Všeobecné nariadenie o ochrane osobných údajov a ich požiadavky na kľúčové procesy v organizácií

Bc. Nikola Oboňová

Diplomová práce

2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Nikola Oboňová**
Osobní číslo:	**A16546**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Obecné nařízení o ochraně osobních údajů a jeho požadavky na klíčové procesy v organizaci**
Téma anglicky:	**General Data Protection Regulations and Their Requirements for Key Processes in Organisations**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma GDPR.**
2. **Popište požadavky na klíčové procesy k zajištění shody s podmínkami GDPR.**
3. **Navrhněte postup řízení procesů pro interní audit organizace z pohledu GDPR.**
4. **Aplikujte vlastní návrh řešení ve zvolené organizaci dle možností.**
5. **Vyhodnoťte zvolené řešení a jeho reálnou replikovatelnost.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.**
2. **NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.**
3. **NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.**
4. **SOMMERVILLE, Ian. Softwarové inženýrství. Brno: Computer Press, 2013, 680 s. ISBN 9788025138267.**
5. **Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.**
6. **Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR – obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů : redakční uzávěrka 28.8.2017. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.**

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **1. prosince 2017**

Termín odevzdání diplomové práce: **16. května 2018**

Ve Zlíně dne 11. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Mgr. Roman Jašek, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 11.05.2018

Oloňová

.....

podpis diplomanta

ABSTRAKT

Diplomová práca sa zaoberá všeobecným nariadením o ochrane osobných údajov (angl. General Data Protection Regulation, čiže GDPR). Ide o novú revolučnú legislatívu EÚ, ktorá výrazne zvýši ochranu osobných údajov občanov. GDPR je komplexná norma s ďalekosiahlymi dopadmi. Je tvorená viacerými časťami dotýkajúcimi sa organizácií na všetkých úrovniach. Je viac ako školenie zamestnancov, riadenie dát alebo bezpečnosť informácií. Cieľom práce je definovať požiadavky na kľúčové procesy a navrhnúť postup na zabezpečenie zhody s podmienkami GDPR. Súčasťou práce bude aj návrh vhodného postupu na riadenie procesu pri internom dátovom audite organizácie.

Kľúčové slová: GDPR, ochrana osobných údajov, návrh, audit, informačné technológie

ABSTRACT

The diploma thesis deals with the General Data Protection Regulation (GDPR). It is a new revolutionary EU legislation that will significantly increase the protection of citizens' personal data. GDPR is a comprehensive standard with far-reaching implications. It is made up of many parts of organizations at all levels. It is more than employee training, data management, or information security. The aim of the thesis is to define requirements for key processes and to propose a procedure for ensuring compliance with GDPR conditions. Part of the work will also be a proposal for an appropriate procedure for managing the internal data audit of the organization.

Keywords: GDPR, protection of personal data, design, audit, information technology

Chcem sa poďakovať svojmu konzultačnému vedúcemu prof. Mgr. Romanovi Jašekovi, Ph.D. za cenné rady, odbornú pomoc a konzultácie, ktoré mi poskytol pri vypracovaní diplomovej práce. Osobitné poďakovanie patrí mojej rodine a priateľom za podporu počas celého štúdia. Tiež sa chcem poďakovať pedagogickým pracovníkom a vedeniu univerzity Tomáše Bati v Zlíne za nadobudnuté vedomosti počas celého štúdia. Nakoniec sa chcem poďakovať hotelu Elizabeth, kde pracujem, za umožnenie študovať a upravovať si pracovný čas a za poskytnutie informácií počas celého štúdia.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahratá do IS / STAG sú totožné.

OBSAH

ÚVOD

GDPR (anglicky General Data Protection Regulation) je všeobecné nariadenie na ochranu osobných údajov. Ide o nariadenie Európskej únie, ktoré nahrádza a upravuje doterajší zákon o ochrane osobných údajov. Tento súbor ucelených pravidiel na ochranu dát nadobudne účinnosť 25.5.2018, kedy musia všetci zjednotiť informačné systémy a postupy pri práci s údajmi v súlade s GDPR. V rámci Európskej Únie je ich tok podporovaný a nariadenie predstavuje vysokú ochranu pred zneužitím citlivých informácií. GDPR je použiteľné vo všetkých členských štátoch bez ohľadu na vnútroštátnu právnu úpravu. Zjednodušene povedané dochádza k významnému sprísneniu regulácie v oblasti spracovania osobných údajov. Nová európska norma si vyžaduje úpravu existujúcich procesov, ako aj povinnú implementáciu množstva ďalších opatrení a veľmi komplexný prístup k celej problematike ochrany informácií. Vznikajú nové povinnosti v rámci automatizovaného spracovania dát vedúce k väčšej transparentnosti a predovšetkým bezpečnosti. Je nevyhnutné komplexne prepojiť všetky oblasti bezpečnosti IT, bezpečnosti fyzickej, administratívnej, organizačnej a procesnej, aby ochrana osobných údajov fungovala ako jednotný systém.

Diplomová práca si kladie za cieľ zoznámiť organizácie s problematikou ochrany osobných údajov, objasniť hlavné pojmy, ale tiež pomôcť lepšie sa orientovať v povinnostiach, ktoré pre nich GDPR stanovuje. Po prečítaní tejto práce by mali byť schopní vyznať sa v pojmoch ako osobný údaj, správca či spracovateľ, poznať základné zásady ochrany osobných údajov, všeobecne posúdiť dôsledky nariadenia na ich prostredie a rozhodnúť sa, akým spôsobom budú ďalej postupovať.

Cieľom práce je definovať požiadavky na kľúčové procesy a navrhnúť postup na zabezpečenie zhody s podmienkami GDPR. Súčasťou práce bude aj návrh vhodného postupu na riadenie procesu pri internom dátovom audite organizácie.

Prvá kapitola diplomovej práce predstavuje zoznámenie sa so základnými pojmami nariadenia GDPR. Je potrebné poznať základné termíny pre pochopenie a správny výklad nariadenia, prečo vzniklo, koho sa týka a aké sú dôsledky nedodržania povinností.

V druhej kapitole popisujeme požiadavky na kľúčové procesy k zaisteniu zhody s podmienkami GDPR. Definujeme význam analýzy, posúdenie vplyvu na ochranu osobných údajov a implementáciu do praxe.

V tretej časti navrhujeme postup pre interný audit organizácie a priebeh auditu.

Štvrtá kapitola definuje aplikovanie vlastného návrhu vo zvolenej organizácií. Detailne popisuje povinnosti spoločností a podnikateľov, práva dotknutých osôb a zmeny v oblasti spracovania osobných údajov na praktických príkladoch. Zaoberá sa bezpečnosťou a zálohovaním dát, technickými opatreniami a novými technológiami v rámci GDPR. Vlastný návrh popisuje kompletný faktický stav a opatrenia z hľadiska zodpovedných osôb, zásad spracovania údajov, fyzickej ako aj IT bezpečnosti, archivácie, kontrolnej činnosti, likvidácie a i. zavedené v zariadení v rámci prípravy na GDPR.

Posledná kapitola je venovaná vyhodnoteniu zvoleného riešenia a jeho reálnej replikovateľnosti. Definuje prínosy vzniku nariadenia ako aj jeho negatívne dopady.

Dôvodom výberu tejto témy je aktuálnosť problematiky a potreba uceleného postupu na zabezpečenie zhody s podmienkami GDPR.

Pre každú spoločnosť, ktorá spravuje citlivé informácie je ochrana súkromia veľkým problémom. S príchodom GDPR pre všeobecnú ochranu osobných údajov je spracovanie osobných údajov dôležitejšie ako nikdy predtým.

I. TEORETICKÁ ČASŤ

1 GDPR

GDPR (anglicky General Data Protection Regulation) je nariadenie európskeho parlamentu a Rady EÚ 2016/679 schválené 27.04.2016, ktoré zavádza nové pravidlá ochrany fyzických osôb v oblasti spracovania osobných údajov a o voľnom pohybe týchto dát, ktorým sa zrušuje smernica 95/46/ES. Ide o najviac skompletizovaný súbor pravidiel pre zvýšenie ochrany dát občanov. GDPR sa v rámci EÚ uplatní jednotne. Zavádza nové povinnosti, príprava vyžaduje veľa času a zásadne sprísňuje pravidlá ich správy. GDPR vstúpi do platnosti v rámci celej EÚ od 25. mája 2018. [15]

Charakteristickou vlastnosťou sú jednotné pravidlá pre spracovanie údajov a univerzálna použiteľnosť v štátoch EÚ, Nórsku, Lichtenštajnsku a na Islande. Dôležité je zanalyzovať všetky oblasti, na ktoré nariadenie vplýva. GPRS zaisťuje kybernetickú bezpečnosť, nastavenie procesov vnútri firmy, šifrovanie údajov, zaistenie pseudonymizácie alebo bezpečnosť tlačového prostredia. [12]

1.1 Osobný údaj

Nariadenie definuje osobný údaj ako všetky informácie o fyzickej osobe, na základe ktorých vieme danú osobu priamo alebo nepriamo na základe získaného údaju identifikovať. Jedinečným údajom je meno, identifikačné číslo, IP adresa alebo údaj o lokalizácií danej osoby. [16]

1.2 Spracovávanie osobných údajov

Rozumie sa akákoľvek činnosť alebo sústava činností, ktoré spracovateľ alebo správca vykonáva s osobnými údajmi automatizovane alebo iným spôsobom. Pod týmto pojmom sa rozumie hlavne zhromažďovanie, ukladanie na nosiče, úprava, zmeny, sprístupnenie a vyhľadávanie. Taktiež používanie, šírenie, predávanie, uchovávanie, zverejňovanie, triedenie, blokovanie a likvidácia. [1]

1.3 Poverenec pre ochranu osobných údajov

Toto poverenie je jedným z nových prostriedkov ochrany dát. Nie je dôležitý počet zamestnancov vo firme pre jeho vymenovanie, ale splnenie jednej z troch podmienok. Vtedy správca určí v organizácií osobu, ktorá sa bude ochrane údajov venovať. Samozrejme, aj keď sa nás dané podmienky netýkajú, môžeme si ho zvoliť dobrovoľne,

ak je to užitočné. Mali by sme mať určenú osobu, ktorá sa bude ochrane dát venovať. Správca môže určiť aj necertifikovanú osobu. Poverenec by mal mať odborné znalosti práva a schopnosť plniť úlohy definované nariadením. [7]

1.4 Rozdiel medzi GDPR a novým zákonom o ochrane osobných údajov

GDPR má prednosť pred všetkými európskymi zákonmi o ochrane osobných údajov. Tie budú mať najmä doplnkovú funkciu. 30.01.2018 bol prijatý nový zákon o ochrane osobných údajov č. 18/2018 Z.z., ktorý nahrádza v súčasnosti platný a účinný zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Rieši najmä oblasti, ktorým sa GDPR nevenuje a podrobnejšie upravuje niektoré pravidlá ochrany osobných údajov. Začne platiť rovnako ako GDPR od 25.05.2018 a občanom uľahčí prístup k vlastným osobným údajom, ktoré o nich firmy zhromažďujú. [9]

1.5 Dôvod vzniku GDPR

Cieľom obecného nariadenia je zaistenie harmonizovaného právneho rámca ochrany dát, ktoré doteraz spôsobovalo správcom pôsobiacim vo viacerých zemiach problémy. Snahou je dosiahnutie zjednoteného výkladu nariadenia ako aj posilnenie práv občanov a vrátenie im kontroly nad osobnými údajmi spať do rúk. Dôvodom je taktiež prispôsobenie ochrany osobných údajov dnešnej dobe, pretože spracovanie dát je komplexnejšie ako pred desiatkami rokov. Zavádza pravidlá týkajúce sa voľného pohybu údajov v rámci EÚ aj mimo nej. [12]

1.6 GDPR a IT technológie

Nariadenie predstavuje viaceré požiadavky týkajúce sa informačných systémov. Zložitými systémovými zmenami je vo svojej podstate napríklad právo na prenos alebo výmaz osobných údajov a právo na obmedzenie spracúvania. Právo na prístup k osobným dátam predpokladá extrakciu dát z databázy na základe vopred stanovených pravidiel. Právo na výmaz predpokladá nastavenie retenčných periód. Je potrebné zabezpečiť implementáciu technických opatrení takým spôsobom, aby priniesli očakávaný výsledok. Okrem iného je potrebné vypracovať bezpečnostné opatrenia na informačné systémy na základe auditu, technické opatrenia zamerané na fyzickú ochranu a na informačno-

technologickú ochranu systému, organizačné opatrenia, personálne opatrenia, zálohovanie, likvidáciu osobných údajov ako aj kontrolný mechanizmus. [18]

1.7 Koho sa GDPR týka

GDPR sa vzťahuje na skoro každého podnikateľa, súkromnú či verejnoprávnu organizáciu. Dotkne sa spoločností a inštitúcií pôsobiacich v rámci EÚ ako aj zahraničných subjektov spracovávajúcich ,,európske,, osobné údaje.

