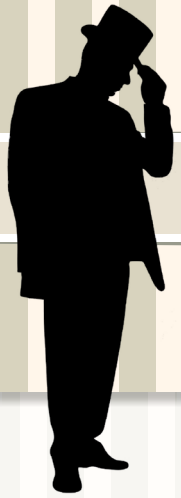
iA
interní auditor
ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 22, ČÍSLO 3–2018 (89) 3|2018

General **D**ata **P**rotection **R**egulation

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

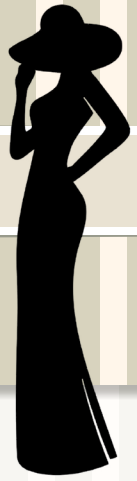
NÁRODNÍ KONFERENCE



23.—24. 10. 2018

NÁVRAT KE KOŘENŮM

PARKHOTEL PLZEŇ



PLZEŇSKÝ KRAJ

Město Plzeň

Konference je realizována pod záštitou hejtmana Plzeňského kraje Bc. Josefa Bernarda a primátora města Plzně Martina Zrzaveckého.
Za podpory náměstka ministra financí PhDr. Tomáše Vyhnánka.

PROGRAM

23. října 2018

8:30–9:30 Registrace

9:30 Zahájení
Tomáš PIVOŇKA, prezident ČIIA
Tomáš VYHNÁNEK, náměstek ministra financí

9:50–10:30 **Hervé GLOAGUEN**, Allianz Group
„Vedení a nastavení globální funkce auditu“

10:30–10:50 Přestávka

10:50–11:15 **David UDAL**, Plzeňský Prazdroj
„Spolupráce managementu a Interního Auditu“

11:15–12:00 **Tomáš PIVOŇKA**, ČEZ
„Méně znamená více. Praktické tipy, jak řídit malý útvar interního auditu ve velké nadnárodní společnosti“

12:00–13:10 Oběd

SEKCE A

13:10–13:50 **Petr BUBENÍK**, Zebra Technologies
„Implementace datové analýzy v interním auditu“

13:50–14:30 **Štěpánka ČERNÁ**, KPMG
„Odhalování podvodů v nákupním procesu“

14:30–14:50 Přestávka

14:50–15:30 **Pavla PAVLÍKOVÁ**, INNERGY
„A jaký byl ten audit?“

SEKCE B

13:10–13:50 **Ivana GÖTTINGEROVÁ**, Statutární město Brno
„Naše cesta za kvalitou anebo jak si zachovovat zdravý rozum“

13:50–14:30 **Ilona DUBOVÁ**, Plzeňský Prazdroj
„Pokrytí rizik a audity v FMCG – případové studie“

14:30–14:50 Přestávka

14:50–15:30 **Markéta HRUBOŇOVÁ a Václav ZYCHÁČEK**, Česká pojišťovna
„Outsourcing z pohledu interního auditu“

17:30 Gala večer „Číše vína“

24. října 2018

8:30–9:00 Registrace

9:00–10:30 PANELOVÁ DISKUSE NA TÉMA
AUDITNÍ SOFTWARE
Martin BUBENÍK, ČEZ
„ECM pro interní audit ve Skupině ČEZ“
Miroslava BUL'UBAŠ MILECOVÁ, UniCredit Bank Hungary
„Audimex“
Lenka MUŠKOVÁ, BOHEMIA ENERGY
„SW řešení auditních složek a monitoring doporučení v IA Bohemia Energy“

10:30–11:00 Finalisté Ceny za inovaci 2018 v interním auditu
(představení tří úspěšných projektů)

11:00–11:20 Přestávka

11:20–12:10 Výsledky mezinárodního průzkumu
Michal ČUP, KPMG
Jitka KAZIMÍROVÁ, Allianz pojišťovna

12:10–12:50 **Michal NULÍČEK**, ROWAN LEGAL
„Skrytá rizika GDPR a témata pro interní audit“

12:50–13:00 Ukončení konference

13:00 Oběd

ZDARMA KONFERENČNÍ AUTOBUS Z PRAHY DO PLZNĚ A ZPĚT

ORGANIZÁTOR

HLAVNÍ PARTNER

PARTNER

SPOLUPRACUJÍCÍ ORGANIZACE

MEDIÁLNÍ PARTNER

Vážené kolegyně a kolegové, čtenáři časopisu Interní auditor,

v čase, kdy dostáváte do rukou toto vydání, již snad pominula tropická vedra, která sužovala nejen Českou republiku, ale prakticky i celou Evropskou unii. Asi podobně jako pominulo „horké období" první poloviny letošního roku „zahřívané větrem" nabývající účinnosti nařízení EU – všem dobře známým nejméně od loňského roku pod zkratkou GDPR. Období finišující reálné změny „ovzduší" ochrany našich osobních údajů. Změny týkající se prakticky všech subjektů a institucí ve veřejné i soukromé sféře, kteří se bez použití údajů nás – fyzických osob – prostě neobejdou. Osob označovaných podle situace jako občané, zákazníci, zaměstnanci, pacienti, klienti, obchodní partneři a mnoha dalšími názvy, typickými pro danou činnost, profesi nebo službu.

Rychlému růstu teplot vyvolaných „změnou ovzduší ochrany osobních údajů" nepochybně přispěla zejména často prezentovaná upozornění na dramatické zvýšení výše finančních sankcí, které lze za porušení Obecného nařízení o ochraně osobních údajů (GDPR v českém vyjádření) uložit. Částky až 20 milionů EUR a u podniků až 4 % celosvětového ročního obratu v případech zejména velkých podnikatelských subjektů jsou v porovnání s dosavadní sankcí nejvýše 20 milionů českých korun podle českého zákona o ochraně osobních údajů jistě podstatným důvodem odpovědného přístupu k řešení ochrany osobních údajů. K růstu „teplot" nepochybně přispěla i skutečnost, že GDPR, jak i z názvu vyplývá, je obecnou právní normou, která postrádá konkrétnější prováděcí předpisy nebo alespoň „návody" jak některá důležitá ustanovení interpretovat a v praktickém životě uplatňovat.

K ochlazování přispěla i veřejná vystoupení nanejvýše povolaných osob, jako eurokomisařky paní Věry Jourové: „GDPR má hlavně dopadnout na firmy, které obchodují s údaji a daty a brutálním způsobem je mohou zneužívat… Tady jsou v panice ale především malé firmy, účetní kanceláře, ambulantní lékaři, obce." A také předsedkyně Úřadu pro ochranu osobních údajů paní Ivany Janů: „My jsme nikdy firmy či obce neničili pokutami. Spíše jsme jim ukládali nápravná opatření, aby se s ochranou osobních údajů naučily pracovat… Sankce proto budeme dávat podle toho, zda ve firmách bude snaha včas oznámit únik dat jak nám, tak poškozeným, aby se eventuální škoda snížila…" Obě vystoupení doplňuje jejich odvolání na dosud platný zákon o ochraně osobních údajů a osmnáctiletou tradici a praxi ochrany osobních údajů v České republice, které jsou z velké části dále využitelné i v podmínkách nové právní úpravy – GDPR.

Tato „ochlazující" vyjádření mohou pomoci ke snížení obecně přehnaných obav z dopadů a důsledků nové, sjednocené evropské legislativy. Jako znalí a zkušení interní auditoři ale víte, že aktuální výši rizika spojenou s případným porušením GDPR dokážete odhadnout až poté, co si „ohledáte" stav své instituce nebo firmy nástroji a postupy interního auditu. Pokud jste se na zavádění GDPR u vás již podíleli, máte jistý náskok proti těm, které tato „výzva" čeká.

V každém případě vám přeji „nohy na zemi a zdravý – chladný rozum", neboť pro nikoho z nás GDPR neskončilo nabytím účinnosti 25. května 2018, ba právě naopak. Alespoň pro některé zůstane v zóně priorit i další roky…

JUDr. Vladimír Valenta
past prezident a člen Čestného prezidia
Českého institu interních auditorů

OBSAH / CONTENTS

90% míra zjištěných nedostatků v auditech GDPR před námi – a co znamená? 4
Vladimír Valenta

Minimum ochrany osobních údajů pro auditory 9
Soňa Matochová

Proč si chránit osobní údaje, proč vznikl Úřad pro ochranu osobních údajů, proč vzniklo GDPR? 13
Vladimír Konečný

Interní audit již nebude sedět v koutě 17
Ján Bača

Noví členové 21

GDPR v praxi: bezzubý strašák, nebo téma pro interní audit? 22
Michal Nulíček

Chráníte osobní údaje standardně, nebo záměrně? 26
Rodan Svoboda

Jak přinášet přidanou hodnotu v ochraně osobních údajů 31
Stanislav Klika

GDPR, příležitost se nebát! 36
Zdeňka Jarošová

Kolíkování nepřehledného terénu 40
Václav Peřich

Setkání interních auditorů a kontrolorů moravských měst 42
Libuše Habartová

Čeho si Petr povšiml nejen v legislativě 43
Petr Kheil

Nač je třeba mladých íáčků aneb dnešní dávka filozofie 44
Lucie Vašková

Změny v certifikacích IIA 46
Tomáš Pivoňka, Petr Hadrava

4 Vladimír Valenta – Expecting a 90% rate of deficiencies identified in the GDPR audits – what does it mean?

9 Soňa Matochová – The minimum of personal data protection for auditors

13 Vladimír Konečný – Why shall one protect personal data, why was the Office for Personal Data Protection established, why was the GDPR created?

17 Ján Bača – Internal Audit will not sit in the corner anymore

22 Michal Nulíček – GDPR on practice: empty threat or a theme for internal audit?

26 Rodan Svoboda – Do you protect personal data by default or by design?

31 Stanislav Klika – How an added value could be generated in personal data protection?

36 Zdeňka Jarošová – GDPR: on opportunity not to be afraid!

40 Václav Peřich – Mapping a chaotic terrain

44 Lucie Vašková – Why we need the young internal auditors, or today's dose of philosophy

ROČNÍK 22, ČÍSLO 3–2018 (89)

3|2018

Vydává
Český institut interních auditorů, z.s.
Karlovo nám. 3
120 00 Praha 2
tel.: +420 224 920 332
+420 224 919 361
e-mail: casopis@interniaudit.cz
www.interniaudit.cz

Redakce INTERNÍ AUDITOR
Karlovo nám. 3
120 00 Praha 2
Registrace: MK-ČR-E-12322
ISSN 1213-8274

Vydavatel nenese odpovědnost za údaje a názory autorů jednotlivých článků.

Redakční rada:
Vedoucí – Jan Kovalčík, Petr Hadrava, Daniel Häusler, Ludmila Jiráňová, Andrea Lukasíková, Šárka Nováková, Petra Škvorová, Eva Štěpánková, Lucie Veselá, Milena Widomská, Kateřina Zonygová

Foto: archiv ČIIA, fotobanka 123RF
Obálka: 123RF(eobrazy)
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1500 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

iA interní auditor

90% míra zjištěných nedostatků v auditech GDPR před námi – a co znamená?

Dvacátý pátý květen 2018 je minulostí. Obecné nařízení o ochraně osobních údajů EU (GDPR) nabylo účinnosti. Jsou evidovány první případy zahájených vyšetřování společností pro porušování GDPR a oznámena podání stížností na toto porušování i tak známými a úspěšnými společnostmi, jako jsou Facebook nebo Google. A svět se točí dál.

JUDr. Vladimír Valenta,
je absolventem právnické fakulty UK v Praze. Od roku 1993 byl ředitelem odboru interního auditu v Agrobance Praha. Od roku 1998 působil v útvaru compliance GE Capital Bank (později GE Money Bank), a od roku 2005 jako senior compliance manažer i pro skupinu GE Money ČR. Současně od roku 2010 zastával roli Privacy Leader v této skupině. Od roku 2015 pracuje v útvaru corporate compliance ČEZ, a.s., s působností pro Skupinu ČEZ, nejprve jako compliance expert a od roku 2017 jako compliance manažer. Od téhož roku byl také členem Hlavního týmu Programu implementace GDPR Skupiny ČEZ.
Je členem ČIIA od ustavujícího sněmu v roce 1995. Do roku1997 byl členem Kontrolní komise ČIIA a v letech 1997–1998 působil jako prezident ČIIA. Od roku 1999 je aktivním členem čestného prezidia ČIIA. V letech 2005–2015 se rovněž aktivně podílel na činnosti Komise pro bankovní regulaci ČBA jako její člen. V roce 2016 spolupracoval na vzniku České Compliance Asociace (ČCA) a je činný v organizačním týmu. Je také členem Unie podnikových právníků ČR, kde od roku 2017 působí jako vedoucí Sekce Compliance. V průběhu své odborné praxe vystupoval mnohokrát jako lektor na odborných školeních nebo seminářích s příspěvky zaměřenými na aktuální témata IA a compliance.

Koncem června 2018 webové stránky Corporate Compliance Insights publikovaly článek s titulkem, který jsem si dovolil vypůjčit. Jeho autorem je Terry Ray, Chief Technology Officer americké společnosti Imperva, odpovědný za rozvoj této společnosti a formulování jejích technických vizí a strategie. Tato i předchozí pozice prohloubily jeho zkušenosti získané z konzultací poskytovaných globálním společnostem mimo jiné v oblastech implementace ochrany dat a odvětvových regulací. Terry je navíc pravidelným vystupujícím na akcích celosvětových organizací, zabývajících se podnikovým poradenstvím nebo bezpečností a ochranou dat, jako jsou Gartner, RSA, ISSA, ISACA a dalších. Nejen „šokující“ znění titulku, ale i názory, úvahy a argumenty autora, někdy odlišné od mých, mne přivedly k tomu, abych vám ty podstatné z nich přiblížil. Tím spíše, že velká část z nich vystihuje i mé názory a úvahy. Koneckonců i pohled podložený zkušenostmi z mimoevropského prostředí na úskalí GDPR má přinejmenším inspirativní hodnotu, i když se s ním v jednotlivostech nemusíme

„V devíti z každých deseti velkých organizací se nepodaří při prvním auditu shody s GDPR dosáhnout dobrého výsledku.“

ztotožnit. Autorovi článku se omlouvám, pokud volným přepisem jeho názorů a myšlenek v textu uvedených došlo k jejich zkreslení. Nebylo to záměrné.

GDPR je hodnoceno jako řešení slibující, že bude nejdosažitelnějším a nejkomplexnějším regulačním systémem ochrany dat, jaký svět zná, a to z následujících důvodů:

- GDPR klade extrémně přísné požadavky na bezpečnost a soukromí v organizacích, které přicházejí do styku s osobními údaji – bez ohledu na to, zda k tomu používají třetí strany jako zpracovatele.
- GDPR umožňuje za porušení uložit extrémně vysoké maximální pokuty – v některých případech, až do výše 20 milionů EUR nebo 4 % ročního výnosu porušitele (podle toho, co je vyšší).
- Pokud jde o osobní data lidí v EU, v podstatě GDPR představuje globální právo, de facto šíření datové paranoi EU téměř po celém světě.

Ačkoliv sankce za porušování GDPR mohou být zhoubné a dodržování předpisů je nezbytné, Terry Ray zastává názor, že většina společností může zůstat v klidu. I přesto, že mnoho vrcholových manažerů a správců IT se obává oprávněně, že jejich organizace nedodržují požadavky GDPR. A tuto jejich obavu podporuje svým odhadem, podloženým praktickými zkušenostmi, že v devíti z každých 10 velkých organizací se nepodaří při prvním auditu shody s GDPR dosáhnout dobrého výsledku. Doplněným úvahou, že u mnohých nebudou ani jejich další následné audity shody GDPR úspěšné.

„Dvacátý pátý květen 2018 je minulostí.“

Stejně jako považuje za pravdivé předchozí přiznání obav, považuje za pravdivé i konstatování aktuální neschopnosti mnoha společností z velké části světa držet krok s nejpřísnějšími výklady GDPR, na což některé americké společnosti reagovaly blokováním přístupu návštěvníků z EU na své webové stránky. A odhaduje, že na základě poznání této aktuální situace i příslušné orgány ochrany osobních údajů členských států EU budou svoji pravomoc uplatňovat výběrově a stupňovaně. Předvídá, že menším porušitelům a za méně významná porušení požadavků GDPR hrozí spíše varovné dopisy nebo menší pokuty a svoji pozornost a také pravomoc v podobě vyšších sankcí regulátoři zaměří na největší, nejvíce nedbalé organizace, organizace mající díky shodě okolností „nejméně“ štěstí a také ty nejvíce „politicky“ nepopulární.

Předbíhání GDPR

Pro první roky účinnosti GDPR proto doporučuje organizacím využít strategie „předbíhání“ (myšleno jiné organizace v oboru nebo odvětví) v podobě

úrovně dosažené shody s požadavky GDPR. Spolehlivost této strategie staví na třech podmínkách. Za prvé, že se organizace nebude opakovaně dopouštět stejného porušení GDPR, za druhé, že nebude vykazovat zásadní nedbalost v přístupu k implementaci GDPR. A nakonec za třetí, že v organizaci nedojde k úniku dat.

„Správci IT často tráví spoustu času zaměřením na to, co vědí, bez dostatečné starosti o to, o čem nevědí.“

K zajištění účinnosti nejen strategie „předbíhání“ ale i systému ochrany dat připomíná základní přístupy „datové hygieny“, definované v GDPR. A pojmenované jako úkol organizace: tedy vědět, jaké GDPR relevantní údaje má a kde, klasifikovat je, sledovat je a chránit. Ale současně připouští, že ve velkých a středních podnicích jsou tyto základy „datové hygieny“ naplňovány nedostatečně. Demonstruje současný stav v praxi na tomto příkladu. Jakákoliv organizace má znalost o uložení osobních údajů a řízení přístupu k nim na 10 % svých serverů a je schopna předložit o tom odpovídající dokumentaci. S touto úrovní by se aktuálně umístila na špici těch pokročilých.

Pokud ale přijde auditor dbalý své profese, nezbývá mu než konstatovat, že pro potvrzení shody je nezbytné dokumentovat znalost dat i pro zbývajících 90 % serverů.

„Příslušné orgány ochrany osobních údajů členských států EU budou svoji pravomoc uplatňovat výběrově a stupňovaně.“

Obecná ochrana údajů znamená ochranu souhrnů dat

Praktické zkušenosti z ochrany údajů podle Terryho Raye prokazují, že citlivá data si najdou způsob, jak se dostat na místa, kam by neměla. Správci IT podle něho často tráví spoustu času zaměřením na to, co vědí, bez dostatečné starosti o to, o čem nevědí. Došlo k příliš mnoha významným únikům dat v případech, kdy se útočníci dostali na místa, o kterých dané organizace nevěděly, že zde mají citlivá data – a v důsledku toho nevyužily odpovídající prostředky jejich zabezpečení, jako je promíchání dat nebo jiné techniky úpravy dat, snižující riziko porušení jejich ochrany.

Úroveň ochrany dat nelze jednoduše posuzovat na základě tisíce stránek základních dotazů do databáze. Takový přístup k analýze stavu ochrany je v praxi fyzicky nezvladatelný. I auditoři potřebují konkrétnější, cílená a souhrnná data, označující kdo přistupoval k jaké složce na serveru nebo do které databáze a kdy, a k čemu přesně.

Ve zdůrazňování nezbytnosti ochrany osobních údajů ze strany GDPR, zejména v prostředí IT systémů, vidí Terry Ray hlavní poučení pro oblast zajištění kybernetické bezpečnosti. Postrádá však více praktických příkladů a osvědčených postupů v oblasti „datové hygieny“, jejichž využití by regulátoři podporovali konkrétněji, v jejich dokumentech a doporučeních.

