Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Technický a organizační vliv GDPR na podniky

David Vlček

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. David Vlček

Informatika

Název práce

Technický a organizační vliv GDPR na podniky

Název anglicky

The technical and organizational influence of GDPR on business

---

Cíle práce

Diplomová práce je tématicky zaměřena na problematiku Obecného nařízení o ochraně osobních údajů (GDPR). Hlavním cílem práce je analyzovat současný stav dopadu GDPR na podniky v České republice. Dílčí cíle diplomové práce jsou:
- Vytvořit přehled řešené problematiky
- Analyzovat zavedení GDPR do podniku
- Porovnat dopad GDPR na vybrané státy Evropské unie
- Formulovat doporučení pro vybrané typy podniků

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Praktická část práce je zaměřena na vypracování případové studie analyzující vybrané aspekty nástupu a dopadů GDPR na podniky v ČR. Na základě syntézy teoretických poznatků a výsledků praktické části práce budou formulovány závěry diplomové práce.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

GDPR, Ochrana osobních údajů, přístup k osobním údajům, právo, podniky, právo být zapomenut

Doporučené zdroje informací

CALDER, Alan. Eu Gdpr. It Governance, 2017. ISBN 9781849288552.
NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
ŽŮREK, Jiří. 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. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

Ing. Jan Jarolímek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 10. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 24. 11. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Technický a organizační vliv GDPR na podniky" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28.11.2019 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Janu Jarolímkovi, Ph.D za odborné vedení, za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování diplomové práce.

Technický a organizační vliv GDPR na podniky

Abstrakt

Diplomová práce se zabývá obecným nařízením o ochraně osobních údajů (angl. General Data Protection Regulation, neboli GDPR). Jedná se o nařízení Evropské unie, které nahrazuje a upravuje dosavadní zákona o ochraně osobních údajů, který byl v českém právním řádu do doby účinnosti GDPR účinný. Tento soubor ucelených pravidel na ochranu dat platí od května loňského roku, kdy všechny firmy musely sjednotit informační systémy a postupy při práci s daty v souladu s GDPR. Práce se proto nejprve zabývá touto problematikou z teoretického hlediska – vymezuje toto nařízení z legislativního hlediska a orientuje se zejména na jeho negativní, pozitivní, věcnou, osobní, časovou a územní působnost. V praktické části analyzuje problémy související s únikem dat a GDPR, nastiňuje náklady na implementaci GDPR různých konkrétních firem, definuje požadavky na zajištění shody s GDPR, definuje řízení procesů z hlediska interního auditu v souvislosti s GDPR, popisuje průběh auditu a jeho postup a komentuje předpoklady implementace GDPR na konkrétní firmě. Cílem práce je tedy definovat požadavky na klíčové procesy a navrhnout postup k zajištění shody s podmínkami GDPR. Součástí práce bude i návrh vhodného postupu na řízení procesu při interním datovém auditu organizace.

Klíčová slova: GDPR, Ochrana osobních údajů, přístup k osobním údajům, právo, podniky, právo být zapomenut

Technical and organizational influence of GDPR on business

Abstract

The thesis deals with the general data protection regulation (General Data Protection Regulation, or GDPR). It is a regulation of the European Union that replaces and modifies the existing Personal Data Protection Act, which was effective in the Czech legal system until the GDPR became effective. This set of comprehensive data protection rules has been in place since May last year, when all companies had to unify information systems and data-handling practices in line with the GDPR. Therefore, the thesis first deals with this issue from a theoretical point of view - it defines this regulation from the legislative point of view and focuses mainly on its negative, positive, factual, personal, time and territorial scope. The practical part focuses on problems related to data leakage and GDPR, explains the costs of implementation of GDPR of different companies, describes requirements for ensuring compliance with GDPR, defines the process control from the perspective of internal audit in relation to GDPR, describes the audit process and its progress and comments on the assumptions of GDPR implementation for a particular company. The aim of the thesis is to define the requirements for key processes and to propose a procedure to ensure compliance with GDPR conditions. The work will also include a proposal for a suitable process management process in an internal data audit organization.