GDPR sa týka širokého spektra komerčných firiem, spracovateľov a správcov osobných údajov, tiež orgánov štátnej správy alebo nimi zriaďovaných organizácií. Teda každého, kto pracuje s osobnými údajmi. Výhodou je, že takisto občania sa môžu brániť voči nezákonnému zaobchádzaniu s osobnými údajmi. [16]

Ide o väčšie spoločnosti aj menšie firmy, ktoré využívajú údaje o svojich klientoch, dáta pre marketingovú činnosť, rozosielanie newsletterov, zbierajú informácie o správaní svojich zákazníkov, vlastnia e-shop, hotel či kamerový systém. Zahŕňa spoločnosti s dochádzkovým systémom svojich pracovníkov alebo pacientov, uchádzačov o prácu, databázu klientov, subjekty, ktoré zálohujú a archivujú dáta či zmluvy alebo šifrujú údaje. Týka sa teda všetkých firiem, ktoré majú osobné údaje uložené na serveroch, posielajú ich po sieťach do dátových úložísk a využívajú rôzne aplikácie. Dotkne sa až 530 tisíc subjektov na Slovensku a zmeny v systémoch a procesoch si vyžiada vyše 40 miliónov eur. [11]

1.7.1 Cieľová skupina

• Riaditelia a manažéri

• Právni poradcovia a personalisti

• Správcovia dát, databáz, operátori

• Vedúci IT, bezpečnosti, marketingu

• Štatutárne orgány spoločnosti a prokuristi

• Úradníci verejnej správy, neziskových organizácií

• Poverenci pre ochranu osobných údajov | Data Protection Officer (DPO) [17]

1.8 Koho sa GDPR netýka

Nariadenie GDPR sa nevzťahuje na osobné údaje právnických osôb, spracovanie pre účely historického alebo vedeckého výskumu, účely archivácie vo verejnom záujme alebo spracovania anonymných údajov pre výskumné alebo štatistické účely. Pravidlá sa nedotknú súdov, cirkvi, osobných dát mŕtvych osôb, anonymizovaných dát, aktivít vzťahujúcich sa na trestné činy, národnú bezpečnosť či činnosti osobnej povahy alebo aktivity vykonávané výhradne v domácnosti. [26]

1.9 Kedy začne GDPR platiť

Nariadenie GDPR bolo prijaté v roku 2016 a jeho platnosť začína od 25.5.2018. Dovtedy by sa všetci, ktorých sa to týka, mali zoznámiť a včas pripraviť na nové pravidlá. Opatrenia môžu firmám zabrať aj niekoľko mesiacov, keďže okrem úpravy a spracovania dokumentácie môže ísť aj o zmenu nastavení IT systémov alebo prijatí technicko – organizačných krokov. [8]

1.10 Odborný audit

Spoločnosti budú musieť podstúpiť audit všetkých informačných systémov, revíziu spracovávaných údajov, prehodnotenie nastavení procesov a taktiež zmlúv, ktorých sa týka spracovanie osobných údajov. Preškolenie všetkých pracovníkov a oboznámenie ich s podmienkami spracúvania osobných údajov je absolútnou nevyhnutnosťou. [25]

Pre firmy môže byť nastavenie nových predpisov a posúdenie súladu s nariadením problémom. Riešenie ponúkajú odborní audítori, ktorí sa venujú analýze spracovania údajov. Väčšie spoločnosti by mali audit vykonať čím skôr, nakoľko zavedenie nových systémov a bezpečnostných procesov môže byť náročné na čas. Výsledkom auditu je nájdenie všetkých nedostatkov a navrhnutie vhodných zmien alebo riešení. [12]

1.11 Poskytovateľ auditu

Garanciu zhody s GPRS nám zabezpečí jedine komplexné posúdenie. Je potrebné nájsť spoľahlivého dodávateľa, ktorý overí všetky potrebné údaje v zmluvách, šablónach dokumentov alebo firemných smerniciach. Rozsah auditu je zásadný. Ideálny poskytovateľ preverí z bezpečnostného hľadiska nielen používané technológie, ale aj softwarové nástroje, dátovú databázu, úložisko a akúkoľvek manipuláciu s ich osobnými

údajmi vo firme. [12]

1.12 Sankcie

GPDR zavádza niekoľkonásobne vyššie pokuty ako doteraz. Subjekty budú sankciované za nepripravenosť, porušenie alebo ignorovanie nariadení. Horná hranica pokuty je 20.000.000 euro alebo 4% obratu firmy za jeden rok. Ak spoločnosť nevykonáva princípy a povinnosti vyplývajúce z GDPR, maximálna výška pokuty môže byť udelená rovnako malej firme, tak aj nadnárodnej spoločnosti. Závisieť bude taktiež na závažnosti porušenia, dĺžky nedodržiavania nariadení, povahy, poškodených občanov a rade iných. Môže ísť napríklad o porušenie podmienok súhlasu so spracovaním osobných údajov alebo porušenie zásad prenosu dát mimo územia EÚ. Závažnejšími problémami však môžu byť žaloby od fyzických osôb, prípadne strata dôvery a reputácie. [10]

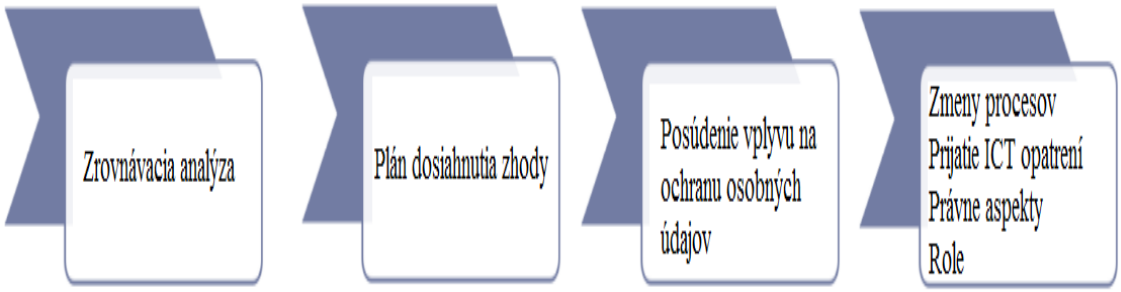
Pri porušení iných zásad môže firma dostať sankciu do 10.000.000 euro alebo do výšky 2% obratu spoločnosti za 1 rok. Ide o uzavretie zmluvy so sprostredkovateľom, ktorý nepostupuje podľa GDPR, neohlásenie úniku osobných údajov, odignorovanie žiadosti o vymazanie údajov alebo nepoverenie zodpovednej osoby pre prípady, v ktorých si to nariadenie vyžaduje. [3]

Nie každé porušenie Obecného nariadenia znamená udelenie finančnej pokuty. Sankcie sa udeľujú v závislosti od konkrétneho prípadu. Správca môže byť najskôr upozornený, že spracovanie údajov porušuje Obecné nariadenie alebo mu môže byť uložené napomenutie, prípadne nariadenie, aby uviedol spracovanie do súladu s Obecným nariadením. [12]

Pozitívnou správou je, že poisťovne dnes majú v ponuke špeciálne druhy poistenia. Takéto poistenie kryje riziká týkajúce sa spracúvania osobných údajov. [8]

2 POŽIADAVKY K ZAISTENIU ZHODY S GDPR

Základom k naplneniu požiadaviek nariadenia GDPR je detailné preskúmanie aktuálneho stavu ochrany osobných údajov v organizácií. Na základe porovnania súčasného stavu s požiadavkami je možné vykonať vhodný postup a zabezpečiť efektívnu implementáciu takým spôsobom, aby bola GDPR – compliance.



Obr. 1. Priebeh GDPR 1

2.1 Analýza GDPR

Ide o prvý krok, ktoré vykonáme pre dosiahnutie zhody s GDPR. Na základe analýzy zistíme nedostatky v plnení nariadenia. Analýza sa zaoberá porovnaním stavu ochrany osobných údajov zadávateľa s požiadavkami nariadenia. Stanovíme oblasti ochrany údajov, ktoré treba zlepšiť, pretože nedosahujú potrebnú úroveň. Zistené poznatky nám poskytujú informácie o slabinách a nedostatkoch ochrany osobných údajov klienta. Výstupné dokumenty obsahujú detailný aj súhrnný prehľad hodnotenia pre jednotlivé požiadavky GDPR. [31]

2.2 Zostavenie plánu zhody

V náväznosti na analýze je spracovaný detailný návrh zmien. Plán zhody organizáciu privedie až do cieľa. Cieľom je podrobné definovanie dielčích úloh a postupov realizácie k dosiahnutiu súladu s GDPR. [31]

2.3 Posúdenie vplyvu na ochranu osobných údajov

Druhým krokom, ktorý umožňuje posúdiť spracovanie osobných údajov a plánované opatrenia z pohľadu skutočných rizík je posúdenie vplyvu na ochranu osobných údajov. GDPR požaduje prevádzať posúdenie primeranosti a nevyhnutnosti operácií pri spracovaní údajov z hľadiska účelu a posúdenia rizík. Pôjde o najviac kontrolovanú

povinnosť a GDPR priamo stanoví zodpovednosť za takéto posúdenie v rámci organizácie.

Spracovanie hodnotenia obsahuje spracovanie formulára, identifikáciu respondentov, zaistenie potreby a hodnotenie rizík nakladania s osobnými údajmi klienta, dopad na súkromie a spracovanie záznamu z hodnotenia rizík práce s osobnými údajmi a predanie tohto záznamu klientovi. [31]

2.4 Implementácia GDPR do praxe

Posledným krokom k dosiahnutiu zhody s GDPR sú zmeny procesov. Vychádzame z analytickej fázy a informácií o nezhodách. Implementácia predstavuje úpravy, nasadenie technológií, upgrade systému, doplnenie procesov a definovanie pravidiel ochrany osobných údajov.

2.4.1 Zmena procesov organizácie

Cieľom je zabezpečiť zefektívnenie práce s osobnými údajmi a minimalizovanie uloženého, spracovávaného a prenášaného množstva. Výhodou je zmenšenie rozsahu, v ktorom je nutné prijímať opatrenia pre ich ochranu a zníženia nákladov na dosiahnutie zhody. Ide predovšetkým o zriadenie, odstránenie, zmeny, prenos osobných údajov, hlásenie incidentov a riadenie kontinuity systémov. [31]

2.4.2 Návrh ICT opatrení

Ide o významnú fázu, ktorej cieľom je zmeniť infraštruktúru IS organizácie, aby bola schopná vykonávať technické opatrenia v súlade s požiadavkami GDPR. Kľúčové oblasti sú riadenie prístupu, ukladače a zálohovanie dát, monitorovanie a logovanie, IDS/IPS, kryptografia, siete, mobilné zariadenia, antivírová ochrana a iné. [31]

2.4.3 Právne aspekty

Zmeny nastávajú taktiež vo vzťahoch v organizácií a ich klientmi, dodávateľmi alebo kontrolnými orgánmi. Zmeny v zmluvných a právnych vzťahoch môžu obsahovať súhlas subjektov, zamestnanecké zmluvy, zmluvy s dodávateľmi, zmluvy o zachovaní dôvernosti informácií a ďalšie. [31]

2.4.4 Role

Je potrebné definovať rolu, kto bude riadiť ochranu osobných údajov a ponesie zodpovednosť. Poverenec pre ochranu osobných údajov musí byť vymenovaný, ak spracovanie prevádza orgán verejnej moci či verejný subjekt, jeho činnosť vyžaduje rozsiahle pravidelné a systematické monitorovanie subjektov údajov alebo spracovanie špeciálnych kategórií údajov. [31]

2.5 Kľúčové vlastnosti k dodržovaniu GDPR

Z hľadiska nariadenia je potrebné sa zamerať na 5 kľúčových oblastí, ktoré nám pomôžu k získaniu zhody s GDPR.

2.5.1 Riadenie

Je dôležité definovať, ako preniesť GDPR do noriem, hodnôt a akcií. Zistiť, aké opatrenia je treba uskutočniť, či sú účinné a ako ich vieme ďalej zefektívniť. [16]

2.5.2 Ľudia a komunikácia

Zamestnanci potrebujú poznať riziká a dôsledky nesprávneho využívania dát. Preto je dôležité zabezpečiť pre pracovníkov školenia v oblasti požiadaviek GDPR. [16]

2.5.3 Procesy

Súčasťou analýzy je zameranie sa na procesy, akým spôsobom ich GDPR ovplyvní, aké budú dopady a ako sa budú riešiť požadované zmeny. [16]

2.5.4 Dáta

Zistíme, aké dáta máme a k čomu ich využívame. Je potrebné zaistiť kvalitu a riadenie údajov, ako aj interakciu s klientmi a tretími stranami. Je to nevyhnutnou súčasťou pre zabezpečenie dôveryhodnosti a transparentnosti. [16]

2.5.5 Zabezpečenie

Musíme zabezpečiť ochranu a dôvernosť osobných údajov ako aj zabezpečiť ich riadne použitie zahŕňajúce možnosti voľby, súhlasu, upozornenia, prístupu, nápravy alebo odstránenie ďalších aspektov. [16]

3 RIADENIE PROCESOV Z HĽADISKA INTERNÉHO AUDITU

Cieľom interných auditov je definovanie efektívnosti a spoľahlivosti celého systému, zabránenie nezhodám a jeho stále zlepšovanie. Interné audity stanovujú existujúce nedostatky, slabé miesta, hľadajú ich príčiny a navrhujú nápravné a preventívne opatrenia pre zlepšenie systému. [2]

Cieľom interného auditu je presvedčenie sa, že sa riešili existujúce aj novo vznikajúce riziká súvisiace so zabezpečením ochrany dát. Interný audit formuluje vhodné odporúčania, ako predísť ujme a efektívne využiť zdroje na prípravu na nové povinnosti. Interný audit GDPR kladie značné požiadavky na zloženie a odbornosť audítorského tímu. Členovia tímu by mali mať prinajmenšom dobrý prehľad o informačných a komunikačných technológiách, riadení bezpečnosti informácií, riadení procesov a o práve ochrany osobných údajov. [30]

Výstupom auditu je auditný záznam informačného systému o udalosti, ktorá môže ovplyvniť bezpečnosť informačného systému. [4]

3.1 Audit organizácie z pohľadu GDPR

Audit je nezávislý, systematický a dokumentovaný proces získania dôkazov z auditu a ich hodnotenia. Cieľom je definovať rozsah splnenia kritérií. Poskytuje nenahraditeľné informácie pre zlepšovanie systému riadenia, ide o efektívny a spoľahlivý nástroj pre podporu úspešného riadenia a zladenie spracovania osobných údajov so záväznými predpismi. [2]

3.2 Základné typy auditov

- Audity prvou stranou – sú označované ako interné audity. Firmy si tieto audity vykonávajú samé pre seba. Organizácia si volí pravidlá, ktorými sa audit riadi a výsledky využíva výlučne pre vlastné vylepšovanie. Rozhoduje o prioritách, cieľoch, rozsahu a určuje oblasti, ktoré potrebuje najviac preveriť. Tento typ auditu môže byť vykonávaný internými pracovníkmi ako aj externými subjektmi.
- Audity druhou stranou – sú známe ako odberateľské audity. Vykonávajú ich prevažne externé subjekty, ktoré majú voči firme konkrétne záujmy. Môže ísť o audity vyplývajúce zo vzájomných zmluvných vzťahov. Odberateľ môže preveriť mieru zabezpečenia údajov u dodávateľov a na základe auditu vykonať opatrenia

a príslušné rozhodnutia. Využíva sa hlavne v automobilovom priemysle.

- Audity treťou stranou – sú vykonávané externou organizáciou. Pravidlá, ktorými sa riadi, odsúhlasuje regulačný alebo akreditačný orgán. Tretia strana môže rozhodovať o vydaní alebo odobratí certifikátu a na základe objektívnych informácií aj o stave auditovanej oblasti. [2]

Úlohou auditu je na základe vopred definovaných požiadaviek zistiť súlad v organizácií. Požiadavky definuje firma interne vlastnými predpismi, legislatíva, ktorá je záväzná alebo pomocou zvoleného štandardu napr. ISO normou. Prioritou je zvoliť správny spôsob a použité nástroje pre overenie subjektu na základe zamerania daného auditu. Pri bezpečnostnom audite sa zameriavame na zabezpečenie, pri procesnom budú sledované interné postupy. Vzhľadom na ochranu osobných údajov sa vykonáva kombinácia týchto druhov. GDPR vyžaduje nielen zodpovedajúce technické opatrenia, ale aj vhodné organizačné riešenia. Práve prostredníctvom auditu dokážeme skutočne zaistiť správnosť dokumentovaných a zavedených opatrení. [20]

3.3 Priebeh auditu

Audit je proces skladajúci sa zo vstupných a výstupných informácií. Medzi vstupné dáta patrí všetko, čo sa spája s výskytom a spôsobom spracovania osobných údajov. Overenie súčasného stavu s definovanými požiadavkami nám dáva výsledok výstupu. Ak nebola stanovená zhoda, výstupom môže byť odporučenie audítora ako efektívne riešiť alebo zlepšiť existujúce opatrenia. Výsledkom môže byť takisto stav „zhoda“ alebo „nezhoda“.