Obecná ochrana údajů a její „bílý pes“ (odpoutání pozornosti od podstatného)

V závěru svého článku autor porovnává GDPR s jinými podrobnými nebo obecnějšími předpisy zaměřenými na ochranu dat, aby formuloval nejzásadnější aspekt každé jednotlivé regulace ochrany dat, i když je aktuálně tou nejodkazovanější právě GDPR. A tímto aspektem je: **Potřebujete vědět, kdo přistupuje k jaké konkrétní informaci kdy, kde a jak (a jak často).**

Primární část o GDPR – která vede organizace k panikaření – je, že jde o šíři dat, které se reálně dotýkají mnoha oddělení, bez ohledu na odvětví nebo propojení. Tím se vytváří dva rébusy pro rádoby GDPR shodu organizace:

1) Jak zajistíme audit všech svých dat a přístupů k nim? Je to proveditelné?

2) Jestliže není možné auditovat všechna svá data a přístup k nim, jak můžeme data konsolidovat tak, že to bude kontrolovatelné?

Často jediný způsob k řešení těchto otázek je přes podrobný proces identifikace toho, kdo potřebuje GDPR relevantní data a dále jak centralizovat data odpovídajícím způsobem.

Co by ale organizace měly dělat především, když většině chybí něco, jako je dobrá hygiena ochrany dat? Poukazuje na nedávnou studii společnosti Ponemon Institute, která uvedla, že v 76 % dotazovaných globálních organizací chybí formální a důsledně aplikovaný plán řešení incidentů kybernetické bezpečnosti.

A nakonec autor opakuje svůj úvodní názor na schopnost organizací přečkat bouři GDPR několik dalších let, dokud se:

1) obecně budou snažit odvádět skutečně dobrou práci na dodržování GDPR,

2) začnou svoji cestu vhodným sledováním a klasifikací všech jejich dat a

3) budou monitorovat a kontrolovat veškerý přístup k osobním údajům tak, aby otázky auditora mohly být zodpovězeny, a v případech úniku dat byly snadno dostupné informace o řešení bezpečnostních incidentů. A to vše budou konat tak, že se dokáží zařadit z pohledu regulátora do skupiny pokročilých organizací i v dlouhodobém horizontu. (Tolik myšlenky a názory Terryho Raye).

IMPLEMENTACE GDPR DO ČINNOSTI ORGANIZACÍ Z POHLEDU ČESKÉ REPUBLIKY

Po překonání prvních emocí, vyvolaných především panikou (možná živenou i záměrně), stimulovanou obecností právních formulací, doprovázených interpretační nejistotou, protože netlumenou včas vydávanými upřesňujícími „vodítky“ (nyní Pokyny Evropského sboru pro ochranu osobních údajů), a udržovanou stále ještě chybějícím českým zákonem o zpracování osobních údajů, konkretizujícím některá ustanovení GDPR pro území České republiky, lze s odstupem času a potřebným nadhledem shrnout aktuální stav věci následně.

GDPR nepřináší žádné převratné povinnosti v porovnání s dosavadní právní úpravou, ani pro podnikatelskou sféru, ani pro státní nebo samosprávné instituce, a stejně tak pro neziskové organizace nebo jiné subjekty. Při větším detailu se mnou někteří kolegové, zejména právníci, nebudou možná souhlasit s poukazem na řadu novinek, jako je pověřenec pro ochranu osobních údajů, taxativní výčet práv subjektu údajů a tomu korespondující povinnosti správce údajů k jejich zajištění, povinnost správce údajů ohlašovat Úřadu pro ochranu osobních údajů případy porušení zabezpečení osobních údajů a dalších.

Dopad implementace požadavků GDPR v podnikatelské sféře oproti ostatním skupinám povinných subjektů je částečně odlišný v tom směru, že značná část podnikatelských subjektů předcházející požadavky vyplývající ze zákona o ochraně osobních údajů buď přehlížela, což vedlo i k neplnění povinnosti registrace u Úřadu pro ochranu osobních údajů, nebo řešila především viditelné části povinností typu získávání souhlasů se zpracováním osobních údajů, a prakticky ignorovala povinnost uloženou dosud stále platným zákonem o ochraně osobních údajů (ustanovením §13 odst. 2), zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy. A to nejen formou obecného dokumentu, uloženého ve složce kdesi v šanonu povinných dokumentů společnosti, bez faktického přenosu a vlivu na vlastní postupy a procesy zpracování a zajištění ochrany osobních údajů. Situace ve státních institucích je v tomto směru lepší přinejmenším díky „zvykům“ a praxi uchovávané ve vnitřních předpisech, které podporovaly odpovědný přístup k ochraně osobních údajů. A nepochybně ještě lepší v oborech, jako jsou lékaři, advokáti nebo bankéři s mnohaletou, zákony podporovanou, profesní povinností mlčenlivosti.

„GDPR nepřináší žádné převratné povinnosti v porovnání s dosavadní právní úpravou.“

Ze své předchozí i současné praxe a zkušeností mohu potvrdit, že na území ČR působí řada společností, pro které už dosavadní právní úprava vyplývající ze zákona o ochraně osobních údajů nebyla jen „slaměným strašákem“, kterého není třeba se bát, ale přistupovaly k naplnění jeho požadavků stejně odpovědně a důsledně jako k jiným klíčovým právním povinnostem. A pro takové společnosti je zavedení odlišností, které GDPR proti dosavadní právní úpravě přináší, snadněji splnitelným úkolem než pro jiné společnosti, které si „své domácí úkoly splnily jen na dostatečnou“ a zlepšení alespoň na „dobrou“ pro ně představuje nejen potřebu většího úsilí (finančních zdrojů a lidských kapacit), ale i času k překonání existující mezery pod hrozbou „Damoklova meče“ v podobě možné sankce podle GDPR.

ZÁVĚREM

Pro srovnání s úvahami a názory Terryho Raye a současně jako závěr mého příspěvku si dovolím ocitovat dvě vyjádření, ve zkrácené podobě použitá v úvodníku Interního auditora.

„GDPR má hlavně dopadnout na firmy, které obchodují s údaji a daty a brutálním způsobem je mohou zneužívat. GDPR je legislativa, která byla nutná, aby se zabránilo zneužívání dat v moderním světě, což by mělo nedozírné následky. Týká se především firem nad 250 zaměstnanců. Tady jsou v panice ale především malé firmy, účetní kanceláře, ambulantní lékaři, obce.“ (Mgr. et Mgr. Věra Jourová, komisařka EU).

„My jsme nikdy firmy či obce neničili pokutami. Spíše jsme jim ukládali nápravná opatření, aby se s ochranou osobních údajů naučily pracovat. Sankce proto budeme dávat podle toho, zda ve firmách bude snaha včas oznámit únik dat jak nám, tak poškozeným, aby se eventuální škoda snížila. Budeme se dívat na to, zda se společnost snažila takovému incidentu zabránit dostatečným zabezpečením. Pokud ale žádné zabezpečení neměla, tak je pak těžké pokutu neudělit. GDPR nově stanovuje, že sankce mají být pro ostatní výstrahou.“ (JUDr. Ivana Janů, předsedkyně Úřadu pro ochranu osobních údajů).

„GDPR má hlavně dopadnout na firmy, které obchodují s údaji a daty.“

K tomu není téměř co dodat. Snad jen popřát, ať se vašim organizacím podaří „předběhnout“ jiné s vámi srovnávané při dokončování změn, nezbytných k dosažení optimální shody zpracování osobních údajů a úrovně zajištění jejich ochrany s požadavky GDPR. A vám – interním auditorům, potvrdit, že dokážete své organizaci významně pomoci také se správným určením míry rizika a závažnosti dopadů aktuálních neshod s požadavky GDPR. A rovněž se stanovením optimální posloupnosti zavádění nápravných opatření a případným výběrem z variant změn procesů nebo technologických řešení. Konec konců, není nezbytné pořizovat „mercedesku“, když stejně spolehlivě a vytrvale může posloužit i „škodovka“! ■

Minimum ochrany osobních údajů pro auditory

„Rozlišení role pověřence a interního auditora a jejich vzájemný vztah je zásadní otázkou, kterou musí správce (zpracovatel) ve své plné a výlučné kompetenci řešit. Tento článek poskytuje přehled nejčastějších problémů a upozorňuje na kritéria, k nimž je nutno při zřízení role pověřence, vedle často již v organizaci existující funkce auditora, přihlédnout. Současně upozorňuje na některé nevhodné zjednodušující přístupy k funkci pověřence, které mohou vést ke znehodnocení mechanizmů ochrany osobních údajů v organizaci, neboť klíčovou osobou a garantem opatření ochrany údajů pro správce musí být v prvé řadě vlastní pověřenec.“

JUDr. Soňa Matochová, Ph.D.
vedoucí oddělení analytického
Úřad pro ochranu osobních údajů

Již v průběhu přípravy na účinnost obecného nařízení o ochraně osobních údajů[1] se začalo spontánně objevovat srovnávání funkce auditora a pověřence pro ochranu osobních údajů, případně interního auditu a auditu ochrany osobních údajů. Názory na tato témata nebyly jednotné a teprve v průběhu času začala být problematika chápána v hlubších souvislostech. Do jisté míry kontroverzním tématem se stala především slučitelnost funkce auditora a pověřence, přičemž praxe za situace neustálenosti autoritativního názoru směřovala k nastavování ad hoc řešení podle konkrétních podmínek. Zároveň bylo zřejmé, že existuje větší počet otázek týkajících se vzájemného vztahu ochrany osobních údajů a auditu. Lze uvést jejich příklady:

- Existují nějaké společné rysy ochrany osobních údajů a auditu (interního auditu)? Případně jaké jsou rozdíly mezi těmito oblastmi?
- Jakou roli by měli hrát auditoři (interní auditoři) při zajišťování souladu s ochranou osobních údajů?
- Do jaké míry je potřebné, aby se auditoři orientovali v problematice ochrany osobních údajů?
- Může interní auditor vykonávat funkci pověřence ochrany osobních údajů?
- Jaká je role Úřadu pro ochranu osobních údajů, ústředních orgánů státní správy a profesních komor auditorů při hledání odpovědí na otázky vztahu interního auditu a ochrany osobních údajů?

Při odpovědi na vznesené otázky je potřebné vyjít z širších východisek platných pro oblast ochrany osobních údajů a audit obecně. Úvodem

1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

je třeba říct, že právě ono hledání správných odpovědi je v logice obecného nařízení, které velmi často nenabízí jednu předem danou správnou odpověď, ale spíše předpokládá systematický přístup vycházející z relevantní právní úpravy, shromáždění rozhodných skutečností a argumentů pro posouzení a poté nalezení nejvhodnějšího řešení. V každém případě je při posuzování nastolených otázek nutné vyjít z účelu, systematiky, institutů a principů právní úpravy ochrany osobních údajů na jedné straně, a z účelu, úkolů a metodik auditu či interního auditu na druhé straně.

Je vhodné začít tím, že ochrana osobních údajů upravená obecným nařízením představuje zásadní komplexní právní úpravu, jejímž účelem je zajištění ochrany osobních údajů v dané oblasti, sektoru či organizaci prostřednictvím aplikace a implementace institutů a principů obecného nařízení. Naopak audit (z lat. *auditus*, slyšení) obecně znamená úřední přezkoumání a zhodnocení dokumentů, zejména účtů, nezávislou osobou. Účelem je zjistit, zda doklady podávají platné a spolehlivé informace, a zhodnotit kvalitu vnitřní kontroly firmy. Obvykle se audit zabývá jen vzorky a jeho výsledek neznamená naprostou jistotu, nýbrž jen rozumnou pravděpodobnost konečného hodnocení. Pokud jde o interní audit ve smyslu zákona o finanční kontrole,[2] je definován jako nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesů v organizaci. Pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení správy organizace.

Z výše uvedeného je zřejmé, že audit a ochrana osobních údajů představují dvě rozdílné oblasti, které vyžadují ke svému zvládnutí odborníky se zcela rozdílnou kvalifikací a předpoklady. V obou případech se přitom jedná o vysoce specializované odbornosti. I když v současné době neexistuje dostatek odborníků zabývajících se ochranou osobních údajů, jde pouze o přechodnou situaci, jejímž řešením by jistě nebylo svěřit ochranu osobních údajů auditorům. To však nic nemění na tom, že existují i přirozené průniky obou oblastí. U činností souvisejících s prováděním auditu musí být vždy vyřešeny i dílčí otázky ochrany osobních údajů, zatímco vynaložené náklady na ochranu osobních údajů se nevyhnou posouzení auditorem, pokud jde o jejich hospodárné vynakládání. Také sofistikované a rozpracované metody a poznatky interního auditu, které využívají systémové a analytické přístupy a metody, je jistě možné v obecné rovině využít i při auditu osobních údajů.

V kontextu vztahu interního auditu a ochrany osobních údajů bývá často poukazováno na podobnost mezi pověřencem pro ochranu osobních údajů a auditorem. Domnívám se, že tuto podobnost lze spatřovat především v tom, že obě funkce vyžadují vysokou specializovanou odbornou kvalifikaci, nadto v rámci širšího vědomostního základu (zpravidla právnické nebo ekonomické vzdělání). Ovšem zatímco pověřenec pro ochranu osobních údajů musí znát právní úpravu a praxi ochrany osobních údajů a souvisejících oblastí, náležitě se orientovat v IT odbornosti a kybernetické bezpečnosti, interní auditor je odborníkem v jiných oblastech, zaměřuje se i na velmi specifické otázky, což např. ve veřejné správě verifikuje služební zkouška. U obou odborností je společná také nezbytnost stálého odborného růstu, kontinuálního vzdělávání a samostudia. Je přitom v zájmu organizace (statutárního orgánu), aby pro výkon obou funkcí našel ty nejlepší odborníky, protože jen tak zajistí soulad s požadavky interního auditu nebo ochrany osobních údajů. Výslovně je třeba také zdůraznit etické či morální předpoklady pro výkon obou profesí,

„V kontextu vztahu interního auditu a ochrany osobních údajů bývá často poukazováno na podobnost mezi pověřencem pro ochranu osobních údajů a auditorem.“

„Auditor i pověřenec tedy mají své místo v organizaci a předpokládá se jejich spolupráce a sdílení know-how.“

© 123RF.com [Peter Kslnan]

2 Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

osobnostní integritu a spolehlivost. Je zřejmé, že rozdílné úkoly vyžadují nejen rozdílné profesní předpoklady, ale i rozdílný způsob myšlení, přístupů k řešení problémů, a dokonce rozdílné osobní vlastnosti. Zatímco interní auditor pracuje víceméně samostatně, případně v rámci útvaru vnitřního auditu, a výsledky své práce odevzdává vedoucímu organizace, u pověřence budou velmi důležité jeho komunikační a negociační schopnosti, včetně schopnosti srozumitelně vysvětlit otázky ochrany osobních údajů ostatním pracovníkům či tazatelům (subjektům údajů), případně přesvědčit vedení organizace o potřebě realizovat vhodné postupy k ochraně osobních údajů. V zásadě lze říct, že problematika ochrany osobních údajů je širší, dotýká se více právních oblastí a není oddělitelná od otázek prosazování základních práv, včetně aplikace principu proporcionality. Navíc, protože jde o problematiku novou a v řadě aspektů dosud výkladově neustálenou, vyžaduje zvýšené úsilí a nasazení zejména v počátečním období účinnosti obecného nařízení.

K otázce, zda může být interní auditor zároveň pověřencem, se v nedávné době vyjádřilo také stanovisko ministerstva financí. Z tohoto stanoviska[3] vyplývá, že interní auditor podle zákona o finanční kontrole[4] nemůže být jmenován pověřencem pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů. Naopak pověřenec nemůže být organizačně začleněn do útvaru interního auditu nebo podřízen vedoucímu útvaru interního auditu nebo internímu auditorovi. V odůvodnění se uvádí, že aby interní audit mohl plnit své úkoly v souladu s požadavky zákona o finanční kontrole, musí být funkčně nezávislý a organizačně oddělen od řídicích výkonných struktur[5]. Stanovisko shrnuje, že i když na první pohled může vymezení úkolů pověřence evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze je zaměňovat. S tímto závěrem ministerstva financí lze souhlasit.

Zajímavou otázkou je podrobnější srovnání nezávislosti pověřence a auditora. V obou případech je nezávislost definována přímo právní úpravou, avšak s použitím mírně odlišných slovních formulací. Nezávislost interního auditora je definována jako funkční a organizační, což spočívá v tom, že je přímo podřízen vedoucímu orgánu veřejné správy a je oddělen od řídicích výkonných struktur. Dále je stanoveno, že útvar interního auditu nelze pověřovat úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.[6] U pověřence je nezávislost formulována obecněji,[7] a to tak, že nedostává žádné pokyny týkající se jeho úkolů a je přímo podřízen vrcholovým řídicím pracovníkům správce nebo zpracovatele. Za specifické a ojedinělé je v rámci našeho právního řádu třeba považovat ustanovení, podle něhož pověřenec nemůže být propuštěn ani sankcionován v souvislosti s plněním svých úkolů. Účelem tohoto přímo účinného ustanovení obecného nařízení je preventivně chránit pověřence, aby se nemohl stát předmětem postihu např. v situacích, kdy by navrhoval a prosazoval opatření směřující k vyššímu standardu ochrany osobních údajů, se kterými by vedení organizace nesouhlasilo.

Nicméně za důležitější než výše citované odlišné slovní znění obou ustanovení vztahujících se k nezávislosti interního auditora a pověřence je třeba považovat účel činnosti, ke kterému je nezávislost vztažena. Úkolem pověřence je zajištění vysoké úrovně ochrany fyzických osob a odstranění překážek bránících volnému pohybu osobních údajů, zatímco interní audit sleduje cíle v oblasti odpovědnosti za řízení a kontrolu veřejných financí. Z praktického hlediska je tedy zřejmé, že interní auditor je víceméně součástí kontrolních mechanizmů v oblasti ekonomiky organizace, zatímco pověřenec pracuje primárně s osobními údaji a navrhuje vhodné postupy při jejich ochraně. Znamená to, že jak nezávislost pověřence, tak auditora je v jim svěřených oblastech samostatná. Musí tedy vždy navrhovat opatření podle toho, za jakou činnost jsou odpovědni, což bude prakticky znamenat odlišné návrhy postupů v odlišných oblastech.

K činnosti pověřence lze ještě dodat, že se předpokládá, že kolem sebe vytvoří neformální tým osob, které ve své činnosti v rámci organizaci zajišťují některé aspekty ochrany osobních údajů. Takový tým lze považovat za nanejvýš vhodnou platformu ke sdílení zkušeností v oblasti ochrany osobních údajů a formulování projektů, návrhů a doporučení, které povedou k následnému vytváření nové kultury ochrany osobních dat v organizaci. To vlastně také bylo smyslem zavedení institutu pověřence do právní úpravy obecného nařízení.

3 https://www.mfcr.cz/cs/legislativa/metodiky/2018/stanovisko-ministerstva-financi-k-proble-31614
4 Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).
5 Ustanovení § 29 odst. 1 zákona o finanční kontrole.
6 Ustanovení § 29 odst. 4 zákona o finanční kontrole.
7 Čl. 38 odst. 3 obecného nařízení.

