

GDPR analýza s přehledem a v pohodě

aneb i s GDPR se dá pobavit :-)



Jaroslava Ester Evangelu

KATALOGIZACE V KNIZE – NÁRODNÍ KNIHOVNA ČR

Jaroslava Ester Evangelu

GDPR analýza s přehledem a v pohodě (aneb i s GDPR se dá pobavit)

ISBN: 978-80-906211-2-1

Jaroslava Ester Evangelu

GDPR analýza s přehledem a v pohodě (aneb i s GDPR se dá pobavit)

© 2018 Jaroslava Ester Evangelu

HANDPICKED Publishing

ISBN 978-80-906211-2-1

GDPR analýza s přehledem a v pohodě

aneb i s GDPR se dá pobavit :-)

Příručka pro provedení vlastního auditu krok po kroku

Jaroslava Ester Evangelu



Zodpovědnost za správnost údajů v publikaci:

V příručce zaznamenáváme náš pohled na oblast GDPR a praktický návod krok po kroku, jak tuto záležitost nejlépe zavést do praxe. Dokument je zpracován na základě vlastní úvahy, účasti na seminářích k tématu GDPR, studiem tematických publikací a článků na specializovaných webových stránkách, diskuzí s odborníky. Zejména jsme však vycházeli ze zkušeností, dotazů a přání našich zákazníků, u kterých zpracováváme personální a manažerské audity. Dovolujeme si však zdůraznit, že se může objevit ještě další upřesnění k tématu, takže nemůžeme garantovat naprostou správnost podávaných informací. Předpokládáme, že v případě závazného upřesnění dopracujeme další vydání, které bude tuto skutečnost reflektovat.

Cena publikace:

Naše příručka je poskytována bezplatně. Napsali jsem ji jen tak, pro radost z práce samotné a ze snahy přesvědčit, že i takové nudné a nutné záležitosti mohou být pojaty s humorem. Navíc je to naše jubilejní publikace, takže se hodí čtenářům něco zajímavého darovat jen tak, také pro radost.

Obsah

O autorce	4
Kde se to tu vzalo?	4
Kdo za to může?	7
Co to vlastně znamená?	9
Jak mám na to jít?	24
Poradí mi někdo, když budu v koncích?	28
Jak poznám, že je to správně?	29
Dvacet nejčastějších otázek z diskuzí našich zákazníků	33
Závěrečný příklad místo závěru	38
Jaké další publikace jsme pro vás vydali?	40
Co dalšího pro vás v Brněnské personalistice děláme?	41

O autorce

Jmenuji se Jaroslava Ester Evangelu a odjakživa jsem známá tím, že ráda píšu. Stejně ráda i mluvím, ale to se v tištěné knize moc neprojeví. Láska k psaní se projevila nejen tím, že vám předkládám svoji dvacátou publikaci, ale také založením vlastního nakladatelství www.handpicked.cz, ke kterému se hrdě hlásím jako ke svému koníčku. Někdo hraje golf, někdo si vydává knihy.

Mnohem déle, než nakladatelství HANDPICKED Publishing se věnuji své firmě, Brněnské personalistice www.bp.cz. Ta si dala do vínku motto „na základě vysoce etického, odborného a profesionálního přístupu umožnit plně využívat hlavní potenciál každého člověka,“ čemuž jsem podřídila plných 22 let své kariéry. Jsem vděčná, že se mi již v mladém věku podařilo najít to, co mě naplňuje a těší, i že se mi totéž stalo prací i koníčkem zároveň.

Je až s podivem, jak v naší branži doslova platí, že člověk sklízí to, co sází: zatímco se věnuji rozvoji jednotlivců i firem, sama od nich čerpám někdy ještě více a rozvíjím se často dynamičtěji, než moji klienti. Neztrácím čas chybami, ze kterých naše zákazníci v průběhu své práce dostávají, získávám nesmírné kvantum informací z nejrůznějších oborů. Jak jsem již zmínila dříve, právě díky těmto podnětům i skvělým lidem vznikla další z našich knih.

Kde se to tu vzalo?

Jako většina firem, i my jsme se rozhodli řešit s předstihem otázku GDPR. Protože jsme vzdělávací společnost, rozhodli jsme se udělat to, co doporučujeme našim zákazníkům – hledat radu u odborníků. A protože není potřeba se bavit s kovářičkem, když je možnost diskuze s kovářem, objednali jsme si zrovna kurzy u lidí, kteří byli u celé problematiky od počátku. Co následovalo?

Po prvních pár minutách kurzu jsme získali pocit, že nás v květnu někdo neurčitý docela určitě zavře, protože není v lidských silách problematiku GDPR zvládnout. A že také vlastně nikdo neví, co je nutné přesně dělat, takže pokuty, které budou následovat, zruinují i ty, co náhodou zůstanou na svobodě. Zveličování problému, tlak na to, abychom cítili co největší zodpovědnost, bylo tak silné, až byl výsledek opačný. Měli jsme chuť se tím raději nezabývat. Zvolili jsme jiný kurz s jiným lektorem. Vypadalo to, že byl mladším bratrem toho předchozího,

protože začal následovně: „Víte, kolik vám ušetříme? Až pět miliónů! A to tehdy, pokud vám pomůžeme uspořádat procesy okolo GDPR.“ Následoval výčet toho, co máme ve firmě určitě špatně a co nám v budoucnu v oblasti GDPR přinese ohromné problémy.

Vyvolali jsme na toto téma diskuzi u našich známých, zákazníků, dodavatelů, náhodných kontaktů. Zjistili jsme, že všichni řeší stejný problém – začali mít pocit, že nám Evropská unie provedla naschvál nějakou lumpárnu, nastolila něco, co nejde dodržet a vytvořila si půdu pro možnost pořádných pokud.

Rozhodli jsme se na celou věc podívat z jiného úhlu. Stanovili jsme si, že se na celou záležitost podíváme co nejméně zaujatě. Představili jsme si, že jsme na žádném školení nebyli a zeptali jsme se sami sebe: Jak bychom postupovali v případě, kdy bychom nevěděli všechno to negativní kolem? Kdybychom se nenechali ihned zpočátku vystrašit?

Vypsali jsme si oblasti, ze kterých vyvstali zajímavé otázky. Z otázek se vyklubaly hypotetické nebo i skutečné situace k řešení. Překvapilo nás, že jsme se u toho celkem dost pobavili a velmi často od srdce zasmáli. Určitě jsme se poučili. A tak nás napadlo, že se o naše poznatky podělíme s těmi, kteří zůstali ve stádiu obav nebo dokonce znechucení.

Protože ono nové nařízení EU o ochraně osobních údajů není nic jiného, než snaha ochránit osobitý a jedinečný majetek každého z nás – data o nás samotných. A ač je to smutné, u některých lidí je to i majetek jediný... Takže proč v tom nebýt nápomocný a neporozumět principům? Kolikrát jsme to i my samotní, kteří potřebuji leckdy ochránit.



Př. Sedíte v čekárně u lékaře a pozorujete, jak sestra u objednávacího okýnka pokládá každému stejné otázky: „Která pojišťovna? A vaše rodné číslo? Ulice stále Bělohorská 18?“ Uvědomujete si, že před chvílí někdo takto pozoroval vás. Vadí? Nevadí? V každém případě je anonymita pasé.

Jiný příklad: V mém oblíbeném obchodě s kosmetikou se mě vždy dožadují, abych si založila kartičku. „Abyste měla slevy,“ slibují. Jasně, a aby měli přehled o tom, co nejčastěji a za kolik nakupuji, aby znali moje telefonní číslo, adresu, email a kdo ví co ještě. Mimochodem, pokusili jste se někdy z databáze těchto řetězců vymanit? Z vlastní zkušenosti vím, že ani doporučený dopis, ani emailová korespondence, ani vzteklý telefonát nic nepořešil. Zprávy o jedinečných slevách stále zahlcují můj telefon.

Toho – a ještě dalších situací nás má GDPR uchránit. Tedy pokud my sami chceme. Rozhodneme-li se nevyužít této možnosti, nic se pro nás nemění. Máme svobodu, máme

příležitost, máme volbu. Můžeme přestat pracovat s osobními údaji, můžeme změnit styl, jakým s nimi pracujeme, můžeme si udělat vlastní audit nebo prostě risknout, že se na nás zrovna nepříjde.

Pokud jsme zpracovatelé a využívatelé osobních údajů, stále se ve většině případů nic dramatického dít nebude. Protože pokud jste firma, která ctí tzv. „stojedničku“ (tj. zákon č. 101/2000 Sb.), máte z velké části vyhráno. Víte, že s daty nelze nakládat dle vlastní vůle, ale je potřeba respektovat práva majitelů údajů a postupovat dle zákona. Nařízení EU 2016/679 vychází z podobných principů, pouze je více definují. Byla k nim přidána pravidla pro získávání dat, dále bylo posíleno povědomí o možnosti rozhodovat o osobních datech – určovat jejich způsob a délku zpracování, míru informovanosti apod.



Př. Evidentně budou mít problém firmy, které získávaly data pokoutně. Nebo odcházející zaměstnanci, kteří si sebou jako suvenýr odnášeli databázi zákazníků. Popř. firmy, které předávaly informace s osobními údaji dále jako svůj produkt, přičemž se dotyčných vůbec neptali. Jenže toto chování již bylo špatně morálně kdykoliv a od platnosti 101/2000 i právně. GDPR tuto praxi pouze prakticky a otevřeně nazve pravým jménem.