GDPR upravuje požiadavky na ochranu osobných údajov fyzických osôb. Tieto požiadavky sú určené :

• v procesnej rovine – potreba dokumentovania a zavedenia interných metód spracovateľa a správcu pri získavaní osobných dát. Samozrejmosťou je potreba zabezpečiť práva subjektov.

• v administratívno – organizačnej rovine – ide o zaistenie organizačných opatrení spojených s bezpečným používaním OÚ oprávnenými, poučenými a vyškolenými osobami.

• v technickej rovine – ako požiadavky na zavedenie technických a technologických opatrení, ktoré zaistia bezpečnosť spracúvaných OÚ vo všetkých fázach ich životného cyklu. [20]

3.4 Zameranie auditu

Pripravenosť na plnenie kritérií nariadenia môžu audítori overiť z týchto hľadísk:

- plnenie pravidiel právnych predpisov pre spracovanie osobných dát a pripravenosť na nové pravidlá
- spracovávanie dokumentácie systému riadenia osobných údajov
- nastavenie a fungovanie technických a organizačných opatrení a kontrol
- riadenie ľudských zdrojov v rámci bezpečnosti osobných dát [30]

3.5 Postup auditu

Cieľom auditorských postupov je získanie dôkazov, na základe ktorých audítor dospeje k primeraným záverom pre vyjadrenie výroku.

3.5.1 Porozumenie organizácii

Audítor definuje všetky informácie o charaktere a o predmete činnosti spoločnosti a organizačných jednotiek, jej štruktúre, používaných IS, kategóriách spracovávaných osobných dát a o spracovateľoch. Na základe takýchto údajov audítor predbežne identifikuje oblasti a procesy, v rámci ktorých sa spracúvajú osobné údaje. Ďalej navrhne stratégiu overovacieho auditu.

3.5.2 Predbežné vyšetrovanie

V tejto časti audítor komunikuje so zástupcami spoločnosti, zhodnotí vnútorné predpisy a metodiky a ďalšie podklady týkajúce sa spracovania osobných údajov. Pokračuje predbežným klasifikovaním rizík pre firmu a pre subjekty osobných údajov. Spresní vymedzenie oblastí, kde sa pracuje s osobnými údajmi. Predbežným vyšetrovaním upresní ciele a predmet auditu tak, aby boli významné z hľadiska ochrany overované kľúčové procesy spracovania osobných údajov a skutočností. Môže ísť napr. o zabezpečenie personálnej činnosti a miezd, zaistenie fyzickej bezpečnosti prostredníctvom kamerových systémov, účtovníctvo, obchodné a marketingové aktivity. Audítor taktiež posúdi nevyhnutnosť použitia sofistikovaných nástrojov dátovej analýzy a pridanú hodnotu prípadného penetračného testovania. Výstupom tohto vyšetrovania je program interného auditu.

3.5.3 Audit na mieste

Audítor získava a zhromažďuje všetky potrebné dokumenty a informácie ako formuláre, žiadosti alebo zmluvy. Vykonáva rozhovory s pracovníkmi spoločnosti, ako sú bezpečnostní pracovníci, vlastníci aktív a IT celkov, správcovia prevádzkových postupov a aplikácií, personalisti, účtovníci alebo marketingoví zamestnanci a vykonáva plánované testy. Audítor môže vykonať aj fyzickú previerku priestorov, v ktorých sa osobné údaje nachádzajú alebo zariadenie, ktoré ich spracováva. Získané informácie vyhodnotí a posúdi správnosť existujúcich postupov a dokumentácie a riziká procesov spracovania osobných údajov.

3.5.4 Reportovanie

Audítor vytvorí návrh správy na základe vyhodnotených informácií, ktorá obsahuje všetky závery z auditu. Jej súčasťou sú odporúčania na odstránenie nedostatkov a na zníženie identifikovaných rizík. Vytvorený návrh správy prerokuje s príslušnými zástupcami spoločnosti a na základe výsledkov prerokovania audítor pripraví konečnú verziu správy.

3.6 Desatoro dobrého audítora GDPR

1. Je úprava zodpovednosti dostatočná v rámci spracovania osobných údajov?
2. Je dostatočná úprava pravidiel v oblasti IT (politiky prístupov, správy hesiel, zavedenie a uplatňovanie technických opatrení)?
3. Sú plnené povinnosti voči subjektom údajov (povinnosť poskytovať informácie o kategóriách spracovávaných osobných údajov, účeloch spracovania, príjemcoch údajov, právach dotknutých osôb)?
4. Existuje register spracovávaných osobných údajov? Musí obsahovať aspoň kategórie takýchto osobných údajov, kategórie dotknutých osôb, povahu a účel spracovania. Ďalej miesto, kde sú osobné dáta zhromažďované, zodpovednosť za jednotlivé fázy spracovania, lehoty, po ktorej majú byť osobné údaje spracovávané a právne tituly oprávňujúce správcu k ich spracovaniu.
5. Je práca a súhlasy so spracovaním osobných údajov vykonávaná správne? Zahŕňa vymedzenie, kde je súhlas nevyhnutný na spracovanie osobných údajov, a kde je spracovanie osobných údajov odôvodnené iným právnym titulom. Je nevyhnutné jasné odlíšenie súhlasu od zmluvných podmienok, plnenie informačnej povinnosti

a konkrétne vymedzenie účelu.

6. Je úprava zmlúv medzi správcom a spracovateľmi osobných údajov dostatočná? Napr. dojednanie o zárukách súčinnosti spracovateľa v súvislosti s vybavením požiadaviek dotknutých osôb uplatnených u správcu týchto údajov.
7. Je zabezpečené zvyšovanie povedomia zamestnancov v oblasti ochrany osobných údajov a školenia?
8. Je dostatočné nastavenie postupov pre uchovanie a likvidáciu osobných údajov s ohľadom na zásadu minimalizácie osobných údajov a obmedzenia uloženia osobných údajov?
9. Existujú postupy v prípade narušenia ochrany osobných údajov?
10. Existujú postupy pre komunikáciu s Úradom pre ochranu osobných údajov?

II. PRAKTICKÁ ČASŤ

4 NÁVRH RIEŠENIA V ORGANIZÁCIÍ Z HĽADISKA GDPR

Nariadenie zavádza nové definície pojmov a povinnosti týkajúce sa ochrany osobných údajov. Táto časť popisuje najdôležitejšie povinnosti spoločností a podnikateľov, práva dotknutých osôb ako aj zmeny v oblasti spracovania osobných údajov na praktických príkladoch. Definuje bezpečnosť, možnosti zálohovania z hľadiska GDPR, technické opatrenia a nové technológie. Detailne popisuje zavedenie GDPR nariadenia v konkrétnej spoločnosti, vrátane postupov a opatrení v ňom obsiahnutých.

4.1 Povinnosti podnikateľov a spoločností

- **GDPR zavádza povinnosť ustanoviť zodpovednú osobu (DPO)**

Podnikatelia musia zvoliť v organizácií zodpovednú osobu, ak vo veľkom rozsahu a pravidelne monitorujú fyzické osoby. Bude mať pod dohľadom poskytovanie informácií, kontrolu postupov spracúvania osobných údajov a komunikáciu s Úradom na ochranu osobných údajov. Zodpovedná osoba musí spĺňať kvalifikačné podmienky, môže ísť o vlastného zamestnanca ako aj externého dodávateľa. [8]

Uvedená povinnosť sa týka nasledovných subjektov, ktoré spracúvajú osobné údaje:

- Orgánov verejnej moci (ministerstvá, úrady) a verejnoprávnych subjektov (obce, školy, nemocnice) s výnimkou súdov pri výkone ich právomocí
- Prevádzkovateľov a sprostredkovateľov, ktorých hlavnou činnosťou sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu
- Prevádzkovateľov a sprostredkovateľov, ktorých hlavnou činnosťou je spracúvanie osobitných kategórií údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky
- Prevádzkovateľov, u ktorých to stanoví zvláštny právny predpis [8]

- **Povinné nahlasovanie bezpečnostné incidentov**

Každé narušenie ako aj únik osobných údajov musia spoločnosti nahlásiť Úradu na ochranu osobných údajov. Túto povinnosť musia vykonať do 72 hodín od vzniku bezpečnostného incidentu. Podnikatelia sú povinní narušenie alebo únik hlásiť aj

dotknutým osobám, ak situácia predstavuje vážne riziko a ohrozuje údaje týchto osôb. Ak by to však vyžadovalo nadmerné úsilie, môže zvoliť organizácia aj informovanie verejnosti. [8]

Oznamovacia povinnosť sa vyhodnocuje na základe vážnosti problému a konkrétnych okolností. Za porušenie ochrany sa rozumie strata nosiča s nezakódovanými klientskymi dátami, nedovolené vniknutie do siete a zásah do uchovávaných údajov. Môže nastať aj situácia, kedy hacker kontaktuje prevádzkovateľa a žiada o výkupné za sprístupnenie databázy, do ktorej neoprávnene vnikol. [25]

- **Zrušenie bezpečnostných projektov**

Bezpečnostný projekt je v podstate nepoužiteľný pre legislatívu podľa GDPR. Dochádza ku zániku povinnosti vypracovať bezpečnostný projekt. Dôležitým diferenciačným prvkom je, že pri bezpečnostnom projekte je potrebné sa zameriavať na riziká bezpečnosti a záujmy firmy, pri DPIA sa zameriavame na riziká práv a slobody dotknutých osôb. Aj napriek určitým podobnostiam a identickej povinnosti spracovávať prijaté bezpečnostné opatrenia bezpečnostné projekty a DPIA nemôžeme stotožňovať ako ich pozná naše aktuálne účinné právo. [6]

- **Niektorí podnikatelia musia vykonať analýzu vplyvov na ochranu osobných údajov (DPIA) a konzultovať svoje aktivity s Úradom na ochranu osobných údajov**

Firmy musia vypracovať analýzu vplyvu plánovaných spracovateľských operácií týkajúcich sa ochrany osobných údajov, ak nejaký druh spracovania dát môže znamenať riziko pre slobody a práva dotknutých osôb. Týka sa osobitných kategórií údajov o etnickom alebo rasovom pôvode, zdravotnom stave alebo politických názoroch. Taktiež situácií systematického monitorovania verejne prístupných priestorov. Ak spoločnosť skonštatuje, že jej aktivity by mohli byť hodnotené ako rizikové, musí podľa nariadenia požiadať o konzultáciu Úrad na ochranu osobných údajov. [8]

- **Bezpečné spracovanie osobných údajov**

Firmy musia vykonať opatrenia pre bezpečné spracovanie dát. Môžu údaje pseudonimizovať, napríklad šifrovať. To znamená, že až po odšifrovaní vieme osobu identifikovať. Za vhodné opatrenia môžeme považovať v prípade incidentu schopnosť včas obnoviť dostupnosť údajov, periodické testovanie a iné. Dôležitá je tiež minimalizácia údajov. Firmy by nemali spracovávať zbytočné údaje o klientovi. Výhodné

je, aby spoločnosti zapracovali požiadavky vyplývajúce z GDPR už pri vývoji nových produktov alebo služieb. [27]

- **Obmedzenie účelu spracovania osobných údajov**

Firmy zhromažďujú rôzne skupiny osobných údajov v niekoľkých rôznych databázach. Nariadenie prísne stanovuje, ktoré právne základy sú zákonné a obmedzuje účely spracovania údajov. Neobstojí spracúvanie údajov pre marketing alebo také údaje, ktoré už boli zverejnené. Spoločnosti sa musia preukázať platným súhlasom pre použitie týchto informácií. Mlčanie a nečinnosť už neznamená súhlas. [28]

- **Rozšírenie pôsobnosti**

GDPR rozšírilo pojem osobný údaj. Nemusí ísť o konkrétnu identitu osoby, ale aby bola za splnenia podmienok identifikovateľná. Medzi osobné údaje vrátane mena, dátumu narodenia, či záznamu z kamerového systému bude patriť aj email, IP adresa a geolokalizačný údaj z mobilu. Dokáže presne definovať, kde sa práve nachádzame. [27]

- **Byrokracia zostáva**

Uzatváranie mnohostranných zmlúv pred prenosom údajov mimo EÚ nariadenie neodstraňuje. Osobné údaje môžu byť prenesené k príjemcom do tretích krajín. Dôležité je, či krajina, do ktorej prenášame osobné údaje zaručuje alebo nezaručuje určitú úroveň ochrany. Podľa toho sa jednotlivé podmienky prenosu odlišujú. [25]

4.2 Práva dotknutých osôb

Nariadenie GDPR výrazne zvyšuje práva občanov. Môžu mať prístup ku všetkým svojim osobným údajom, ktoré prevádzkovateľ má, či už v softvéroch, e-mailoch alebo listinnej podobe. Osoby majú v rukách dôležitý nástroj kontroly nad osobnými údajmi. [19]

- **Transparentná komunikácia**

Prevádzkovateľ musí komunikovať s dotknutou osobou takým spôsobom, aby porozumela, čo jej oznamuje a ako zaobchádza s jej údajmi. Poskytnuté informácie musia byť transparentné, dostupné, stručné a zrozumiteľné. V záujme toho je potrebné zvyšovať zrozumiteľnosť a prehľadnosť využívaním rôznych ikon alebo vizualizácií. [1]

- **Oznamovacia povinnosť**

V čase, keď dotknutá osoba poskytuje prevádzkovateľovi svoje údaje, musí byť upozornená na aký účel a na základe čoho budú jej dáta spracovávané. Komu sú tieto dáta poskytované, ako dlho ich prevádzkovateľ bude uchovávať a či budú prenášané do zahraničia. [1]

- **Dotknuté osoby majú podľa GDPR právo na prístup a poskytnutie osobných údajov**

Ak dotknutá osoba požiada o kópie osobných údajov, ktoré o nej spracovávajú, kto k nim má prístup a za akým účelom, spoločnosť je povinná jej tieto údaje poskytnúť. Tieto požiadavky si vyžiadajú zásah do existujúcich informačných systémov. Systémy takéto funkcionality bežne neobsahujú. Firma však môže takúto požiadavku odmietnuť alebo spoplatniť, ak pôjde o opakované alebo nepodstatné žiadosti. [27]

Je možné poskytnúť priamy vzdialený prístup k údajom, ktoré si bude môcť sama upraviť alebo doplniť. Samozrejme takýto prístup nesmie ohroziť vlastníctvo prevádzkovateľa ani údaje tretích osôb. [25]

- **Dotknuté osoby majú právo na prenos svojich osobných údajov**

Právo na portabilitu dát je novým právom, ktoré má podporiť konkurenciu prevádzkovateľov. [25]

Ľudia budú mať právo na bezplatné nadobudnutie svojich osobných údajov. Tieto údaje slobodne poskytujú prevádzkovateľovi a ten je povinný kedykoľvek tieto dáta poskytnúť a s cieľom ďalšieho použitia umožniť ich bezpečný prenos napr. pri zmene internetovej služby. [8]

- **Dotknuté osoby majú právo byť vymazané alebo úplne zabudnuté**

Ak je spracovanie dát v rozpore s oprávnenými záujmami dotknutej osoby, má právu byť zabudnutá. Ak fyzická osoba požiada o výmaz svojich osobných údajov, spoločnosť je povinná tieto údaje vymazať a informovať prevádzkovateľov, ktorí tieto dáta spracovávajú. Firma však nemusí žiadosti vyhovieť, ak by vymazanie stálo neprimerane veľa peňazí alebo by sa museli použiť zložité technické prostriedky. [26]