Auditor i pověřenec tedy mají své místo v organizaci a předpokládá se jejich spolupráce a sdílení know-how. Sloučení obou činností nebude přicházet v úvahu již proto, že auditor a pověřenec jsou odborníky „na něco jiného," a není tedy ani vhodné. Nejde však o dogma a vždy je třeba posoudit konkrétní situaci. Je třeba rozlišovat činnost interního auditora podle zákona o finanční kontrole a auditora, jehož postavení není upraveno tímto způsobem. Nadto je okruh interních auditorů podle zákona o finanční kontrole omezen jen na určený okruh subjektů ve veřejné správě, zatímco pověřence musí mít všechny veřejné subjekty. Pokud se tedy praxe v počátečním období účinnosti obecného nařízení snažila nalézt ekonomicky úsporná řešení ve spojení obou odpovědností u jedné osoby, je to třeba považovat za přechodné řešení. Navíc obecné řešení umožňuje pružná řešení, pokud jde o pověřence, takže správci (zpracovateli) nic nebrání, aby pověřence zaměstnával na částečný úvazek nebo externě.

„U obou odborností je společná také nezbytnost stálého odborného růstu, kontinuálního vzdělávání a samostudia."

Závěrem je na místě učinit zmínku o roli státních orgánů a profesních komor v procesu implementace obecného nařízení. Zatímco, ve shodě s kompetenčním zákonem, ústřední orgány státní správy mají své místo při metodickém vedení subjektů v jim svěřených oblastech, kam patří i právně nezávazná doporučení vhodných postupů v oblasti ochrany osobních údajů, Úřad pro ochranu osobních údajů je nezávislým dozorovým úřadem, který se v rámci své působnosti podílí na vzdělávání a poskytuje obecné konzultace v oblasti ochrany osobních údajů, nikoliv však konkrétní návody k postupu dotčených subjektů. V tomto ohledu je třeba zdůraznit plnou odpovědnost správce (zpracovatele), který jediný zná veškeré konkrétní okolnosti a požadavky týkající se jeho činnosti, a podle nich musí nastavit pravidla ochrany osobních údajů. Výslovně je také v kontextu otázek řešených v tomto článku zdůraznit významnou a dosud plně v praxi neuchopenou roli profesních komor při výkladu otázek ochrany osobních údajů nastolených obecným nařízením v oblasti jejich zájmu.

Výše uvedená vysvětlení týkající se otázek ochrany osobních údajů a auditu (interního auditu) umožňují učinit následující závěry:

- Zatímco praxe ochrany osobních údajů představuje implementaci principů ochrany osobních údajů, jejímž cílem je dosáhnout náležité ochrany soukromí a osobních údajů, audit obecně je především činností metodickou, která směřuje k optimálnímu nastavení procesů v organizaci.
- Jak ochrana osobních údajů, tak interní audit, představují vysoce odborné činnosti předpokládající, že je budou vykonávat specializovaní odborníci, kteří se budou průběžně vzdělávat a zvyšovat svou kvalifikaci.
- Jak pro funkci pověřence, tak auditora je podstatné, aby splňovali morální a etické předpoklady vážící se k jejich činnosti.
- U obou funkcí jsou samostatně formulovány požadavky na nezávislost, kterou je nezbytné vnímat především v rámci účelů jim svěřených odlišných činností.
- Střet zájmů musí být vždy posuzován v konkrétním případě vzhledem k okolnostem a celkovému nastavení činností správce (zpracovatele) prostřednictvím právní úpravy i interních předpisů.
- Lze souhlasit se stanoviskem ministerstva financí, které dospělo k závěru, že i když na první pohled může vymezení úkolů pověřence evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze obě činnosti zaměňovat.
- V praxi se předpokládá spolupráce obou profesí, takže interní auditor by měl být součástí širšího zázemí ochrany dat v organizaci a přispívat ke zvyšování kultury zacházení s osobními údaji.
- V každém případě je konkrétní řešení otázek ochrany osobních údajů vždy plně a výlučně odpovědností správce (zpracovatele).

Proč si chránit osobní údaje, proč vznikl Úřad pro ochranu osobních údajů, proč vzniklo GDPR?

Technologický pokrok v oblasti informačních a komunikačních technologií přináší neustálé zdokonalování, rozvíjení. Osobní údaje se zpracovávají stále rozsáhleji za využití metod jako profilování či automatizované zpracování osobních údajů. Přitom je nutné si uvědomit, že právo na soukromí je jedním ze základních lidských práv, že Listinou základních práv a svobod je zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více podrobováno zkouškám. Aféra zneužití milionů osobních dat fyzických osob na internetových stránkách jedné ze sociálních sítí je příkladem, že bychom ochranu osobních údajů neměli podceňovat. A že nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů), kterým se ruší směrnice 95/46/ES (dále „GDPR“) – přichází v pravou chvíli a že jeho cílem je posílit ochranu dat občanů.

Ing. Vladimír Konečný
interní auditor
Úřad pro ochranu osobních údajů

Je nutné připomenout, že ochrana osobních údajů u nás platí od roku 1993 a dosavadní zákon o ochraně osobních údajů v Česku platí už od roku 2000. Úřad pro ochranu osobních údajů byl zřízen 1. června 2000 jako nezávislý správní orgán v oblasti ochrany osobních údajů, který např. provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů, přijímá podněty a stížnosti občanů na porušení zákona a poskytuje konzultace v oblasti ochrany osobních údajů. Přesto se s příchodem obecného nařízení o ochraně osobních údajů objevila negativní kampaň, s čím že to ten Brusel opět přichází. Motivem této kampaně však byl pouze účel zisku řady poradenských firem. Obecné nařízení dnes představuje aktualizovaný právní rámec ochrany osobních údajů v evropském prostoru, který od 25. května 2018 přímo stanovuje pravidla pro zpracování osobních

údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak obecné nařízení nahradilo zákon č. 101/2000 Sb., o ochraně osobních údajů. Práva a povinnosti v tomto zákoně o ochraně osobních údajů byla nahrazena právy a povinnostmi přímo vyplývajícími z obecného nařízení. Do budoucna je nutné přijmout tzv. adaptační zákon o zpracování osobních údajů, který je v současné době ve schvalovacím řízení. Tento zákon bude upravovat aspekty týkající se Úřadu pro ochranu osobních údajů a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou obecným nařízením upraveny nebo které obecné nařízení umožňuje upravit na vnitrostátní úrovni.

„Každé nakládání s osobními údaji musí mít svůj legitimní a legální účel.“

Co jsou to osobní údaje a jaké termíny obecné nařízení používá?

Osobní údaje jsou veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě. Rozlišujeme obecné, jako jsou jméno, pohlaví, věk, datum narození, osobní stav, občanství, IP adresa; potom organizační: pracovní, osobní adresa, telefonní číslo, e-mail, ověřovací identifikační údaje; a citlivé osobní údaje: zvláštní kategorie osobních údajů, která je více zpřísněna, a to jsou informace o rasovém původu, politické názory, genetické údaje (např. DNA), biometrické údaje (např. otisk prstu). Z působnosti GDPR jsou vyloučeny anonymizované údaje (tj. údaje, které ani nepřímo nepomáhají v identifikaci určitého člověka, a nejsou s ním tedy nijak spojitelné) a údaje zesnulých osob.

Subjekt údajů je fyzická osoba, to je každý, jehož osobní údaje jsou zpracovávány (zaměstnanec, zákazník, klient).

Správce určuje účel a prostředky zpracování osobních údajů. Jedná se o orgány veřejné moci, OSVČ, právnickou osobu, která nabízí zboží a služby rezidentům EU a při své činnosti zpracovává osobní údaje. Odpovídá za dostatečné zabezpečení osobních údajů, za dodržování zásad zpracování a povinností upravených nařízením. Zpracovatel zpracovává osobní údaje pro správce.

Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce.

Zpracování je operace nebo soubor operací s osobními údaji prováděných pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření, seřazení, omezení, výmaz nebo zničení.

Automatizace znamená, že jde o zpracování pomocí informačních systémů.

Profilování je forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu. Profilování je běžné např. ve finančních službách, kdy finanční subjekty profilují např. klienta žádajícího o hypoteční úvěr, u kterého hodnotí schopnost klienta hypoteční úvěr splácet.

Nová práva v souvislosti s GDPR

Nová pravidla občanům garantují například právo žádat výmaz svých údajů z marketingových databází. A nejen odtud, firmy a instituce musí provést výmaz také v případě, že pominul účel, pro nějž informace o klientech sbíraly. Lepší ochranu nové evropské nařízení garantuje občanům také v případě, že dojde k úniku či krádeži dat. Ty totiž musí správce hlásit Úřadu pro ochranu osobních údajů bez zbytečného odkladu a pokud možno, do 72 hodin od okamžiku, kdy se o tom dozvěděl. Pokud by hrozilo, že kvůli úniku dojde třeba ke zneužití bankovních účtů klientů, musí informovat o ztrátě údajů i nebezpečí jejich zneužití všechny klienty, o jejichž data se přišlo. Další novinkou je také právo na přenos údajů od jednoho poskytovatele služeb k druhému. To má podle představ Evropské komise lidem usnadnit třeba změnu e-mailové schránky a dalších služeb. Doposud uživatele od změny poskytovatele odrazoval čas, který by museli strávit přepisováním svých údajů z jedné aplikace do druhé.

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Pokud se osobní údaje

zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány. Subjekt údajů je na toto právo výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Nařízení je aplikovatelné v celé EU. GDPR zpřesňuje souhlas se zpracováním osobních údajů. Vyžaduje vyšší technickou a organizační bezpečnost správců a zpracovatelů. Za určitých podmínek požaduje jmenování pověřence pro ochranu osobních údajů. Zavádí novou povinnost – vést záznamy o činnostech zpracování. Při rizikových zpracováních osobních údajů požaduje předchozí provedení posouzení vlivu na ochranu osobních údajů a případně též konzultaci s Úřadem na ochranu osobních údajů. Zavádí vyšší sankce za porušení ochrany osobních údajů, což bude částečně upraveno adaptačním zákonem. A umožňuje ukládat opravná a restriktivní opatření.

„Interní auditorky a auditory bude v prvé řadě zajímat zmapování nakládání s osobními údaji.“

GDPR a interní audit

Interní auditorky a auditory bude v prvé řadě zajímat zmapování nakládání s osobními údaji.

To znamená zjištění, s údaji jakých osob je nakládáno, například zaměstnanci, spotřebitelé apod.

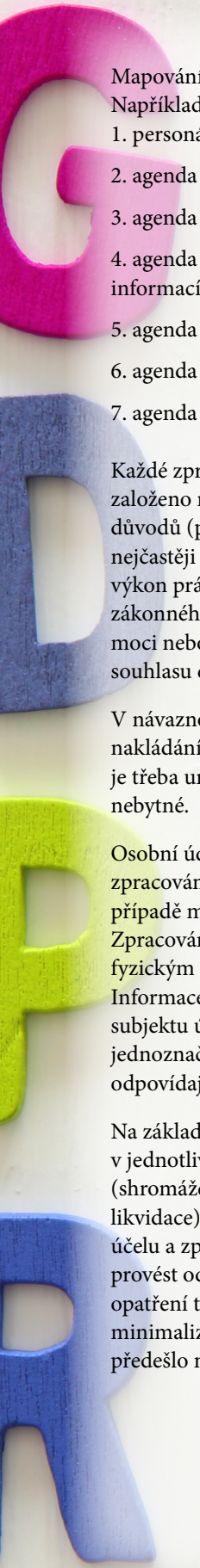
Poté s jakými osobními údaji dotyčných osob je nakládáno. Tedy identifikační – jméno, příjmení, bydliště, datum narození. Kontaktní – adresa, telefonní spojení, e-mail apod. Dále například údaje o pracovním výkonu, o majetkových poměrech, o rodinném stavu apod.).

Také v jaké formě (listinné, IT systém), resp. na jakých nosičích jsou údaje vedeny.

Dále jaké operace se s údaji provádějí, například kopírování, zpřístupňování, předávání, včetně předávání do třetích zemí.

A nakonec jaké osoby a kdy s údaji pracují (například personalistka či mzdová účetní při výpočtu mezd, např. i externí poskytovatel služeb, který má postavení zpracovatele).

Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce, nebo po dohodě či se souhlasem dotčených osob, musí být legitimní a nesmí být v rozporu s právními předpisy či morálkou. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr – účel zpracování údajů.



Mapování lze zakončit přiřazením účelu. Například:
1. personální a mzdová agenda
2. agenda související se správou majetku
3. agenda ekonomického oddělení
4. agenda přístupu k utajovaným informacím
5. agenda dodavatelů a odběratelů
6. agenda marketingu
7. agenda kamerového systému

Každé zpracování údajů musí být založeno na některém ze základních důvodů (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.

V návaznosti na účel a právní podklad nakládání (zpracování) s osobními údaji je třeba určit, jaké osobní údaje jsou nebytné.

Osobní údaje musí být z hlediska účelu zpracování přesné. Přesností se v tomto případě míní i komplexnost údajů. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno férově. Informace o zpracování poskytované subjektu údajů musí být zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci.

Na základě úvahy o možných rizicích v jednotlivých fázích nakládání s údaji (shromáždění, uložení, zpracování, likvidace) je třeba ke každému jednomu účelu a zpracování určit a následně provést odpovídající bezpečnostní opatření tak, aby byla rizika minimalizována a aby se pokud možno předešlo nepříznivým důsledkům.

Druhy bezpečnosti

Bezpečnost osobní, tj. určení kdo, kdy a z jakého důvodu k údajům bude mít přístup, a určení oprávnění k nakládání s nimi (například personalista při zpracování mezd).

Bezpečnost prostorová zabezpečení přístupu ke spisům (zámky, kamery, mříže).

Bezpečnost výpočetní techniky, tj. uživatelská oprávnění, hesla, antivirové programy.

„Přesto se s příchodem obecného nařízení o ochraně osobních údajů objevila negativní kampaň, s čím že to ten Brusel opět přichází. Motivem této kampaně však byl pouze účel zisku řady poradenských firem.“

Mezi prvky k zajištění bezpečnosti spadá i uzavření smlouvy se zpracovatelem. Dále je třeba zajistit bezpečnost vůči třetím osobám, například IT podpora, strážní služba, úklidová služba.

Obecné nařízení je postaveno na zásadách zákonnosti, korektnosti, transparentnosti – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně. Na omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely. Na minimalizaci údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány. Na přesnosti – osobní údaje musí být přesné. Na omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány. A na integritě a důvěrnosti, tj. technické a organizační zabezpečení osobních údajů.

GDPR a Úřad pro ochranu osobních údajů (ÚOOÚ)

Na webových stránkách Úřadu pro ochranu osobních údajů – www.uoou.cz – jsou uvedeny důležité informace ke konkrétním oborům a činnostem, ať již formou odpovědí na nejčastější dotazy, nebo odkazu na zřízenou telefonní linku pro rychlé konzultace a linku pro konzultace ke kamerovým systémům. Další informace jsou o pořádání konzultací pro pověřence. Jsou zde uvedena stanoviska například k otázkám použití fotografie, obrazového a zvukového záznamu fyzické osoby. Stanovisko ke kopírování dokladů nebo k umístění kamerových systémů v bytových domech nebo zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace a řada dalších. Je zde uvedena řada metodických doporučení a jiných informací.

Interní audit již nebude sedět v koutě

V průběhu rozdílových analýz či implementačních projektů GDPR se role interního auditu v mnoha organizacích zúžila na pouhého pozorovatele. Den účinnosti máme již dávno za sebou, a někteří klienti ho dokonce i bujaře oslavili. Dobíhající implementační projekty se však dnes tiše ptají, nezapomněli jsme na nic?

Ing. Mgr. Ján Bača, CIPP/E, CIPT
Senior Associate
PricewaterhouseCoopers Audit, s.r.o.

Během léta jsme v prostorách pražského Experience Centra PwC nelenili a uspořádali pro své klienty interaktivní GDPR workshop, s cílem podělit se o své zkušenosti, ale i názory na budoucnost tohoto nařízení. Řeč byla o dobré, špatné i ošklivé praxi, prvních pokutách, ale i o tom, jak může interní audit pomoci s reziduálním rizikem nebo slepými místy GDPR projektu v organizaci.

Co přineslo léto

Dle aktuálního průzkumu deklarovalo soulad s GDPR pár dní po jeho účinnosti pouze 27 % evropských společností, přičemž 53 % dotázaných společností s implementací ještě pořád zápasí. Průzkum je uzavřen s tím, že až 74 % společností předpokládá dosažení souladu do konce roku 2018.[1] Měla by nás však tato čísla překvapit? Vzpomeňme si na prosinec 2017, kdy každá druhá česká společnost přiznala, že se s požadavky GDPR teprve seznamuje.[2]

1 20% of Companies Report Being GDPR Compliant Post May 25 Deadline. Cision [online]. 2018 [cit. 2018-08-10]. Dostupné z: https://www.prnewswire.com/news-releases/20-of-companies-report-being-gdpr-compliant-post-may-25-deadline-300679827.html

2 Každá druhá firma nebude včas připravena na GDPR. Novinky.cz [online]. 2018 [cit. 2018-08-10]. Dostupné z: https://www.novinky.cz/internet-a-pc/458511-kazda-druha-firma-nebude-vcas-pripravena-na-gdpr.html

Navzdory několikaměsíční účinnosti se i nám dále ozývají organizace, které s implementací ještě nezačaly, ale uvědomují si, že je povinnosti z nařízení vyplývající neminou. Některé dokonce mylně se začátkem implementace vyčkávají na lokální právní úpravu. Pouze v ojedinělých případech mají naši klienti za sebou již také post-implementační audit.

„Dobíhající implementační projekty se však dnes tiše ptají, nezapomněli jsme na nic?“

I když náš dozorový úřad během léta nezahálel a vydal například metodiku pro přípravu kodexu chování, na kterou asociace netrpělivě čekaly, neudělil zatím od účinnosti GDPR (do uzávěrky tohoto čísla) žádnou pokutu. Oproti tomu francouzský dozorový orgán již stihl udělit pokutu ve výši 250 tisíc euro. Rozhodnutí sice padlo ještě před účinností GDPR, nicméně dozorový orgán již bral přicházející GDPR v úvahu. V případě, že by se případ řešil již pouze podle GDPR, byla by pokuta pravděpodobně vyšší. Jako nedostatečnou shledal úroveň zabezpečení osobních údajů u prodejce optických a naslouchacích zařízení.[3]

Svou rozhodovací praxí nás již stihly překvapit i evropské soudy. Tak například svědkové Jehovovi budou kromě pootevření vašich dveří žádat také souhlas se zpracováním osobních údajů a každá facebooková skupina bude mít svého správce odpovědného za zpracování – jejího zakladatele. Na první pohled to jsou spíše úsměvné závěry. Jejich dopad do praxe však může být zásadní. Právě rozhodovací praxe dozorových orgánů a soudů bude tím, co bude v následujících měsících dodávat hodně obecnému nařízení zcela konkrétní kontury.

Dobrý, zlý a ošklivý

Pokud jste stejnojmenný kultovní western viděli *(anglicky The Good, the Bad and the Ugly)*, budete možná souhlasit, že kladný hrdina *(„The Good“)*, ztvárněn Clintem Eastwoodem, je přinejmenším hodně velký pragmatik. Není divu. V době, ve které se film odehrává, by ho čistá duše mohla stát provaz, případně kulku z revolveru. Domnívám se, že jistá dávka pragmatizmu byla v průběhu implementačních projektů naprosto nezbytná. A to u všech, právníky a ajťáky nevyjímaje. Jak veliké však byly tyto kompromisy? Nebyla zvolená úroveň pragmatizmu důvodem, proč se implementace nezbytné dokumentace, procesů a technických funkcionalit zanedbala, případně odložila na neurčito?