1. Úkol pro GDPR audit:

- a) Vypište si všechny oblasti, u kterých se domníváte, že v nich pracujete s údaji, které spadají do současné „stojedničky“.
- b) O totéž požádejte vybrané zaměstnance (stačí 1 – 6 lidí, podle velikosti vaší firmy). Každý pěkně zvlášť, důležité je, aby se nezačali spolu radit, protože cvičení by ztratilo význam.
- c) Zkontrolujte rozdíly a pomocí diskuze si vyjasněte rozdílné pohledy na problematiku.
- d) Vychutnejte si údiv z naprosto rozdílného pohledu na věc. Zákazníkům ani úřadům to však neříkejte.

Kdo za to může?

Podle toho, za co.

Za samotnou skutečnost, že je potřeba upravit práci s osobními daty, může digitální svět a my, že se v něm pohybujeme. Možnost využívat počítače změnila všechny procesy ve všech firmách. Data se už neuchovávají v popsaných šanonech a nearchivují v přehledných policích, ale chovají se zcela jinak: faktury i objednávky se zasílají elektronicky, vzájemná vnitrofiremní komunikace probíhá také tak. Noví zaměstnanci se hlásí do firmy stejnou cestou, zpravidla i vstupní dotazník nebo osobnostní test již bývá elektronický. A tak lze ve výčtu možností pokračovat dále. Kromě samotných informací v zasílaných zprávách se na elektronické procesy nabalují další data ve formě osobních údajů, jako jsou e-mailová adresa, odkaz na LinkedIn, facebookovou adresu, Skype, Messenger atd. V případě, že se aktuálně nenasadí nějaká přijatelná forma kontroly a regulace, za nějaký ten rok bychom byli s našimi osobními a citlivými údaji vydáni na pospas kdečemu a naše data by mohly být nekontrolovaně zneužívány.



Př. Což se občas děje i nyní. Kolikrát nám již zazvonil telefon, kde se nás neznámý hlas na neznámém čísle vyptával na naše pojištění či oblíbený kredit. Když se v takovém případě zeptáme na zdroj informací o našem jméně, příjmení, bydlišti a telefonního čísla, nikdy se nedočkáme konkrétní odpovědi.

Konkrétně za GDPR může EU. Na samotném GDPR nic negativního není – to nás má jenom provést co nejlepší ochranou osobních dat a nastavit jednotná základní pravidla pro všechny zúčastněné subjekty. Skutečným problémem je však skutečnost, že to vše má platit již od května, a přitom stále chybí něco jako podpurná cesta, např. ve formě národních prováděcích předpisů. A tak většina z nás, poučená minulostí, se chytá podvědomě negativních sdělení, přeje si neutřít ztrátu a reaguje podrážděně na vše, co s GDPR jen trošičku souvisí.



Př. V únoru jsme diskutovali o GDPR s lékaři – měli obavu, zda unesou pokutu, která jim určitě hrozí, protože ani lékařská komora nedala ještě žádné podrobnější instrukce. Ptali se mě zaměstnanci v malé firmě, co budeme dělat v tak složité situaci. Avšak

ve velké výrobní firmě mi s klidem odpověděli: „Počkáme, až čas ukáže, jak je to horké.“ A přitom je GDPR důležité právě pro firmy nad 250 zaměstnanců, nikoliv pro malé rybičky, které se paradoxně třesou v předstihu.

2. Úkol pro GDPR audit:

- a) Vypište si jen tak pro vlastní nácvik racionálního a logického myšlení co nejvíce bodů, které vás na GDPR štvou; stačí stručně a v odrážkách.
- b) Podívejte se na soupis ještě jednou a vyškrtněte všechny body, které nejsou podloženy racionální informací nebo zákonem. Většinu z nás ten prázdný seznam zklidní.

Co to vlastně znamená?

GDPR znamená, že tzv. stojednička je nahrazena v současné době zřejmě nejkomplexnějším souborem pravidel. Má působnost ve většině státech EU, ale zasáhla i další tři – Norsko, Island a Lichtenštejnsko. GDPR v této situaci znamená, že bude zrušeno 31 národních zákonů.

Pro klidný průběh auditu a procesu nastavení GDPR je důležité se vyznat v jednotlivých pojmech, se kterými GDPR pracuje. U jednotlivých definic si vyznačte, zda se vás týkají. Také si můžete u každého bodu do připraveného prostoru vypsát poznámky, které vás v této souvislosti ve vaší firmě napadnou. Tak jdeme na to:

Osobní údaje: Zahrnujeme sem všechny informace, podle které se dá identifikovat konkrétní fyzická osoba. Patří sem jméno a příjmení, věk, datum narození, pohlaví, rodinný stav, občanství, fotografie, IP adresa, ID adresa, osobní a pracovní telefon a email, osobní i pracovní adresa, různé identifikační údaje (např. na vstupní kartě) a určitě spousta dalšího, na co narazíte v průběhu analýzy cesty, kterou urazí data ve vaší firmě, než je nepotřebné někam uložit či vymazat.



Př. Pokud máte pečlivě zpracovanou databázi zákazníků, kde máte i jejich data narození, abyste jim poblahopřáli k výročí, máte asi od května smůlu. Musíte si vymyslet jiný způsob, jak jim dát najevo, že patří mezi vaše oblíbence.

Může se to zdát až směšné, protože většina lidí polovinu z vyjmenovaného sama udává na různých sociálních sítích; mě například Facebook upozorňuje na všechny narozeniny lidí, které jsem si připojila do „přátel“ či přátel. Jenže nyní ejhle, sami bez jejich svolení nic z toho použít nemůžeme. Naštěstí osobní údaje lidí, kteří již nežijí, můžete zpracovávat, jak libo. Stejně tak anonymizované údaje, např. nepojmenovanou fotografii (nesmí však být možné identifikovat, o koho se jedná). Aspoň něco, i když business nám to asi nepodpoří.

Prostor pro vaše poznámky:

.....

.....

.....

.....

Citlivé osobní údaje: Jedná se o kategorii, která vyžaduje ještě pečlivější přístup. Jednoduše řečeno jsou to osobní údaje, o kterých se hovoří ještě méně, než o těch v předchozím bodě. Co se m patří? Jsou to informace typu politické názory, náboženské vyznání, zdravotní stav, sexuální orientace, trestní delikty, členství v odborech, čísla kreditních karet apod. V první chvíli to může vypadat, že se s něčím takovým příliš nesetkáváme, ale při detailnější úvaze sem můžeme zahrnout lékaře, psychology, terapeuty, firmy s odbory, nakonec i kohokoliv, kdo má pokladnu na příjem plateb přes platební karty.



Př. Firmy, které podle zákona vyžadují lékařskou prohlídku při nástupu nového pracovníka do zaměstnání, již spadají do této kategorie.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Genetické a biometrické údaje: Patří sem jakékoliv analýzy biologického vzorku, takže se týkají zejména lékařů, laboratoří apod. Vzhledem k tomu, že sem řadíme i informace, které se týkají zděděných nebo získaných osobnostních charakteristik, je zřejmé, že s touto kategorií pracují kromě lékařů i psychologové a personalisté. Do této kategorie zařadíme i otisky prstů či snímky obličeje, takže se týká i policie.



Př. V této souvislosti může být vtipné, pokud se pachatel začne jen tak ze sportu dožadovat výmazu svých dat. Nějaký čas tím získá.

Prostor pro vaše poznámky:

.....

.....

.....

.....

Osobní údaje dětí: Školy, školky, různé sportovní kluby či zájmové kroužky zpracovávají informace o dětech. Tato kategorie vyžaduje zvláštního zřetele – vždy je nutno mít souhlas rodičů či jiných zodpovědných osob. U nás je to do 16 let věku dítěte, ale může se to měnit podle členského státu EU.



Př. Zajímavosti zde může být skutečnost, jak to bude zajišťovat Facebook, Instagram či jiné sítě. Do virtuálního světa lze napsat cokoliv, jen ne pravdu o svém věku... Může se hojit na Facebooku rodič desetiletého dítěte, které by se stalo obětí trestného činu a přitom Facebook neměl povolení rodiče pro založení stránky onoho nešťastného dítěte?

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Správce osobních údajů: Jedná se o každého, kdo určuje, jakým způsobem, za jakým účelem, jak podrobně a kým se budou osobní údaje zpracovávat. Nezáleží na tom, zda se jedná o fyzickou či právnickou osobu; v každém případě je správce ten, kdo má za správné nakládání s osobními údaji zodpovědnost. (Všimněte si prosím, že slovo „správce“ i „správné“ mají stejný slovní základ.)

Jednoduše řečeno, správcem je každý, kdo má přístup k osobním údajům a něco s nimi dělá.



Př. Setkáváme se s otázkou: Co když jsem živnostník a o moje data se stará účetní? Nebo zaměstnávám 20 lidí, jejichž výplatu zpracovává externí firma? Navíc do počítačové sítě má přístup ajťák z externí firmy, nebo je to dokonce student, který si tím přivydělává na studia? Jak mohu v takovém případě zajistit, že se s daty nic nekalého nestane? Teoreticky můžeme ve směrnicihopsat co chcete, ale v praxi je to ošemetná otázka. Ale i takové situace nastanou a je potřeba se s nimi co nejlépe poprat. Prakticky to znamená, že váš nastavený systém ochrany dat se bude vztahovat i na vaše externí dodavatele. Doporučujeme vypracovat firemní směrnici, která každého seznámí s pravidly práce s osobními

údaji a tu pak skutečně vyžadovat v reálném pracovním životě. A směrnice je vždy vhodné nechat podepsat, jistota je jistota.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Zpracovatel osobních údajů: Je to jednotlivec nebo firma, kterou správce pověří, aby s osobními údaji něco konkrétního prováděla a zadá ji pokyny, jak to má dělat. Pokud máte externího zpracovatele, doporučujeme upravit způsob zpracování dat v závazné smlouvě, a to vždy konkrétně mezi správcem a daným zpracovatelem.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Zpracování osobních údajů: Řadíme sem jakýkoliv úkon, který se s osobními údaji („běžnými“ i citlivými) provádí. Je důležité si uvědomit, že vůbec nezáleží na tom, zda se jedná o papírové či elektronické procesy.