Podľa GDPR bude mať každý za určitých podmienok navyše právo požadovať,

aby jeho osobné údaje boli úplne vymazané z internetových vyhľadávačov ako Google, Yahoo, Bing či Zoznam. [8]

GDPR má však aj výnimky, ak pôjde o povinné uchovávanie údajov napríklad na daňové účely alebo uchovávanie dát pre obhajobu právnych nárokov. Prevádzkovateľ vtedy žiadosti nemusí vyhovieť. [25]

- **Vznesenie námietky**

Občania môžu vzniesť námietku voči spracovaniu osobných údajov. Prevádzkovateľ je povinný o tejto možnosti osobu výslovne informovať. [25]

- **Uplatnenie práv**

Dotknutá osoba si sama vyberá formu komunikácie ústne, písomne, telefonicky alebo elektronicky. Prevádzkovateľ má byť schopný v týchto formách žiadosť spracovať a sprístupniť občanom hot linku, sprístupnenie dotazníkov alebo formulárov. Teda určitým spôsobom uľahčiť výkon práv dotknutých osôb. [25]

- **Vybavenie žiadosti dotknutej osoby**

Na vybavenie žiadostí ma prevádzkovateľ jeden mesiac, v prípade náročných žiadostí môže túto dobu predĺžiť o 2 mesiace od doručenia. Prijaté žiadosti musí vyriešiť bezodkladne a bezplatne. Poplatok však môže požadovať, ak ide o nedôvodnú, neprimeranú alebo opakovanú požiadavku. [25]

4.3 Zmeny v oblasti spracovania osobných údajov na praktických príkladoch

Podnikatelia, ktorí vlastnia webové portály alebo eshopy sa musia taktiež oboznámiť s nariadením GDPR. Implementácia žiadúcich zmien nemusí byť pre nich až taká náročná. Najdôležitejšie je zabezpečiť správnosť súhlasu so spracúvaním údajov a používaním cookies ako aj formuláciu účelu spracúvania osobných údajov. Skontrolovať aktuálnosť podmienok ochrany údajov a zabezpečiť, aby posielanie marketingových ponúk nebolo protiprávne. I keď je nariadenie č. 2016/679 (GDPR) pomerne rozsiahle, medzi hlavné zmeny, ktoré podnikateľov ovplyvnia najviac, môžeme zaradiť predovšetkým nasledujúce novinky: [8]

- **Firmy, Eshopy alebo prevádzkovatelia kamerových systémov musia viesť zápisy o spracúvaní osobných údajov**

Firmy zamestnávajúce viac ako 250 pracovníkov majú povinnosť mať špeciálnu evidenciu o spracúvaní osobných údajov. Túto povinnosť majú taktiež podnikatelia zaoberajúci sa špecifickou kategóriou dát. Ide napríklad o zdravotné údaje alebo také, ktoré sa nespracúvajú príležitostne. [8]

Nariadenie obsahuje výnimku pre spoločnosti s menej ako 250 pracovníkmi, napríklad ak spracovanie údajov nevedie k riziku alebo je príležitostné pre práva a slobody občanov. [25]

- **Na webovej stránke nemôže byť vopred označený súhlas so spracovaním osobných údajov**

Ak je ikona pre udelenie súhlasu na eshope alebo webe vopred zaškrtnutá, musíme ju zmeniť na neoznačenú. Súhlas s marketingovým spracovaním osobných údajov musí byť slobodný, jednoznačný a konkrétny. [8]

- **V obchodných podmienkach nemôže byť automaticky uvedený súhlas so spracovaním osobných údajov pre marketingové účely**

Ak sa súhlas so spracovaním údajov vykonáva automaticky podpísaním zmluvy, ide o neplatný a neslobodný úkon a marketingové spracovanie údajov sa považuje za protizákonné. Reklamné ponuky nemôžu byť súčasťou zmluvy, obchodných podmienok ani formulárov určených pre objednávku. [8]

- **Spoločnosť musí vedieť preukázať udelenie súhlasu so spracovaním osobných údajov**

Spoločnosť musí vedieť kedykoľvek preukázať udelenie súhlasu fyzickej osoby so spracúvaním osobných údajov. Ak podnikateľ nebude schopný túto skutočnosť preukázať, hrozia mu vysoké sankcie. Vhodné je používať tzv. double opt-in nástroje najmä pre prevádzkovateľov eshopov alebo internetových obchodov. Ide o poslanie potvrdzujúceho emailu o spracovaní dát. Zákazník tento email dostane a následne ho potvrdí, čím potvrdzuje svoj súhlas. [8]

- **Cookies môžeme zbierať, len ak návštevník webovej stránky udelí svoj súhlas**

Súbory cookies sú považované za osobný údaj, a preto ich môžeme používať až vtedy, ak návštevník web stránky udelí svoj slobodný súhlas**.** Ak v súčasnosti webová stránka využíva cookies ukladajúce sa u zákazníka pred vyjadrením jeho súhlasu, na základe nariadenia toto nastavenie systému bude musieť zmeniť do začiatku platnosti GDPR. [8]

- **Pri spracovaní osobných údajov detí, ktoré majú menej ako 16 rokov, je potrebný rodičovský súhlas**

Prevádzkovateľ musí overiť, že zákazníkovi, ktorý nedovŕšil 16 rokov, je udelený súhlas zákonného zástupcu s odovzdaním jeho osobných údajov. Podľa nariadenia tak musí urobiť každý, kto spracúva osobné údaje na základe súhlasu alebo prevádzkuje web alebo eshop s online službou. Pri zaškrtávacej ikonke by mala byť doplnená formulka o vetu: „Prehlasujem, že ak mám menej ako 16 rokov, tak som požiadal svojho zákonného zástupcu (rodiča) o súhlas so spracovaním mojich osobných údajov.“ Je to dôležité z toho dôvodu, že overenie veku návštevníka webu je takmer nemožné. [8]

- **Prenos osobných údajov zo služby ku konkurencii musí byť bezplatný a v meta dátach**

Užívateľ môže požiadať o sprístupnenie osobných údajov konkurenčnej aplikácií alebo webovej stránke. Tieto údaje poskytneme z databázy našej aplikácie alebo webovej stránky, len ak sú splnené potrebné podmienky:

- Sám používateľ poskytol osobné údaje prevádzkovateľovi aplikácie alebo webu
- Na základe splnenia zmluvy, môže byť v záujme poskytnutia určitej služby alebo súhlasu spracovanie osobných údajov
- Automatizovane spracované osobné údaje, môže ísť o kliknutie na tlačidlo „zaregistrovať sa“ [8]

4.4 Bezpečnosť a zálohovanie osobných údajov

V rámci nariadenia GDPR hovoríme o ochrane osobných údajov. Jednou z najdôležitejších vecí je preto bezpečnosť a zálohovanie osobných údajov. Zálohovanie

dát je podstatné pre zabezpečenie nepretržitej prevádzky IS. V malých a stredných spoločnostiach sa využívajú jednoduché spôsoby zálohovania dát. Ukladanie údajov býva najmä podľa potreby a to na disky, resp. NAS servery. V menších firmách býva taktiež zálohovanie často riešené nevhodným spôsobom alebo zanedbávané, hlavne z pohľadu nariadenia GDPR. Osobné údaje majú byť uchovávané vo forme, ktorá poskytuje identifikáciu dotknutej osoby, kým je to nevyhnutné pre potrebný spracovávaný účel. Na jednej strane ide o jednoduché znenie zákona založeného na nariadení GDPR, na druhej strane ide o pomerne problematickú implementáciu. V každom prípade je potrebné definovať spôsob zálohovania. Za nevhodné považujem zálohovanie v nešifrovanej podobe z hľadiska veľkého rizika straty dát. Taktiež využívanie verejne dostupných a bezplatných cloudových úložísk v nešifrovanej podobe. Kvôli rozsahu spracúvania množstva informácií v spoločnosti vrátane osobných údajov býva riešenie zálohovania pomerne zložité. Doteraz stačilo preukázať zálohy a zabezpečené úložisko záloh v rámci bezpečnostného projektu. Dáta sa zálohovali aj na tzv. block – chains úložiskách. Z pohľadu bezpečnosti predstavujú decentralizovaný model ukladania údajov a z pohľadu ochrany údajov výborné riešenie. Z pohľadu GDPR a ochrany osobných údajov ide však o nevhodné riešenie, najmä ak ide o bezodkladný výmaz osobných údajov dotknutej osoby. Problém je aj vo virtualizovaných informačných systémoch. Znamenajú prínos vo svete IS. Ak však niekto zálohuje počítač, ktorý virtualizuje spolu s virtualizovanými počítačmi, tie obsahujú osobné dáta, a teda aj záloha obsahuje osobné údaje. Žiadosť o vymazanie osobných údajov znamená vymazať dáta vo virtualizovanom počítači, tak aj v podkladovej zálohe virtualizačného počítača. Vymazať údaje z takejto zálohy je v podstate nemožné. Firma by sa potom mohla dostať do konfliktu s nariadením GDPR a porušiť práva a slobodu osôb.

Reálne by sme mali ukladať osobné údaje samostatne na jedno miesto, databázu, disk, takým spôsobom, aby na osobné údaje mohol byť aplikovaný plán záloh nezávislý na zvyčajnom zálohovacom postupe. Z toho vyplýva minimalizovať množstvo spracúvaných osobných dát, údaje ukladať pseudonymizovane, prípadne anonymizovane. Používať čo najmenej databáz a súborov, aby v prípade potreby bolo možné dotknutým osobám vyhovieť. V jednoduchom príklade by sa dalo uviesť, že ak organizácia má osobné dáta v súborovej databáze, je možné uvažovať nad tým, že bude na samostatnom disku ukladaná, tento disk bude samostatne zálohovaný na šifrovanom záložnom zariadení, napr. bitlockerom šifrovaný. Zvyšný systém mimo osobných údajov na inom disku bude

zálohovaný bežným spôsobom. V prípadne komplexnejších systémov to bude výrazne zložitejšie. [23]

Podľa môjho názoru jedným z najlepších a najjednoduchších riešení je mať cloudové úložisko, ktoré má zmluvne ošetrené prevzatie záruk v rámci nariadenia GDPR. Existuje niekoľko špecializovaných riešení pre organizácie. Toto riešenie je založené na šifrovaných kanáloch, šifrovaných technológiách a najnovších technológiách autentifikácie používateľa. Pri prechode na cloud je častou prekážkou bezpečnosť, pretože firmy chcú mať údaje pod kontrolou, avšak častokrát majú zabezpečenie údajov oveľa horšie než akýkoľvek poskytovateľ tohto riešenia. Základnou myšlienkou je efektivita, teda k údajom sa dostaneme odkiaľkoľvek a prakticky z čohokoľvek, napríklad z mobilného telefónu. Cloudové riešenia vedia prispieť k naplneniu agendy GDPR.

4.5 Technické opatrenia

GDPR nariaďuje spoločnostiam vykonávať potrebné organizačné a technické opatrenia pre riadenie rizík. Popisuje vzory opatrení, ale neposkytuje podrobné informácie o tom, prečo sú nevyhnutné alebo z čoho sa skladajú. Táto časť vypĺňa túto medzeru, popisuje kontroly zraniteľnosti, penetračné testy a ich spôsob spolupráce.

4.5.1 Chyby zabezpečenia

Veľa spoločností zabezpečuje ochranu sietí prostredníctvom antivírusového softvéru a správy patchov. Sú zásadné, ale skúma sa konfigurácia, aplikácie a hardvér tretích strán. To je to, čo overuje zraniteľnosť.

Skenovanie zraniteľností môže byť interné alebo externé. Ide o proces automatizovaný, hľadá a upozorňuje spoločnosť na slabiny v systéme. Vnútorné skeny zisťujú hrozby vo vnútri firmy, napríklad potenciál zneužívania privilégií a externé skenovanie hľadá, akým spôsobom vedia outsideri využiť spoločnosť. Je potrebné zabezpečiť pravidelné kontroly zraniteľnosti, zabrániť narušeniu dát zabezpečením najbežnejších bezpečnostných nedostatkov a taktiež sa správne naučiť interpretovať výsledky vyhľadávania zraniteľností.

Mnohokrát sa stáva, že riziká sú označované ako "nízke" alebo "stredné" a odborníci označia zabezpečenie organizácie ako primerane účinné. Všetky slabiny však môžu byť

využívané kriminálnymi hackermi. Pre zabránenie takejto situácie sa vykonávajú pravidelné penetračné testy.

4.5.2 Penetračné testy

Vykonávanie penetračného testovania si vyžaduje určitú úroveň praktickej práce a odbornosti. Tester dokáže vytvárať skripty, ladiť nastavenie nástrojov a meniť parametre útoku. Profesionálny tester v mene organizácie používa rovnaké praktiky ako kriminálny hacker a hľadá zraniteľnosti v aplikáciách alebo sieťach spoločnosti. Testy dokážu skontrolovať celú infraštruktúru a všetky aplikácie a rozsah testovania môžeme upraviť na základe funkcií, oddelení alebo určitých aktív.