Téměř denně je široká veřejnost prostřednictvím médií svědkem mnoha příkladů *zlé*, a v některých případech i *ošklivé* praxe. Vzpomeňme si například na medializovanou kauzu zneužití osobních údajů uživatelů sociálních sítí k politickým účelům nebo početná selhání v případě úniků osobních údajů. V praxi vidíme, že k rozsáhlému narušení zabezpečení osobních údajů není potřeba dobrého hackera, ale plně postačí i špatný zaměstnanec, respektive jeho špatné bezpečnostní povědomí v kombinaci s absencí základních bezpečnostních opatření v organizaci.

Nebylo toho už dost?

Během zmiňovaného interaktivního workshopu měli naši klienti možnost účastnit se pomocí svých mobilních telefonů anonymního průzkumu, ze kterého vyplynulo, že až 55 % účastníků workshopu považuje GDPR za příležitost udělat si pořádek v datech a lépe je vytěžovat. Následovalo „nutné zlo“ s 35 %.

3 OPTICAL CENTER: sanction de 250.000€ pour une atteinte à la sécurité des données des clients du site internet www.optical-center.fr. Ncil.fr [online]. 2018 [cit. 2018-08-10]. Dostupné z: https://www.cnil.fr/fr/optical-center-sanction-de-250000eu-pour-une-atteinte-la-securite-des-donnees-des-clients-du-site

„Z GDPR byla již unavena jak široká veřejnost, tak projektové týmy.“

Z vlastní zkušenosti však vím, že časová a finanční náročnost implementačních projektů, ale i mediální a „souhlasová“ masáž posledních květnových dní způsobila, že z GDPR byla již unavena jak široká veřejnost, tak projektové týmy. Toto vyčerpání by však nemělo být důvodem, proč od splnění požadavků nového nařízení odvracet zrak. Ba právě naopak. Rozsáhlé čerpání zdrojů k tomuto účelu v minulém roce by mělo být důvodem, proč by měl nezávislý audit poskytnout projektovému týmu, ale hlavně vedení společnosti informace o výsledcích implementačního projektu a jeho reziduálních rizicích.

Nezapomněli jsme na nic?

Hlavním cílem post-implementačního auditu by mělo být ověření úspěšné implementace opatření, které nařizuje GDPR správcům a zpracovatelům osobních údajů. Vypracování záznamů o činnostech zpracování, zavedení procesů pro výkon práv subjektů údajů a zajištění zabezpečeni osobních údajů jsou jenom jedny z těch nejdiskutovanějších oblastí. Předmětem ověření by měl být nejen jejich design, ale také fungování v praxi Na co se v rámci auditních testů zaměřit? (viz obrázek).

3. Provedení auditních testů

Testování designu opatření:

- Záznamy o zpracování
- Souhlas zaměstnanců a souhlas zákazníků
- Vzorové zpracovatelské smlouvy
- Informační povinnost vůči zaměstnancům a zákazníkům
- Analýza rizik a DPIA
- Opatření k zajištění bezpečnosti
- Obecná politika ochrany osobních údajů
- Ohlašovací povinnost
- Řízení dodavatelů
- Výkon práv subjektů (proces)
- DPO
- Projekty a změny
- Archivace a likvidace

Testování efektivity opatření v oblastech:

- Řešení identifikovaných dopadů na organizaci
- Předávaní osobních údajů do třetích zemí
- Aktivity spojeny se zvyšováním povědomí
- Zvláštní kategorie osobních údajů
- Vysoce rizikové zpracování (analýza rizik a DPIA - test kompletnosti)
- Organizace jako společný správce
- Organizace jako zpracovatel
- Opatření k zajištění bezpečnosti
- Příjemci (test kompletnosti)
- Zpracovatelské smlouvy
- Projektové řízení a běžící projekty
- Procesní řízení ke kontrole dodržovaní přijatých opatření

Testování IT prostředí:

- Kontroly v oblasti komplexního profilu a identifikace právního titulu
- Kontroly nad retencí dat
- Výkon práv subjektů údajů (technická funkcionalita)
- Administrativní a procesní opatření k zajištěni IT bezpečnosti (ISMS)
- Technická opatření k zajištěni IT bezpečnosti
- Kontroly nad Shadow IT
- Řízení dodavatelů v IT
- Řízení IT rizik
- Ohlašovací povinnost v IT
- IT projekty a změny

Nabízí se proto například i možnost vzorkování zpracovatelských smluv nebo také různé formy „mystery shoppingu“ v případě výkonu práv subjektů údajů.

„Dle aktuálního průzkumu, deklarovalo soulad s GDPR pár dní po jeho účinnosti pouze 27 % evropských společností.“

Hlavní zadání od našich klientů bývá jednoduché: *„Podívejte se, zda jsme na nic nezapomněli.“* Tito klienti vědí, že slepá místa projektu a tunelové vidění jsou ty nejzákeřnější. Jsou to rizika, která se neeliminují ani neakceptují. Tato rizika zůstávají bez dalšího a čekají na svou příležitost.

Z tohoto důvodu by jedním z primárních úkolů revize implementace mělo být ověření kompletnosti implementačního projektu. V případě, že některá z činností zpracování nebyla identifikována v průběhu rozdílové analýzy, je pravděpodobné, že chyběla také implementace související dokumentace a procesů. Z již provedených projektů se doporučuji podívat například na běžící *smart* projekty, partyzánské akce oddělení marketingu, a pro jistotu prověřte i existenci firemní školky či ubytovny.

Spolupráce, která se osvědčila

Dnem účinnosti GDPR neskončilo. Právě naopak. Kontrolní činnost vystřídá pracovní skupiny a důraz bude kladen na efektivitu přijatých opatření. Jak však post-implementační revizi a následné pravidelné kontroly zabezpečit? Interně dnes chybí lidé i kvalifikace. Z vlastní zkušenosti doporučuji využít kombinaci interních a externích zdrojů.

Organizaci auditu, sběr dokumentace, workshopy, zpracování výstupů, identifikaci nápravních opatření a kontrolu jejich plnění si můžete podělit. Využijete znalost interního prostředí i externí kvalifikaci a zkušenosti. Znalosti zůstanou. Dlouhodobá udržitelnost však vyžaduje dlouhodobou kontrolu. Nezávislou. Interní. Interním auditem.

„55 % účastníků workshopu považuje GDPR za příležitost udělat si pořádek v datech.“

Noví členové

- Ing. Lenka Bednárová, Železničná spoločnosť Slovensko, a. s.
- Ing. Tomáš Borovec, Ph.D., Ph.D., APS Management Services s.r.o.
- Ing. Hedviga Csíriová, Plzeňský Prazdroj Slovensko, a.s.
- Ing. et Bc. Veronika Cyprysová, BOHEMIA ENERGY entity s.r.o.
- Ing. Dominik Dýma, Allianz pojišťovna, a.s.
- Ing. Marta Filipcová, Olomoucký kraj
- Bc. Jitka Frölichová, KOMSOFT, s.r.o.
- Ing. Mgr. Jiří Galuška, APS Management Services s.r.o.
- Ing. Ondřej Hruška, Karlovarský kraj
- Ing. Petra Janíčková, MBA, Individuální členka
- Ing. Hana Jílková, MERO ČR, a.s.
- Ing. Petra Kišová, Ph.D., Individuální členka
- Ing. Amália Klímová, Česká pošta, s.p.
- Bc. Monika Kopsová, Česká pošta, s.p.
- Ing. Alexander Kopún, Západoslovenská energetika, a.s.
- Bc. Martina Legnerová, České Radiokomunikace a.s.
- Ing. Martin Lovász, APS Management Services s.r.o.
- Ing. Jana Mihóková, Východoslovenská energetika Holding a.s.
- Ing. Anežka Mrázová, MPA, Česká správa sociálního zabezpečení
- Ing. David Mysík, Fio banka, a.s.
- Mgr. Sněžana Pellarová, Městská část Praha 3
- JUDr. Pavel Podaný, Citfin, spořitelní družstvo
- Michal Pochobradský, Deloitte Audit s.r.o.
- Ing. Martin Poláček, Individuální člen
- Ing. Jaroslava Pražáková, Národní technická knihovna
- Ing. Petr Slezák, NEY spořitelní družstvo
- Ing. Věra Suchodolová, Individuální členka
- Martin Štembírek, Fio banka, a.s.
- Bc. Jitka Vaníčková, Statutární město Prostějov
- Ing. Kamila Veselá, Statutární město Havířov
- Ing. Irena Wasserbauerová, CIA, Česká národní banka
- Ing. Žaneta Vomáčková, Městský úřad Svitavy

GDPR V PRAXI: bezzubý strašák, nebo téma pro interní audit?

Mgr. Michal Nulíček, LL.M.
Partner
ROWAN LEGAL, advokátní kancelář s.r.o.

Od účinnosti obecného nařízení o ochraně osobních údajů (GDPR) uplynuly již téměř čtyři měsíce. Pro mnohé představovalo toto nařízení, kvůli vysoko nastaveným stropům pro sankce, strašáka, který poháněl kupředu implementační projekty jak v soukromém, tak ve veřejném sektoru. Stejného tempa se však nepodařilo dosáhnout při přijímání legislativy provádějící potřebné související změny v českém právním řádu a výsledkem je, že přístup Úřadu pro ochranu osobních údajů (ÚOOÚ) k ukládání pokut za porušování GDPR je zatím velmi opatrný. Představuje tedy GDPR jen bezzubou hrozbu, nebo je skutečně tématem, které si zasluhuje pozornost interních auditorů? A pokud by se mu interní auditoři měli věnovat, jak jej uchopit?

Nový zákon bude projednáván na podzim

Ačkoli ÚOOÚ obdržel od účinnosti GDPR stovky stížností, zatím neoznámil uložení žádné pokuty. To lze zčásti přičíst krátké době, která od účinnosti GDPR uplynula, roli ale hraje nejspíše také to, že se stále čeká na doplňující legislativu v podobě tzv. adaptačního zákona. Ten má vedle úpravy přestupků na úseku ochrany osobních údajů a úpravy pravomocí ÚOOÚ přinést také dílčí odchylky od GDPR především v podobě snížení sankcí pro veřejnou správu a stanovení určitých výjimek z nastavených pravidel. Tyto výjimky však budou opět cílit převážně na veřejnou správu, a pro soukromé subjekty tak nelze mnoho změn očekávat. Kdy se dočkáme vydání a účinnosti nového zákona, přitom zatím není jasné. Vzhledem k odložení jeho druhého čtení v Poslanecké sněmovně na září je však už nyní zřejmé, že to nebude dříve než koncem tohoto roku.

Do té doby se bude ÚOOÚ dle svého vyjádření zaměřovat na předběžné zvyšování povědomí o vhodné ochraně údajů, a zejména u subjektů, jako jsou menší obce a drobní podnikatelé, před ukládáním pokut volit nápravná opatření. Důvodem může být i poněkud nejasná pravomoc ÚOOÚ v mezidobí takové pokuty (tj. pokuty dle GDPR) ukládat.

Stížnosti u nás i v zahraničí se množí

Sama skutečnost, že ÚOOÚ se do účinnosti adaptační legislativy bude snažit působit spíše preventivně a směrem k nápravě porušení, neznamená, že by neměl materiál ke kontrole. Od 25. května, kdy nabylo GDPR účinnosti, se Úřad pro ochranu osobních údajů potýká s nárůstem počtu stížností a podnětů jednotlivců – k 15. červenci, tedy necelé dva měsíce po nabytí účinnosti GDPR, evidoval ÚOOÚ přes 630 podaných stížností. Ačkoliv se většina stížností týká kamerových systémů a telemarketingu, začíná přibývat také stížností v souvislosti s nezákonným vyžadováním souhlasu.

Tato situace přitom není z evropského pohledu nijak výjimečná – se zvýšeným náporem stížnosti se potýkají všechny evropské dozorové úřady v oblasti ochrany osobních údajů. Velké společnosti přitom často nečelí jen stížnostem jednotlivců, ale také organizací, které je zastupují. Příkladem jsou aktivity skupiny noyb.eu, vedené známým aktivistou Maxem Schremsem, který již v minulosti dosáhl zrušení pravidel, na základě kterých velké společnosti předávaly osobní údaje do USA. Tato skupina podala v několika

„Jakkoli tedy ÚOOÚ zatím přistupuje k vymáhání GDPR uvážlivě, množící se stížnosti u nás i v zahraničí spolu s rostoucím počtem zpráv o narušení bezpečnosti naznačují, že aktivita dozorových úřadů v čase poroste.“

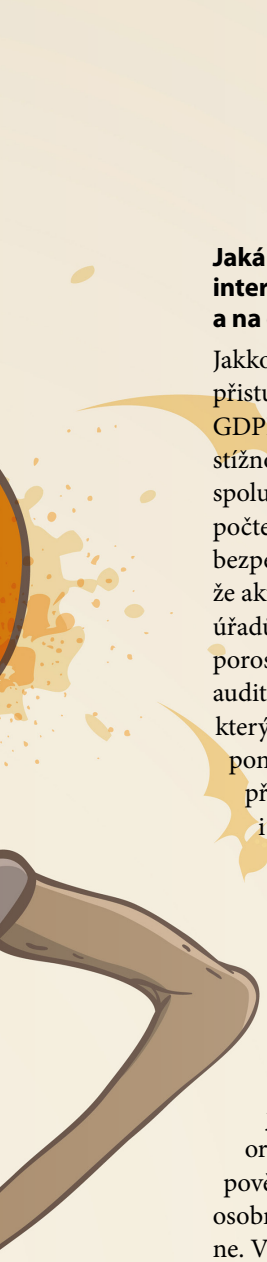
státech EU stížnosti proti společnostem Facebook, Google, Instagram a WhatsApp, které viní z toho, že klienty nutí, aby souhlasili s použitím jejich dat pro cílení reklamy, a hrozí blokací služby nebo smazáním účtu.

Bude tedy zajímavé sledovat, jak se k těmto stížnostem postaví dozorové v zahraničí – jejich rozhodovací praxe bude jistě pro ÚOOÚ inspirací, a to díky koordinaci dozorových úřadů v nově vzniklém Evropského sboru pro ochranu osobních údajů (EDPB). EDPB je orgán EU, který nahradil původní pracovní skupinu podle čl. 29 (WP29), a od 25. května 2018 je tak hlavní evropskou autoritou při uplatňování GDPR. Jeho úlohou přitom není jen koordinace úřadů při přeshraničním uplatňování GDPR, ale také vydávání pokynů a stanovisek k výkladu GDPR. EDPB výslovně převzal pokyny vydané WP29 k výkladu GDPR, lze však očekávat, že bude vydávat další materiály k problémům, se kterými se potýkáme v praxi.

Co přináší praxe

Praktických problémů vznikajících při fungování podle pravidel GDPR přitom není málo. Oblast, která představuje zátěž pro řadu správců osobních údajů, je oblast požadavků subjektů údajů o výkon práv – například o přístup k jejich osobním údajům nebo jejich výmaz. Jedná se o procesně náročnou agendu, a to nejen po stránce administrativní. Praktický problém představuje také ověřování totožnosti žadatelů a předávání vyžádaných dat – vydání údajů neoprávněné osobě, která jen předstírá, že je oprávněným subjektem údajů totiž může představovat bezpečností incident.

Sama problematika bezpečnostních incidentů je rovněž horkým tématem. Že nejde o problém virtuální, dokládá vyjádření ÚOOÚ, že již vyšetřuje několik rozsáhlých úniků osobních údajů, zejména z oblasti ubytovacích služeb. Významnější porušení zabezpečení je totiž podle GDPR příslušný správce osobních údajů povinen v krátké lhůtě oznámit ÚOOÚ. Tato povinnost vyžaduje dobrou připravenost na straně správce osobních údajů, a představuje tak jedno z témat pro interní audit.



Jaká má být role interních auditorů a na co se zaměřit?

Jakkoli tedy ÚOOÚ zatím přistupuje k vymáhání GDPR uvážlivě, množící se stížnosti u nás i v zahraničí spolu s rostoucím počtem zpráv o narušení bezpečnosti naznačují, že aktivita dozorových úřadů v čase poroste. S tím poroste i význam interního auditu v této oblasti, který může organizacím pomáhat efektivně předcházet sankcím i negativní publicitě, která je s narušením bezpečnosti osobních údajů často spojena.

Role interních auditorů přitom bude záležet mimo jiné na tom, zda organizace jmenovala pověřence pro ochranu osobních údajů, nebo ne. V organizacích, které pověřence mají, by měla mezi pověřencem a týmem interního auditu probíhat úzká spolupráce, aby bylo zajištěno, že relevantní procesy v oblasti ochrany osobních údajů probíhají správně. To však neznamená, že by sám pověřenec měl být z pravomoci interního auditu vyňat – jakkoli jeho role musí být nezávislá a nesmí mu být udělovány pokyny, nedostatečné plnění jeho povinností může pro organizaci rovněž představovat riziko, a to jak u interního, tak zejména u externího pověřence.

V organizacích, kde není jmenován pověřenec, je role interního auditu o to významnější, neboť musí suplovat jeho auditní funkci.

První téma na pořadí interního auditu budou přirozeně ty činnosti, které se v rámci implementačního projektu nepodařilo řádně a včas dokončit před nabytím účinnosti. Vedle již zmíněných oblastí výkonu práv subjektu údajů a bezpečnostních incidentů (resp. přirozeného tématu bezpečnosti osobních údajů obecně), je pak třeba neponechat stranou zejména oblast vztahů se třetími stranami – u velkých organizací s desítkami či stovkami dodavatelů zpracovávajíce osobní údaje je úprava smluv, nastavení praktických bezpečnostních opatření i přiměřené transparentnosti vůči osobám, s jejichž daty se pracuje, náročnou úlohou, kterou však není vhodné opomenout. Dokladem je i to, že řada významných úniků osobních údajů v posledních letech proběhla přes dodavatele.

„K 15. červenci, tedy necelé dva měsíce po nabytí účinnosti GDPR, evidoval ÚOOÚ přes 630 podaných stížností.“

Z hlediska praktického provedení je pak ideální realizovat audity v multidisciplinárních týmech, schopných posoudit otázky praktického zabezpečení osobních údajů, složitější právní požadavky na nastavení jednotlivých procesů a poskytnout výklad relevantních ustanovení GDPR. Z hlediska struktury je v případě středních a větších organizací vhodné postupovat podle jednotlivých obchodních funkcí jako je prodej, marketing, HR, IT apod.

Závěrem

Ačkoli stále čekáme na domácí adaptační legislativu ke GDPR a přístup ÚOOÚ k ukládání sankcí je uvážlivý, nemělo by toto téma zůstat mimo pozornost interních auditorů, a to zvláště v organizacích, které nemají pověřence pro ochranu osobních údajů. Důvodem jsou množící se stížnosti u dozorových úřadů i četná hlášení narušení bezpečnosti dat. Interní auditoři by proto měli pomoci organizacím identifikovat a odstranit rizika plynoucí jak z nedodělků v rámci implementačních projektů, tak v rámci významných oblastí, jako je řízení bezpečnostních incidentů nebo vztahy s třetími stranami. ■

Chráníte osobní údaje standardně, nebo záměrně?