Př. Věta „My už to máme všechno v počítači, my s daty nijak nepracujeme“, tím pádem neobstojí.

Takže si do této kolonky zařaďte zejména: získávání informací, jejich evidenci, zařazování do různých databází nebo souborů, následné vyhledávání, využití pro telefonát/e-mailing/výzkum/statistiku/apod., úpravy a dopisování podrobnějších informací, vymazávání

části nebo celku, šíření pro další využití, archivování atd.



Př. Dvakrát se mi zadařilo v diskuzi se správcem osobních údajů slyšet naivní větu: „Ale my s těmi osobními údaji nic neděláme. Jenom je vždycky zaneseme do systému.“ Omyl. Správce musí řídit i to, co s daty provádí systém.



Obr. č. 1: Proces zpracovávání osobních údajů

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Zákonnost zpracování osobních údajů: Chcete-li zpracovávat osobní údaje, musíte mít předem splněny minimálně jednu ze tří zákonných podmínek. Zdůrazňujeme slovo „předem“ a upozorňujeme na pojem „zákonných podmínek“. Zde jsou:

- a) Máte souhlas: V tomto případě máte tedy vyhráno. Pozor – nikdy však nedávejte souhlas přímo do smlouvy, vyhněte se mnoha nepříjemnostem. Je výhodné mít

souhlas mimo smlouvu; už jenom proto, že smlouva může přestat platit a souhlas pokračuje. Nebo protože by souhlas mohl být díky smlouvě zavádějící nebo něčím podmíněný. Pak by nebyl platný.

- b) Zpracování vyplývá z právní povinnosti, popř. jednáte v zájmu toho, komu data patří: Jako příklad si můžeme uvést havárii, u které zasahují záchranáři. Informace potřebují příliš rychle, než aby se zdržovali písemným souhlasem. (My máme za to, že sem patří i informace pacientů u lékaře, jak o tom píšeme dále.)
- c) Jedná se o veřejný zájem nebo o zájmy správce, který jedná v zájmu osoby, které data patří. Patří sem veřejná správa, policie, pojišťovny apod. Možná i něco dalšího, jak vyplyne z přijatého upřesňujícího národní prováděcí předpisu, který bude v budoucnu přijat.



Př. neboli poznámka: Vzhledem k obecnosti posledních dvou bodů si právníci v případě potřeby smlsnou....



Obr. 1: Kdy je zákonné zpracovávat osobní údaje (vysvětlení v textu)

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Zpracování citlivých osobních údajů: Zjistíme-li, že musíme zpracovávat údaje z této oblasti, zbystríme pozornost, začneme být ještě více obezřetní a vždy si zajistíme souhlas. Naprosto nutně a bezpodmínečně je potřeba nadefinovat důvod, proč tyto informace musíme zpracovávat.



Př. Nejčastěji se bude v našich podmínkách jednat o citlivé informace pro potřeby lékařství, právní, sociálního zabezpečení, personální oblast, vědecké nebo statistické zpracování.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Souhlas ke zpracování osobních údajů: Osoba, po které vyžadujeme souhlas, nesmí být pod žádným viditelným nebo nenápadným tlakem a musí souhlas udělit dobrovolně. Udělovaný souhlas musí být formulován tak, aby:

- byl konkrétní,
- byl jednoznačný,
- poskytnul informace o tom, co budeme s údaji provádět,
- seznámil, za jakých podmínek je možné souhlas odvolat.

Doporučujeme proto vytvořit pro vhodnou a srozumitelnou instrukci, která sdělí, proč se údaje zpracovávají, jak dlouho se budou uchovávat a kde, kdo další bude mít k datům přístup, jak je možné se nechat vymazat.



Př. Nestačí tedy mít takové to zaškrtnuté políčko, na které jsme doposud na webových stránkách nebo na dotaznících zvyklí. Od května se musí dostat dotyčné osobě obsáhlého poučení. Také již nestačí předpokládat, že když někdo nezašle svůj nesouhlas, že prostě souhlasí.

Některé obchodní firmy měly nápad, jak získat souhlas snadněji – podmínily získání dárčku souhlasem. To bohužel není chápáno jako dobrovolný souhlas, takže to raději nezkoušejte.



Obr. č. 2: Co musí obsahovat souhlas ke zpracování osobních údajů

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Ochrana osobních údajů: Hlavní myšlenkou GDPR je ochránit osobní údaje. Proto je logické, že se zabývá i případným porušením a sankcemi. Všimněte si prosím, že se jedná pouze o jeden z bodů, nikoliv o nosné téma, jak to občas vypadá na seminářích nebo obchodních sděleních s tématem GDPR.

Nově se objevuje, že hříšník, tedy správce, kterému data utekla, se sám nahlásí patřičným úřadům. Nepříjemné, ale zřejmě jedna z možností, jak dopady zmírnit neb ose jim dokonce vyhnout.

A jaké incidenty spadají do nahlášovací povinnosti? Můžeme si je pro lehčí zapamatovatelnost pojmenovat jako pravidlo 5xZ:

- zcizení,
- zničení,
- ztráta,
- zkreslení,
- změna nechtěná.

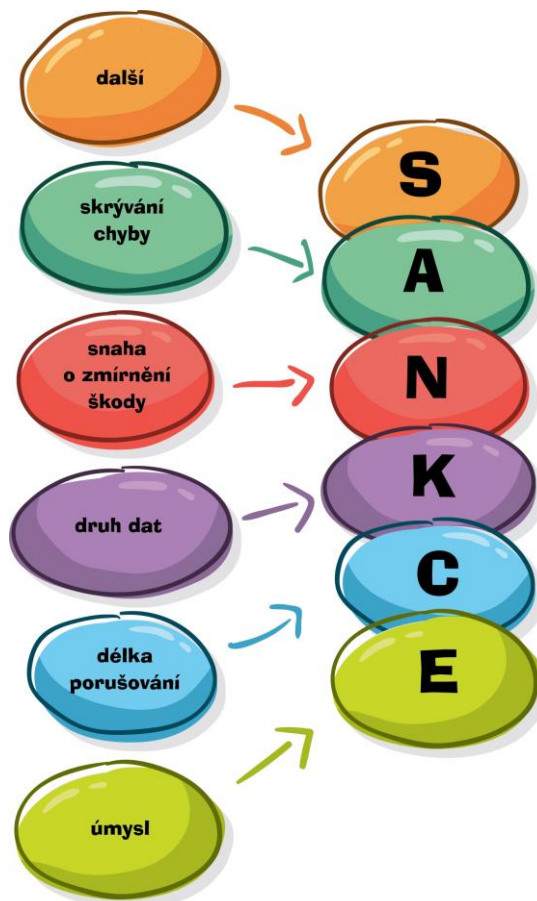
Jsou dána jasná a přesná pravidla, do kdy je nutno informovat úřady a co vše mají správci v podobných situacích za povinnost.

Samozřejmě se dá očekávat, že normální člověk má tendenci maléry ututlat. Už jenom kvůli těm stále omílaným obřím pokutám. Je lepší však být v pozici spolupracující strany, než té, která musí posléze koktat výmluvy. Sankce se také posuzují podle úmyslu, délky porušování povinnosti, o jaký druh dat se jednalo, jak se pokusil správce zmírnit škodu apod.



Př. neboli doporučení: Je nanejvýš žádoucí, aby pravidla a způsob nahlášení incidentů byly součástí firemních pravidel nakládání s osobními údaji. Máme zkušenost, že

pokud k nějakým rizikům nakonec skutečně dojde, v 90% se jedná o nevědomé nebo škodolibé selhání zaměstnance: interního či externího, brigádníka, stážisty, konzultanta. Závazná pravidla o nakládání s osobními údaji jsou sice další papírování, ale mohou vám pomoci zejména v oblasti právní a morální.



Obr. č. 3: Co má vliv na výši sankce

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

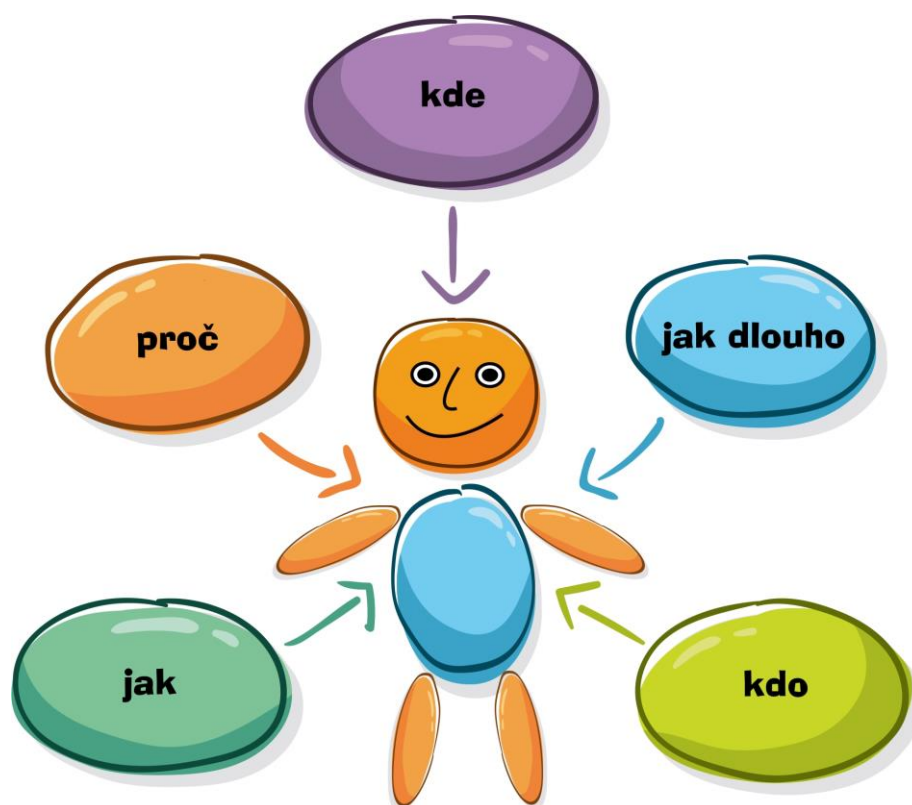
Hlavní práva subjektů („majitelů“) osobních údajů: Práva majitelů osobních údajů (subjektů), jsou od května 2018 jsou významným způsobem posílena a kromě vyjmenovaných výjimek v podstatě mohou vystupovat jako jejich skuteční majitelé.