Keywords: GDPR, Privacy, access to personal data, law, businesses, right to be forgotten

Obsah

Seznam obrázků

1. Úvod

GDPR představuje obecné nařízení na ochranu osobních údajů. Jde o nařízení Evropské unie, které nahrazuje a upravuje dosavadní zákona o ochraně osobních údajů, který byl v českém právním řádu do doby účinnosti GDPR účinný. Tento soubor ucelených pravidel na ochranu dat nabyl účinnosti 25. 05. 2018. V této souvislosti musely všichni sjednotit postupy při práci s daty v souladu s GDPR. V rámci Evropské unie je jejich tok podporován a nařízení představuje vysokou ochranu před zneužitím citlivých informací. GDPR je použitelné ve všech členských státech bez ohledu na vnitrostátní právní úpravu. Zjednodušeně řečeno dochází k významnému zpřísnění regulace v oblasti zpracování osobních údajů.

Nová evropská norma vyžaduje úpravu stávajících procesů, jakož i povinnou implementaci množství dalších opatření a velmi komplexní přístup k celé problematice ochrany informací. Vznikají nové povinnosti v rámci automatizovaného zpracování dat vedoucí k větší transparentnosti a především bezpečnosti. Je nezbytné komplexně propojit všechny oblasti bezpečnosti IT, bezpečnosti fyzické, administrativní, organizační a procesní, aby ochrana osobních údajů fungovala jako jednotný systém. Diplomová práce si klade za cíl zmapovat řešenou problematiku ochrany osobních údajů, objasnit hlavní pojmy, ale také pomoci lépe se orientovat v povinnostech, které pro ně GDPR stanovuje. V praktické části práce je cílem implementovat GDPR v rámci vybrané organizace. Formulovat základní zásady ochrany osobních údajů, obecně posoudit důsledky nařízení na jejich prostředí a rozhodnout se, jakým způsobem budou dále postupovat. Cílem diplomové práce je definovat požadavky na klíčové procesy a navrhnout postup pro zajištění shody s podmínkami GDPR ve společnosti v praktické a návrhové části diplomové práce.

2. Cíl práce a metodika

Diplomová práce si klade za cíl analyzovat problematiku GDPR z teoretického hlediska – vymezuje toto nařízení z legislativního hlediska a orientuje se zejména na jeho negativní, pozitivní, věcnou, osobní, časovou a územní působnost. V praktické části je cílem implementovat GDPR v rámci vybrané společnosti, formulovat základní zásady ochrany osobních údajů, obecně posoudit důsledky nařízení na jejich prostředí a rozhodnout se, jakým způsobem budou dále postupovat. Součástí cíle je rovněž definovat požadavky na klíčové procesy a navrhnout postup pro zajištění shody s podmínkami GDPR v určité společnosti.

Hlavním cílem diplomové práce s názvem: „Technický a organizační vliv GDPR na podniky“ je analyzovat nástup a dopad GDPR na podniky v České republice se zaměřením na informační technologie. Pro lepší organizaci lze práci rozdělit na několik dílčích cílů:

- Charakterizovat řešenou problematiku
- Řádně nastudovat a následně podrobně charakterizovat veškeré zdroje včetně odborné literatury, které se týkají problematiky
- Analyzovat a charakterizovat současný přístup a technologie využívané k ochraně osobních údajů
- Historický vývoj ochrany osobních údajů
- Zmapovat stávající přístup k ochraně osobních údajů ve vybrané firmě
- Analyzovat procesy využívané ve firmě při ochraně osobních údajů teď a po zavedení GDPR do firemních procesů
- Navrhnout potřebná opatření, která by firma měla splnit pro aktualizaci stávajícího systému zabezpečení na úroveň splňující nároky GDPR
- Vyhodnotit dopady GDPR na využívané technologie a procesy v podnicích