4.5.3 Testovanie podľa rozpočtových požiadaviek

V minulosti bolo penetračné testovanie chybne interpretované ako nákladný spôsob pre zistenie, kde je potreba vynaložiť viac peňazí. Organizácia sa bez potrebného testovania vystavuje útokom a narušeniu dát, čo predstavuje vyššie náklady ako je cena penetračného testu. Využívajú sa taktiež spôsoby, ako znížiť náklady na penetračné testovanie. Nie je potrebné vždy testovať všetky časti siete alebo aplikácie. To sa vykonáva len pri uchovávaní vysoko citlivých údajov alebo ak máme dôvod myslieť si, že sme zacielení hackermi. [5]

4.6 Zrušenie voľne dostupných Wi-fi

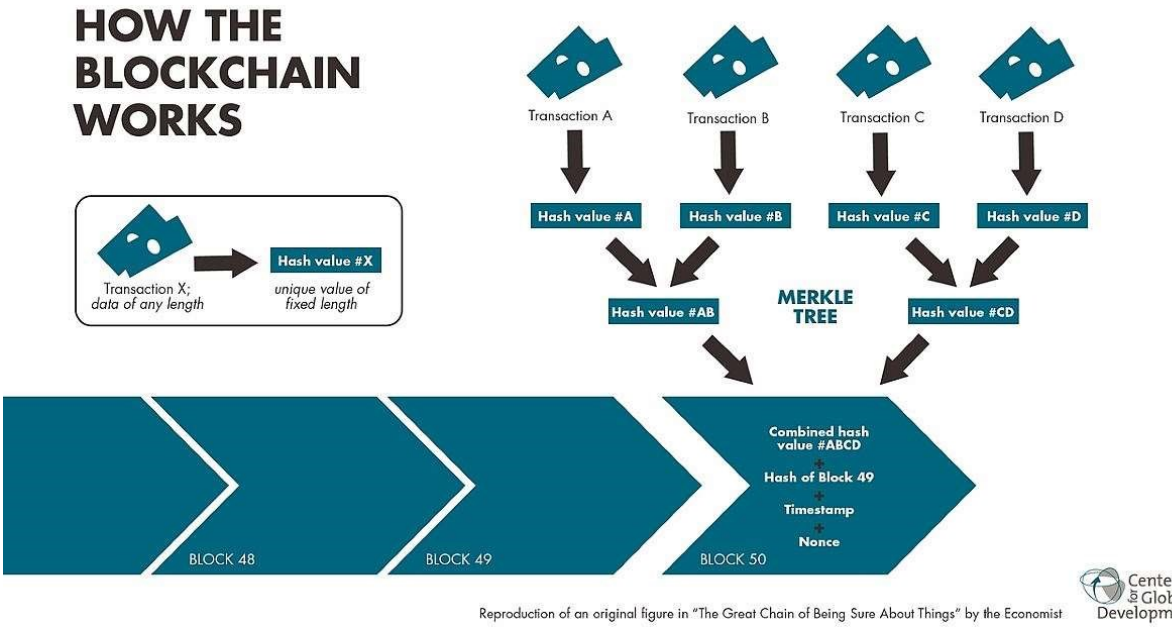
Siete vo veľkej väčšine hotelov, reštaurácií či nákupných centier nie sú dostatočne zabezpečené. Prevádzkovatelia firiem, škôl, barov alebo reštaurácií by mali mať prehľad o každom človeku pripojenom do siete a o tom, kde všade je k dispozícii ich heslo. Je to ale reálne takmer nemožné. Firma, ktorá nám poskytuje internet, monitoruje len činnosť vo svojej sieti. Ak sme teda napríklad majiteľom hotela a dôjde k útoku prostredníctvom free Wi-fi, tak hotel je zodpovedný za túto nezabezpečenú Wi-fi a prípadné problémy alebo žaloby od poškodených. Preto je nevyhnutné poznať osobu, ktorá pošle cez Wi-fi nelegálny obsah alebo poplašnú správu. Vo svete je zabezpečenie siete štandardom a podľa nového nariadenia GDPR nutnosťou. Chránené musia byť najmä meno, priezvisko, email, dátumu narodenia aj IP adresa. Na základe týchto údajov dokážeme priamo alebo nepriamo identifikovať osoby. [21]

Zabezpečenie prenosu môžeme vyriešiť dvomi spôsobmi. Prvým spôsobom je dôvera

k poskytovateľovi internetového pripojenia. Druhým a lepším spôsobom je vytvoriť vlastný VPN server v prípade, že má spoločnosť k dispozícií verejnú IP adresu a router. Prípadným negatívom tohto riešenia môže byť rýchlosť. Je závislá na priepustnosti serveru a počtom užívateľov pripojených v danom momente na server. [3]

4.7 GDPR a svet nových technológií

Nariadenie GDPR je rozsiahlou reformou a prináša rôzne konsekvencie. Problémom môže byť časť zaoberajúca sa vymazaním osobných údajov. Do rozporu s kompatibilitou nariadenia sa môžu dostať strojové učenie alebo neurónové siete. Napríklad analýzou osobných údajov miliónov návštevníkov sociálnej siete vytvorí neurónová sieť znalostný model. Ten je štatistickým odtlačkom dát každého subjektu a vo vnútornej štruktúre všetko spolu súvisí. Preto je nemožné, aby sme vymazali údaje popisujúce osobu X, pretože by sa zmazal celý model. Rovnakým prípadom je napríklad databázová štruktúra blockchain. Býva spájaný s bitcoinom a inými kryptomenami. Je veľmi odolný voči nelegálnym zmenám. Je charakteristický tým, že jedna hodnota matematicky naväzuje na nasledujúcu hodnotu ako reťaz. Ak by niekto zmenil záznam blockchainu, celý by sa zrútil, pretože náväznosť záznamov by prestala fungovať. Bolo by nutné začať odznova v bode nelegálneho zásahu, pretože záznamy by už nepredstavovali správne kontrolné súčty. Znamená to, že daná technológia pravdepodobne nemôže byť s napadnutím validná. Záznam nemôžeme spätne zmazať alebo upraviť. [24]



Obr. 2. Princíp blockchain 1

4.8 INTERNÝ PREDPIS NA OCHRANU OSOBNÝCH ÚDAJOV

Tento interný predpis pre ochranu osobných údajov, vrátane postupov v ňom obsiahnutých, je určený pre stredné ubytovacie zariadenie, ktoré nevykonáva rizikové spracovanie. Popisuje faktický stav a opatrenia zavedené v zariadení v rámci prípravy na GDPR. Tomuto predpisu predchádzala analýza, mapujúce účely spracovania a zodpovedajúce procesy.

4.8.1 Úvodné ustanovenia

Tento interný predpis upravuje spracovanie osobných údajov na zabezpečenie ochrany osobných údajov v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679, o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov a o zrušení smernice 95/46 / ES ("GDPR"). Cieľom tohto interného predpisu je zabezpečiť dodržiavanie povinností vyplývajúcich z GDPR v spoločnosti a umožniť dotknutým osobám výkon ich práv.

4.8.2 Výklad pojmov

Na účely tohto interného predpisu:

1. **"osobné údaje"** sú všetky informácie o identifikovanej alebo identifikovateľnej fyzickej osobe, tj. osobe, ktorú možno priamo alebo nepriamo identifikovať, najmä odkazom na určitý identifikátor (napr. meno, identifikačné číslo, lokalizačné údaje, sieťový identifikátor alebo jedného alebo viacerých špecifických prvkov, fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo spoločenskú identitu tejto fyzickej osoby);

2. **"osobitné kategórie osobných údajov"** osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženstvo alebo filozofické presvedčenie, členstvo v odboroch, a spracovanie genetických údajov, biometrických údajov s cieľom jedinečnej identifikácie fyzickej osoby a údajov o zdravotnom stave či o sexuálnom živote alebo sexuálnu orientáciu fyzickej osoby;

3. **"spracovanie"** akákoľvek operácia alebo súbor operácií s osobnými údajmi alebo súbory osobných údajov, ktorý je vykonávaný pomocou alebo bez pomoci automatizovaných postupov, ako je zhromaždenie, zaznamenanie, usporiadanie, štruktúrovanie, uloženie, prispôsobenie alebo pozmenenie, vyhľadanie, nahliadnutie,

používanie, sprístupnenie prenosom, šírenie alebo akékoľvek iné sprístupnenie, zoradenie či skombinovanie, obmedzenie, vymazanie alebo zničenie;

4. **"obmedzenie spracovania"** označenie uložených osobných údajov s cieľom obmedziť ich spracovanie v budúcnosti;

5. **"správcom"** fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracovania osobných údajov;

6. **"spracovateľ"** fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje pre správcu;

7. **"príjemca"** je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorým sú osobné údaje poskytnuté, či už sa jedná o tretiu stranu, alebo nie. Avšak orgány verejnej moci, ktoré môžu získavať osobné údaje v rámci osobitného vyšetrovania v súlade s právom členského štátu, sa za príjemcu nepovažujú;

8. **"tretia strana"** je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý nie je subjektom údajov, správcom, spracovateľom ani osobou priamo podliehajúcou správcovi alebo spracovateľovi, ktorá je oprávnená k spracovávaniu osobných údajov;

9. **"súhlas"** subjektu údajov znamená slobodný, konkrétny, informovaný a jednoznačný prejav vôle, ktorým dotknutá osoba dáva vyhlásením či iným zjavným potvrdením svoj súhlas na spracovanie svojich osobných údajov;

10. **"porušením zabezpečenia osobných údajov"** porušenie zabezpečenia, ktoré má za následok náhodné alebo nezákonné zničenie, stratu, zmenu alebo neoprávnené poskytnutie alebo sprístupnenie prenášaných, uložených alebo inak spracovávaných osobných údajov;

11. **"dozorný úrad"** Úrad na ochranu osobných údajov Slovenskej republiky

12. **"likvidáciou"** osobných údajov sa rozumie fyzické zničenie ich nosičov alebo ich vymazanie

4.8.3 SÚVISIACE PREDPISY A DOKUMENTY

4.8.3.1 LEGISLATÍVA

• Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679, o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46 / ES

• Zákon č. č. 122/2013 Z.z., O spracovaní osobných údajov

• Zákon č. 262/2006 Zb., Zákonník práce, v znení neskorších predpisov

• Zákon č. 326/1999 Zb. o pobyte cudzincov na území SR, v znení neskorších predpisov

• Zákon č. 565/1990 Zb. O miestnych poplatkoch v znení neskorších predpisov

• Zákon č. 337/1992 Zb. O správe daní a poplatkov v znení neskorších predpisov

• Zákon č. 586/1992 Zb. O daniach z príjmu, v znení neskorších predpisov

• Zákon č. 48/1997 Zb. O verejnom zdravotnom poistení v znení neskorších predpisov

• Zákon č. 143/1997 Zb. O plate a odmene za pracovnú pohotovosť, v znení neskorších predpisov

• Zákon č. 100/1998 Zb. O sociálnom zabezpečení v znení neskorších predpisov

• Zákon č. 155/1995 Zb., O dôchodkovom poistení v znení neskorších predpisov

4.8.3.2 INTERNÉ PREDPISY

Organizačný poriadok, predpisy personálneho oddelenia, predpisy fyzickej bezpečnosti, predpis pre prácu s kreditnou kartou, predpis na ochranu informácií, predpis pre riadenie rizík, predpis na riadenie bezpečnostných incidentov, predpis na riadenie užívateľských prístupov, skartačný a archivačný rád, systém vnútorných zásad pre chod hotelovej zmenárne.

4.8.4 Role a zodpovednosti

4.8.4.1 Zamestnanci

Každý zamestnanec zodpovedá za to, že spracovanie osobných údajov vykonáva v súlade s právnymi predpismi a týmto interným predpisom a ďalšími predpismi a dokumentmi spoločnosti. Každý zamestnanec je povinný zachovávať mlčanlivosť o osobných údajoch

a opatreniach prijatých na ich ochranu, o ktorých sa v súvislosti s výkonom svojho zamestnania dozvedel, a to aj po skončení pracovného pomeru. Ak poruší povinnosť mlčanlivosti, bude to zamestnávateľ považovať za porušenie pracovnej disciplíny zvlášť hrubým spôsobom a môže so zamestnancom okamžite rozviazať pracovný pomer podľa § 55 ods. 1 písm. b) Zákonníka práce.

4.8.4.2 Zodpovedná osoba za ochranu osobných údajov

V závislosti na organizačnej štruktúre identifikujeme osobu alebo rolu v spoločnosti zodpovednú za agendu ochrany osobných údajov a zabezpečenie plnenia tohto predpisu.

Upravíme zodpovednosti ďalších osôb v súvislosti so spracovaním osobných údajov a plnením povinností podľa tohto predpisu. V prípade, že je v spoločnosti IT manažér bezpečnosti alebo samostatne manažér HR, môže byť zodpovednosť rozdelená medzi tieto, prípadné ďalšie role.

4.8.5 Zásady spracovania osobných údajov

Pri spracovaní osobných údajov v spoločnosti je nevyhnutné dodržiavať nasledujúce zásady:

a) vo vzťahu k dotknutej osobe musia byť osobné údaje spracovávané korektne, zákonne a transparentným spôsobom ("zákonnosť, korektnosť a transparentnosť");

b) osobné údaje sa musia zbierať pre určité, jasné a zákonné účely a nebudú sa ďalej spracovávať spôsobom, ktorý je s týmito účelmi nezlučiteľný ("účelové obmedzenia");

c) spracovanie musí byť primerané, relevantné a obmedzené na nevyhnutný rozsah vo vzťahu k účelu, pre ktorý sú osobné údaje spracovávané ("minimalizácie údajov");

d) osobné údaje musia byť presné a v prípade potreby aktualizované; musia sa prijať všetky rozumné opatrenia, aby osobné údaje, ktoré sú nepresné s prihliadnutím na účely, pre ktoré sa spracovávajú, boli bezodkladne vymazané alebo opravené ("presnosť");

e) osobné údaje musia byť uložené vo forme, ktorá umožňuje identifikáciu dotknutej osoby po obdobie nie dlhšie, než je potrebné na účely, pre ktoré sú spracovávané ("obmedzenia uloženia");

f) osobné údaje sa musia spracovávať spôsobom, ktorý zabezpečí náležité zabezpečenie osobných údajov, vrátane ich ochrany pomocou vhodných technických alebo organizačných opatrení pred neoprávneným alebo protiprávnym spracovaním a pred

náhodnou stratou, zničením alebo poškodením ("integrita a dôvernosť");

4.8.6 Technicko - organizačné opatrenia na zabezpečenie ochrany osobných údajov

Systém ochrany osobných údajov je tvorený komplexom organizačných a technických opatrení, ktoré sú v spoločnosti realizované za účelom zabezpečenia ochrany a bezpečnosti osobných údajov.

4.8.6.1 Bezpečnostné opatrenia

- Riadenie rizík

Popisuje, akým spôsobom sú v spoločnosti identifikované a hodnotené rôzne závažné a pravdepodobné riziká a následne navrhujú a prijímajú opatrenia na zníženie vplyvu týchto rizík. Revízia vyhodnotenia rizík je v spoločnosti vykonávaná pravidelne 1 krát ročne. Ad hoc revízia rizík je vykonávaná najmä v prípade výraznejších zmien v spoločnosti s možným vplyvom na ochranu osobných údajov alebo v prípade narušenia zabezpečenia ochrany osobných údajov. Za vykonanie revízie zodpovedá zodpovedná osoba.

Vyhodnotenie rizík uvažuje nasledujúce:

a) Riziko voči právam a slobodám dotknutých osôb z nasledujúcich pohľadov:

1. Porušenie princípov primeranosti a nevyhnutnosti spracovania

2. Porušenie práv dotknutých osôb

3. Neoprávnený prístup k osobným údajom

4. Neoprávnená zmena osobných údajov

5. Nedostupnosť alebo vymazanie osobných údajov

b) Možný vplyv v prípade realizácie rizík napríklad spracovanie osobných údajov bez právneho titulu môže viesť k zasielaniu nevyžiadaných obchodných správ alebo neschopnosti zabezpečiť výkon práva dotknutej osoby a následnému spôsobeniu hmotné alebo nehmotné ujmy, neoprávnený prístup k citlivým osobným údajom môže viesť k odcudzeniu identity a pod.

c) Hodnotenie závažnosti vplyvu: Na základe definície možných vplyvov v bode b) je určená jedna z nasledujúcich kategórií.

1. Zanedbateľné: Subjekty údajov nebudú dotknuté, alebo budú dotknuté minimálne bez akýchkoľvek väčších problémov (napr. opätovné zadávanie informácií do systému, obťažovanie pri opätovnom marketingovom oznámení)

2. Obmedzené: Subjekty údajov sa môžu stretnúť s nepríjemnosťami, ktoré budú schopné relatívne ľahko vyriešiť (dodatočné náklady, popretie prístupu k obchodným službám, strach, nedostatok porozumenia, stres atď.).