Co všechno musí správce majitelům dat zajistit a zaručit? Jsou to zejména následující situace:

- Subjekt má právo vědět **kdo – co – kde – jak – jak dlouho – proč**.
- Požádá-li subjekt o kopii údajů, má právo je mít.
- Pokud se subjektu povolený souhlas rozleží, má právo říci „beru souhlas zpět“, a to v různých podobách: může si vymoci přístup k datům a zkontrolovat si je, může se dožadovat opravy, celého výmazu a možnosti „být zapomenut“, omezit částečně zpracování, vznést námitku.



Př. Je otázkou, jak se bude dožadovat subjekt výmazu stop, které zanechává svým surfováním na sociálních sítích, ale budiž. Zákon je zákon.



Obr. č. 4: Co musíte sdělit osobě, jejíž údaje zpracováváte

Podívejme se podrobněji na jednotlivá práva majitelů osobních dat:

- a) Výmaz: Provádí se poté, co již není potřeba data uchovávat, popř. když vypršel termín povolení je zpracovávat. Stejně tak se výmaz provádí, pokud se subjekt rozhodne svůj

souhlas odvolat nebo pokud se zjistilo, že data jsou uchovávaná protiprávně.

Př. neboli poznámka: Vypadá to, že mnohé obchodní databáze vezmou za své....

b) Právo „být zapomenut“: Na první pohled zajímavý bod, který potěší zejména technicky orientované čtenáře, kteří začnou spekulovat, jak to lze uchopit doslova a do písmene. Jedná se totiž o poměrně široký zásah do procesu uchovávání informací, zejména v elektronickém světě. V dnešní době internetu a mnohých programů pro sledování jeho uživatelů se jedná o naprosto pochopitelný požadavek – v určitém věku člověk zmoudří a mrzí ho stopa, kterou po sobě v informačním světě zanechal.

c) Tzv. omezené zpracování: Jedná se o nižší formu výmazu. Subjekt výslovně definuje čas, formu a míru zpracování. Správce je povinen toto přání splnit, i když mu přinese v procesu zpracovávání komplikace.

d) Možnost přenést údaje: Subjekt může vyžadovat předání svých zpracovaných údajů a přenést je k jinému správci, aniž by se musel dožadovat povolení správce původního.

Př. Naskýtá se jako příklad situace, kdy subjekt vyžádá informace u jedné pojišťovny a v nezměněné podobě je předá jiné pojišťovně. Pomůže si tak k lepším podmínkám.

e) Právo vznést námitku: Tohoto práva využije subjekt, pokud získá dojem, že s jeho daty je nakládáno jinak, než je podle jeho soudu správné – avšak správce si myslí něco jiného.

Př. Stane se to v případě, kdy se data zpracovávají ve veřejném zájmu nebo oprávněném zájmu správce.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

Pověřenec pro ochranu osobních údajů: Tato funkce se týká zejména větších organizací. Zda se bude jednat o novou pracovní pozici nebo o pouhé „přidání práce“ někomu, záleží na tom, co firma dělá a kolik informací zpracovává. Hlavním úkolem této pracovní pozice bude dohlížet na dodržování ochrany osobních údajů, předkládání návrhů pro předcházení incidentů, provádění interních cyklických auditů pro ochranu osobních údajů, školení zaměstnanců na toto téma.

Prozatím není zpracován pracovní profil této pracovní pozice, ale pokud se bude jednat o kumulovanou funkci, musí se pohlídat střet zájmů (který může reálně hrozit). Může se jednat o externího i interního pracovníka.

Pro malé firmy se zřejmě tolik měnit nebude, tam předpokládáme přidání zodpovědnosti vhodné osobě.



Př. či spíše upozornění: Je důležité znát skutečnost, že pověřenec pro ochranu osobních údajů není zodpovědný za případné incidenty a nedodržení pravidel GDPR – tato povinnost jde pouze a jen za firmou samotnou.

Prostor pro vaše poznámky:

.....

.....

.....

.....

.....

3. Úkol pro GDPR audit:

V níže uvedené tabulce jsou uvedeny jednotlivé body, které jsme v kapitole probrali. U každého z nich si napište poznámku, která bude vystihovat u konkrétního bodu aktuální stav ve vaší firmě.

Název položky	Úkol pro analýzu
Osobní údaje	Zjistěte si, kde všude zpracováváte: jméno, věk, datum narození, pohlaví, rodinný stav, občanství, fotografie, IP adresa, osobní a pracovní telefon a email, osobní i pracovní adresa, různé identifikační údaje. Zapište si to. Logicky si vyvodte, zda všechny tyto informace musíte zpracovávat (možná máte některé navíc, pro pořádek nebo do zásoby – vypište si i tyto možnosti).
Citlivé osobní údaje	Proveďte analýzu vašich dokumentů, zda najdete i citlivé osobní údaje. Pokud ano, vypište si jaké a kde. Poté se zamyslete nad tím, proč je zpracováváte. Odpovězte si na otázku, zda je musíte zpracovávat, zda vám to projde v případě kontroly. Definujte si písemně důvody zpracovávání citlivých osobních údajů.
Genetické a biometrické osobní údaje	Stejně tak jako v předchozím bodě, i zde si vypište, které údaje z tohoto ranku zpracováváte. Odpovězte si na otázku, zda byste se bez těchto informací obešli. Předpokládáme, že spíše ne, ale buďte k sobě kritičtí. I tento výsledek si zapište. Také zde si definujte důvody zpracování těchto údajů.
Osobní údaje dětí	Zjistěte, zda evidujete i tyto údaje. Pokud ano, a pokud je navíc opravdu potřebujete, zapište si, kde a proč. A nachystejte si formulku pro souhlas rodičů. Zkontrolujte, zda zformulovaný souhlas obsahuje všechny potřebné oblasti, jak jsme popisovali v předchozím textu.
Správce osobních údajů	Odpovězte si na otázku, kdo je správcem údajů. Pokud vy, zbystřete pozornost. Pokud někdo jiný, spojte se s ním a iniciujte debatu o GDPR auditu.
Zpracovatel osobních údajů	Vypište si všechny zpracovatele osobních údajů, které máte (IT servis, externí účetní, externí personální služby, externí callcentrum, právnické služby apod.). Zanalyzujte, jak nyní předáváte těmto lidem či firmám osobní údaje a vypište si všechny nedostatky a nepřesnosti. Připravte si pro zpracovatele psaná firemní pravidla, nejlépe ve formě směrnice, a seznamte je všechny s tímto postupem. Zajistěte, aby všichni pochopili nový postup i důvod, proč je potřeba ho dodržovat.
Zpracování osobních údajů	Popište co nejpřesněji cestu, kterou osobní údaj ve vaší firmě urazí, a to od jeho získání, až po jeho archivaci a vymazání (způsob získání, evidenci, zařazení, vyhledávání, využití pro kde co, úpravy, dopisování, vymazávání, šíření, archivování atd.). Vypište u každé oblasti i rizika, která se mohou v průběhu zpracování objevit (ztráta, zcizení, zkreslení atd.) – bude se to hodit v dalším kroku. Pokuste se ta rizika, kterým lze předejít jiným způsobem zpracování, směrnicemi, školením zaměstnanců, omezením přístupů apod. co nejvíce zmírnit.
Zákonnost zpracování osobních údajů	Máme tři možnosti, díky kterým je zpracovávání údajů zákonné. Zapište si, které možnosti přicházejí pro vaši potřebu v úvahu. Vymyslete způsob, jak si je zajistit.
Zpracování citlivých osobních údajů	Pokud jste ve druhém bodu této tabulky usoudili, že musíte tento druh údajů zpracovávat, definujte si jasně, konkrétně a písemně důvody a zajistěte si souhlas se zpracováním těchto údajů. Pokud jste usoudili, že tyto údaje nezpracováváte, tento bod přeskočte.
Souhlas ke zpracování osobních údajů	Vytvořte si formulaci, kterou budete předkládat subjektům k podpisu. Je důležité, aby byl souhlas dobrovolný (ničím nepodmíněný), bez nátlaku, konkrétní, jasně formulovaný. Konkrétně formulujte, co se bude s údaji dít, proč se zpracovávají, jak dlouho a kde se uchovávají, kdo kromě správce údajů bude přístup, za jakých podmínek lze souhlas odvolat. Je to fakt dlouhý, ale nic s tím nenaděláte.