Pro splnění výše stanovených cílů je nejprve nutné provést průzkum literárních pramenů a na základě tohoto průzkumu vyhotovit teoretické poznatky související s problematikou GDPR. Dalším krokem je zhodnocení současného, výchozího, stavu firmy, tedy jaký je její současný systém nakládání s osobními údaji či analýza vnitřních předpisů. V rámci praktické části je uskutečněn kvalitativní výzkum sběru informací ve formě rozboru interních dokumentů firmy. Následně jsou definována bezpečnostní a technická opatření ve

společnosti Alza za účelem GDPR a je formulován interní předpis GDPR ve společnosti Alza.

V závěru vlastní práce vyhodnocení zjištěných poznatků, jejich rekapitulace. Přínos tohoto nařízení v oblasti ochrany osobních údajů. Dále je z výsledku práce vyhodnoceno, jaký dopad má nařízení nejen na podniky, ale i co bude znamenat toto nařízení pro veřejnost. Formulovat základní kroky a doporučení, kterých by se podnik měl držet při zajištění shody. Do budoucna se ze závěrů diplomové práce dá říci, že GDPR se stane pro většinu malých a začínajících firem přímo likvidačním nástrojem. Každý, kdo chce začít svůj vlastní podnik, by se nad tímto nařízením měl pozastavit dřív než se vrhne do podnikání.

3. Přehled řešené problematiky

3.1 GDPR a vymezení tohoto nařízení

Historicky prvním a klíčovým dokumentem pro ochranu osobních údajů (dále jen OÚ) je Úmluva o ochraně lidských práv a základních svobod, přijatá v roce 1950. Úmluva uvádí dvě hlavní práva, které vymezují základní hranice ochrany OÚ. Jsou to:[1]

- článek 8 - *"právo na respektování rodinného, soukromého života, obydlí a korespondence";*
- článek 10 - *"svoboda projevu".*

Dalším relevantním dokumentem je Úmluva Rady Evropy 108 z roku 1981 o ochraně osob při automatizovaném zpracování OÚ. Jde o první právně závazný mezinárodní dokument v oblasti ochrany OÚ. Cíle úmluvy jsou formulovány v článku níže, konkrétně:[2]

- článek 1 - *"respektování práv a základních svobod, zejména práva na soukromí při automatizovaném zpracování osobních údajů".*

Důležitým mezinárodním mezníkem v ochraně OÚ bylo přijetí Směrnice OECD o ochraně soukromí a přeshraničním toku OÚ v roce 1980. I když tento dokument není právně závazným, obsahuje principy ochrany OÚ, které byly později převzaty do legislativ mnoha zemí. Tyto principy byly obsaženy také v pozdější evropské legislativě, konkrétně

[1] *Úmluva o ochraně lidských práv a svobod* [online]. USA: USA, 1950 [cit. 2018-12-01]. Dostupné z: https://www.ustrcr.cz/data/pdf/projekty/usmrceni-hranice/umluva.pdf

[2] *Evropská úmluva o ochraně lidských práv* [online]. EU: EU, 2018 [cit. 2018-12-01]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

například ve Směrnici o ochraně OÚ 95/46 / ES. Principy této směrnice jsou obsaženy také v české právní úpravě, a to v rámci zákona o ochraně osobních údajů.[3]

Několik zemí přijalo vlastní legislativu na ochranu OÚ, první zemí byla německá spolková země Hesensko, která přijala první zákon na ochranu OÚ už v roce 1970. Jak už bylo uvedeno, tak v rámci ČR byl přijat první zákon o ochraně osobních údajů na základě směrnice 95/46 / ES v roce 2000 a následně byly některé relevantní části zákona postupně novelizovány.