Ing. Rodan Svoboda, CIA, CICA, CRMA
jednatel vzdělávací a poradenské společnosti Eurodan, s. r. o.,
konzultant v oblasti VŘKS a IA
svoboda@eurodan.cz

Na první pololetí roku 2018 jen tak nezapomenu. Vypořádat se s implementací nových požadavků obecného nařízení na ochranu osobních údajů u více než stovky správců údajů představovalo zcela novou zkušenost, na kterou se nedalo předem připravit. Skočil jsem do rozbouřených vod nové legislativy po hlavě a nezbývalo nic jiného než plavat. Zpočátku jsem hledal správnou cestu z pohledu interního auditora, postupně však bylo třeba se změnit na konzultanta, stát se metodikem, využívat schopností komunikátora, a nakonec skončit v roli pověřence.

Stále tomu však něco chybělo. To přišlo až ve chvíli, kdy mi došlo, o co tady vlastně jde. Celá ochrana osobních údajů je v podstatě řízení rizik. Ne těch vlastních, které nám znemožňují dosáhnout cílů našeho snažení, ale rizik dopadajících na fyzické osoby, které jsou s našimi organizacemi v jakémkoliv vztahu, předávají nám své osobní údaje s očekáváním poskytnutí odpovídajících služeb a s vírou, že těchto dat nijak nezneužijeme.

A z tohoto důvodu do toho vstupuje státní autorita se svou regulací. Nabádá nás k ochraně osobních údajů, jež se dotýkají soukromí každého člověka, k zabezpečení neoprávněného přístupu, zachování integrity a časového omezení jejich uchování. Takže my, co se na tom podílíme, jsme de facto risk manažeři.

Každý, kdo jste se k implementaci opatření stanovených GDPR dostal, máte určitě svou vlastní zkušenost. Zmíním se o té mé a můžeme ji spolu porovnat. Z mého pohledu jsem se setkával převážně se zástupci organizací, kteří potřebu chránit osobní údaje v plném rozsahu obecného nařízení řešili jen jako povinnost, která jim byla vnucena. Teda vlastně je zajímalo především to, co jim případně bude hrozit, až k nim dorazí kontrola dozorového orgánu. Takže zadání bylo jednoznačné. Připravit dokumenty, aby je mohli, bude-li to třeba, vytáhnout ze šuplíku a kontrole předložit. Z mého pohledu to však nestačí. Jde o mnohem víc. Dovolte mi tedy tři krátká zamyšlení na základě mé zkušenosti s implementací obecného nařízení.

ZAMYŠLENÍ PRVNÍ: Kdo by se měl o ochranu osobních dat postarat?

Prvními, na které vedení organizací ukázalo, byli zpravidla právníci. Souvisí to patrně s tím, o čem jsem se již zmínil. Zadání spočívající v nastudování požadavků právního předpisu a v minimálním rozsahu je bez větších nároků na zdroje naplnit. Tady skutečně právník může být tou nejlepší zárukou, že to klapne. Kde je však každodenní chod organizace? Shromažďování údajů, jejich zpracování, ukládání v informačních systémech, zpřístupňování, zveřejňování či skartace? Budou tu právníci skutečně stát za zády nás ostatních a hlídat, že je to tak správně?

Ve finančním sektoru je určitou zárukou pro dosahování souladu s požadavky právního předpisu ustavení funkce compliance. Setkal jsem se s institucemi, kde právě compliance officer zastává pozici pověřence pro ochranu osobních údajů a koordinuje jak nastavení vlastní ochrany dat, tak i výkon, zejména prováděním příslušných compliance kontrol. Řekl bych, že mi je tento model blízký, protože právě funkce compliance má k řízení rizik nesouladu nejblíže.

„Celá ochrana osobních údajů je v podstatě řízení rizik.“

Vím, jaké vášně vzbudilo stanovisko Centrální harmonizační jednotky nedoporučující zapojit do výkonu ochrany osobních údajů interní auditory, koneckonců jsem se k tomu obdobně metodicky vyjadřoval osobně i já. Mám však na druhou stranu kolem sebe mnoho kolegů z řad interních auditorů, kteří se do implementace požadavků aktivně zapojili a nyní vykonávají souběžně i funkci pověřence. Naše profesní standardy už na to pamatují a mají pojistky, jak to zvládnout bez narušení nezávislosti a objektivity. Teď však to hlavní, proč právě interní auditor? Spousta organizací klasický risk management nemá. Kdo jiný o tom má alespoň nějakou představu? Kdo se dokáže postarat o opatření ke snížení projevu rizik? Jako manažer bych taky neváhal a do interního auditu se vydal s prosbou o pomoc.

V organizacích zejména střední velikosti se objevila rovněž zajímavá praxe. O ochranu osobních údajů se začali starat ajťáci. Souvisí to pochopitelně se zásadou integrity, kdy osobní data jsou uložena převážně v elektronické podobě v informačních systémech a, pokud dojde k nějaké odchylce od smyslu obecného nařízení, bude to právě v úniku a zneužití uchovávaných dat. Domnívám se, že bez zapojení IT specialistů se požadavky GDPR implementovat nedají, ale komplexní řešení bych tam nehledal.

Kde hledat toho správného člověka, když právníka, interního auditora, compliance manažera ani vlastní IT podporu nemáme? Mnoho organizací sáhlo ven mimo organizaci a najalo si externího dodavatele. To má dvě roviny. Určitě je rozumné se opřít o znalosti a zkušenosti, které nám v organizaci chybí, mohou však dva tři dny v organizaci během měsíce nahradit každodenní práci zaručující soulad s požadavky obecného nařízení? Možná tehdy, když se nastaví decentralizovaný model

řízení rizik s odpovědností liniových manažerů...

Posledním modelem, který nebyl zcela výjimečný, bylo si vytvořit novou funkci pověřence prakticky na zelené louce. Bez historie, bez kumulace činností s jinou funkcí. Proč ne. Je to sice průlom, který se klasickému risk managementu zpravidla doposud nepodařil, ale v zásadě cesta dobrým směrem. Zřízení profesionálního pověřence pro ochranu osobních údajů, jinými slovy manažera řízení rizik osobních údajů, se kterými organizace přichází do styku. Jen, aby nezačal někdo poukazovat na to, že vlastně nemá co dělat, a nezačal mu přidávat další a další odpovědnosti.

ZAMYŠLENÍ DRUHÉ: Jak dosáhnout požadavků na ochranu osobních údajů?

Státní regulace vychází vždy z jednoho základního principu. Identifikovat nejvýznamnější rizika, která se mohou v dané oblasti projevit, nastavit k nim rámcově zásadní opatření, která daná rizika budou snižovat co do významu a pravděpodobnosti na přijatelnou úroveň, a poté provádět dohled s příslušnými sankcemi, který bude zaručovat dodržování nastavených legislativních požadavků, a tudíž minimalizaci projevu identifikovaných rizik. Touto cestou jde i obecné nařízení na ochranu osobních údajů.

Žijeme v moderní době s podporou automatizovaného zpracovávání osobních dat v univerzálních databázích s použitím až zneužitím pro jakékoliv účely. Dá se to ještě uhlídat z jednoho dozorového orgánu? Přišlo se tedy se zajímavou myšlenkou. Pojďme do regulace zapojit přímo i všechny subjekty osobních údajů. Ať si sami hlídají, co se s jejich daty děje. Tak se jim poskytla práva, až možná nadstandardní ve srovnání s možnostmi v rámci jiných činností státu a služeb právnických osob.

Tento přístup se souhrnně nazývá standardní ochranou osobních údajů. Po mém tedy řízení rizik standardizovaným způsobem, kdy aplikujeme zásady zpracování osobních údajů popsané v obecném nařízení, přizpůsobujeme je našim procesům, kategoriím subjektů, jejichž osobní údaje zpracováváme, legislativním předpisům a smluvním vztahům. Pochopitelně nelze zapomínat i na dohodu se subjektem, kdy mu zasahujeme do jeho soukromí a ke zpracování svých údajů nám musí dát souhlas. Pro pochopení, v čem spočívá standardní ochrana, předkládám následující zjednodušení:

ŘÍZENÍ RIZIK V RÁMCI STANDARDNÍ OCHRANY

Riziko zpracování osobních údajů	Uplatnění zásady dle obecného nařízení
■ Dochází ke zpracování OÚ, které byly k danému účelu získány bez vědomí subjektu.	■ Zásada zákonnosti – musí existovat jeden z vyjmenovaných zákonných základů pro zpracování OÚ.
■ Dochází ke zpracování OÚ, které subjekt nemůže ovlivnit, a případně s ním nesouhlasit.	■ Zásada korektnosti – subjekt má právo se ke zpracování vyjádřit, a případně to odmítnout.
■ Dochází ke zpracování OÚ, aniž by subjekt věděl proč, jak, ke komu se dostanou, na jak dlouho a jaký to může mít dopad, když je poskytne.	■ Zásada transparentnosti – subjekt musí vědět, že se jeho údaje zpracovávají a co se s nimi bude dít.
■ Dochází ke zpracování poskytnutých OÚ i pro jiné účely bez vědomí subjektu.	■ Zásada účelovosti – subjekt musí být o každém účelu zpracování informován, a v některých případech tomu může zabránit.
■ Dochází ke zpracování OÚ, které nejsou k danému účelu potřebné.	■ Zásada minimalizace – správce nesmí zpracovávat nadbytečné údaje, v tom případě je musí vymazat.
■ Dochází ke zpracování nepřesných a neaktuálních OÚ daného subjektu.	■ Zásada přesnosti – správce musí zajistit aktualizaci OÚ pro daný účel zpracování.
■ Dochází ke zpracování OÚ po dobu delší, než je nezbytné pro naplnění daného účelu.	■ Zásada omezení uložení – správce musí nastavit skartační plán a po nezbytné době OÚ vymazat.
■ Dochází k neoprávněnému či protiprávnímu zpracování, k náhodné ztrátě, zničení nebo poškození OÚ.	■ Zásada integrity a důvěrnosti – správce musí náležitým způsobem zabezpečit OÚ.

„Z mého pohledu jsem se setkával převážně se zástupci organizací, kteří potřebu chránit osobní údaje v plném rozsahu obecného nařízení řešili jen jako povinnost, která jim byla vnucena.“

Setkal jsem se, že je k těmto zásadám uplatňovaným pro řízení rizik osobních údajů přidávána rovněž zásada odpovědnosti. To však je jen požadavek na vlastní systém řízení rizik, kdy je správce povinen uvedená opatření na standardní ochranu před riziky zpracování osobních údajů realizovat a dodržení tohoto souladu se zásadami doložit.

Z praxe vím, že je největší pozornost věnována zásadě transparentnosti. Organizace si udělaly analýzu, jaké údaje a od jakých subjektů, pro jaký účel a jak dlouho, případně jak zpracovávají a komu je předávají. A poté podrobně či jednoduše to oznámily převážně dálkovým přístupem na webu. Je teď na nás, fyzických osobách, abychom začali dohlížet a domáhat se naplnění všech ostatních zásad. Tuším, že některé z nich, zejména požadavky na minimalizaci, přesnost a omezení zpracování, jsou ony kostlivci ve skříni, které na nás časem vypadnou a nestačíme se divit, až dohledový úřad začne uplatňovat své sankční nástroje.

„Ve finančním sektoru je určitou zárukou pro dosahování souladu s požadavky právního předpisu ustavení funkce compliance.“

ZAMYŠLENÍ TŘETÍ:
Jak zajistit záměrnou ochranu osobních údajů?

Co jsem popsal v předchozí části, asi ještě nikoho moc nepřekvapilo. Jsme na to zvyklí, že právní předpis něco ukládá a my to pak plníme. Obecné nařízení jde však dál. Jde tam, kde se již delší dobu pohybují instituce ve finančním sektoru a v omezené míře i obchodní společnosti. Ukládá provést analýzu rizik zpracování osobních údajů, kde je zasahováno do soukromí subjektu, a v těchto případech přijmout opatření k omezení daného rizika. V obecném nařízení se tato analýza nazývá posouzení vlivu na ochranu osobních údajů a přijatým opatřením pak záměrná ochrana osobních údajů.

Dle mé zkušenosti je toto ještě dosti neprobádaná oblast. Vyskytují se sice již metodiky a výklady, ale s jejich uchopením a praktickou aplikací si málokterá organizace dokáže poradit. Tam, kde jsem prováděl tuto analýzu a chystal se diskutovat možná řešení, zavládlo přímo zděšení. Už mají za sebou všichni takové množství práce s analýzou a vytvořením sady informací pro subjekty a já po nich chci teď ještě řídit další rizika?

Začínám zpravidla selekcí operací zpracování. Předpokládám, že tam, kde zpracování vychází z plnění právní povinnosti, tuto analýzu vlivu na ochranu osobních údajů již provedl legislativec. Ale pozor, lidská tvořivost je nevyzpytatelná. Takové zpracování osobních údajů při výplatě mezd sice vychází z právního předpisu, ale když se pak jednotlivé mzdové pásky s údaji válí po stolech a vedoucí, který je rozdává, si přečte, jaké alimenty kdo platí, tak je to přímo ukázková operace zpracování zasluhující si posouzení vlivu.

Po selekci mi zbydou operace zpracování, u nichž je zákonným titulem veřejný či oprávněný zájem, smlouva či souhlas. Tady všude je třeba posoudit, zda se využívají citlivé osobní údaje, zda se údaje využívají k předvídání osobních preferencí, umístění, pohybu osob, finanční situace, zdraví nebo pracovního výkonu, zda dochází na základě osobních údajů k rozhodování, které může významně ovlivnit jednotlivce, např. odmítnutím poskytnutí služby, zda dochází k systematickému sledování veřejných prostor nebo zda existují další rizika s dopadem na práva a svobody jednotlivců.

Pokud organizace dojde k závěru, že jsou naplněny zákonné důvody k provedení posouzení vlivu na ochranu osobních údajů, musí identifikovat rizika a přijmout nápravná opatření v plném rozsahu předepsaného způsobu posouzení vlivu.

Teď to nejdůležitější. Jak na tuto identifikaci jít? Opírám se o metodiku Úřadu na ochranu osobních údajů a posuzuji to z následujících 15 parametrů rizikovosti.

Řízení rizik v rámci záměrné ochrany

Riziko operace zpracování osobních údajů

- Subjekt je na základě zpracovávaných OÚ identifikovatelný, lokalizovatelný, uchovávají se jeho záznamy.
- Shromažďují se OÚ daného subjektu, na základě kterých je možno určit jeho chování.
- V rámci dané situace jsou zpracovávány OÚ, které subjektu mohou způsobit jeho zranitelnost.
- Při zpracování OÚ může nastat situace, že OÚ nebudou dostupné a na subjekt to bude mít negativní dopad.
- OÚ se zpracovávají ve velkém rozsahu, správce tak zasahuje vůči množství správců a zpracovává velký objem jejich OÚ.
- Zpracování neprobíhá na místní či lokální úrovni, ale zasahuje rozsáhlé území, kde se pak mohou OÚ vyskytnout.
- Subjekt nemůže ovlivnit zpracování svých OÚ, ačkoliv operace zpracování na něho mají dopad.
- OÚ subjektu jsou veřejně přístupné.
- Dochází k soustavnému zpracování OÚ.
- OÚ se předávají k dalšímu zpracování.
- Správce údajů má širokou působnost.
- Správce zpracovává údaje bez omezení.
- Správce využívá složitý systém pro zpracování OÚ.
- Správce má vazby na jiné správce při zpracování OÚ.
- Zpracování OÚ probíhá nestandardizovaně.

„Jako manažer bych taky neváhal a do interního auditu se vydal s prosbou o pomoc.“

Pro všechny rizikové operace zpracování jsou stanoveny metriky pro identifikaci významnosti daného rizika. Na správci osobních údajů pak je, aby přijatými opatřeními snížil vysoká rizika zpracování, případně tuto situaci konzultoval s dozorovým úřadem. Ze zkušenosti vím, že řada opatření v rámci posouzení vlivu se bude opírat o standardní ochranu, jen půjde o konkrétní aplikaci zásady do daného procesu tak, aby riziková operace zpracování nemohla být projevem incidentu s dopadem do soukromí subjektu. Naprosto ojedinělou operací je pořizování kamerových záznamů, kde je vhodné přijmout opatření v rozsahu metodického pokynu Úřadu pro ochranu osobních údajů. Dost často se k tomu organizace hlásí, v praxi to však nedodržuje.

Z toho, co jsem popsal, vyplývá, že otázka v nadpisu byla spíše provokativní. Není ani při ochraně osobních údajů něco lepšího a něco horšího. Musí se k rizikům zpracování osobních údajů přistupovat jak z pohledu standardní ochrany, tak záměrné ochrany. Největší chybou by bylo zůstat u vytvoření vnitřního předpisu a jeho uložení na dně šuplíku pracovního stolu ředitele. Na nás, interní auditorech, teď bude, abychom prověřili, jak se rizika zpracování osobních údajů řídí. Doufám, že popsané zkušenosti k tomu pomohou. ■

Jak přinášet přidanou hodnotu v ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů[1] (General Data Protection Regulation, „GDPR“) nabylo účinnosti 25. 5. 2018. Nařízením došlo ke změně evropské legislativy v oblasti ochrany osobních údajů. Co to však znamená pro firmy a organizace v České republice? A jaké z toho vyplývají dopady do činnosti interních auditorů?

Mgr. Stanislav Klika
senior manažer
BDO Audit s.r.o.
Stanislav.Klika@bdo.cz

Jaké jsou dopady GDPR?

GDPR platí pro všechny subjekty – velké i malé, soukromé i veřejné, firmy i neziskovky. Jedinou podmínkou je, aby firma či organizace zpracovávala osobní údaje občanů Evropské unie.

GDPR přináší některé nové povinnosti, které mohou nemálo zatížit firemní rozpočty. Mezi tyto povinnosti patří například zavedení role pověřence pro ochranu osobních údajů nebo nové nároky v souvislosti s rozšířením práv lidí na přístup k jejich osobním údajům. Firmy tak musí být například schopné osobní údaje ve svých systémech vyhledat, a pokud o to zákazník požádá, tak musí předat kopie osobních údajů, které o zákazníkovi zpracovávají. Firmy musí také umět tyto údaje případně smazat. To někdy naráží na informační systémy, které firmy mají. Ty se často vytvářely postupně a jednotlivé verze na sebe nenavazovaly. Aby informační systém zvládl požadavky dané GDPR, tak bude občas potřeba systém upravit, a to může být velmi nákladné.

Je GDPR skutečně revoluční?

Osmdesát procent požadavků GDPR již dnes obsahuje zákon o ochraně osobních údajů nebo tyto požadavky vyplývají z judikatury či stanovisek regulátora. Pro firmy a organizace by tak tyto požadavky neměly představovat úplnou novinku. Při našich auditech se však setkáváme s tím, že firmy a organizace bohužel často neplní ani dosavadní povinnosti podle zákona o ochraně osobních údajů.

Na celou záležitost je tedy možné pohlížet i tak, že ta skutečná revoluce nespočívá v nových pravidlech (která vycházejí ze stávajících principů), ale v přístupu k plnění těchto norem. Mediální tlak a hrozba vysokých pokut způsobily, že firmy přehodnocují svoje priority a více investují do nastavení procesů zpracování osobních dat v souladu s novou legislativou.

GDPR a konkurenceschopnost

Nové nařízení – či spíše reálná implementace někdy až příliš formalistických zásad ochrany osobních údajů si vyžádá nemalé finanční náklady na zavedení potřebných opatření i náklady na průběžné dodržování stanovených pravidel. GDPR tak nepřináší jen lepší postavení subjektů údajů a opatření pro účinnější ochranu soukromí občanů Evropské unie. Evropské požadavky na ochranu osobních údajů nejnověji vyjádřené v GDPR přináší i negativa. I když je úmysl evropských orgánů chránit soukromí principiálně správný, evropským firmám vzniknou nové

1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

náklady, které rozhodně nejsou zanedbatelné a ve výsledku mohou dlouhodobě navyšovat ceny výrobků a služeb.