Název položky	Úkol pro analýzu
Ochrana osobních údajů	V osmém bodě této tabulky jste si vypsalí možná rizika. Zkontrolujte tuto oblast ještě jednou podle pravidla 5 x Z (zcizení, zničení, ztráta, zkreslení, změna nechtěná) a případně ji ještě rozšiřte o zjištěné skutečnosti. Poradte se s někým dalším, zda můžete udělat něco dalšího pro zabezpečení zpracovávaných dat. Zjistěte si také, kdo je váš nadřízený orgán, kterému máte hlásit případné incidenty. Zpracujte písemný postup, který v případě incidentu může použít zodpovědná osoba (nahlášení, co největší snížení škod apod.).
Práva subjektu osobních údajů	Subjekt má právo vědět své kdo – co – kde – jak – jak dlouho – proč. Popište si proces zpracování osobních údajů tak, abyste na tyto otázky uměli kdykoliv odpovědět a data najít. Seznamte lidi, kteří mají proces zpracování dat, s právy subjektů a nadefinujte, jak je budou naplňovat v případě požadavků subjektů.
Pověřenec pro osobní údaje	Podle množství vašich údajů se rozhodněte, zda musíte vytvořit tuto funkci. V každém případě popište, co by měl takový člověk u vás ve firmě na starosti. Jsou to standardy, které je nutno zachovávat. Také vytvořte psaný, hraný, mluvený materiál, který bude sloužit jako školení pro všechny pracovníky ve firmě, kteří budou s údaji přicházet do styku. Čas od času tento dokument prozkoumejte, zda je stále aktuální a zda ho není možné ještě vylepšit.

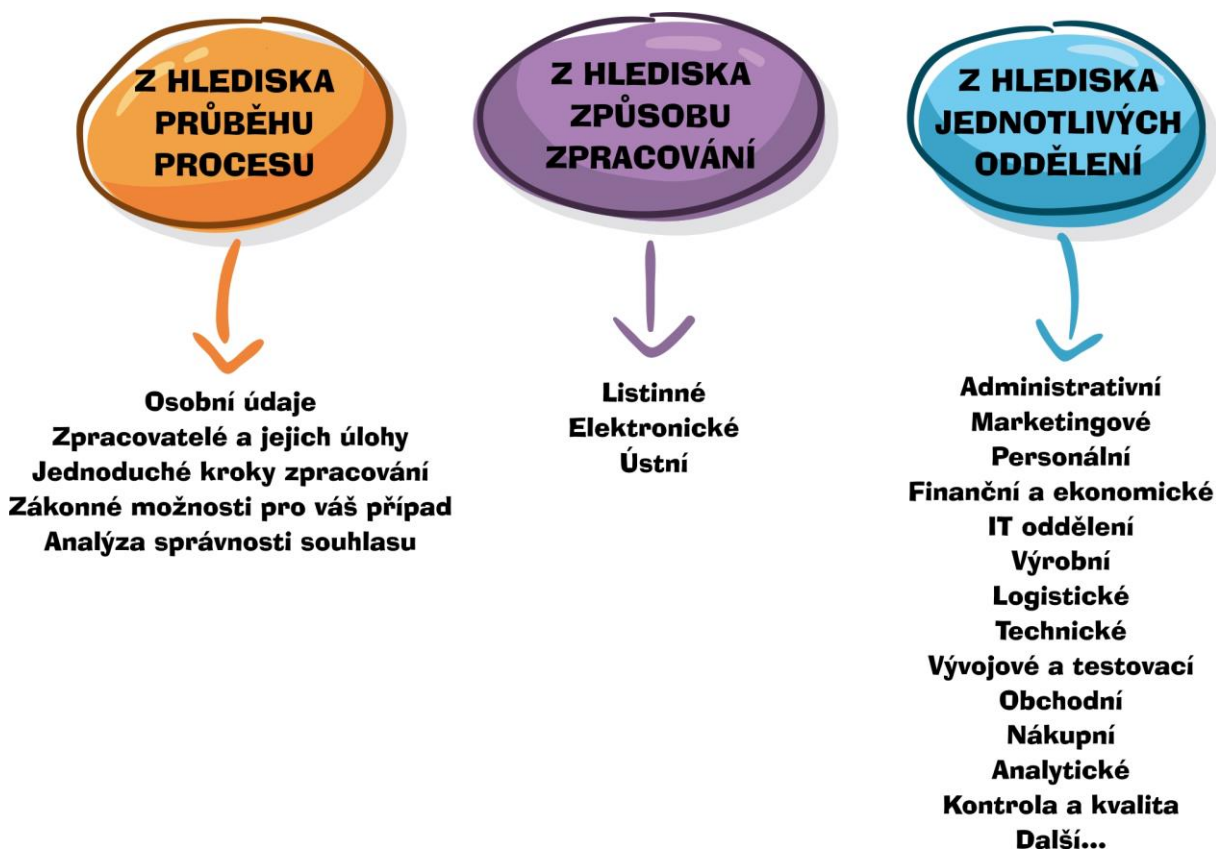
Jak mám na to jít?

Pokud jste si provedli analýzu podle předchozích doporučení, zanalyzovali jste si problematiku z pohledu procesu zpracování osobních údajů a připravili potřebné kroky k realizaci. Díky tomu máte velkou část práce za sebou. Může se však stát, že jste na něco zapomněli, což by bylo při kontrole nemilé. Proto se při auditech vždy pokoušíme podívat na analyzovanou situaci z několika úhlu. Provedeme to i nyní, abyste měli jistotu, že je proces zpracování osobních údajů ve vaší firmě v pořádku.

Z pohledu procesního jsme již analýzu provedli.

V našem případě provedeme analýzu ještě ze dvou úhlu:

- a) Z hlediska způsobu zpracování
- b) Podle oddělení ve firmě.



Obr. č. 5: Třífázová analýza zpracování osobních údajů

ad a) **Z hlediska způsobu zpracování** se může jednat o listinné, elektronické a ústní zpracování osobních údajů.

Listinné zpracování se týká všech situací, kdy zachycujete osobní údaje v papírové podobě.

Jsou to vstupní dotazníky, návštěvní kniha, objednávky a faktury, zápisy z porad a schůzek, podklady pro docházku a výplatu na dílnách, zápisy o jakosti/nejakosti na směnách ve výrobních podnicích, materiály, které původně byly v elektronické podobě a pro lepší přehled jste si vytiskli, podepsané prezenční listiny ze školení, podpisové listy na schůzích družstva vlastníků apod. Je jich kolem nás více, než si vůbec představujeme.

Je důležité si udělat soupis všech těchto možností. Definujte všechny body, ve kterých může dojít k nežádoucím incidentům (viz „5 x Z“) a raději si je poctivě vypište. Zvažte, které můžete oželeť a které musíte dále používat. První skupinu zrušíte, druhou zpracujete z pohledu GDPR (viz předchozí kapitola – 3. úkol).

Elektronické zpracování se eviduje a analyzuje o něco snáze, také se lépe hlídá samotný průběh zpracování. Flexibilněji a přesněji lze též reagovat na možné nesrovnalosti a chyby, zejména pokud vycházejí z lidského faktoru. I v tomto případě se pokuste definovat všechna místa, kam údaje ukládáte, i procesy, které s nimi provádíte. Zcela určitě sem zařadíte takový obsah, jako jsou osobní složky zaměstnanců, databáze zákazníků a odběratelů, e-mailové adresy, telefonní seznamy apod. I zde si pečlivě vypište jednotlivé možnosti a jejich možné incidenty.

Nezapomeňte na různé poskytovatele služeb, hostingové služby apod. I ty spadají do vaší zodpovědnosti, pokud u nich nakládáte s daty. I s těmi daty naložte stejně, jako u dat listinného zpracování – rozhodněte, co zrušit a s čím pokračovat dále. Ty údaje, které budete dále zpracovávat, podrobte procesu z předchozí kapitoly, tj. 3. úkolu.

Poslední je ústní zpracování osobních údajů. V dnešní době se to může zdát asi směšné, ale přesto popřemýšlejte, zda nepoužíváte osobní údaje i v ústním podání. Zavolá někdo na ústřednu, že chce telefonní číslo na určitého pracovníka? Doposud jste ho bezmyšlenkovitě nadiktovali, od května tomu bude jinak.

Nepodceňujte ani situace s ústním zpracováním a také si je vypište. A opět si zaznačte body, které vám mohou v budoucnu přinést problémy. I zde se rozhodněte, jak jednotlivé situace ošetříte do budoucna – pomocníkem je vám opět 3. úkol z přechozí kapitoly.

Ad b) **Podle oddělení ve firmě:** Pro představu nabízíme výčet oddělení, které se ve firmě mohou vyskytnout. Zaškrtněte si ty, které se u vás ve firmě vyskytují, popř. si dopište, pokud vám některé chybí. Jste-li malá firma, zaměňte slovo „oddělení“ za „oblasti“ a můžete

pokračovat stejným způsobem:

- Administrativní oddělení (ve školství to může být studijní oddělení)
- Marketingové oddělení
- Personální oddělení
- Finanční a ekonomické oddělení
- IT oddělení
- Výrobní oddělení
- Logistické oddělení
- Technické oddělení
- Vývojové a testovací oddělení
- Obchodní oddělení
- Nákupní oddělení
- Analytické oddělení
- Oddělení kontroly a kvality
- Další, vypište:

Ve všech těchto odděleních nechejte popsat zodpovědné osoby situace, ve kterých se setkávají s osobními údaji. Také ať popíší místa, kde může dojít k incidentům – a zároveň mohou navrhnout nápravu.