3. Významné: Udalosť môže mať významný dôsledok pre dotknuté osoby. Tieto dôsledky by subjekty mali byť schopné prekonať, hoci s vážnymi ťažkosťami (napr. zneužitie finančných prostriedkov, škody na majetku, strata zamestnania, zhoršenie zdravotného stavu, atď.)

4. Vysoké: Udalosť môže mať vysoké alebo nezvratné dôsledky pre dotknuté osoby, ktoré nemusia byť možné prekonať (napr. finančné problémy, značný dlh, pracovná neschopnosť, dlhodobé fyzické alebo psychické choroby, smrť atď.)

d) Hodnotenie pravdepodobnosti výskytu udalosti, ktorá môže mať negatívny vplyv na dotknuté osoby. Táto metodika uvažuje nasledujúce kategórie:

1. Zanedbateľné: V spoločnosti ani v odvetví sa udalosť ešte nevyskytla, jej výskyt však nie je vylúčený.

2. Obmedzené: V spoločnosti sa udalosť v minulosti ešte nevyskytla, jej výskyt však bol už zaznamenaný v rámci odvetvia.

3. Významné: V spoločnosti sa udalosť v minulosti už vyskytla.

4. Vysoké: V spoločnosti sa udalosť už vyskytla opakovane.

e) Zavedené a plánované ochranné resp. nápravné opatrenia

Vyhodnotenie rizík - na základe analýzy v spoločnosti.

- **Fyzická bezpečnosť**

Popisuje technické opatrenia, ktoré slúžia k zaisteniu bezpečnosti osobných údajov. Zameriava sa na využitie kamerových systémov, zámkov, zábran, mreží, uzavretých objektov, trezorov a podobných prostriedkov fyzického zabezpečenia.

Pre kontrolu fyzického prístupu do priestorov spoločnosti je využívaná recepcia. Vstup je umožnený iba oprávneným osobám.

• Fyzické bariéry sú tam, kde je to použiteľné, postavené tak, aby chránili pred neoprávneným vstupom a kontamináciou.

• Požiarne dvere sú v definovanom bezpečnostnom perimetri opatrené elektronickým zabezpečovacím systémom a sú monitorované.

• Vonkajšie dvere a dosiahnuteľné okná sú chránené vhodným detekčným systémom, ktorý zodpovedá miestnym, národným a medzinárodným normám a je pravidelne testovaný.

• Zariadenia na spracovanie informácií spravované organizáciou sú fyzicky oddelené od prostriedkov neoprávnených osôb.

• Nie je dovolené nechávať osobné údaje voľne k dispozícii bez dohľadu. Platí, že písomnosti a iné nosiče osobných údajov je dovolené uchovávať samostatné len v uzamykateľných miestnostiach, prípadne iba v uzamykateľných skriniach.

• Prístup do kancelárií alebo archívov, kde sú tieto osobné údaje uložené, je umožnený iba oprávneným zamestnancom spoločnosti, a to pomocou prístupovej karty / fyzického kľúča.

• Priestory spoločnosti, v ktorých sú uložené osobné údaje, sú pod 24 hodinovým kamerovým dohľadom. Spracovanie formou kamerového systému je upravené v samostatnom internom predpise.

• Fyzický prístup do serverovne je umožnený len pracovníkom IT.

• Je vyžadované dodržiavať zásady prázdneho stola a zamknutej obrazovky.

- **IT bezpečnosť**

Popisuje prijaté technické opatrenia, ktoré slúžia na zaistenie bezpečnosti osobných údajov v elektronickej forme. Zameriava sa na to, ako sú nastavené prístupové oprávnenia do informačného systému spracovávajúceho osobné a citlivé údaje, aby bolo zaistené pristupovanie iba oprávnených osôb k údajom zodpovedajúcim práve týmto oprávneniam. Ďalej akým spôsobom sa obstarávajú elektronické záznamy (logy), ktoré

umožnia určiť a overiť, kedy a kým sa nakladalo s údajmi. Ako je zabránené neoprávnenému prístupu k dátovým nosičom a ako je s nimi nakladané v prípade nepredvídateľnej udalosti - požiar, povodeň, sťahovanie, výpadok prúdu a pod.

• Riadenie prístupov sa riadi interným predpisom na riadenie prístupov spoločnosti a stanovuje pravidlá pre riadenie prístupov bežných aj privilegovaných užívateľov do systémov spoločnosti.
• Prístup k osobným údajom je prideľovaný len v rozsahu nevyhnutne potrebnom pre výkon funkcie a revíziu týchto pridelených prístupov prebieha pravidelne. V prípade zistenia neoprávneného prístupu sa tento prístup následne odoberá. Ďalej je zabezpečená kontrola nezlučiteľných oprávnení.
• Je zavedená a udržovaná evidencia jednotlivých rolí týkajúcich sa bezpečnosti IT, pri ktorých je jednoznačne stanovená zodpovednosť a pracovná náplň s cieľom znížiť riziká vyplývajúce z ľudského faktora (neúmyselných chýb, krádeže, podvodu alebo zneužitia).
• Ak prevádzka IT, spracovanie účtovníctva či iné externe spracovávané agendy vyžadujú prístup dodávateľov, musí byť tento prístup riešený zmluvne, v súlade s bezpečnostnou dokumentáciou tak, aby bola zaistená bezpečnosť osobných údajov vnútri aj mimo spoločnosti.
• Používatelia, IT administrátori aj dodávatelia môžu využívať vzdialené prístupy k IT prostrediu spoločnosti len na základe ich pracovných a zmluvne prevzatých povinností a kompetencií, a to len s využitím schválených komunikačných prostriedkov. Možnosť využívania vzdialeného prístupu musí podliehať pravidelnej revízii.
• O jednotlivých prístupoch na úrovni domény sú automaticky zhotovované logy s kapacitou cca 30 dní.
• Hlavný PMS systém automaticky vyhotovuje logy o všetkých aktivitách používateľov s kapacitou cca 30 dní.
• Je zabezpečené pravidelné vyhodnocovanie logovaných aktivít a ochrana logov (tzv. zaistenie nepopierateľnosti vytvorených logov, overenie možnosti ich modifikácie vonkajšími vplyvmi (malware, ľudský faktor)).
• Prideľovanie hesiel sa riadi interným predpisom.
• Je povolené prevádzkovať len schválený, legálne nadobudnutý a evidovaný SW a HW v zhode s licenčnou dohodou výrobcu a spôsobov využitia. Tento SW a HW majetok je evidovaný v evidencii informačných aktív a ich nákup je vždy diskutovaný a schválený

IT oddelením.

• Je zabezpečená správa opravných a aktualizačných balíkov programového vybavenia.

• Informačné aktíva musia byť chránené pred počítačovými vírusmi, spamom, spyware a iným škodlivým kódom správnym nastavením bezpečnostných mechanizmov a použitím vhodného SW aplikovaného na relevantné komponenty počítačovej siete (servery, firewally aj jednotlivé pracovné stanice a mobilné zariadenia v správe spoločnosti).

• IT oddelenie musí definovať a udržiavať plán obnovy po infiltráciu IT prostredia škodlivým kódom. Tento plán musí byť pravidelne raz za rok aktualizovaný na základe aktuálnych potrieb.

• Zálohovanie osobných údajov sa riadi interným predpisom na zálohovanie dát spoločnosti. Zálohy sú uchovávané v trezore spoločnosti umiestnenom v inom priestore, ako je serverová miestnosť.

• Použitie USB kľúčov (okrem USB kľúča poskytnutého IT oddelením) je blokované. USB kľúče poskytnuté IT oddelením sú šifrované.

• Použitie verejných úložísk, služieb a nástrojov (Dropbox, Google Drive, uloz.to, uschovna.cz, leteckaposat.cz, torrents, P2P, Basecamp, Slack, apod.) je zakázané.

• Osobné a citlivé údaje nesmú opustiť chránené IT prostredie spoločnosti v nezašifrovanej forme. K ich zabezpečeniu zaisťuje IT oddelenie kryptografické prostriedky a pravidlá riadenia šifrovacích kľúčov.

• Komunikačné rozhrania so systémami spoločnosti musia byť zabezpečené.

• Informačné aktíva, ktorá slúžila k uchovávaniu alebo prenosu osobných údajov a už nie sú ďalej potrebné alebo dosiahli koniec svojej životnosti, sú bezpečne zlikvidované a je uchovaný záznam o ich likvidácii.

• V prípade interného vývoja a zmien v informačných systémoch sú stanovené zásady a pravidlá pre evidenciu a riadenie vývoja nového a zmien existujúceho informačného systému spoločnosti

- **Narušenie zabezpečenia osobných údajov**

Ide o riešenie zistenia a posúdenia narušenia zabezpečenia osobných údajov, tzn. postup, ak nastane udalosť, ktorá môže mať za následok vznik bezpečnostného incidentu. Popisuje zodpovednosť za riešenie incidentu, kam je zaznamenaný a aké kroky nasledujú po zistení incidentu. Povinnosťou je prijať opatrenia k zamedzeniu opakovania bezpečnostného incidentu.

V prípade zistenia porušenia zabezpečenia osobných údajov je nevyhnutné:

1. Oznámiť zistenie zodpovednej osobe

2. Zamedziť ďalšiemu úniku - fyzickým zamknutím dokumentov alebo v prípade elektronickej formy zamedzením prístupu alebo vypnutím IT systémov

3. Prípad narušenia zabezpečenia posúdiť a zdokumentovať (čo sa stalo, aké a čie osobné údaje unikli, možné následky, opis prijatých opatrení s cieľom vyriešiť daný prípad, identifikácia rizika / vysokého rizika)

4. Ohlásiť porušenie zabezpečenia dozornému úradu bez zbytočného odkladu a pokiaľ možno do 72 hodín od okamihu, keď sa o ňom spoločnosť dozvedela

5. Oznámiť porušenie zabezpečenia bez zbytočného odkladu subjektu údajov, ak je pravdepodobné, že daný prípad bude mať za následok vysoké riziko pre práva a slobody fyzických osôb

Kontaktné miesto pre oznámenie zistenia porušenia zabezpečenia:	Kontakt na zodpovednú osobu, vrátane kontaktných informácií, t.j. telefón a email

- **Kontrolná činnosť**

Kontrola prístupu a práca s osobnými údajmi, a to vrátane periodicity kontrol zodpovednou osobou, výstupy kontrol a pod.

Osoby zodpovedné za jednotlivé oblasti podľa katalógu spracovania osobných údajov zabezpečia kontrolu plnenia povinností vyplývajúcich z tohto interného predpisu. Kontroly sú v nasledujúcom rozsahu:

a) 1 krát ročne dôkladná kontrola celej spoločnosti zodpovednou osobou

b) 1 krát mesačne náhodná kontrola vybraného informačného systému alebo úseku zodpovednou osobou

c) Každodenne kontrola fyzickej ochrany rizikových miest zodpovednou osobou

d) Kontrola po zmene a následnom školení k zmenám zákonov alebo interných predpisov, vrátane tohto interného predpisu

e) Mimoriadna kontrola po riešení narušenia zabezpečenia osobných údajov

O pravidelných kontrolách je vykonaný záznam a ten je uložený. V prípade nálezov kontroly prebieha konzultácia, prípadne ad hoc preškolenie.

- **Školenie zamestnancov**

Zahŕňa proces vzdelávania zamestnancov v súvislosti s ochranou osobných údajov, periódy školenia, výstupy zo školení. Ďalej postup preškolenia v prípade prijatia nového zamestnanca alebo preradenie zamestnanca na inú pozíciu.

Preškoľovanie zamestnancov prebieha formou e-learningu zameraného na informačnú bezpečnosť a ochranu osobných údajov a to ako pri nástupe, tak pravidelne aspoň 1 krát ročne. Evidencia o absolvovaní školenia je spracovávaná personálnym oddelením spoločnosti. Za preškolenie zamestnancov zodpovedá zodpovedná osoba.

4.8.6.2 Ostatné opatrenia

- **Pravidelná revízia a aktualizácia interných predpisov**

Popisuje spôsob zaistenia pravidelnej revízie v spoločnosti a aktualizáciu interných predpisov, vrátané tých týkajúcich sa ochrany osobných údajov.

Všetky interné predpisy spoločnosti, vrátane tých, ktoré sa týkajú ochrany osobných údajov sú revidované pravidelne 1 krát ročne. Ad hoc revízia je vykonávaná najmä v prípade výraznejších zmien v spoločnosti s možným vplyvom na ochranu osobných údajov alebo v prípade narušenia zabezpečenia ochrany osobných údajov. O vykonaní revízie a aktualizácie je vedená evidencia. Za revíziu a aktualizáciu zodpovedá zodpovedná osoba.

- **Vedenie a aktualizácie katalógu spracovania**

Obsahuje postup pre vedenie a aktualizáciu katalógu spracovania, osobu zodpovednú za vedenie a aktualizáciu a miesto zaznamenania.

Katalóg spracovania v prílohe tohto dokumentu je súčasťou pravidelnej revízie a aktualizácie interných predpisov. Revízia kompletnosti a presnosti katalógu spracovanie je vykonávaná pravidelne 1 krát ročne. Ad hoc revízia je vykonávaná najmä v prípade výraznejších zmien v spoločnosti s možným vplyvom na ochranu osobných údajov. O vykonaní revízie a aktualizácie je vedená evidencia. Za revíziu a aktualizáciu zodpovedá

zodpovedná osoba.

- **Spracovateľské vzťahy**

Opisujú postup pre riadenie vzťahov s dodávateľmi, ktorí v rámci svojej činnosti spracúvajú osobné údaje. Popisujú, kto schvaľuje výber spracovateľov a na základe akých kritérií.

Výber spracovateľov schvaľuje zodpovedná osoba. Pri výbere spracovateľov hodnotí najmä nasledujúce faktory:

• Schopnosť dodávateľa uzavrieť a dodržiavať povinnosti ustanovené spracovateľskou zmluvou

• Dostatočné zabezpečenie osobných údajov

• Dobrá povesť dodávateľa v rámci ochrany osobných údajov

• Relevantné certifikácie ochrany osobných údajov alebo ochrany informácií všeobecne

• Ďalšie relevantné faktory vo vzťahu ku konkrétnemu účelu spracovania

O splnení kritérií výberu dodávateľa je vedená evidencia.

- **Riadenie projektov a zmien**

Popisuje postup pre zohľadnenie aspektov ochrany osobných údajov v rámci nových projektov a riadenie zmien podľa princípu zámernej a štandardnej ochrany. Uvádza osoby, ktoré sú v rámci tohto postupu zapojené a výstupy vyplývajúce z posúdenia aspektov ochrany osobných údajov.

V prípade významnejších zmien v spoločnosti s vplyvom na ochranu osobných údajov (napr. nový IT systém, nový účel spracovania, vrátane novej služby alebo produktu, a pod.) Je do týchto aktivít zapojená zodpovedná osoba, ktorá identifikuje prípadné riziká pre ochranu osobných údajov a pomôže navrhnúť adekvátne opatrenia na zníženie týchto rizík. V prípade potreby vykoná revíziu a aktualizáciu tohto interného predpisu, vrátane analýzy rizík alebo aktualizácie katalógu spracovania, prípadne ďalších relevantných interných predpisov.