Dá se tedy předpokládat, že nařízení z hlediska světového obchodu může ztížit postavení evropských firem, zejména vůči již dnes velmi levné produkci z Asie, které je velmi těžké konkurovat a kde tak přísná pravidla neplatí. Tomu se snaží Evropská unie čelit zavedením povinností i pro mimoevropské firmy, které například cílí na evropské spotřebitele. Je však těžké si představit vymáhání povinností stanovených GDPR po firmách z druhého konce světa navyklých na zcela jiné standardy, a mnohdy i etiku podnikání.

Nejen povinnosti, ale i příležitosti

GDPR nepřináší jen povinnosti. V některých případech může být zpracování osobních údajů snazší. GDPR například nově umožňuje založit zpracování na základě „oprávněných zájmů“, přičemž těmito zájmy mohou být i subjektivní potřeby správce osobních údajů. Lze tak zpracovávat osobní údaje z více důvodů a zahrnout pod tento titul více zpracovatelských operací. Mezi taková zpracování pak může patřit například přímý marketing, prevence podvodů, předávání osobních údajů v rámci skupiny podniků nebo zpracování osobních údajů z důvodu zajištění

„V důsledku mohou dlouhodobě navyšovat ceny výrobků a služeb.“

síťové bezpečnosti.

Co to však znamená pro interní auditory?

Úkolem interních auditorů je pomáhat organizaci, aby mohla dosahovat svých cílů a obstát při naplňování svojí mise. Uspět však není jednoduché. Organizace se potýkají s tlakem od konkurence, regulátorů, zákazníků nebo vlivných zájmových skupin. Interní auditoři mohou sehrát klíčovou úlohu navigátora. Ten propočítává nejvhodnější trasy a vyhlíží při tom nejen zrádné útesy, ale také příznivý vítr, který může dodat firemní lodi tu správnou dynamiku.

Nejinak je tomu v souvislosti s ochranou osobních údajů. Interní auditoři by měli podávat ujištění, že rizika spojená se zpracováním osobních údajů jsou pod kontrolou. Současně by měli umět posoudit, zda tato kontrola není již přehnaná a zda odpovídá celkovému přístupu k rizikům uplatňovanému v dané organizaci. Od dobrého auditora se jistě také očekává, že poradí ohledně zlepšení stávajících procesů s ohledem na ochranu osobních údajů a upozorní na možné příležitosti včetně případných úspor.

Aby mohl interní auditor uvedené plnit, měl by mít obstojnou znalost principů právní úpravy GDPR, dobré praxe v ochraně osobních údajů a v bezpečnosti informací a povědomí o nejdůležitějších typických rizicích, která jsou se zpracováním osobních

„Vyhlíží přitom nejen zrádné útesy, ale také příznivý vítr.“

údajů spojena.

Čím by se tedy měl interní auditor zabývat?

1) Odpovědnost za ochranu osobních údajů v organizaci

Tak jako kapitán bezpečně vede svoji loď rozbouřenými vlnami, i projekt implementace GDPR či zavedený systém ochrany osobních údajů si zaslouží zodpovědné řízení. Interní auditor (případně jiný interní nebo externí odborník) může pomoci s navigací. O tom, kdy vyplout, kam až se vydat, však může rozhodnout jen zástupce vedení organizace mající potřebnou autoritu. Interní auditor by se měl zabývat tím, zda vedení nastavilo účinný rámec řízení rizik souvisejících se zpracováním osobních údajů a přiřadilo dílčí odpovědnosti a pravomoci kompetentním osobám.

2) Zásady ochrany osobních údajů

Interní auditor by měl prověřit, zda organizace přijala a v každodenní činnosti uplatňuje zásady ochrany osobních údajů, které popisují, jak jsou data shromažďována, používána a spravována. Tyto zásady by měly být vyjádřeny v interních politikách a směrnicích organizace. Východiskem je osm hlavních principů GDPR:

- Zákonnost – zpracovávat osobní údaje je možné pouze tehdy, pokud existuje alespoň jeden z právních titulů (důvodů) pro zpracování osobních údajů – souhlas, plnění smlouvy, plnění právní povinnosti, ochrana životně důležitých zájmů člověka, plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, oprávněné zájmy správce či třetí osoby.
- Transparentnost – důležitou zásadou ochrany osobních údajů je transparentnost vůči subjektům údajů (zaměstnancům, klientům apod.), a to ohledně způsobu shromažďování a použití osobních údajů. Všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Od organizací bude požadováno, aby informovaly zúčastněné subjekty údajů o důležitých aspektech zpracování osobních údajů.
- Omezení účelem – osobní údaje musí být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.
- Minimalizace – osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- Přesnost – osobní údaje musí být přesné a v případě potřeby aktualizované.
- Omezení uložení – osobní údaje musí být uloženy po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.
- Bezpečnost – organizace musí jí spravované osobní údaje chránit, ať už jde o informace v listinné, nebo elektronické podobě. V praxi to znamená, že přístup k těmto informacím mají mít jen oprávněné osoby, informace budou dostupné v okamžiku jejich potřeby a bude zajištěna jejich správnost a úplnost.
- Přístup založený na riziku – organizace musí hodnotit zamýšlené činnosti a procesy zpracování z hlediska rizik, které z těchto činností a postupů plynou pro práva a oprávněné lidí, jejichž osobní údaje mají být zpracovávány. Praktickým dopadem je nutnost zpracovat analýzu rizik.

„Ověření, že jsou kontroly přiměřené rizikům, patří mezi evergreeny interního auditu.“

3) Povědomí v oblasti ochrany osobních údajů

Jakmile jsou stanovena pravidla, musí být sdělena zaměstnancům, kteří osobní údaje zpracovávají. Tohoto cíle lze dosáhnout prostřednictvím videí, e-learningu, prezenčních školení, informačních schůzek, porad apod. Ty by měly být kombinovány s tipy a technikami pro zvyšování povědomí v oblasti bezpečnosti informací a kybernetické bezpečnosti. Dobrý interní auditor nezapomene prozkoumat, zda ke zvyšování povědomí v oblasti ochrany osobních údajů dochází, a možná také svým příkladem, podávanými informacemi a užitečnými radami ke zvyšování povědomí dále přispěje.

4) Evidence osobních údajů

Aniž by měla organizace přehled o zpracovávaných osobních údajích, nemůže účinně kontrolovat nakládání s těmito údaji. Vytvoření registru osobních údajů tak představuje základ pro zajištění souladu s GDPR a poskytuje první pohled na druhy a množství osobních údajů v rámci organizace. Interní auditor by měl zjistit, zda v organizaci takový registr existuje, jakým způsobem jej organizace vytvořila, co všechno registr obsahuje a jak je aktualizován. V registru by mělo být zaznamenáváno především:

- Kategorie zpracovávaných osobních údajů
- Účel zpracování
- Kategorie osob, jejichž osobní údaje jsou zpracovávány (zaměstnanci, klienti atd.)
- Kde (v jakých systémech) a jak jsou údaje zaznamenávány
- Kdo zodpovídá za shromažďování, aktualizaci a likvidaci údajů
- Doba, po kterou jsou údaje uchovávány

Pokud v organizaci neexistuje přehled zpracovávaných údajů nebo existují důvodné pochybnosti o jeho spolehlivosti, měl by auditor pro potřeby auditu provést vlastní průzkum. Mapování provedené interním auditorem se může později stát cenným zdrojem informací pro manažery, zvláště v úvodních fázích projektu implementace GDPR.

5) Řízení rizik a bezpečnostní opatření

Přístup založený na riziku umožňuje organizacím napnout síly směrem, kde je největší riziko. Pomáhá tak organizaci rozhodnout, kam alokovat omezené zdroje.

Předpokladem řízení rizik je řádně provedená analýza rizik. S tím GDPR počítá a dokonce uplatnění některých povinností je také přímo navázané na míru rizika spojeného se zpracováním osobních údajů.

Opatření přijatá k zajištění ochrany osobních údajů by měla být úměrná faktické citlivosti těchto údajů. Organizace by měla vždy brát v potaz potenciální újmu pro člověka, jehož osobní údaje zpracovává, v případě porušení povinností stanovených GDPR nebo zneužití těchto údajů. Samotná bezpečnostní opatření jsou obvykle kombinací organizačních a IT opatření a nástrojů. Jedná se například o směrnice, prováděcí postupy, role, hesla, opatření proti škodlivému software (viry) atp. Ověření, že jsou kontroly přiměřené rizikům, patří mezi evergreeny interního auditu.

6) Souhlasy se zpracováním osobních údajů

Souhlas je pouze jedním z právních titulů (důvodů), na kterém může být založeno zpracování osobních údajů. Byť to na první pohled nemusí být patrné, použití souhlasů jako právního titulu není jednoduché. Toto by měl také zohlednit interní auditor, když bude prověřovat systém ochrany osobních údajů.

V zásadě by organizace měla uvažovat o souhlasu teprve tehdy, pokud není dán jiný z právních titulů pro zpracování. Na použití a podobu souhlasu jsou kladeny náročné požadavky, a pro organizace není tak vždy lehké je naplnit. Nedodržení těchto požadavků může mít za následek i neplatnost souhlasu. V případě použití souhlasu by proto měl interní auditor ověřit, že:

- Není dán jiný právní důvod pro zpracování osobních údajů.
- Vyjadřuje-li se subjekt údajů ke zpracování osobních údajů a toto prohlášení se vztahuje i k jiným skutečnostem, že souhlas je od těchto jiných skutečností jasně oddělitelný.
- Je souhlas informovaný, tedy jsou poskytnuty všechny relevantní informace požadované GDPR.
- Je souhlas prokazatelný, tedy že organizace může bez pochybností prokázat, že jí byl souhlas řádně udělen.

7) Postupy pro vyřizování požadavků subjektů údajů

Subjekty údajů (zaměstnanci, zákazníci fyzické osoby atd.) se mohou na správce osobních údajů obracet s žádostmi, a uplatňovat tak svoje práva. Mezi tato práva patří:

- právo na přístup k osobním údajům, včetně kopií zpracovávaných osobních údajů,
- právo na přenositelnost osobních údajů,
- právo na opravu nebo výmaz osobních údajů,
- právo na omezení zpracování,
- právo vznést námitku proti zpracování.

Vyřídit požadavky je třeba ve lhůtě podle GDPR. Interní auditor by měl zjistit, zda organizace nastavila procesy, které zajistí efektivní a včasné vyřizování vznesených požadavků. Tyto postupy by měly zahrnovat postupy pro posouzení oprávněnosti žádosti, včetně ztotožnění žadatele, vyhledání, zpracování a předání informací. Nároky na efektivitu daných postupů, včetně případné potřeby zapojení automatizovaných nástrojů, se budou odvíjet od množství a složitosti (předpokládaných) požadavků.

8) Smlouvy s dodavateli – zpracovateli osobních údajů

GDPR rozlišuje mezi správci, kteří určují účel a zdroje pro zpracování, a zpracovateli (dodavatelé, kteří zpracovávají data na žádost a podle pokynů správce). Příkladem je externí mzdová účetní, která zpracovává osobní údaje (např. osobní údaje obsažené ve výplatních páskách) jako zpracovatel na žádost svých klientů, správců osobních údajů.

GDPR vyžaduje, aby správce a zpracovatel (pracující na žádost správce) uzavřeli písemnou smlouvu. V této smlouvě musí být jasně definovány role a povinnosti týkající se ochrany osobních údajů. Mezi tyto povinnosti spadá např. závazek zajistit mlčenlivost nebo poskytnout součinnost správci pro splnění správcovy povinnosti reagovat na oprávněné žádosti subjektů údajů. Už víte, kdo je ve vztahu k vaší organizaci zpracovatelem a zda máte se všemi zpracovateli uzavřenou zpracovatelskou smlouvu obsahující potřebné náležitosti?

9) Příprava na horší časy

Úřad pro ochranu osobních údajů, a případně také subjekty údajů, budou muset být informovány o narušení ochrany osobních údajů. Interní auditor by měl ověřit, zda jsou pro tyto účely zavedeny vhodné postupy. V rámci těchto postupů musí být evidovány a analyzovány zjištěné incidenty. Cílem je vyhodnocení závažnosti incidentu – na základě tohoto se rozhodne, zda je třeba informovat Úřad pro ochranu osobních údajů a subjekty údajů.

Odpovědnost organizace a výše případných pokut se bude odvíjet od toho, jaké úsilí organizace vynaložila k zabránění narušení osobních údajů, případně jaké kroky podnikla k vyřešení daného narušení.

Zaměstnanci, kteří budou v případě bezpečnostního incidentu vykonávat definované činnosti, by k tomu měli být řádně proškoleni.

10) Pověřenec pro ochranu osobních údajů

GDPR vytváří novou pozici pověřence pro ochranu osobních údajů. Pověřenec odpovídá za kontrolu dodržování zásad GDPR v rámci organizace. Pověřenec by měl vedení organizace také dávat doporučení k zajištění souladu s GDPR. Pověřenec se může také vyjadřovat k posouzení vlivu na ochranu osobních údajů, účinnosti bezpečnostních opatření, návrhům dohod se zpracovateli. Kromě toho může mít řadu dalších stálých úkolů jako je pořádání informačních schůzek týkajících se ochrany osobních údajů, prošetřování stížností v této oblasti a odpovídání na dotazy ohledně ochrany osobních údajů nebo prověřování bezpečnosti osobních údajů u třetích stran. Úřad pro ochranu osobních údajů může pověřence kontaktovat kvůli poskytnutí informací a pověřenec je povinen poskytnout součinnost.

Funkci pověřence musí zřídit všechny orgány veřejné moci a veřejné subjekty (např. obce, kraje, ministerstva). Jiné subjekty budou muset zřídit funkci pověřence, pokud je s jejich hlavní činností spojeno rozsáhlé zpracování osobních údajů. Do této kategorie budu spadat např. nemocnice, banky, pojišťovny, telefonní operátoři a další subjekty. Interní auditor by měl prověřit, zda je organizace povinna roli pověřence zřídit.

Z hlediska modelu tří linií obrany spadá pověřenec do druhé linie obrany. Úkolem interního auditora je zabývat se, jak je v organizaci role pověřence zajištěna a zda přispívá k ošetření příslušných rizik. Interní auditor by však měl také s pověřencem spolupracovat. Organizace tak může získat větší míru a rozsah ujištění a interní auditor může efektivněji pokrýt audit universe.

GDPR, příležitost se nebát!

Myšlenka realizovat audit připravenosti na GDPR vznikla na sklonku roku 2017, při tvorbě nového plánu interního auditu. Přiznávám, že mé preference zařadit do plánu na r. 2018 toto téma, byly stejným dílem vedeny analýzou rizik jako vlastním zájmem o danou problematiku.

Ing. Zdeňka Jarošová
Oddělení interního auditu
Ministerstvo spravedlnosti ČR
zjarosova@msp.justice.cz

Ministerstvo spravedlnosti při výkonu své působnosti nakládá s osobními údaji v širokém spektru jejich forem a účelů. Co do počtu zpracovaných osobních údajů se nepochybně nachází na vrcholu žebříčku ústředních správních orgánů.
V současnosti eviduje 126 agend, ve kterých dochází ke zpracování osobních údajů. Drtivá většina osobních údajů je spravována v informačních systémech.
Příprava auditu: konec roku 2017. Základním pomocníkem bylo prakticky jen znění evropského Nařízení, výstupy pracovní skupiny WP 29, několik málo odborných publikací na trhu a pár průkopnických článků na internetu. Pro naplnění účelu auditního šetření nepředstavoval zásadní překážku fakt, že novela zákona o ochraně osobních údajů, která podrobněji rozpracovává dílčí záležitosti, jež Nařízení upravuje obecnou formou, se nachází v legislativním procesu.

Zohlednit bylo třeba i specifika činnosti organizace spočívající ve skutečnosti, že z působnosti Obecného nařízení je vyloučeno zpracování osobních údajů za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Tento účel zpracování se v současnosti stále řídí Směrnicí Evropského parlamentu a Rady EU 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování

či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Samotné znění Nařízení GDPR je z pohledu metodologie auditu a stanovení cílů dílčích auditních ověřování pro auditora návodné. Díky tomu vznikly první check listy, jejichž úkolem bylo chronologicky mapovat realizaci klíčových aktivit nezbytných pro dosažení souladu s GDPR. Vznikly poměrně snadno, a v krátkém čase. S ohledem na specifičnost IT problematiky jsme pro ověření souladu v této oblasti vytvořili rozsáhlý check list, který reflektoval nejen požadavky Nařízení, ale rovněž platnou legislativu v oblasti kybernetické bezpečnosti.

„Zjištění, že tento ani obdobný dokument formálně neexistuje, představovalo pohled tvrdé realitě do tváře.“

Předběžné hodnocení rizik vycházelo ze znalosti vlastní organizace a rizik definovaných samotnými nositeli procesů, tzn. vedoucími jednotlivých útvarů ministerstva. Přiznávám, že obrovským benefitem pro mě, jako auditora, byl v 1. pololetí r. 2017, vykonaný audit kybernetické bezpečnosti.

Bez potřebné znalosti informačních technologií a procesů, ve kterých osobní údaje zpracováváme, nejsme schopni objektivně zhodnotit soulad praxe s požadavky Nařízení.

Při plánování auditu jsem, byť nevyřčeně, počítala s existencí projektu či plánu implementace Nařízení. Do nabytí účinnosti Nařízení zbývalo pět měsíců. Zjištění, že tento ani obdobný dokument formálně neexistuje, představovalo pohled tvrdé realitě do tváře. S ohledem na absenci projektu bylo třeba přizpůsobit metody auditu a zaměřit se na získávání potřebných informací způsobem, časově mnohem náročnějším – auditními rozhovory.

Objektivně nemohu říci, že by se tématu na ministerstvu zcela nevěnovala pozornost, tak, jak tomu bylo do poslední chvíle u mnoha jiných organizací veřejného sektoru. Provedení analýz zpracování osobních údajů a navazujících opatření k odstranění neshod bylo však ponecháno na samostatné odpovědnosti jednotlivých útvarů. Což se záhy projevilo, jako nefunkční.

Provedené předběžné šetření identifikovalo nedostatky spočívající v roztříštěnosti implementačních aktivit dané absencí jednotné koordinace a nevytvořenou komunikační strategií. Rovněž nalézt vhodného kandidáta a obsadit roli pověřence se počátkem roku 2018 stále nedařilo.

„Řízení rizik spojených s problematikou ochrany dat by nemělo být motivováno pouhou snahou administrativně splnit požadavky Nařízení.“

To samo o sobě představovalo riziko, že se pověřenec „z venku“ včas nezvládne detailně seznámit s vnitřními procesy organizace, ani se způsoby nakládání s osobními údaji, navíc v drtivé většině zpracovávanými v informačních systémech.

Aktivní zapojení pověřence do procesu implementace od počátku považuji za nezbytné i z důvodu, že obvykle kmenoví zaměstnanci čelí tlaku zaměřit svou pozornost prioritně na plnění vlastních pracovních úkolů vyplývajících ze strategických a legislativních úkolů.