Př. Máme zajímavé zkušenosti s tím, když tyto situace a možné incidenty popisují nezávisle na sobě dvě osoby: vedoucí oddělení a jeho nadřízený, dva lidé z daného oddělení apod. Rozdílné pohledy na problematiku jsou natolik velké, že se ani jednou nestalo, aby se tito lidé shodli ve většině uváděných informací.

4. Úkol pro GDPR audit:

- Vraťte se k analýze, kterou jste si vypracovali při pohledu „podle způsobu zpracování“. Máte-li možnost, požádejte, aby nezávisle totéž udělal někdo další, kdo je znalý činnosti ve firmě. Porovnejte oba výsledky. Zřejmě je díky nápadům dvou lidí budete kompletovat – ale to je ku prospěchu věci. Nezapomeňte si prohlédnout znovu všechny smlouvy, které máte uzavřeny s různými dodavateli, jejichž činnost se týká GDPR. Nezapomeňte ani na

své zaměstnance. Zkontrolujte, zda jsou v pořádku. Pokud ne, domluvte se na nápravě – pro všechny smlouvy platí, že nesmí být napadnutelné z pohledu GDPR.

- b) Vypište si jednotlivá oddělení ve vaší firmě (jste-li menší firma, tak oblasti) a požádejte odpovědné osoby o písemné zpracování analýzy, jak v daném oddělení pracují s osobními údaji. Zvláště oceňte, pokud se jim podaří vypíchnout krizová místa. I zde je vhodné pro co největší přesnost pracovat ve dvojici, ovšem nezávisle na sobě a poté oba výsledky porovnat.
- c) Zpracujte si tabulku pro možné chyby a incidenty. Vycházejte přitom z analýzy všech tří oblastí (procesu, způsobu zpracování a oblastí). Vyplňte si u každého bodu, co s tím uděláte, abyste možným chybám předešli. Pro svůj vnitřní klid zkontrolujte, zda se některý z incidentů objevil pouze v jedné možnosti analýzy. Pokuste se definovat, proč si ho nikdo nevšiml při dalších dvou možnostech.

Ukázku přinášíme v níže uvedené tabulce:

Situace k řešení	Způsob řešení	Do kdy	Kdo
Chybí souhlas ke zpracování osobních údajů u nových zaměstnanců a zákazníků.	Zpracovat správně formulovaný souhlas, zadat na webové stránky, zpracovat formulář pro nové zaměstnance, zakomponovat do zákaznických služeb, proškolit příslušné zaměstnance, kteří mají souhlas používat.	K jednotlivým úkolům přiřadit data.	K jednotlivým úkolům přiřadit konkrétní osoby.
Předávání telefonních čísel na recepci.	Zpracování směrnice, se kterou se seznámí pracovníci recepce a vedoucí jednotlivých oddělení.	Konkrétní datum.	Konkrétní jména.
Synchronizovat způsob zpracování osobních údajů s externí účetní.	Definovat způsob zpracování, vypracovat směrnici, seznámit s ní externí účetní, nechat ji to podepsat	Konkrétní datum.	Konkrétní jména účetní a např. jednatele.

Poradí mi někdo, když budu v koncích?

Zavádět GDPR je výhodné minimálně ve dvojici (ale v menším rozsahu, jak tomu zřejmě bude u malých firem, to hravě zvládne i jeden člověk s dobrým logickým myšlením). Ve větších firmách doporučujeme pracovat v týmech, které se skládají ze zkušených lidí v oblasti:

- Managementu
- Práva
- Personalistiky
- IT
- Hodil by se také někdo, kdo bravurně ovládá vedení projektů, protože to celé sesynchronizuje a povede nejkratší cestou k cíli.



Př. Často se ve firmách zpočátku uchylují k tomu, že na tuto práci zvolili mladé lidi. Argumentují tím, že je to přece nová pozice, tak není potřeba ani zkušeností. Pravda je, že není potřeba zkušeností se zaváděním GDPR. Je však potřeba mít zkušenosti s procesy ve firmě, a tak se mnohem více do těchto týmů hodí zkušení harcovníci.

Na správnost dodržování pravidel bude dohlížet nezávislý orgán veřejné moci, jehož pravomocí jsou v oblasti vyšetřovací, nápravné, poradní a povolovací. Takže v případě nouze se nabízí možnost využít pravomoci poradní a žádat o radu. Proč nejít zrovna ke kováři? 😊

5. Úkol pro GDPR audit:

Nebudte na všechno sami a pokud to jde, vytvořte si pro zpracování GDPR auditu a zavedení jeho standardů tým zaměstnanců z vaší firmy. Je výhodou, pokud budou odborníci ve svém oboru a praktici, protože vám nejlépe identifikují potřebné informace.

Jste-li z menší firmy, zkuste pro tuto práci získat ještě někoho do dvojice, kdo vás bude inspirovat svými provokativními dotazy. Ale mějte na paměti, že i jeden člověk to zvládne sám. Odměnou vám bude zcela jiný úhel pohledu na vlastní firmu.

Jste-li líný nebo máte málo času, jsou tady pro vás konzultanti, kteří s na problematiku GDPR specializují. Oslovte je.

Sepište si průběh a výsledky auditu procesu zpracování osobních údajů a ponechejte si to do dalších let. Bude se to hodit, až se budete muset k něčemu vracet.

Jak poznám, že je to správně?

Nejlepší je asi přečíst si celý dokument GDPR. Ale to asi nechcete, protože kdybyste chtěli, nestudovali byste naši publikaci. Anebo jste sice chtěli, ale text vám připadal stejně nejasný a nesrozumitelný, jako nám všem, kteří jsme se jím několikrát prokousávali.

Takže si pojďme shrnout pravidla, která vám na otázku odpoví:

- a) Zpracování údajů musí být legální, podle pravidel GDPR. Znamená to, že musíte splňovat minimálně jednu z podmínek:
 - Zpracování osobních údajů je nezbytné pro účely oprávněných zájmů ÚOOÚ. Ani zde však jejich zájmy nesmí převažovat nad zájmy a právy subjektů, jejichž údaje zpracováváte.
 - Osobní údaje zpracováváte pro vědecký, statistický nebo historický výzkum. (Nepočítejte však, že se na to dá odvolávat v případě, kdy u vás kontrola nalezne pochybení. Musí se jednat o skutečně podložené důvody.)
 - Osobní údaje jsou nezbytné z důvodu veřejného zájmu.
 - Osobní údaje jsou potřebné pro výkon veřejné moci.
 - Osobní údaje jsou nutné k ochraně života subjektu údajů.
 - Osobní údaje jsou potřebné vzhledem k oprávněným zájmům správce. Na tento bod spoléhá mnoho podnikatelů v oblasti obchodu a marketingu – vždyť je v jejich zájmu mít adresy lidí nebo organizací, kterým produkty nabízejí. Nejsme si však jistí, zda to takto bude fungovat.



Př. Zde se musíme přiznat, že se názory odborníků velmi liší – někteří razantně odmítají tento důvod, jiní zase zastávají názor, že při dobré argumentaci je možné tuto skutečnost použít. Máte-li zkušeného právníka, pozvěte ho na dobrou kávu a proberte to s ním.

- Osobní údaje musíte zpracovávat, protože vás k tomu vybízí zákon. Jedná se např. o povinnost archivovat údaje o zaměstnání, účetní doklady apod. Pokud máte osobní údaje na účetních dokladech, je pak všechno v pořádku. Otázkou je, zda můžete spravovat databázi zákazníků bez jejich souhlasu, i když v nich budete mít pouze ta data, která se dala vyjmout a použít z účetních dokladů. Bude-li provádět kontrolu někdo přepečlivý,

máte co vysvětlovat.

- Osobní údaje potřebujete nezbytně pro realizaci smlouvy se subjektem. Může se to zdát logické – pokud někomu opravuji auto, potřebuji jeho údaje, abych mohl svoji práci zafakturovat. Ale neobhájíte, pokud budete mít mezi osobními údaji datum narození či e-mailovou adresu. Můžete se sice ohánět logickým argumentem, že právě elektronickou poštou s daným zákazníkem komunikujete, ale věřte mi, že vám to asi neprojde. Podle některých přednášejících musíte telefonní nebo emailové spojení po ukončení opravy vymazat.
- To nejjistější nakonec – získali jste souhlasem ke zpracování osobních údajů. K jeho specifikaci jsem v předchozím textu uvedli podrobné informace. Ve zkratce řečeno, musí jít o jednoznačné přání dotyčné osoby.



Př. Představte si situaci, kdy požadujete po zákazníkovi, jemuž opravujete auto, aby vám dal souhlas k využití jeho e-mailové adresy nebo telefonického čísla. Jenže zákazník bude šprýmař a odmítne souhlas podepsat. Podle vyjádření GDPR vás to nesmí ovlivnit v tom, zda mu poskytnete požadovanou službu, případně v jaké kvalitě. Umím si představit, jak to asi v praxi může vypadat – první, co vás u takového zákazníka napadne, bude následující: „kdo dělá problémy na začátku, dělá i na konci...“

Důležité je u souhlasu zajistit, aby byl oddělen od ostatních podmínek služby. Doposud to takto striktně nebylo požadováno, od května ano. Udělení souhlasu musí být také ověřitelné.



Př. Setkali jsme se s názorem, že přece stačí do databáze zákazníků nechat nainstalovat další políčko s názvem „poskytl souhlas v souladu s GDPR“ a to prostě zaškrtnout. Jak by s na to přišlo? Omyl. Je nutno zaznamenat kdo, kdy, jak, jak široký a k čemu byl souhlas udělen.