Směrnice 95/46 / ES o ochraně fyzických osob při zpracování OÚ a volném pohybu těchto údajů, přijatá v roce 1995, byla prvním právně závazným dokumentem přijatým evropským společenstvím. Směrnice není přímo vykonatelná, ale ukládá povinnost členským zemím převzít její cíle a úpravu do národní legislativy. Směrnice stanovila základní pojmy a jejich definice, zavedla obecná pravidla týkající se zákonnosti zpracování OÚ, určila zákonná práva dotčených osob a stanovila nezávislé vnitrostátní kontrolní orgány. Tato směrnice vytvořila i tzv. pracovní skupinu podle článku 29 - WP29, jejímž úkolem je vytvářet metodické pokyny a doporučovat legislativní změny.[4]

K dalším evropským dokumentům upravujícím pravidla ochrany OÚ patří:[5]

- E-Privacy směrnice 2002/58 / ES o zpracování OÚ a ochrany soukromí v odvětví elektronických komunikací, označovaná také jako směrnice o soukromí a elektronických komunikacích, která stanoví pravidla pro přímý marketing a použití cookies v internetovém prostředí a komunikaci i v souvislosti s používáním marketingových nástrojů ve firemní praxi;

---

[3] *Evropská úmluva o ochraně lidských práv* [online]. EU: EU, 2018 [cit. 2018-12-01]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

[4] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[5] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

- směrnice o retenci 2006/24 / ES týkající se uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, jejíž platnost byla napadena u Evropského soudního dvora pro její nepřiměřené zasahování do práv a svobod dotčených osob.

V dubnu 2016 Evropský parlament a Rada (EU) přijaly tzv. Balík reforem ochrany OÚ. Reforma obsahuje Nařízení 2016/679 o ochraně fyzických osob při zpracování OÚ a o volném pohybu těchto údajů (GDPR) a Směrnici 2016/680 / ES o ochraně OÚ pro policii a orgány činné v trestním řízení. Důležitou poznámkou je, že Nařízení je přímo vykonatelné na celém území EU a má přednost před lokální legislativou, kdy členské státy mají za povinnost sladit lokální legislativu do konce přechodného období.[6]

Reforma byla odstartována Evropskou komisí už v lednu 2012. Celkově čtyři tisíce změn udělalo z Nařízení nejvíce komentovaný právní úpravu v historii EU. Ve srovnání s předchozí Směrnicí 95/46 / ES narostl počet článků Nařízení z 33 na 91. V souvislosti s komentovanými změnami se na těchto podílela i ČR, a to zejména z hlediska harmonizace ve vztahu k českému zákonu o ochraně osobních údajů. Cílem Nařízení je možné shrnout následovně:[7]

- sjednocení právní úpravy ochrany OÚ v členských státech Evropské unie;
- zvýšení práv dotčených osob;
- zjednodušení pravidel zpracování OÚ.

Nařízení vstoupilo v platnost 24. května 2016 a v jednotlivých členských státech se začne používat od 25. května 2018. Jak již bylo uvedeno, jde o obecnou právní úpravu, tedy podléhají jí všechny komerční i nekomerční činnosti organizací, při kterých dochází ke

[6] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[7] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

zpracování OÚ, kromě aktivit taxativně vyjmenovaných. Právní úprava se dotýká nejen organizací se sídlem v členských státech EU, ale všech organizací, které monitorují aktivity nebo zpracovávají OÚ rezidentů EU. Právní úprava se v praxi dotýká zejména dvou skupin dotčených osob - **zaměstnanců a zákazníků v maloobchodě.**[8]

Specificky se úprava dotýká oblastí jako například:[9]

- Big Data a Business Intelligence;
- Biometrické, kamerové a přístupové systémy;
- Lokalizační služby;
- Marketing, spotřebitelské soutěže, věrnostní programy, apod.;
- Profilování a automatizované rozhodování;
- Monitoring a měření zákazníků a zákaznických preferenci;
- Další problémové oblasti stanovené individuálně.