- **Predávanie osobných údajov do tretích strán**

Obsahuje postup, podľa ktorého je v spoločnosti postupované v prípade prenosu osobných údajov do tretích krajín. Skladá sa zo zoznamu zmlúv a prípadných dohôd s

partnermi (cestovnými kanceláriami, agentúrami pod., kde je zachytený prenos osobných údajov do tretích krajín. V rámci činnosti spoločnosti nedochádza k prenosu osobných údajov do tretích krajín.

4.8.7 Výkon práv dotknutých osôb

Skladá sa z postupu a kontaktného miesta, kde môžu dotknuté osoby kontaktovať spoločnosť s požiadavkami na realizáciu nižšie uvedených práv. Tieto informácie je možné uviesť v rámci oznámenia na splnenie informačnej povinnosti.

- **Poskytovanie informácií**

Postupy, v rámci ktorých poskytujeme subjektom údajov informácie o spracovaní. Informácie o spracovaní osobných údajov zamestnancov či uchádzačov o zamestnanie môžu byť súčasťou pracovnej zmluvy, osobného dotazníka alebo samostatného formulára alebo interného dokumentu, s ktorým sa musí zamestnanec pri nástupe zoznámiť. Informácie o spracovaní osobných údajov klientov je možné vykonať v rámci registračnej karty, webových stránok alebo ubytovacieho poriadku spoločnosti.

Spoločnosť poskytuje subjektom údajov informácie v súlade s GDPR, a to v požadovanom rozsahu, čím zaisťuje transparentnosť spracovania.

- **Právo dotknutých osôb na prístup k osobným údajom**

Popisuje postup ako je riešené právo na prístup k osobným údajom, a to ako v prípade zamestnancov, tak aj v prípade zákazníkov.

V prípade, že o to dotknutá osoba požiada, spoločnosť poskytne subjektu údajov potvrdenie, či osobné údaje, ktoré sa ho týkajú, sú alebo nie sú spracovávané, a ak je to tak, umožní dotknutým osobám získať prístup k týmto osobným údajom a k informáciám spôsobom a v rozsahu podľa GDPR.

- **Právo na opravu**

Popisuje postup, ako je riešené právo na opravu k osobným údajom, a to ako v prípade zamestnancov, tak aj v prípade zákazníkov.

V prípade, že o to dotknutá osoba požiada, prípadne sa o nepresných osobných údajoch dozvie spoločnosť inak, opraví bez zbytočného odkladu nepresné osobné údaje. V prípade, kedy si to účel spracovania vyžaduje, zaistí spoločnosť doplnenie neúplných osobných údajov podľa GDPR.

- **Právo na vymazanie**

Popisuje postup, ako je riešené právo na vymazanie osobných údajov, a to ako v prípade zamestnancov, tak aj v prípade zákazníkov. Je možné zriadiť zvláštny emailový účet (gdpr@hotel.sk) alebo formulár na webovej prezentácii, na ktorý môžu zákazníci klásť svoje požiadavky a uplatňovať v tomto internom predpise uvedené práva. Nezabudnite na prípadné napojenie na archivačný a skartačný poriadok spoločnosti. V prípadoch a), d) a e) by sa mali zaviesť postupy pre výmaz osobných údajov bez ohľadu na to, či o to subjekt údajov požiada.

V prípade, že je daný jeden z nasledujúcich dôvodov, zaistí spoločnosť na základe uplatnenia práva subjektom údajov bez zbytočného odkladu vymazanie osobných údajov:

a) osobné údaje už nie sú potrebné na účely, na ktoré boli zhromaždené alebo inak spracované;

b) dotknutá osoba odvolá súhlas, na základe ktorého boli osobné údaje spracovávané a neexistuje žiadny ďalší právny dôvod pre spracovanie;

c) dotknutá osoba vznesie námietky proti spracovaniu a neexistujú žiadne prevažujúce oprávnené dôvody pre spracovanie;

d) osobné údaje boli spracované nezákonne;

e) osobné údaje sa musia vymazať na splnenie zákonnej povinnosti, ktorá sa na spoločnosť vzťahuje;

f) osobné údaje boli zhromaždené v súvislosti s ponukou služieb informačnej spoločnosti

- **Právo na obmedzenie spracovania**

Popisuje postup, ako je riešené právo na obmedzenie spracovania osobných údajov, a to ako v prípade zamestnancov, tak v prípade zákazníkov.

V prípade, že je daný jeden z nasledujúcich dôvodov, zaistí spoločnosť obmedzenie spracovania osobných údajov:

a) subjekt údajov popiera presnosť osobných údajov;

b) spracovanie je protiprávne a dotknutá osoba namieta voči vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;

c) spoločnosť už osobné údaje nepotrebuje na účely spracovania, ale subjekt údajov ich

požaduje pre určenie, výkon alebo obhajobu právnych nárokov;

d) dotknutá osoba vzniesla námietku proti spracovaniu.

- **Právo na prenosnosť údajov**

Definuje postup, ako je riešené právo na prenosnosť osobných údajov.

V prípade, že o to subjekt údajov požiada a zároveň je spracovanie založené na súhlase alebo zmluve, a zároveň sa spracovanie vykonáva automatizovane, umožní spoločnosť subjektu údajov výkon práva na prenosnosť. Osobné údaje, ktoré subjekt údajov spoločnosti poskytol, a ktoré sa ho týkajú, poskytne spoločnosť v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte. Súčasťou tohto práva je zabezpečenie možnosti prenesenia predmetných osobných údajov k inému správcovi podľa požiadavky subjektu údajov. Definuje postup, ako je riešené právo na prenosnosť osobných údajov.

4.8.8 Archivácia osobných údajov

Obsahuje postup, prípadne vypísané dokumenty, ktoré upravujú archivácie osobných údajov v spoločnosti. Definuje účel archivácie a dobu archivácie.

Archív je prevádzkovaný samotným správcom. Rozsah údajov k archiváciu a archivačná doba vyplýva z katalógu spracovania osobných údajov. Prístup do archívu majú len osoby v konkrétnych pracovných pozíciách za vopred daných dôvodov a pre naplnenie niektorého z účelov predvídaných GDPR.

Pracovné pozície	**Kategórie osobných údajov**	**Dôvod prístupu do archívu**
Vedúci recepcie	Meno, priezvisko, adresa trvalého pobytu, začiatok a koniec ubytovania	Podanie informácie o pobyte klienta na základe žiadosti cudzineckej polície

- **Archivácia osobných údajov klientov**

Archivácia osobných údajov klientov sa riadi okrem iného § 101 zákona č. 326/1999 Zb. o pobyte cudzincov na území Slovenskej republiky, ktorý ukladá povinnosť ubytovateľmi viesť domovú knihu a uchovávať ju po dobu 6 rokov od posledného zápisu. Podľa zákona č. 565/1990 Zb. o miestnych poplatkoch, vedie organizácia v písomnej podobe evidenčnú knihu, do ktorej zapisuje dobu ubytovania, účel pobytu, meno, priezvisko, adresu miesta

trvalého pobytu alebo miesta trvalého bydliska v zahraničí a číslo občianskeho preukazu alebo cestovného dokladu fyzickej osoby, ktoré ubytovanie poskytol. Zápisy do evidenčnej knihy sú vedené prehľadne a zrozumiteľne a sú usporiadané chronologicky. Evidenčná kniha sa uchováva po dobu 6 rokov od vykonania posledného zápisu.

- **Archivácia osobných údajov ďalších subjektov údajov (napr. zamestnancov)**

Osobné spisy sa archivujú 10 rokov s výnimkou dokladu o dĺžke zamestnania, kde archivačné lehota je 20 rokov, pretože tento doklad môže slúžiť na účely dôchodkového poistenia. Mzdový list musí organizácia archivovať po dobu 20 rokov nasledujúcich po roku, ktorého sa posledné účtovné záznamy v mzdovom liste týkajú. Účtovná závierka a výročná správa sa uschováva po dobu 10 rokov začínajúcich sa koncom účtovného obdobia, ktorého sa týkajú, a účtovné záznamy (napr. na účely sociálneho zabezpečenia, verejného zdravotného poistenia) po dobu 5 rokov začínajúcich sa koncom účtovného obdobia, ktorého sa týkajú.

4.8.9 Likvidácia osobných údajov

Spoločnosť vykonáva likvidáciu osobných údajov, akonáhle pominie účel, na ktorý boli osobné údaje spracovávané, prípadne na základe žiadosti subjektu.

Pri likvidácii sú dodržiavané zákonné výnimky týkajúce sa uchovávania osobných údajov na účely archívnictva a uplatňovaní práv v občianskom súdnom konaní, trestnom konaní a správnom konaní.

Likvidácia osobných údajov je vykonávaná certifikovanou externou spoločnosťou na základe zmluvy o spracovaní osobných údajov. O skartáciu je vydané potvrdenie.

4.8.10 Záverečné ustanovenia

Za dodržiavanie interného predpisu zodpovedajú všetci zamestnanci spoločnosti. Zamestnanci potvrdzujú svojím podpisom, že boli oboznámení s týmto interným predpisom.

5 VYHODNOTENIE ZVOLENÉHO RIEŠENIA A JEHO REÁLNA REPLIKOVATELNOSŤ

Každé riešenie podľa nariadenia GDPR je unikátne. Univerzálne riešenie neexistuje a pre každú spoločnosť znamená niečo iné. Veľa firiem poskytuje typizované produkty, audity, školenia či balíkové software. To však vylučuje rozsiahlu možnosť jeho aplikácie.

Zvolené riešenie popisuje príklad faktického stavu a zvolené opatrenia zavedené v reálnom zariadení v rámci prípravy na GDPR. Definuje jasne a zrozumiteľne nastavenia procesov, ktoré sa vzťahujú k životnému cyklu spracovania osobných údajov. Zoznamuje organizácie s problematikou ochrany osobných údajov, objasňuje hlavné pojmy, pomáha zabezpečiť dodržiavanie povinností vyplývajúcich z GDPR v spoločnosti a všeobecne posúdiť dôsledky nariadenia na prostredie a rozhodnúť sa, akým spôsobom ďalej postupovať. Poskytuje návrh vhodného postupu na riadenie procesu pri internom dátovom audite organizácie, popisuje povinnosti spoločností a podnikateľov, práva dotknutých osôb a zmeny v oblasti spracovania osobných údajov na praktických príkladoch a aplikovanie vlastného návrhu v zvolenej organizácií z hľadiska zodpovedných osôb, zásad spracovania údajov, fyzickej ako aj IT bezpečnosti, archivácie, kontrolnej činnosti, likvidácie a i. zavedené v zariadení v rámci prípravy na GDPR.

GDPR vzniklo pre to, aby si niektoré subjekty uvedomili, že osobné údaje sú vlastníctvom a súčasťou súkromia občana. Digitalizácia prudko narastá a ochranu súkromia je potrebné v online svete nejakým spôsobom ukotviť, aspoň na úrovni EÚ, ak to nejde globálne.

Myslím si, že nariadenie je formulované nejasne a pokuty sú vysoké. Mnoho vecí bude sporných. GDPR sa netýka fyzických osôb, nepodnikateľov, ktorí používajú osobné údaje pre domáce použitie (napr. kontakty v mobilnom telefóne). Čiže netýka sa úplne každého, ale primárne komerčných subjektov a verejnej správy. Inak okrem výšky pokút obsahoval donedávna platný zákon o OOU veľa z toho, čo je nariadením vyžadované, len to nikto nedodržiaval.

GDPR nemáme vnímať ako nutné zlo zbytočných nákladov. Nariadenie je pre organizáciu veľkým prínosom z hľadiska automatizácie procesov, vyššej bezpečnosti, lepšiemu využitiu dát vzájomným prepojením a lepšej organizácií práce. Kvalitný manažér má náklady na GDPR vedieť čo najlepšie využiť a dokázať nájsť návratnosť

investícií.

Malé firmy sa môžu uspokojiť s tzv. „GAP“ analýzou a implementovaním nevyhnutných požiadaviek. Je možné ich kúpiť od rôznych dodávateľov na trhu. Veľké korporácie a spoločnosti musia podľa môjho názoru bezodkladne rozpracovať komplexnú implementačnú mapu. Tá musí reflektovať na existujúcu stratégiu riadenia dát v danej organizácií. Dôležité je uvažovať v strednodobom horizonte a zvoliť stratégiu s ohľadom na aktuálny stav spoločnosti ako aj očakávaný vývoj. Treba si taktiež rozmyslieť zavádzanie nových technológií, čím môžeme značne ovplyvniť životnosť navrhnutých implementačných opatrení a aj celkový výsledok. 100% súlad s GDPR nám nedá nikto. Samotný zákon je navrhnutý nedokonale s právnymi kuriozitami a technickými obmedzeniami. Z tohto dôvodu bude nevyhnuté akceptovať trhliny a rozplánovať s ohľadom na vývoj legislatívy do nasledujúcich období.

5.1 Prínosy vzniku nariadenia GDPR

- **Úspora a náklady**

Splnenie pravidiel nebudú mať na starosti národné úrady. ale jeden európsky orgán. Rovnako ochranu osobných dát bude upravovať jedna európska norma miesto 28 národných. Prínosom pre firmy bude obmedzenie byrokracie a možnosť rýchlejšie sa rozhodovať.

Harmonizácia pravidiel získavania a uchovávania osobných údajov

Vlajkovou loďou je najmä zjednotenie právneho rámca. Spoločnosti musia však brať do úvahy aj legislatívu platnú na národnej úrovni. Môže ísť napríklad o zabezpečenie ochrany slobôd a práv pri spracúvaní osobných údajov pracovníkov v rámci zamestnania, kde sú dôležité ustanovenia kolektívnej zmluvy alebo národnej legislatívy. Zavedenie nariadenia môže pomerne zjednodušiť cezhraničný dosah spoločností.

- **Ochrana záujmov**

Nariadenie povolí širšie uplatnenie princípu spracovávať osobné údaje len v súlade so záujmami fyzických osôb a na spracovanie dát musia spoločnosti získavať súhlas. Dôvodom na spracovanie dát bude okrem ochrany dotknutých osôb aj ochrana ľudí v blízkom vzťahu s danou osobou.

- **Nové podmienky spracovania údajov a zvyšovanie povedomia o bezpečnosti údajov**

Firmy budú mať voľnejšie ruky. Vzniká nová situácia vytvárajúca právny základ na spracovanie dát s ohľadom na verejný záujem. Údaje môžeme spracovávať aj v záujme ochrany verejného zdravia. Dôvodom na spracovanie osobných dát sú aj vedecké, štatistické alebo historické dôvody.

- **Nie je potrebná identifikácia**

Pri práci s osobnými údajmi, ktoré nevyžadujú získanie totožnosti osoby, spoločnosť nemusí doplnkové informácie získavať, uchovávať alebo spracúvať.

- **Identita**

Ľudia získavajú určité dodatočné práva a prevádzkovateľ má právo vyžiadať si potvrdenie identity skôr ako práva prizná.

- **Zvýšenie bezpečnosti a sloboda vo výbere prostriedkov pre zvýšenie ochrany údajov**

V rámci nariadenia GDPR je potrebné prijať postupy pre bezpečnosť údajov. Zamedziť únik údajov a záznamov prípadne stratu zariadenia (mobil, laptop).