- b) Dávejte pozor, pokud zpracováváte genetické a biometrické údaje. Nadefinujte si důvody, proč a v jaké míře je musíte zpracovávat a projděte to vše raději s právníkem.
- c) Pokud zpracováváte osobní údaje dětí, zajistěte si souhlas zákonných zástupců, u nás je to do 16 let. Doporučuje se postupovat stejně, jako u běžného souhlasu ke zpracování osobních údajů. Pokud jednáte přímo s dětmi (např. jazykové kurzy, zájmové kroužky

apod.), pokuste se napsat informace o ochraně osobních údajů a potřebě souhlasu ze strany rodičů tak, aby to bylo adekvátní nejen k chápání rodičů, ale i jejich dětí.

- d) Zajistěte, aby osobní údaje byly zpracovávány tak, aby bylo možno dodržet práva subjektů, jimž data patří. Prakticky to znamená minimálně skutečnost, že musíte být schopni na začátku práce s daty subjektům poskytnout informaci, co s jejich daty provádíte a proč.



Př. Častý dotaz je na situaci, kdy získáte data z veřejných zdrojů. Musíme vyžadovat souhlas s jejich používáním? Ano, je to tak. I v takovém případě musíte umožnit subjektům využít práva být informován. V praxi to znamená, že jim mimo jiné sdělíte, jakým způsobem jste jejich údaje získali, k čemu je budete používat a že mají možnost být smazáni, budou-li o to žádat.

Mezi další práva patří právo na přístup k údajům, právo na opravu údajů, právo být zapomenut, právo na omezení zpracování údajů, právo na přenositelnost dat, právo na námitku.



Př. Ne vždy ale je nutno bez rozmyslu přistoupit k vykonání práva subjektu. Když např. zákazník, který si u vás nakoupil zboží, požádá o výmaz všech osobních údajů, mějte na paměti, že tady jsou ještě oprávněné požadavky správce údajů (např. potřebujete údaje na fakturaci nebo musíte uchovat informace o prodeji, pro případ reklamace zboží).

- e) Definujte si konkrétní zodpovědnost, kterou za zpracování osobních údajů jako správce nesete a udělejte co nejvíce pro to, abyste se chovali zodpovědně. Mějte dokumenty, firemní směrnice na téma GDPR, proces zpracovávání a proškolení zaměstnanců na takové úrovni, abyste dovedli vždy prokázat, že požadavky GDPR skutečně dodržujete. Zde doporučujeme zpracovat vnitrofiremní dokument, který bude zahrnovat:

- Provedenou analýzu aktuálního stavu a definici možných rizik.
- Definování kroků, které minimalizují popsaná rizika.
- Pravidla ochrany osobních údajů v podobě elektronické, listinné i ústní, a to jak směrem do firmy, tak i směrem ven z firmy. Tato pravidla zpracujete do firemních směrnic, se kterými zaměstnance seznámíte a necháte je to stvrdit podpisem. U externích dodavatelů

vypracujte smlouvy, které také nechávejte podepisovat.

- Cíleně proškolení všechny zaměstnance, kterých se nové standardy GDPR týkají, přičemž je důležité mít opět podepsaný dokument nebo jiné osvědčení (např. v elektronické podobě).
 - Zpracujte směrnici, která určuje způsob chování v případě, že dojde k incidentu. Dopište do ní i adresy na kontrolní orgány. (A nezapomeňte je požádat před tím o souhlas. 😊)
 - Definujte si časové období, kdy provedete cyklickou revizi.
- f) Pokuste se minimalizovat míru osobních údajů, které zpracováváte. Pak také minimalizujete možnosti nechtěných incidentů.
- g) Jste-li organizace nad 250 zaměstnanců, je vaší povinností vést Záznamy o činnosti zpracování. Sem patří: název a identifikace organizace, důvod, proč osobní data zpracováváte, popis kategorií jak subjektů, tak i jejich osobních údajů, kdo je konkrétním příjemcem osobních dat, popis technických a organizačních bezpečnostních opatření, informace o tom, zda a jak se osobní údaje dostávají do dalších zemí.
- Podobné Záznamy o činnosti zpracování budete muset zpracovat, pokud osobní údaje, kterými disponujete, by mohly vést k ohrožení práv subjektu nebo pokud zpracováváte osobní údaje zvláštní kategorie (např. pro účely trestního řízení).
- h) Jste-li velká organizace, zvažte, zda není vhodné zavést pozici Pověřence pro ochranu osobních údajů. Je na personálním oddělení, aby vypracovalo profil takového člověka z personálního a psychologického hlediska a zavedlo tuto pozici do praxe.

6. Úkol pro GDPR audit:

Jak je z výčtu patrné, není zase GDPR takový strašák, jak se na začátku zdálo. Pokud se vám podařilo provést analýzu dle našich pokynů, stačí pak zavést výše uvedených devět bodů do praxe ve vaší firmě a je všechno v pořádku. Můžete s klidem usínat.

Dobrá zpráva pro menší firmy je skutečnost, že pro ně platí jen bodů sedm.

Dvacet nejčastějších otázek z diskuzí našich zákazníků

Na kolik mě GDPR přijde? Na tuto otázku nelze odpovědět zcela přesně. Finanční náročnost nejvíce ovlivní tři oblasti: obor podnikání, současný stav, ve kterém firma aktuálně zpracovává osobní údaje a množství osobních údajů, které jsou zpracovávány. U nadnárodních a velkých firem lze očekávat náklady až v řádech milionů, u malých a středních podnikatelů, které se nezaobírají práci s osobními daty coby hlavním artiklem, se nebude jednat o více, než pár tisícovek.

Např. firmy, podnikající v IT oborech, které poskytují služby jiným subjektům a pracují s jejich daty, musí očekávat časový i finanční vklad skutečně vysoký. Stejně tak na tom budou firmy podnikající ve finančnictví, callcentru, právnictví či zdravotnictví.

Které položky dělají GDPR tak drahou záležitostí? Je nutné si uvědomit, že při zavádění GDPR do firmy se nejedná pouze o zavedení jedné kolonky v IT systému navíc. Je potřeba provést vnitřní audit aktuální situace zacházení s osobními údaji (a to nejen u kmenových zaměstnanců, ale i u externích pracovníků, brigádníků, dodavatelů, odběratelů, spolupracujících firem atd.), definovat rizika a chyby, provést opatření proti nim, zavést nové procesy, zavést zmiňovanou kolonku do IT systému, proškolit zaměstnance v nových procesech při práci s osobními údaji, periodicky provádět kontroly. Velké firmy navíc zavedou novou pozici – pracovníka, který bude mít na starosti dodržování pravidel – musí se počítat s náklady na jeho mzdu.

Vyplatí se objednat si firmu, která servis zavádění GDPR nabízí? Obecně vzato ano. Jenže pro pragmaticky zaměřeného člověka zde vyvstávají zásadní otázky: Jak poznat, zda jsou tito odborníci skutečně odborníci? A jak mohou být odborníky, když se nemohou prokázat pozitivními referencemi, jako jsou např. kontrolní zápisy bez výhrad (protože žádné kontroly ještě neproběhly)? Stále ještě není zpracován národní předpis – jaké jsou tedy metriky správnosti?

Má cenu se účastnit odborných kurzů na téma GDPR? Ano, jednoznačně ano. I když se na nich dozvíte informace, omezené otázkami z předchozího bodu, lektori vám podají zpravidla všechny dostupné podněty pro pochopení problematiky. Menší firmy díky tomu mohou

provést většinu analýzy sami, taktéž i většinu nastavení nového procesu nakládání s osobními údaji. Navíc téměř na každém z kurzů probíhá diskuze účastníků - a obohacení díky zkušenostem a chybám druhých lidí je často k nezaplacení.

Mohu si provést zavedení GDPR sám? Ano, zejména pokud patříte mezi menší firmy, která se k osobním údajům dostává jen u zaměstnanců a ve smlouvách zákazníků. I zde je však vhodné se poradit s právníkem, zda vaše nastavené procesy neodporují některým právním požadavkům; dále i s firemním ajťákem, který zkontroluje stav osobních dat a jejich zaznamenávání v počítačové podobě.

V novinách jsem četl, že k osobním údajům, které dotyčný firmě poskytne, má mít přístup nejlépe on-line a napřímo. Znamená to, že každý zákazník musí mít přístup do naší zákaznické databáze? Také jsme to četli, článek vyšel na začátku března. Nevěřili jsme vlastním očím, a tak jsme si tento odstavec četli několikrát. Stále doufáme, že se jednalo o nešťastnou formulaci.

Jak dlouho trvá zavedení GDPR? Opět záleží na velikosti firmy a na aktuálním stavu, ve kterém se nacházejí procesy zpracovávání osobních údajů. U střední firmy se dá očekávat časový plán, zahrnující 1-2 měsíce. Urychlit to můžete dobře zpracovaným harmonogramem, vyčleněním pracovníka pouze na tuto záležitost, vyčlenění více osob pro projekt GDPR apod. Nejvíce času zabere analýza aktuálního stavu. Zbytek zpravidla už jen frčí.

Napsal jsem svým zákazníkům, aby mi poslali souhlas se zpracováním jejich údajů. Někteří neodpověděli. Co s tím? Nastává úmorná práce, která spočívá v obvolávání a laskavém vysvětlování, proč tento souhlas potřebujete. Pokud máte v databázi tisíce klientů, držíme vám palce. Na konci vás možná čeká svatozář.

V naší databázi jsou zákazníci, kteří již dávno souhlas dali. My jsem ho ale neuložili. Stačí to? Logicky ano, právně neobstojíte. Zejména pokud se zákazník rozmyslel nebo se u něj změnila osoba, se kterou komunikujete. Navíc často tento souhlas není dostatečný pro GDPR, který je proti původnímu rozšířený. Doporučujeme vytvořit souhlas podle požadavků GDPR a vyžádat si ho ještě jednou. Pokud máte v databázi velký počet zákazníků, platí pro vás totéž, co u

předchozí odpovědi.