K tomu, aby mohl být nějaký údaj označen za osobní, se musí týkat určité nebo určitelné fyzické osoby, tedy sám nebo ve spojení s dalšími údaji musí umožňovat její přímou, například jméno, příjmení a adresa nebo nepřímou identifikaci, například unikátní kód v systému. Údaje o právnické osobě jako jsou název a identifikační číslo občanského sdružení či s.r.o. nejsou považovány za osobní. K nejčastěji zpracovávaným osobním údajům, které výše uvedenou definici splňují, tak můžeme zařadit jméno a příjmení, adresu, datum narození, rodné číslo, biometrické údaje, což jsou také snímky obličeje, otisky prstů, podpis, telefonní číslo nebo dostatečně určitou emailovou adresu.[10]

Obecné nařízení na ochranu osobních údajů (GDPR), které vstoupí v platnost 25. 5. 2018, okruh tradičních osobních údajů mírně rozšiřuje. Pod pojem osobní údaje tak podle GDPR

---

[8] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[9] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[10] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

po novém spadají i technické údaje typu IP adresa či cookies. I při těchto údajích však platí výše uvedená pravidla, tedy k tomu, aby je bylo možné označit za osobní a měly tak pro dotčené subjekty určitý význam z hlediska zpracování a ochrany, musí umožňovat identifikaci konkrétní fyzické osoby. Zatímco maskovanou IP adresu nebo IP adresu přidělenou k síti využívané víceuživatelském nebude možné přiřadit ke konkrétní osobě, IP adresa, ať už statická nebo i dynamická počítače v domácnosti ve většině případů osobním údajem bude.

Pojem osobní údaj sám o sobě nezakládá podnikatelům žádné povinnosti. Ty nastupují až tehdy, když mluvíme o jeho zpracování, ke kterému nedochází vždy. Jako příklad lze uvést používání bezpečnostního kamerového systému v kamenné prodejně, který není spojen s funkcí záznamu videa - při monitorování prodejny bez ukládání videa tak ke zpracovávání údajů nedochází a podnikatel má podle zákona pouze povinnost označit svou prodejnu upozorněním, že daný prostor je monitorován. O tom, zda ke zpracovávání osobních údajů dochází nebo ne, bude proto záležet na konkrétních okolnostech, od kterých se budou odvíjet také různé zákonné povinnosti.

Jako příklad povinností spojených se zpracováním a ochranou osobních údajů lze uvést:[11]

- Povinnost oznámit dotyčným osobám účel a rozsah zpracování osobních údajů,
- Povinnost získat souhlas se zpracováním osobních údajů v případech, kdy se tyto údaje nezpracovávají na základě zákona, resp. v rámci plnění smlouvy, konkrétně při vyřízení objednávky zákazníka, kdy souhlas dotčené osoby není nutný,
- Povinnost informovat dotčenou osobu o tom, jaké údaje jsou ní zpracovávány, a na její žádost dané údaje v odůvodněných případech vymazat,
- Povinnost umožnit, v některých případech, snadný přenos osobních údajů od jednoho poskytovatele služeb k jinému,

[11] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

- Povinnost, v některých případech, vést podrobné záznamy o zpracování osobních údajů,
- Povinnost podstoupit konzultaci k ochraně osobních údajů s Úřadem pro ochranu osobních údajů,
- Povinnost zajistit rodičovský souhlas se zpracováním osobních údajů dětí do 16 let,
- Povinnost určit odpovědnou osobu při ochraně osobních údajů.