- **Ochrana dobrého mena a reputácie**

Občania chcú byť informovaní o prípadnej strate osobných údajov. Ak nemajú úplnú kontrolu nad údajmi poskytujúcimi online sú znepokojení. Najväčším rizikom je pre dotknuté osoby zneužitie ich online identity. Len 20% ľudí je oboznámených s privacy policy web stránky.

- **Orientácia na zákazníka (občana)**

GDPR prináša transparentný a lepší vzťah s klientom založený na dôvere. Firma získa viac údajov od zákazníka a bude sa vedieť rozhodnúť sa na základe kvalitnejších dát. Výhodou bude lepšie pochopenie správania zákazníka. [22]

5.2 Negatívne dopady vzniku nariadenia GDPR

- **Nadobudnutie súhlasu**

Pri spracovaní osobných údajov musí dotknutá osoba súhlasiť so spracovaním jej údajov a môže tento súhlas kedykoľvek odvolať. Získanie povolenia bude náročnejšie

a spoločnosť musí vedieť preukázať, že súhlas dostala. Nariadenie sprísňuje ochranu mladistvých. Skomplikovať situáciu môže firmám fakt, že za mladistvé osoby do šestnásť rokov vyjadruje súhlas zákonný zástupca. Hranica veku sa môže v členských štátoch odlišovať.

- **Minimalizácia údajov**

Firmy môžu dáta používať pre spracovanie len v nevyhnutnom období a len tie, ktoré skutočne potrebujú pre svoju činnosť.

- **Prehľadné spracovávanie**

Prevádzkovatelia musia informovať osoby o používaní ich údajov a umožniť im prístup k týmto dátam. Zákonné, spravodlivé a transparentné spracovanie údajov výrazne zaťažuje prevádzkovateľov. Je potrebná dodatočná administratívna práca, čím je aj prehĺbenie „práva byť zabudnutý“.

- **Princípy „protection by design“ a „by default“**

Spoločnosti musia klásť doraz už pri vývoji svojich produktov a služieb na dodatočné kroky ochrany osobných údajov. To môže spôsobiť zaťažujúce a náročné zmeny vo výrobe. Každý musí vykonávať špecifickú ochranu súkromia a myslieť popri ochrane dát aj na spôsob pracovania s údajmi.

- **Územná platnosť**

Dodržiavanie nariadenia GDPR siaha aj za hranice mimo EÚ a zahŕňa veľa dodatočných nákladov. Týka sa firiem poskytujúcich služby alebo tovar dotknutým osobám v EÚ alebo kontrolujú ich správanie. [22]

ZÁVER

Cieľom nariadenia o ochrane osobných údajov je vytvoriť harmonizovaný právny rámec ochrany dát pre celú EÚ. Vrátiť kontrolu nad osobnými dátami späť do rúk občanov a zároveň zaviesť striktné pravidlá pre osoby, ktoré zabezpečujú hosťovanie a spracovanie' týchto dát kdekoľvek na svete. Zároveň zavádza pravidlá týkajúce sa voľného pohybu osobných údajov v rámci EÚ aj mimo nej.

Cieľom práce je definovať požiadavky na kľúčové procesy a navrhnúť postup na zabezpečenie zhody s podmienkami GDPR. Myslím si, že cieľ tejto práce sme splnili. Návrh bude podkladom pre konkrétne zariadenie a zároveň prínosom a pomôckou pre ostatné organizácie pre zabezpečenie jednotných pravidiel pre spracovanie údajov. Poskytuje ucelený postup na zabezpečenie zhody s podmienkami GDPR

Jednotlivci majú oveľa lepší prehľad o význame dát, rozumejú, ako obchodné značky využívajú ich dáta pri predaji a marketingu a uvedomujú si svoje práva vo vzťahu k svojim osobným dátam.

Každý z vyššie uvedených krokov zaberie určitý čas, preto je vhodné pripraviť sa na GDPR s dostatočným predstihom a v spolupráci s kvalifikovaným odborníkom. Príprava totiž nemusí spočívať iba vo vypracovaní a aktualizácii potrebnej dokumentácie, ale aj v podstatných zmenách nastavenia IT systémov či v prijatí rôznych iných opatrení.

Niekomu sa môže zdať, že ide o reguláciu, ktorá sa snaží vziať kúsok našej slobody. Naozaj však ide o skutočné zabezpečenie základnej slobody občanov, nakoľko je zjavné monitorovanie osôb korporáciami a vládou.

Akékoľvek dáta a informácie, ktoré vedú k identifikácií osobných údajov jednotlivcov (v v oblasti zdravia, genetiky, ekonomickej, sociálnej, kultúrnej situácie) budú pod ochranou. Požiadavky a zásady GDPR musí dodržiavať každá spoločnosť aj mimo Únie, ktorá pracuje s údajmi občanov. Európska legislatíva prvýkrát presadzuje zásady ochrany osobných údajov pre zvyšok sveta.

Dôležité je nepodceniť prípravu a nariadeniu o ochrane osobných údajov venovať patričnú pozornosť.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů : redakční uzávěrka 28.8.2017. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.

[2] DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[3] NEZMAR, L. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[4] Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.

[5] IRWIN, L. 2018. The GDPR: What technical measures do you need to conduct?. [online]. [cit. 23. apríla 2018]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-what-technical-measures-do-you-need-to-conduct/

[6] ZIMEN, O. 2018. Posúdenie vplyvu na ochranu údajov podľa GDPR**.** [online]. [cit. 23. apríla 2018]. Dostupné z: https://www.pravnenoviny.sk/posudenie-vplyvu-na-ochranu-udajov-podla-gdpr

[7] QUALITYAUSTRIA. 2017. [online]. [cit. 18. októbra 2017]. Dostupné z: http://www.qualityaustria.cz/ochrana-osobnich-udaju-meni-tvar-aneb-gdpr-v-praxi

[8] VAVRO, T. 2017. Nové pravidlá v oblasti ochrany osobných údajov. [online]. [cit. 17. októbra 2017]. Dostupné z: https://www.podnikajte.sk/pravo-a-legislativa

[9] SNREAL. 2017. [online]. [cit. 16. októbra 2017]. Dostupné z: http://www.snreal.sk/bpis.php

[10] ŠKORNIČKOVÁ, E. 2017. [online]. [cit. 15. októbra 2017]. Dostupné z: https://www.gdpr.cz/gdpr/

[11] SOITRON. 2017. [online]. [cit. 18. októbra 2017]. Dostupné z: https://www.soitron.sk/gdpr/

[12] UOOU. 2017. [online]. [cit. 22. októbra 2017]. Dostupné z: https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-

odpovedich/d-23790/p1=3735

[13] SYSTEMONLINE. 2017. [online]. [cit. 22. októbra 2017]. Dostupné z: https://www.systemonline.cz/it-pravo/resite-uz-gdpr-a-urcite-jste-na-nic-nezapomneli-1.htm

[14] ZACHAR, M. 2017. Skúsenosti z prípravy na GDPR. [online]. [cit. 18. októbra 2017]. Dostupné z: https://www.pcrevue.sk/a/Skusenosti-z-projektov-pripravy-na-GDPR

[15] IDS Advisory. 2017. GDPR. [online]. [cit. 16. októbra 2017]. Dostupné z: http://www.idsa.cz/cs/gdpr?gclid=EAIaIQobChMI5LyfwdXv1gIVhhXTCh0OdQcGEAAYASAAEgJAyfD_BwE

[16] IBM. 2017. [online]. [cit. 14. októbra 2017]. Dostupné z: https://www.ibm.com/

[17] TCOX. 2017. [online]. [cit. 18. októbra 2017]. Dostupné z: http://www.tcox.cz/gdpr/kurz/poverenec-pro-ochranu-osobnich udaju/?gclid=EAIaIQobChMI5LyfwdXv1gIVhhXTCh0OdQcGEAAYAyAAEgIw7PD_BwE

[18] SASINEK, M. 2018. 10 pravidiel implementácie GDPR. [online]. [cit. 25. apríla 2018]. Dostupné z: https://blog.etrend.sk/martin-sasinek/10-pravidiel-implementacie-gdpr.html

[19] Advokátska kancelária RELEVANS s.r.o. 2018. NOVÉ PRAVIDLÁ EÚ O OCHRANE OSOBNÝCH ÚDAJOV VRÁTIA KONTROLU SPÄŤ DO RÚK OBČANOV [online]. [cit. 22. februára 2017]. Dostupné z: http://www.relevans.sk/pravny-bulletin/nove-pravidla-eu-o-ochrane-osobnych-udajov-vratia-kontrolu-spat-do-ruk-obcanov/

[20] AUTOCONT. 2018. Nové pravidlá v oblasti ochrany osobných údajov. [online]. [cit. 3. marca 2018]. Dostupné z: http://www.autocont.cz/Public/Files/produkt-listy/Audit-shody-osobnich-udaju-s-gdpr.pdf

[21] MOBILMANIA. 2018. Blíži se konec volně dostupných Wi-Fi. [online]. [cit. 8. marca 2018]. Dostupné z: https://www.mobilmania.cz/clanky/blizi-se-konec-volne-dostupnych-wi-fi-provozovatele-za-mohou-dostavat-pokuty/sc-3-a-1341064/default.aspx

[22] BOJTOS. 2018. Praktické skúsenosti s prípravou na GDPR z pohľadu poskytovateľov zdravotnej starostlivosti. [online]. [cit. 8. marca 2018]. Dostupné z: http://www.finreport.sk/ekonomika/eu-si-slubuje-od-gdpr-uspory-vyrazne-su-aj-negativa/

[23] ZOOU. 2018. Zálohovanie dát v praxi a GDPR. [online]. [cit. 9. marca 2018].

Dostupné z: http://www.zoou.sk

[24] ČÍŽEK, J. 2018. Blíži se reforma soukromí GDPR. [online]. [cit. 19. marca 2018]. Dostupné z: https://www.zive.cz/clanky/blizi-se-reforma-soukromi-gdpr-experti-varuji-ze-muze-zpusobit-problemy-blockchainu-i-ai/sc-3-a-192034/default.aspx

[25] PEŤKOVÁ, Z. Firmy čaká revolúcia v ochrane dát. Trend. 2017, 26(47), 61-62. ISSN 1335-0684

[26] MEKYŇOVÁ, J. Osobné údaje?. Profit. 2016, 22(11), 12-14. ISSN 1335-4620

[27] STRAKA, I. Pól milióna firiem čakajú pravidlá v ochrane osobných údajov. Kvalita. 2017, 25(3), 30-31. ISSN 1335-9231

[28] KOLLÁROVÁ, Z. Nové pravidlá ochrany osobných dát. 2017, 26(42), 60-62. ISSN 1335-0684

[29] TECHBIT. 2017. Nařízení GDPR z pohledu IT – úvod do problematiky nařízení GDPR. [online]. [cit. 22. apríla 2018]. Dostupné z: https://www.techbit.cz/2017/1-narizeni-gdpr-z-pohledu-it-uvod-do-problematiky-narizeni-gdpr/

[30] TECHBIT. 2018. Interný audit GDPR. [online]. [cit. 26. apríla 2018]. Dostupné z: https://www.bdo.cz/

[31] IAPP. 2018. GDPR. [online]. [cit. 26. apríla 2018]. Dostupné z: https://iapp.org/search?q=gdpr

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

EÚ Európska Únia

GDPR General Data Protection Regulation

ICT Informačno-komunikačné technológie

OOU Ochrana osobných údajov

OÚ Osobné údaje

IS Informačný systém

DPIA Posúdenie vplyvu ochrany údajov

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

SLOVNÍK POJMOV

Tab. 1. Slovník pojmov 1

Anonymizácia	Ide o nevratný proces, kedy zakrytie identity už nikdy nikto nedokáže vyčítať.
Bitlocker	Bitlocker je funkcia šifrovania celého disku, ktorá je súčasťou systému Windows Vista a neskôr. Je určený na ochranu údajov poskytnutím šifrovania pre celé objemy .
Block-chains úložisko	Blockchain je vo svojej podstate distribuovaná databáza chránená šifrovaním tak, aby sa k jej informáciám dostal len ten správny a aby sa v nej navždy uchovali všetky zmeny. Dáta sa ukladajú do samostatných úložných celkov zvaných „block“. Tieto bloky sa ukladajú do reťazca jeden za druhým, preto „chain“.
Compliance	Pod pojmom compliance si možno predstaviť súlad s pravidlami. Cieľom compliance programov je prevencia proti nežiaducim javom a porušeniu v rámci spoločnosti. Complinace zahŕňa problematiku ako je ochrana osobných údajov, trestné právo, korupcia, šikanovanie a diskriminácie na pracovisku, pracovné právo a zmluvné právo.
Double opt-in nástroje	Double opt-in zahŕňa okrem vyplnenia formuláru na webe tiež poslanie potvrdzujúceho mailu. Až po jeho odsúhlasení (kliknutí na potvrdzujúci link) je e-mailová adresa zahrnutá do databázy. Funguje teda ako dvojité potvrdenie súhlasu.
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GAP analýza	Diferenčná analýza (Gap analýza) patrí medzi metódy rozhodovania a riešenia problémov. Jedná sa o jednoduchú

	metodiku, postup a je využiteľná v situáciách, kedy dochádza k plánovaniu nejakej stratégie alebo zmeny.
Patch	Označuje sa ním súbor alebo kľúč k programu, ktorý po zadaní dokáže upraviť = vylepšiť software v prospech užívateľa. Ak zadáme správny patch, resp. ak doinštalujeme software v počítači patchom, tak zvyčajne získame ďalšiu funkciu daného software.
Pseudonimizácia	Ide o zakrytie alebo nahradenie mena pseudonymom. S príslušným kľúčom dokážeme priradiť osobám znovu ich pôvodné mená. Je to vratný proces. Je to spracovanie osobných údajov spôsobom, ktorý neumožňuje ich priradenie ku konkrétnemu človeku bez použitia dodatočných informácií. Tie musia byť uchované oddelene s dostatočnou technickou a organizačnou ochranou.
NAS server	Sú samostatné funkčné zariadenia umožňujúce jednoduché zálohovanie, ukladanie alebo zdieľanie dát z viacerých počítačov. NAS server (Network Attached Storage) je vo svojej podstate malý počítač, ktorý je vybavený slotmi pre pevné disky. Je v ňom procesor, pamäť a operačný systém, ktorý celých chod riadi. K NAS servera nie je možné pripojiť klávesnicu, myš ani monitor. Ovláda sa prostredníctvom webového rozhrania. Ide o sieťové úložisko a zariadenie sa do siete zapája ideálne prostredníctvom sieťového kábla vedeného z routera, prípadne bezdrôtovo pomocou WIFI.
Privacy by default	Minimalistický princíp, ktorý na spracovanie dodatočných údajov potrebuje explicitný súhlas alebo právne doložiť, že ich pre svoju činnosť potrebuje.
Privacy by design	Všetky databázy a nové systémy musia mať perfektnú ochranu riadenia prístupu a spĺňať ďalšie prísne bezpečnostné podmienky smernice. Musí byť jasné a auditovateľné, čo kto a kedy robil s dátami.

ZOZNAM PRÍLOH