Na základě výsledků předběžného šetření jsme byli schopni začátkem února podat vedení ucelenou informaci o aktuálním stavu připravenosti na účinnost Nařízení GDPR. Reportovali jsme nejvýznamnější rizika, která by svým zapůsobením negativně ovlivnila následující fáze implementace. Ve zprávě jsme se zejména zaměřili na problematiku vydefinování odpovědností, provedení komplexní analýzy osobních údajů, nastavení incident managementu, nastavení procesů a nástrojů pro vyřizování žádostí subjektů údajů, včetně potřeby včas upravit a uvést do praxe vnitřní předpisy organizace a splnit informační povinnost.

Ministr spravedlnosti se ztotožnil se závěry předběžného šetření a přijal příslušná organizační opatření. Zcela zásadní krok vedoucí k posunu představovalo určení koordinátora implementace. Vymezení odpovědností pak u všech přímo zainteresovaných zaměstnanců logicky zvýšilo zájem i dynamiku, potřebnou pro dosažení souladu s Nařízením v tak krátkém čase.

Následně jsme se dostali do fáze, kdy jsme rozsahem ověřovaných

skutečností předběhli samotnou implementaci. Z důvodu zachování efektivnosti bylo vhodné audit přerušit, a současně tím i poskytnout auditovaným časový prostor implementaci dokončit. K auditu jsme se opětovně vrátili počátkem měsíce dubna. V mezidobí naše check listy, obsahující přehled časově uspořádaných klíčových aktivit projektu implementace, současně posloužily koordinátorovi coby vodítko k vytvoření postupu prací – jednoduchého plánu implementace.

„Na závěr bych snad jen doporučila k auditu GDPR přistupovat s určitým nadhledem, držet se zásady přiměřenosti.“

Za základní předpoklady pro dosažení souladu se zásadami ochrany osobních údajů považuji funkční komunikaci v organizaci založenou na řízeném sdílení informací, vymezení odpovědností zaměstnanců za oblasti zpracování osobních údajů ve vnitřních předpisech a směrnicích.

Elementární odpovědnost za zpracování osobních údajů leží na jednotlivých zaměstnancích, kteří jsou bez výjimky z povahy pracovně-právního vztahu k zaměstnavateli (dle zák. č. 262/2006 Sb., zákoník práce, zák. č. 234/2014 Sb., zák. o státní službě, zák. č. 273/2008 Sb., o Policii ČR, zák. č. 555/1992 Sb., o Vězeňské službě a Justiční stráži ČR…), povinni dodržovat zásady ochrany osobních údajů.

Úspěšnou implementaci Nařízení do každodenní praxe organizace podmiňuje změna přístupu všech zaměstnanců spočívající v posílení vědomí potřeby nepřetržitě dodržovat zásady ochrany osobních údajů.

Měsíc před nabytím účinnosti Nařízení jsme auditní šetření nasměrovali na posouzení rozsahu a kvality provedeného mapování zpracování osobních údajů a problematiku správy dat v informačních systémech.

Koordinátor implementace zvolil cestu „sebehodnocení“, tzn. za provedení mapování výchozího stavu zpracování osobních údajů odpovídal v rámci své agendy vedoucí příslušného útvaru. Pro účely zaznamenání činností zpracování osobních údajů byly svépomocí na ministerstvu vytvořeny záznamové archy. Tyto archy rovněž v současnosti, po nabytí účinnosti Nařízení, plní funkci záznamu o zpracování dle čl. 30 Nařízení. Toto „smart řešení“ se mi osobně velmi líbilo a s upřímnou radostí jsem jej vyzdvihla v reportingu.

Získané souborné informace o zpracování osobních údajů byly koordinátorem (pracovní skupinou) posouzeny a zjištěné nesoulady zapracovány do souhrnného dokumentu včetně navržených opatření k odstranění neshod.

Nespornou výhodou sběru informací o zpracovávaných osobních údajích způsobem „sebehodnocení“ je detailní znalost odborné problematiky – agendy a dalších činností, v rámci kterých k nakládání s osobními údaji dochází. Znalost prostředí umožňuje

postihnout zpracování v co nejširším rozsahu. Naproti tomu tento způsob generuje i značné nevýhody, které jsme měli sami možnost v rámci provedených auditních ověřování odhalit. Vlivem individuálního výkladu Nařízení v kombinaci subjektivního hodnocení činností zpracování osobních údajů mohou být výstupní informace do určité míry zkresleny.

Otázku zákonnosti zpracování osobních údajů v prostředí ministerstva nebylo složité vyřešit. Pro zajímavost uvádím poměr jednotlivých titulů zpracování osobních údajů. Osobní údaje v rozsahu 64 % jsou zpracovávány v rámci plnění právní povinnosti, 17 % ve veřejném zájmu, 7 % jako oprávněný zájem (nástroje ochrany a ostrahy objektů…) a z 12 % v souvislosti s plněním smluvních vztahů.

V případě souběžného zpracování osobních údajů na základě více právních titulů nemusí být snadné určit ten převažující. Posuzování sporných případů je vhodné v organizaci zabezpečit nastavením jednotného postupu ve spolupráci s DPO.

V oblasti ověření správy dat v informačních systémech se doporučuji primárně opřít o bezpečnostní politiky organizace a následně o posouzení jejich dodržování v praxi. Pozornost je třeba věnovat identifikaci uložení dat povahy osobních údajů v prostředí IT, včetně datových toků. Zdokumentovat provazbu mezi daty a konkrétními informačními systémy, aplikacemi, síťovými disky, adresáři a jejich uživateli. Tento postup je nezbytný nejen pro prokázání souladu v případě šetření dozorovým orgánem, nýbrž i podmínkou pro systematický přístup k zabezpečení dat v informačních systémech včetně předpokladu pro naplnění práv subjektů údajů. Nespornou výhodou byla skutečnost, že se nevyužívá cloudových služeb.

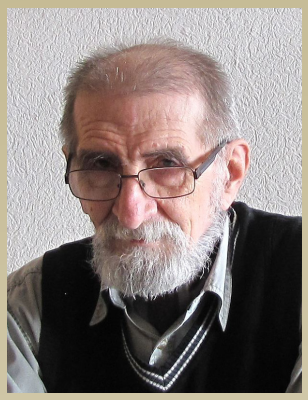
Řízení rizik spojených s problematikou ochrany dat by nemělo být motivováno pouhou snahou administrativně splnit požadavky Nařízení. Principem Nařízení je stanovení odpovědnosti za spravované osobní údaje založené právě na hodnocení rizik.

Poznatky a postřehy z auditu GDPR by vydaly na mnoho stran. Vlivem dynamického rozvoje masových komunikačních technologií narůstá potřeba data uživatelů dostatečně chránit. Nařízení pomohlo, doufejme, zvýšit i obecné povědomí veřejnosti o potřebě primárně vnímat, komu a jaká data o vlastní osobě poskytujeme. Význam auditů GDPR ruku v ruce s audity bezpečnosti IS v čase nepochybně poroste.

Na závěr bych snad jen doporučila k auditu GDPR přistupovat s určitým nadhledem, držet se zásady přiměřenosti. Někdy při výkonu auditu sklouzáváme k ověřování složitých mechanizmů, dlouhé hodiny trávíme studiem dokumentů, přitom opomeneme hned na počátku vnímat viditelné známky elementárních problémů v komunikaci, odpovědnostech, povědomí zaměstnanců o auditované problematice…

Přeji vám hodně úspěchů nejen při realizaci auditu ochrany osobních údajů! ■

Kolíkování nepřehledného terénu



PhDr. Václav Peřich, člen Čestného prezidia ČIIA od roku 1996

„Opoždění implementačních zákonů za dnem účinnosti obecného nařízení přispívá k nepříznivým postojům obecné veřejnosti vůči institucím EU a jejich výstupům.“

Nebývá to časté, aby preambule nějakého legislativního aktu zaujímala více než třetinu celkového normativního textu, jímž jsou upravována pravidla pro vymezený předmět působnosti. Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) shrnuje odůvodnění svého vydání ve 173 bodech na 37 stranách. Nemám v úmyslu podávat referát o celku těchto důvodů, chtěl bych však doporučit jeho co možná pečlivé prostudování zejména těm, kdo se rozčilují nad dalším příkladem „bruselského diktátu“ ve vztahu ke členským zemím EU.

V naší zemi je situace možná obzvlášť rozjitřená. Obecné nařízení nabylo u nás účinnosti stejně jako v ostatních členských zemích již 25. 5. 2018, zatímco vládní návrhy implementačních zákonů upravující související problematiku do souladu s českým právním pořádkem byly v Poslanecké sněmovně teprve ve fázi projednávání ve výborech před řádným druhým čtením. V době psaní tohoto článku je připraveno 12 usnesení sněmovních výborů k návrhu zákona o zpracování osobních údajů a sedm usnesení k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. Průběh projednávání obou návrhů zákonů si tak může vyžádat ještě poměrně dlouhý čas, i optimistické odhady předpokládají, že k účinnosti obou zákonů může dojít až ke konci roku 2018. Taková situace jistě není optimální a opoždění implementačních zákonů za dnem účinnosti obecného nařízení působí nejen řadu praktických problémů pro veřejné i podnikatelské zpracovatele nejrůznějších kategorií osobních údajů, ale hlavně přispívá k nepříznivým postojům obecné veřejnosti vůči institucím EU a jejich výstupům.

Předpokládám, že většina příspěvků tohoto čísla Interního auditora se bude věnovat spíše praktickým nebo technologickým aspektům řešení otázek kolem GDPR. Já bych se rád zaměřil spíše na celkové souvislosti, jejichž připomenutí by mohlo zmírnit převažující nevlídné přijetí nové úpravy pravidel v této oblasti.

Množství kritických hlasů je vznášeno zejména proti údajně nadměrné byrokratizaci zaváděné kvůli ochraně osobních údajů, avšak většina kritiků si pravděpodobně neuvědomuje, že jejich nespokojenost je hlavně projevem nesouhlasu se složitostí světa a tím, že pro většinu provozních situací v hospodářském a právním světě musíme být způsobilí takové situace co možná přesně popsat, a v případě potřeby zpětně přezkoumat jejich průběh. V některých oblastech jsme již na potřebu co možná objektivní přezkoumatelnosti navyklí (viz zásada audit trail neboli stopy pro audit), v jiných oblastech nás však potřeba podobně přesného dokumentování poněkud překvapuje. Ústavně a mezinárodními úmluvami chráněným právům obecně rozumíme, pojmy jako právo na soukromí a dále i právo na informace nejsou pro nás vlastně nic nového, mnoho nových věcí však přinesl rychlý technologický rozvoj a spolu s ním proměny mnoha oblastí hospodářského, veřejného, a dokonce také společenského života. Svoje osobní údaje z úředně stanovené povinnosti, v zájmu pohodlnějších nákupů či pro zapojení do sociální sítě, svěřujeme nejrůznějším provozovatelům, a dokonce jim (ať už vědomě, či bezděčně) dovolujeme vyhodnocovat naše preference, posloupnosti kroků a jiné jedinečné skutečnosti. Čas od času se pak dozvídáme, že někdo nahromaděné údaje různým způsobem zneužil, vyhodnocoval nekalým způsobem či postoupil zcela jinému zpracovateli, u něhož si nelze zacházení s našimi osobními údaji nijak kontrolovat či ovlivnit.

„Množství kritických hlasů je vznášeno zejména proti údajně nadměrné byrokratizaci.“

Proto je zcela nezbytné, aby se ochrana našeho ústavně zaručeného práva na soukromí odpovídajícím způsobem vyvíjela souběžně se způsoby a možnostmi uplatňování a zpracování osobních údajů. Také je tomu ze strany odborníků věnována pozornost už přes 20 let, a to jak u nás, tak v mezinárodním prostředí. Obecná veřejnost tématu věnuje pozornost teprve od velkých případů krádeží či úniků velkých objemů dat, případně po odhalení velkých kriminálních případů spojených se zneužitím osobních údajů. Z toho důvodu vlastně jen nemnoho zasvěcenců oceňuje vydání Obecného nařízení 2016/679 z 27. 4. 2016 jako nesmírně potřebný a užitečný krok, který nejenom posouvá nástroje ochrany osobních údajů na mezinárodní úroveň, ale přináší řadu antibyrokratických a racionalizačních novinek, které mohou při náležité implementaci usnadnit život všem činitelům v dané oblasti. V této souvislosti je nutno také ocenit přístup českého Úřadu pro ochranu osobních údajů, který hned od roku 2017 začal systematicky pracovat na přípravách implementace do zdejšího prostředí. V rámci své přednáškové, konzultační a metodické činnosti poskytuje informace na svých webových stránkách (www.uoou.cz), odpovídá na dotazy veřejnosti a postupně v rámci svých personálních možností zajišťuje širší okruh aktivit, včetně vzdělávacích. Ve své výroční zprávě za rok 2017 ÚOOÚ mj. uvádí, že lze vcelku vítat živelně vznikající širokou nabídku vzdělávacích a přípravně servisních prací pro správce a zpracovatele osobních údajů. Na druhé straně však někdy v těchto nabídkách konstatuje patrnou snahu vyvolat dojem, že pro správce a zpracovatele je nejlepší cestou k řešení použití outsourcingu. To má však základní úskalí ve skutečnosti, že příslušný správce či zpracovatel může podcenit potřebné analýzy, k nimž externí subjekt nemusí mít dostatečné podklady a zkušenosti. Také tím oslabuje svůj kontakt s okruhem subjektů, jejichž osobní údaje zpracovává. Přitom detailní znalost charakteru zpracovávaných osobních údajů a vnitřního fungování organizace je pro každé specifické podmínky klíčová.

Proto lze jak správcům a zpracovatelům, tak i všem subjektům poskytujícím osobní údaje ke zpracování jen doporučit, že by se měli v každém případě se základními principy GDRP seznámit alespoň tak, aby dobře porozuměli svému postavení a svým úlohám a aby svá vlastní rizika náležitě zhodnotili dříve, než začnou vyjednávat s případnými externími dodavateli. ■

Setkání interních auditorů a kontrolorů moravských měst

Ve dnech 17.–18. 5. 2018 se konalo v Lesním penzionu na Bunči již 10. odborné a vzdělávací setkání interních auditorů a kontrolorů moravských měst. Pořádajícím městem bylo Uherské Hradiště a celé toto pracovní setkání se konalo pod záštitou starosty města Uherské Hradiště Ing. Stanislava Blahy.

Mile nás překvapil zájem o toto setkání, kterého se zúčastnilo 45 interních auditorů a kontrolorů. Bylo nám ctí, že se našeho setkání zúčastnil ředitel ČIIA Ing. Dan Haüsler, Ing. Dana Ratajská, vedoucí oddělení interního auditu MMR ČR a kolegové z krajského úřadu Zlínského a Olomouckého kraje.

Na úvod tohoto setkání nás přijel pozdravit tajemník městského úřadu Uherské Hradiště Mgr. Josef Botek. V rámci své zdravice představil našim kolegům město Uherské Hradiště.

V rámci našeho odborného programu nás Ing. Dan Haüsler seznámil s novinkami v ČIIA, dále jsme viděli velmi přínosnou prezentaci problematiky spisové služby, spisového a skartačního řádu, kterou si pro nás připravila kolegyně z městského úřadu Šumperku, Ing. Jaroslava Kopová. Velkou část programu jsme věnovali, v dnešní době velmi aktuálnímu tématu, Obecnému nařízení o ochraně osobních údajů – GDPR. Dále jsme diskutovali o problematice řídicí kontroly u příjmů a marginálního porušení rozpočtové kázně a problematice veřejné finanční podpory, kterou prezentovala Ing. Dana Ratajská. V průběhu odborného programu jsme se také zabývali zajímavými podněty z veřejno-správních kontrol.

V rámci neformálního programu jsme měli naplánovanou tzv. auditní stopu na Brdo, což je nejvyšší vrchol pohoří Chřiby, ve kterém se nachází Lesní penzion. Vzhledem k tomu, že nám nepřálo počasí, tak jsme společně navštívili nedaleké poutní místo Velehrad a část osazenstva věnovala podvečer sledování zápasu naší hokejové reprezentace v rámci MS.

Večerní diskuze byly také trochu pracovní, protože nás přijel pozdravit pan starosta Ing. Stanislav Blaha.

Štafetu pro další ročník převzalo město Prostějov, tak se už všichni těšíme za rok na společné setkání. ■

Ing. Libuše Habartová

Ing. Petr Kheil
metodika interního auditu a vyhodnocování řídicího a kontrolního systému
Česká spořitelna, a.s.

Čeho si Petr povšiml *nejen* v legislativě

Pokud se ohlédnu za aktuálně publikovanými materiály pro naši profesi, výběr toho nejzajímavějšího by mohl vypadat následovně.

Novinky se v několika uplynulých měsících opět nesly na vlně další regulace pro finanční instituce. Přispěl k tomu významně Evropský orgán pro bankovnictví (European Banking Authority – EBA – *www.eba.europa.eu*), který publikoval pokyny k dalšímu posílení řízení rizik, k oblasti platebních služeb PSD2 a k oblasti outsourcingu. Pokud se zajímáte o problematiku platebního styku nebo máte na starosti audit IT, za pozornost stojí stanovisko (EBA-Op-2018-04) a konzultační dokument (EBA/CP/2018/09) s cílem poskytnout účastníkům trhu pomoc při implementaci principů založených na silné autentizaci zákazníků a bezpečné komunikaci. Požadavky pro další zvýšení bezpečnosti plateb v EU přinášejí pokyny **„Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)"** (EBA/GL/2018/05), které se týkají reportingu o vyhodnocování bezpečnostních událostí nebo hrozeb podvodů. EBA dále předložil do připomínkového řízení návrh pokynů **„Guidelines on outsourcing"** (EBA/CP/2018/11), které mají za cíl vytvořit harmonizovaný rámec pro uzavírání smluv o outsourcingu ve finančních institucích.

Na internetu IIA (*www.global.theiia.org*) byla publikována dvě **Stanoviska** (IIA Position Paper). Stanovisko **„Who Conformance Matters"** vychází ze skutečnosti, že interní audit musí fungovat na nejvyšší úrovni etických a odborných kompetencí. Soulad se standardy IIA je nezbytným předpokladem pro úspěšné naplnění úlohy interního auditu a posilování důvěryhodnosti interního auditu. Stanovisko **„Internal Auditing's role in corporate governance"** zmiňuje působení funkce interního auditu jako nepostradatelného zdroje podpory řádného řízení a správy společnosti, a to zejména v současné době, kdy se rizika stávají složitějšími. Působení interního auditu se bude muset rozšířit do oblastí, jako např. kultura a etika nebo udržitelnost.

Závěrem předkládám užitečnou informaci pro subjekty, ve kterých je zřízen výbor pro audit. Na konci července byly na stránkách Rady pro veřejný dohled nad auditem publikovány **Dotazníky ke zprávám o činnosti výborů pro audit** v CZ a EN verzi. Doprovodné informace jsou dostupné na *www.rvda.cz/metodika.*

Nač je třeba mladých íáčků* aneb dnešní dávka filozofie

Nezáleží na tom, zda se jako (mladý) íáček někdy cítíte, nebo se s tímto označením cítíte nesvá či nesvůj, nebo se tak zkrátka necítíte za žádných okolností. Spojuje nás stejná profese, podobné zaměření, možná i nátura, způsob myšlení, někdy starosti, a jindy zase radosti auditorského života.

Lucie Vašková
Sberbank CZ, a.s.

Právě teď, během dneška, zítřka či příští týden (to už je na vás), je možná vhodný čas na to se zamyslet, co pro profesi interního auditu mladá či mladší generace znamená a čím může být užitečná, a naopak co se od ní očekává a kam by se měla posunout.