Uchováváme osobní údaje o zaměstnancích, kteří u nás kdysi pracovali, tak, jak nám stanoví zákon. Musíme je dohledávat a požadovat od nich souhlas? Zajímavá otázka. Ještě zajímavější je, pokud někdo měl smůlu a mezitím zemřel (a vy stejně musíte uchovávat jeho údaje několik let). Přiznám se, že jsem nikde informace na tuto otázku nenašla. Předpokládáme, že měl pravdu právník, který nám sdělil, že zde se uplatňuje zásada retroaktivity (jednoduše řečeno: co se dělalo podle práva z té doby, není nutno předělávat podle práva současnosti). Ale uvidíme, co se ještě k tomuto tématu objeví.

Co když mi ukrade data zaměstnanec a zneužije je? Tak to máte asi dost velkou smůlu. Za zabezpečení dat zodpovídáte vy jako správce, vaším úkolem je také data opatřit tak, aby se nic takového stát nemohlo. Doporučujeme samozřejmě výslovně tuto skutečnost uvést na pravou míru při školení o nakládání s osobními údaji, ve firemních směrnících, v dodatcích ke smlouvě apod. Budete si moci pak hojit rány na zaměstnanci (zřejmě v té době již bývalém), ale v první řadě za nesprávné nakládání s daty budete postihován vy. V takovém případě je také ihned nutno nepříjemnost hlásit.

Co když dotyčná osoba sice dá souhlas, ale poté ho bude chtít odvolat? Má na to právo. A vy povinnost vyhovět. Pouze v případě, že máte závažné prokazatelné důvody k uchování dat, tak učinit nemusíte. Jenže je stále poněkud nejasné, co jsou ony prokazatelné důvody. Snad se dočkáme co nejdříve upřesnění po zpracování národního předpisu. Laicky si umíme představit, že to může být situace, kdy od vás zákazník odebere zboží, ale abyste ho netrápili fakturami, požádá o vymazání svých údajů. Zde předpokládáme, že existují prokazatelné důvody...

Jsem lékař. Co když mi pacient nebude chtít podepsat souhlas? Přitom bude u mne registrovaný a bude se dožadovat ošetření? Oříšek, hodný odborníků, kteří tady budou po uvedení národního předpisu. Předpokládáme, že tyto „třešničky na dortu“ pořeší Lékařská komora. Z obecných informací, které jsou nyní k dispozici, se zde bude zřejmě využívat „prokazatelných důvodů“ k nevymazání. Pak se naskýtá ještě jedna možnost – požádat pacienta, aby zvolil lékaře, kterému nechá své údaje.

Když jsme u těch pacientů – co když budou chtít vymazat jen některá data? Např. o některých nemocech nebo úrazech, aby získali možnost výhodnějšího pojištění, nebo plnění pojistky? Tato otázka evidentně patří do kategorie ještě nevyřešených. A můžeme doufat, že její řešení nastíní očekávaný vnitrostátní prováděcí zákon, který je však nyní pouze v legislativním procesu. Ale vypadá to, že pokud by lékař poslechl, napomáhal vy trestnému činu, a to by asi moc nechtěl....

Připadá mi, že všechny informace, které jsem doposud načerpal, jsou velmi obecné. A to jsem se účastnil kurzů s touto tematikou, sleduji specializované weby, čtu literaturu a denní tisk, který se tomu věnuje. Hledám informace špatně? Nikoliv. Trpíte tím, co my všichni. Příslušné ministerstvo prozatím nezvládlo nachystat prováděcí zákony, které mají za úkol obecná evropská nařízení upřesnit a objasnit podrobnosti, popř. definovat výjimky.

Jakou mám záruku, že mi někdo informace prostě „nehackne“? Žádnou. Nevýhodou je i známý fakt, že šikovní hackeři jsou vždy o kousek napřed před programy, které mají informace chránit. Určitou útěchou může být naděje, že se u soudu budete ohánět vším, co jste pro bezpečnost údajů udělal, zajistil, zaplatil, koupil a používal.

Na kurzu zdůrazňovali, že pokuty za chybné procesy s GDPR půjdou do miliónu. Jak je velké riziko, že to firmu nepoloží? Doporučujeme optimistický pohled. Málokdo z nás se ocitne v situaci, že si někdo na něj chce „zakleknout“ a zničit jeho podnikání. (I když asi i to se může bohužel stát.) Fakt je, pokuty jsou odstupňovány podle závažnosti případu a obratu firmy, podle tendence problém ututlat nebo naopak spolupracovat atd. Také je dobré si uvědomit, že se očekává, že nejprve přijde výtka, pak nějaké úměrnější sankce – až jako poslední možnost by měla být sankce bolestivá, které se všichni obáváme jako žáčci před písemkou.

Jsem zvyklí zasílat e-mailovou poštou naše nabídky. Musíme k tomu mít také souhlas příjemce? Pokud ano, může to pro mnoho firem znamenat skutečný problém, jak dál dělat obchod. Na druhou větu odpovídáme „ano“, na třetí bohužel také. Myslíme si, že v této oblasti GDPR pro mnoho firem znamená časovou a legislativní pohromu a jediné, co jim může pomoci, je nezištná nepodmíněná vzájemná výpomoc – my vám potvrdíme souhlas, vy nám také. Asi je to způsobeno tím, že podobné zákony vytvářejí úředníci, kteří nemají potuchy o podnikání,

zejména ne o tvrdé dřině, kterou obchod skutečně je.

V novinách, iDnes, jsem četl, že souhlas je nutný i při využívání sociálních sítí. Znamená to, že musím každého, komu kouknu na facebookovou stránku nebo LinkedIn, požádat nejprve o souhlas? Budeme-li ortodoxně stát za tím, co nám říká GDPR, tak to tak může vypadat. Ale vyčkejme si na upřesňující prováděcí zákony a doufejme ve zdravý rozum.

Nemám rád papírování. Přijde se na mne, když budu GDPR ignorovat? No, po pravdě, při větší dávce štěstí a v určitém časovém horizontu ne. Ale je mnohem strategičtější a konstruktivnější přístup je udělat si v tom pořádek a nebát se žádné kontroly, která může přijít. Je to stejné, jako když si má dítě uklidit v pokoji. Chvíli se bouří a cuká se, ale když se k tomu přiměje, tak to najednou jde zcela hladce a navíc je pak na sebe hrdé, protože zjistí, že je i v neoblíbené činnosti šikovné.

Závěrečný příklad místo závěru

Na závěr si zkusme vyřešit nějaký cvičný příklad, abychom se mohli pochválit, jak nám to vlastně dobře jde. Správná řešení, zaslaná do 30. 6. budou slosována (před kamerou) a dvacet výherců bude mít možnost absolvovat zdarma kurz Úvod do koučinku metodou BP Coaching© nebo KASMY© - kreativní, alternativní a samostatné myšlení.

(PS. Před slosováním vás samozřejmě požádáme o svolení, zda můžeme pracovat s vašimi osobními údaji 😊.)

Nejprve zadání:

Představme si situaci, kdy jste výrobní firma, která si pozve lektora na školení obchodních dovedností. Lektor má svoje kontakty uvedené na webu, na kterém se prezentují další zkušení lektoři. Protože jste o lektorovi chtěli zjistit co nejvíce informací, vyhledali jste jeho profil na stránkách Facebook a LinkedIn. Na obou se vám jeho profil líbil, nadchli vás i jeho reference. Lektor vaši objednávku přijal, ale protože je svědomitý, chtěl si alespoň telefonicky popovídat s účastníky kurzu, aby zjistil jejich vstupní úroveň a připravil si cílená cvičení. Získal tedy od vás jejich telefonní čísla a všechny si je obvolal.

Na kurzu vše proběhlo podle zadání, všichni byli spokojeni. Na začátku se zapsali na prezenční listinu, kde zadavatel potřeboval zachytit nejen jméno, příjmení a konkrétní závod, ale také osobní číslo, protože si eviduje u jednotlivých lidí množství a druh školení v rámci Talent managementu. Lektor ještě požádal o připsání e-mailové adresy, protože chce zaslat zájemcům studijní materiály. Poté, co všichni adresy dopsali, lektor si prezenční listinu ofotil do svého mobilu.

Na závěr rozdál lektor formuláře na zpětnou vazbu, na kterých je možné zaznamenat své názory anonymně i jmenovitě. Lektor si formuláře posbíral a poděkoval za ně.

Další týden se sešel se zástupcem zadavatele a probral s ním osobnostní a profesní kompetence jednotlivých účastníků.

Nyní řešení:

Proberte výše uvedený příklad a zaznamenejte:

- Kolikrát měla proběhnout žádost o souhlas?
- Kolikrát udělal chybu z hlediska GDPR zadavatel školení?
- Kolikrát udělal chybu z hlediska GDPR lektor?

Těšíme se na vaše odpovědi a přejeme hodně úspěchu ve vaší práci.

Jaké další publikace jsme pro vás vydali?



Více informací naleznete na naší [www: http://www.bp.cz/cz/o-spolecnosti/nase-publikace](http://www.bp.cz/cz/o-spolecnosti/nase-publikace)

Co dalšího pro vás v Brněnské personalistice děláme?



OBJEDNÁVKY A DISTRIBUCE



Nakladatelství HANDPICKED Publishing

Údolní 11, 602 00 Brno

Tel.: +420 542 213 076

E-mail: obchod@handpicked.cz

www.handpicked.cz