazníků, kterým byla zasílána automaticky reklama určená pro jejich profil včetně nabídky akčního zboží, vyžádal souhlas s tímto postupem. U těch zákazníků, kteří souhlas odmítli udělit, zasílání individualizované reklamy pokračovalo, avšak o rozesílce nebylo rozhodováno automaticky, nýbrž bylo v gesci pracovníka marketingového oddělení e-shopu. Do všech objednávek byla současně zakomponována základní informace o rozsahu, účelu a době zpracovávání osobních údajů zákazníků a současně i odkaz na politiku ochrany osobních údajů na webu e-shopu. Správně: e-shop se v souladu s GDPR vypořádal s profilováním klientů, informoval je o něm, a buď si zajistil jejich souhlas s rozesílkou individuálních reklamních sdělení, nebo zajistil, aby k rozhodování o rozesílce nedocházelo automaticky, nýbrž s využitím lidského rozhodovacího faktoru. Současně dostál i svým informačním povinnostem vůči svým zákazníkům.

7. KOMPLEXNÍ MODELOVÉ PŘÍKLADY

V předchozích kapitolách jsme si tedy vysvětlili všechny teoretické záležitosti související s úspěšnou přípravou firmy na GDPR, související praktické příklady i náležitosti související s ochranou osobních údajů v klientské a zaměstnanecké agendě. Cílem této poslední kapitoly je přiblížit podnikatelům, kteří vykonávají nejjednodušší agendu typickou pro svůj obor, jak se v konkrétních krocích připravit na GDPR tak, aby splnili všechny povinnosti správců údajů a současně co možná nejvíce šetřili svou administrativní zátěž.

Z FIREMNÍHO ŽIVOTA:VÝROBNÍ FIRMA

Pan F. je fyzickou osobou podnikající – vlastníkem truhlářské firmy, která má několik zaměstnanců. Objednávky přijímá výlučně osobně na své provozovně, neprovozuje e-shop a v rámci podmínek poskytování svých služeb má nastavenu maximální dojezdovou vzdálenost do 50 km od sídla svého podnikání. Mezi jím nabízené služby patří výroba a montáž vyrobeného zboží.

a) Přípravná fáze:

V první fázi pan F. pověřil svou asistentku, aby si do tabulky sepsala, odkud osobní údaje do firmy přicházejí, kdo a jakým způsobem s nimi nakládá, v jakých evidencích jsou vedeny, po jakou dobu uchovávány a komu mimo firmu jsou předávány.

Touto prvotní analýzou bylo zjištěno, že osobní údaje klientů do firmy proudí výlučně skrze objednávkový systém na provozovně, osobní údaje zaměstnanců pak prostřednictvím kontaktu s panem F. v případě, že je čas od času zapotřebí přijmout nového zaměstnance. Osobní údaje zaměstnanců i uchazečů o zaměstnání ve firmě byly po celou dobu od zahájení činnosti firmy shromažďovány v šanonu v kanceláři pana F., s osobními údaji klientů průběžně pracovali zaměstnanci pověření realizací jednotlivých zakázek a po skončení případu byly souhrnně evidovány též v papírové podobě u pana F., současně i v jeho počítači. Osobní údaje zaměstnanců firma pana F. předávala každý měsíc poskytovateli stravenek, externí mzdové účetní a dále orgánům finanční a daňové správy (u příležitosti vedení daňové agendy), orgánům správy sociálního zabezpečení (pro účely důchodového, nemocenského a zdravotního pojištění) a dále byly na žádost jedenkrát poskytnuty inspektorátu práce (při jednou provedené kontrole).

b) Stanovení kroků pro zajištění naplnění povinností dle GDPR:

Po provedení této prvotní soupisky pan F. kontaktoval poradenskou firmu, která mu nabídla své služby v rámci přípravy na GDPR. Touto konzultací zjistil, že by se měl zaměřit zejména na to, aby:

1. k osobním údajům klientů i zaměstnanců měl přístup pouze přesně vymezený okruh osob
2. s poskytovatelem zaměstnaneckých benefitů (stravenek) měl uzavřenu smlouvu o zpracování osobních údajů nebo aby součástí smlouvy o poskytování stravenek bylo i ujednání o způsobu zpracování osobních údajů zaměstnanců
3. podobnou smlouvu o zpracování údajů měl uzavřenu se svou externí mzdovou účetní
4. zaměřil se na zabezpečení údajů ve svém počítači (tj. zajistil, aby k jeho obsahu neměl nikdo kromě něj – včetně členů rodiny – přístup)
5. zaměřil se za zabezpečení údajů, které vede o svých klientech a zaměstnancích v provozovně firmy (tj. evidoval je pouze v uzamykatelných kusech nábytku nebo v uzamykatelné kanceláři, kam má přístup pouze přesně vymezený okruh osob)
6. stanovil povinnosti svých zaměstnanců ve vztahu k nakládání s osobními údaji zákazníků a způsob hlášení eventuálních problémů s jejich zpracováním jako jsou nepřesnosti zjištěné v osobních údajích a nebo ztráta či odcizení dokumentů obsahujících osobní údaje
7. zaměřil se na periodické třídění a skartování dokumentace obsahující osobní údaje v případech, kdy už ji nepotřebuje pro splnění daného účelu a kdy mu ve skartaci nebrání žádná zákonná povinnost
8. publikoval ve své provozovně a na webové stránce své firmy pravidla pro ochranu osobních údajů zákazníků.

c) Implementace kroků směřujících k naplnění povinností:

V návaznosti na tato doporučení pan F. zavedl od května 2018 ve firmě tato nová pravidla:

1. svým zaměstnancům, kteří se podíleli na realizaci zakázkové výroby předával pouze informace o obsahu objednávky vedené pod evidenčním číslem, nedostávali už úplné informace o objednateli; zaměstnanci alokovaní na montážní práce dostávali pouze informace nezbytně nutné pro realizaci montáže (jméno, bydliště a telefonický kontakt zákazníka), okamžitě po dokončení montáže odevzdávali vyplněné a zákazníkem podepsané zakázkové listy do souhrnné evidence v kanceláři pana F.
2. dodatkoval smlouvu uzavřenou s poskytovatelem zaměstnaneckých benefitů a nechal do ní zahrnout ujednání o způsobu zpracování osobních údajů zaměstnanců a zejména o hlášení bezpečnostních incidentů na poli ochrany osobních údajů (tedy ztrátu, odcizení, zničení, znepřístupnění a jiné události, které by mohly ohrozit osobní data zaměstnanců); mimo jiné také začal odesílat všechny údaje zaměstnanců určené ke zpracování výlučně v zaheslovaných souborech, přičemž způsob tvorby hesla (které bylo každý měsíc jiné) byl zanesen do smlouvy s poskytovatelem stravenek
3. obdobně dodatkoval i smlouvu se svou externí mzdovou účetní a i zde zajistil, aby údaje potřebné pro zpracování mezd odcházely taktéž výlučně v zaheslovaných souborech
4. zajistil, aby uživatelské účty v jeho počítači byly oddělené a jeho účet byl opatřen uživatelským jménem a heslem, které znal jen pan F.
5. zajistil, aby jeho kancelář, v níž vedl evidenci zaměstnanců a klientů, byla v jeho nepřítomnosti vždy uzamčena a pro jistotu přetřídil veškerou dokumentaci a všechny spisy obsahující osobní údaje umístil do uzamykatelné skříně
6. doplnil pracovní řád o povinnosti zaměstnanců ve vztahu k nakládání s osobními údaji zákazníků a způsob hlášení změn v osobních údajích klientů i bezpečnostních incidentů, stejně tak informoval zaměstnance o sankcích souvisejících s nesplněním těchto povinností. Zajistil, aby se všichni zaměstnanci s touto změnou seznámili
7. spolu s inventurou materiálu a účetní evidence si jedenkrát ročně nastavil i periodickou inventarizaci osobních dat, které vedl o svých zaměstnancích, uchazečích o zaměstnání, klientech i potenciálních zákaznících. První takovou inventarizaci provedl ještě před účinností GDPR a s překvapením zjistil, že více než 2/3 osobních údajů, resp. dokumentů obsahujících osobní údaje, vedl nadbytečně. Nastavil si lhůtu pro periodické mazání dat uchazečů o zaměstnání na 1 rok a lhůtu pro periodické mazání dat o neuskutečněných nebo nedokončených obchodních případech (které nezahrnovaly plnění daňové povinnosti) na 2 roky
8. zamyslel se a sepsal desatero pro práci s osobními údaji zákazníků, které obsahovalo způsob poskytování informací zákazníkům o způsobu práce s jejich osobními daty, realizace práva na přístup, výmaz a omezení zpracování údajů i o tom, komu jsou údaje zákazníků předávány pravidelně nebo na žádost. Toto desatero vyvěsil do rámečku u přepážky na své provozovně a současně je publikoval na webové stránce své firmy na nové záložce „Pravidla pro ochranu osobních údajů zákazníků“.

d) Periodická preventivní kontrola:

Aniž by do firmy pana F. zavítala kontrola dozorového úřadu, po několika měsících od zavedení nových pravidel firma opět kontaktovala poradenskou firmu, která jí pomohla identifikovat kroky vedoucí k přípravě firmy pana F. na účinnost GDPR. Při konzultaci byly vysvětleny některé nejasnosti a upraveny drobné nepřesnosti, které vznikaly při aplikaci (například ne zcela jednotný přístup zaměstnanců, to, že mzdová účetní ne vždy zaheslovala soubor obsahující vyúčtování mezd zaměstnanců aj.). Pan F. byl také poučen o tom, že pokud by přistoupil v rámci své obchodní strategie např. k zavedení věrnostního zákaznického systému nebo k zavedení online objednávek či e-shopu, bylo by zapotřebí znovu přehodnotit všechny dříve učiněné kroky ve vztahu k ochraně osobních údajů klientů a je vhodné, aby si znovu nechal provést analýzu a podnikl další kroky.

UŽITEČNÉ ODKAZY

- Oficiální text GDPR v češtině: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016R0679
- Web Úřadu pro ochranu osobních údajů: www.uoou.cz
- Webová stránka Evropské komise věnované reformě pravidel EU pro ochranu osobních údajů v roce 2018: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_cs
- Newsroom Pracovní skupiny podle článku 29 Směrnice 95/46/ES (tzv. Article 29 Working Party neboli WP 29): http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- Informace Ministerstva průmyslu a obchodu ČR o GDPR: https://www.mpo.cz/cz/podnikani/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr--228672/
- Informace Ministerstva vnitra ČR o GDPR: http://www.mvcr.cz/gdpr/

Na Františku 32, 110 15 Praha 1

www.mpo.cz

I. vydání, duben 2018, ISBN: 978-80-906942-3-1
Účelová publikace, není určena k prodeji.

MINISTERSTVO
PRŮMYSLU A OBCHODU