Členové rady ČIIA byli tak laskaví, že na zvídavé otázky ohledně pohledu na mladé auditory, jejich slabosti, dovednosti a budoucnost, odpověděli. Reakce spojuje mnohé, kromě pojmů jako *pokračování, rozvoj, výzvy, nové myšlenky, nápady, obohacení* či *svěží vítr*, se objevil v odpovědích i *důvod snažit se držet krok* či *absence profesní slepoty*. Mladší generace může přinést nový vítr (jen aby to nebyla vichřice…) do auditu dané organizace, ale bez zkušených kolegů se ze začátku zkrátka neobejde.

Mladší generace může přinést nový vítr (jen aby to nebyla vichřice…) do auditu dané organizace, ale bez zkušených kolegů se ze začátku zkrátka neobejde.

* íáček/íáčko = interní auditor

Jak se říká, žádný učený z nebe nespadl. Mladým auditorům sice nemusí v dnešní době chybět sebevědomí a snaha, je však třeba zapracovat na sounáležitosti, svědomitosti, smyslu pro odpovědnost, pečlivosti, diplomatickém chování, vhodném vyjadřování, zkrátka a prostě profesně dozrát.

Zajímal by mě i váš názor. Pokud se o něj chcete podělit, napište nám na klubmladych@interniaudit.cz. ČIIA podporuje mladší generaci a její profesní rozvoj a růst formou Klubu Mladých Interních Auditorů. Dobrovolně, bezplatně, s odhodláním a úsměvem. Jaké s námi má Institut plány? Tomáš Pivoňka přál v roce 2015 internímu auditu hodně nových a mladých lidí k zajištění další živé budoucnosti a v roce 2016 plánoval propagaci interního auditu mezi mladou generací, neboť motto, které si vybral pro své druhé funkční období v čele ČIIA, bylo „zajistit úspěšnou budoucnost interního auditu“**. Svým slovům dostál.

A jak praví krásné české přísloví: „Co se v mládí naučíš, ke stáru jako když najdeš.“ Proto mě zajímá, co se teď mohu a optimálně mám naučit, abych to mohla ke stáru najít? Kde je budoucnost interního auditu a jak se na ni začít připravovat – třeba ještě dnes?

Členové rady ČIIA vidí budoucnost ve *větším využití moderních technologií a dat, ve větších nárocích na flexibitu auditu, v poradenské roli auditu uvnitř organizace, v trvalém vzdělávání a udržení pomyslného kroku napřed.*

Na toto téma můžeme najít i ve 23leté historii ČIIA a ve starších číslech časopisu několik odkazů, článků a rozhovorů. Co však všechny do značné míry spojuje, je znalost auditorů v oblastech řízení rizik, informačních technologií, pojmy jako digitální revoluce, informační systémy či datová analýza.

No a právě poslední zmíněné – datová analýza – byla předmětem jednoho z letošních setkání Klubu mladých. Za prakticky zaměřená setkání patří jejím autorům velké poděkování. A co vy? Rádi byste nás něčím obohatili ze svého oboru či letité praxe? I my budeme rádi. Ozvěte se nám. Prozatím alespoň přeji krásné letní/podzimní dny. ■

** http://www.interniaudit.cz/download/clenska-sekce/casopis/interniauditor-2015-03-3g44/files/assets/basic-html/page15.html

https://kariera.ihned.cz/c1-65314620-tomas-pivonka-reditel-utvaru-interni-audit-skupiny-cez-v-cele-ceskeho-institutu-internich-auditoru-ciia

Změny v certifikacích IIA

Vážené interní auditorky, Vážení interní auditoři, dovolujeme si vás touto cestou informovat o několika změnách v mezinárodních certifikacích. Změny plánované ze strany Mezinárodního institutu interních auditorů (dále jen IIA) se dotknou certifikačních programů Certified Internal Auditor (CIA), Certification in Risk Management Assurance (CRMA), Certified Financial Services Auditor (CFSA), Certification in Control Self-Assessment (CCSA) a Certified Govermnment Auditing Professional (CGAP) a čekají nás již od ledna roku 2019. V případě, že disponujete některou z těchto mezinárodních certifikací, jste právě v certifikačním procesu anebo o certifikaci uvažujete, věnujte prosím této informaci zvýšenou pozornost.

V případě nejžádanějšího certifikačního programu CIA dojde od ledna 2019 ke změně struktury zkoušek v anglickém jazyce (viz Obrázek č. 1). Od roku 2020 pak nebude možné zkoušky skládat v českém jazyce. Certifikační programy CFSA a CGAP nebudou od ledna roku 2019 vůbec nabízeny. Zkouška CCSA bude sloučena se zkouškou CRMA.

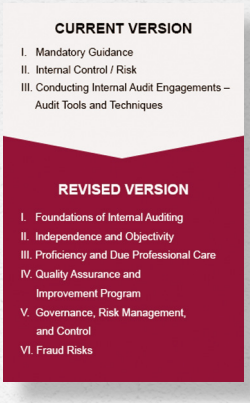
Základní přehled změn je zobrazen v níže uvedené tabulce č. 1 a dále uvádíme další základní informace a návody, jak postupovat u konkrétních certifikací.

tabulka č. 1

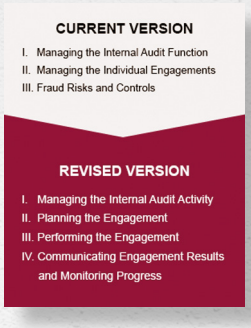
CERTIFIKACE	2018	2019	2020
CIA	Beze změny	Změna struktury zkoušky v AJ a ostatních jazycích, které IIA zachová po roce 2020.	**Do konce roku 2019 možno složit v českém jazyce. Od ledna 2020 bude ukončena čeština ve zkouškách.**
CRMA Certification in Risk Management Assurance™	Beze změny	Změna obsahu zkoušky, sloučení s CCSA	
CGAP Certified Government Auditing Professional®	Registrace možná do prosince 2018	Součást CRMA	
CFSA Certified Financial Services Auditor®	Registrace možná do prosince 2018	Zrušení	
CCSA Certification in Control Self-Assessment®	Registrace možná do prosince 2018	Zrušení	

obrázek č. 1

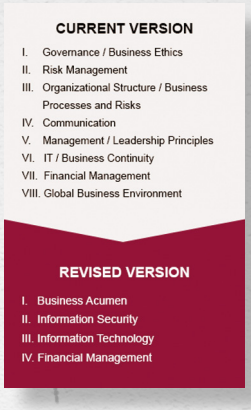
CIA Exam Part One: Essentials of Internal Auditing



CIA Exam Part Two: Practice of Internal Auditing



CIA Exam Part Three: Business Knowledge for Internal Auditing



CIA

V případě že disponujete certifikací CIA, nic se pro Vás nemění. Požadavky, pro hlášení CPE hodin, zůstávají beze změny. Jestliže uvažujete o registraci do certifikačního programu CIA anebo jste již registrovaný kandidát a skládáte zkoušky, plánované změny se Vás pravděpodobně mohou týkat.

Pokud chcete zkoušky skládat v českém jazyce, jednou z nejzásadnějších změn je právě to, že čeština nebude od ledna roku 2020 ve zkouškách dostupná. Ač jsme se od počátku roku 2018, kdy nám byla informace sdělena, snažili s IIA o zachování českého jazyka ve zkouškách CIA intenzivně vyjednávat, bohužel bude český jazyk společně s několika dalšími jazyky (např. polština) ze zkoušek odebrán. Od ledna 2020 budou zkoušky dostupné pouze v aktualizované verzi v angličtině a dalších nabízených jazycích.

Pro kandidáty, kteří skládají zkoušky v angličtině, nastane změna již počátkem roku 2019. IIA provedl analýzu, která ukázala na to, že je třeba obsah a strukturu zkoušky aktualizovat. Důvodem byl i problém s nevyvážeností jednotlivých částí zkoušky a v některých případech i duplikace zahrnutých témat. Detailnější popis změn a harmonogram aktualizace průběžně naleznete na webových stránkách ČIIA.

CRMA

Změny v CRMA programu se týkají pouze kandidátů o tento certifikační program nikoli certifikovaných. Při další aktualizaci se zkouška CRMA spojí se zkouškou CCSA a dojde k rozšíření požadavků na znalosti kandidáta o certifikaci. O konkrétním termínu sloučení zkoušek a konkrétních změnách budeme všechny kandidáty informovat, zatím bohužel neznáme detailnější popis a harmonogram.

CGAP, CFSA, CCSA

Pokud disponujete některou z certifikací CGAP, CFSA anebo CCSA, certifikace Vám zůstává a je Vaší povinností každoročně hlásit CPE hodiny pro její udržení.

Pokud jste v současné době registrovaným kandidátem certifikací CGAP, CFSA anebo CCSA platí, že se můžete pokusit o složení zkoušky do termínu platnosti jejich registrace. Pokud se Vám podaří zkoušku úspěšně složit do 31. prosince 2018 a stanete se certifikovaným, dostanete možnost se posléze registrovat ke zkoušce CIA Challenge Exam (viz. níže).

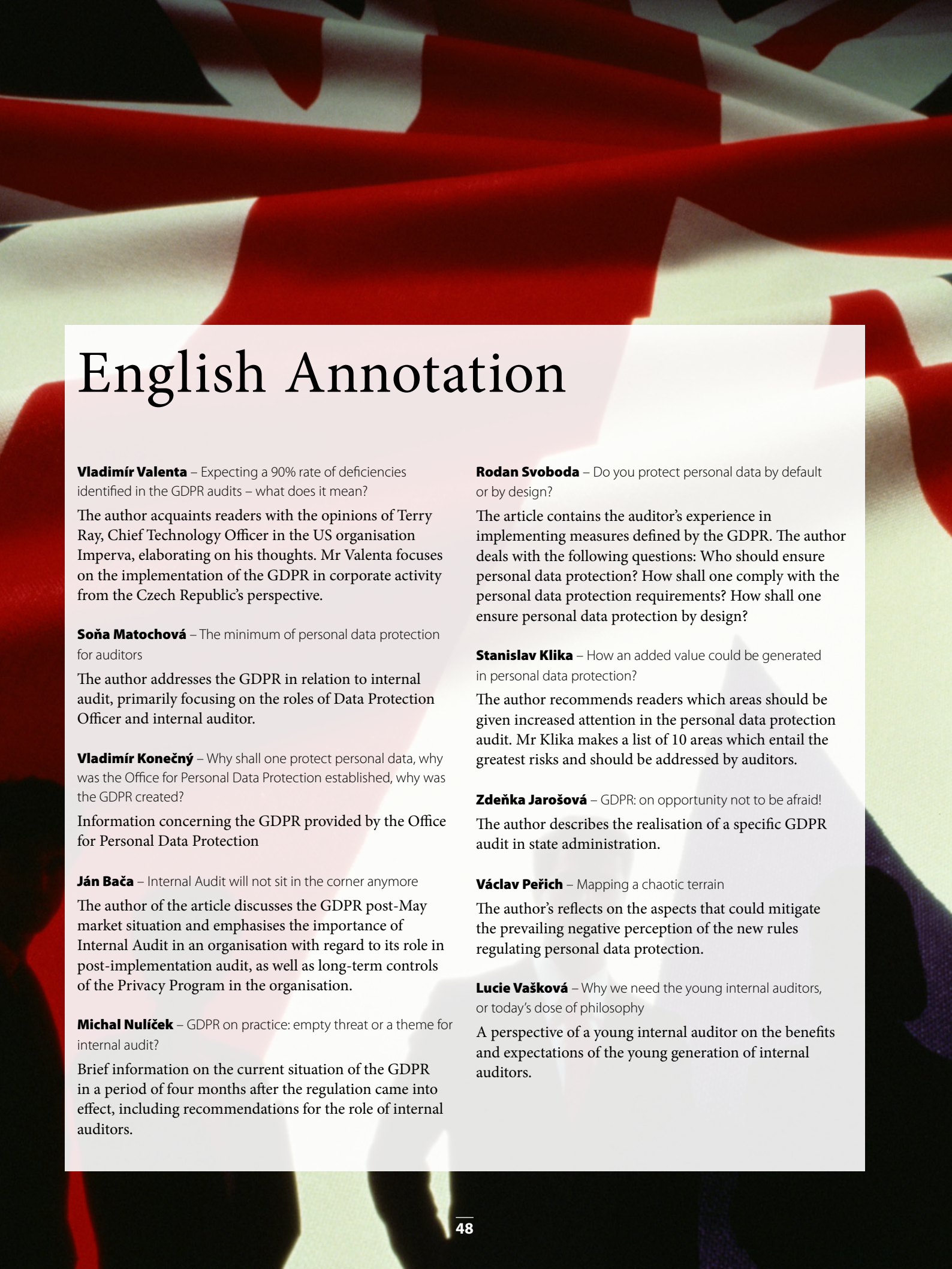
Registrace k certifikacím CGAP, CFSA anebo CCSA nebude od 1. ledna 2019 možná. Pokud uvažujete o registraci do některého z těchto certifikačních programů, prosíme o zaslání vyplněné přihlášky se všemi požadovanými přílohami nejpozději do pondělí 17. prosince 2018, pozdější registrace nebudeme moci včas zpracovat.

V případě, že nedisponujete certifikací CIA, tak IIA pro Vás připravil **CIA Challenge Exam**, kterým Vám dává možnost získat certifikaci CIA, a to jednoduše složením jedné zkoušky. Možnost registrace k CIA Challenge Exam je pouze pro certifikované CGAP, CFSA anebo CCSA, kteří jsou aktivní a dále pro ty, kteří se stanou certifikovanými do 31. prosince 2018. Zkouška CIA Challenge Exam byla vyvinuta na základě rozdílů mezi požadavky ke zkouškám CCSA, CGAP a CFSA a požadavky ke zkoušce CIA s důrazem na Mezinárodní rámec profesní praxe IA (IPPF). Registrace k CIA Challenge Exam bude dostupná od dubna 2019 do prosince 2020. Více informací naleznete s blížícím se termínem na našem webu.

Věříme, že Vám tyto informace budou užitečné a v případě potřeby neváhejte kontaktovat kancelář ČIIA.

Za Radu ČIIA
Mgr. *Tomáš Pivoňka, CIA, CRMA prezident ČIIA*
a *Ing. Petr Hadrava, ACCA, CIA, CISA, CFSA člen Rady ČIIA*

Za Kancelář ČIIA
Ing. Daniel Häusler a Tereza Štětinová



English Annotation

Vladimír Valenta – Expecting a 90% rate of deficiencies identified in the GDPR audits – what does it mean?

The author acquaints readers with the opinions of Terry Ray, Chief Technology Officer in the US organisation Imperva, elaborating on his thoughts. Mr Valenta focuses on the implementation of the GDPR in corporate activity from the Czech Republic's perspective.

Soňa Matochová – The minimum of personal data protection for auditors

The author addresses the GDPR in relation to internal audit, primarily focusing on the roles of Data Protection Officer and internal auditor.

Vladimír Konečný – Why shall one protect personal data, why was the Office for Personal Data Protection established, why was the GDPR created?

Information concerning the GDPR provided by the Office for Personal Data Protection

Ján Bača – Internal Audit will not sit in the corner anymore

The author of the article discusses the GDPR post-May market situation and emphasises the importance of Internal Audit in an organisation with regard to its role in post-implementation audit, as well as long-term controls of the Privacy Program in the organisation.

Michal Nulíček – GDPR on practice: empty threat or a theme for internal audit?

Brief information on the current situation of the GDPR in a period of four months after the regulation came into effect, including recommendations for the role of internal auditors.

Rodan Svoboda – Do you protect personal data by default or by design?

The article contains the auditor's experience in implementing measures defined by the GDPR. The author deals with the following questions: Who should ensure personal data protection? How shall one comply with the personal data protection requirements? How shall one ensure personal data protection by design?

Stanislav Klika – How an added value could be generated in personal data protection?

The author recommends readers which areas should be given increased attention in the personal data protection audit. Mr Klika makes a list of 10 areas which entail the greatest risks and should be addressed by auditors.

Zdeňka Jarošová – GDPR: on opportunity not to be afraid!

The author describes the realisation of a specific GDPR audit in state administration.

Václav Peřich – Mapping a chaotic terrain

The author's reflects on the aspects that could mitigate the prevailing negative perception of the new rules regulating personal data protection.

Lucie Vašková – Why we need the young internal auditors, or today's dose of philosophy

A perspective of a young internal auditor on the benefits and expectations of the young generation of internal auditors.

Nejste si jisti při uveřejňování závazků do Registru smluv?

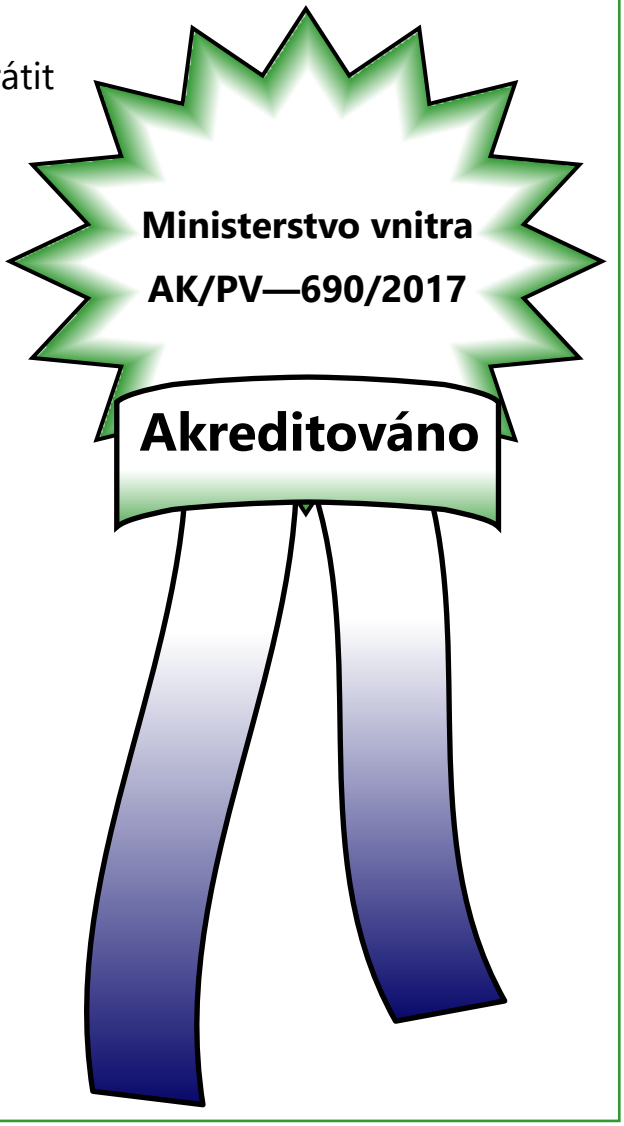
Nechce se vám platit za drahá, celodenní a neosobní školení?

Máte nového zaměstnance, který nezná problematiku Registru smluv?

Využijte našich akreditovaných e-learningových kurzů!

Proč zvolit akreditovaný e-learningový kurz:

1. dostupná cena,
2. čas strávený kurzem se započítá do průběžného vzdělávání,
3. snadné objednání přes internet,
4. bez nutnosti cestovat,
5. při řešení obtížného případu se můžete obrátit na naše certifikované interní auditory ve veřejné správě.



E-learningové kurzy naleznete na:

www.dynatech.cz/vzdelavani

DYNA® TECH

General **D**ata **P**rotection **R**egulation