Jednou z hlavních povinností evropského nařízení č. 2016/679 (GDPR) je povinnost některých provozovatelů stanovit, respektive zajistit tzv. odpovědnou osobu – pověřence pro ochranu osobních údajů, která u nich bude dohlížet na ochranu osobních údajů zákazníků, zaměstnanců, členů, pacientů, studentů či jiných skupin osob. Půjde tak o určitého garanta správnosti postupů při ochraně osobních údajů, jakož i kontaktní místo v rámci komunikace s Úřadem pro ochranu osobních údajů. Uvedená povinnost se podle GDPR týká pouze následujících provozovatelů, tedy subjektů, které zpracovávají osobní údaje:[12]

1. všech veřejných orgánů (ministerstva, úřady, atd.) A veřejnoprávních subjektů (obce, školy, nemocnice atd.) S výjimkou soudů při výkonu jejich pravomocí;

2. provozovatelů a zprostředkovatelů, jejichž hlavní činností jsou zpracovatelské operace, které si vzhledem ke své povaze, rozsahu a / nebo účely vyžadují pravidelné a systematické sledování dotčených osob ve velkém rozsahu; nebo

3. provozovatelů a zprostředkovatelů, jejichž hlavní činností je zpracování zvláštních kategorií údajů ve velkém rozsahu nebo zpracovávání osobních údajů týkajících se uznání viny za trestné činy a přestupky;

4. provozovatelů, u kterých to stanoví zvláštní právní předpis.

[12] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

3.2 Působnost GDPR

Působnost právní normy bývá konkretizována z hlediska, co má být dosaženo z hlediska právní úpravy a co má být mimo příslušnou právní úpravu doplněnou i ustanoveními upravujících pozitivní působnost i negativní působnost GDPR. Z hlediska zachování tradičního rozdělování působnosti právní normy na výše uvedené faktory tomu přizpůsobíme i následující výklad vysvětlující působnost GDPR. Působnost GDPR bude založena v konkrétním případě tehdy, budou-li splněny předpoklady pozitivní věcné působnosti, osobní působnosti a časové působnosti a zároveň budou vyloučeny důvody na aplikaci negativní působnosti.

3.2.1. Negativní působnost

Je velmi důležitou částí GDPR, protože související ustanovení článku 2 odst. 2 písm. a) až d) GDPR stanoví případy představující absolutní vyloučení působnosti celého GDPR.[13]

1. Činnosti, které nespadají do působnosti práva EU

Tento důvod blíže vysvětluje bod odůvodnění v článku 16 GDPR, které říká, že GDPR se *"nevztahuje na otázky ochrany základních práv a svobod ani pro volný tok osobních údajů týkajících se činností, které nespadají do působnosti práva EU, jako jsou činnosti týkající se národní bezpečnosti."*[14] Do působnosti práva EU patří několik výlučných pravomocí zasahujících oblasti jako jsou celní unie, společná obchodní politika, měnová politika eurozóny, ale také pravidla hospodářské soutěže na vnitřním trhu EU, případně společné pravomoci EU a členských států, konkrétně například sociální politika, životní prostředí,

[13] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 2 odst. 2 a) až d)

[14] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 16

ochrana spotřebitele, a také tzv. podpůrné, koordinační a doplňkové pravomoci EU, jako je průmysl, kultura, vzdělávání, cestovních ruch a další.

Do působnosti práva EU nepatří zbytkové pravomoci členských států, tedy takové pravomoci členských států, které nebyly zakládajícími smlouvami (Smlouva o EU a Smlouva o fungování EU) přeneseny na EU. Podle článku 5 odst. 2 konsolidovaného znění SEU: *"Podle zásady svěření pravomocí jedná EU pouze v mezích pravomocí svěřených jí ve smlouvách členskými státy pro dosažení cílů stanovených. Pravomoci, které nejsou smlouvami EU svěřeny, náležejí členským státům."*[15] Podle článku 4 odst. 2 konsolidovaného znění SEU: *"EU ctí rovnost členských států před smlouvami, ale také jejich národní identitu, která spočívá v jejich základních politických a ústavních systémech, včetně místní a regionální samosprávy. Respektuje základní funkce, zejména zajišťování územní celistvosti státu, udržování veřejného pořádku a ochranou národní bezpečnosti. Především národní bezpečnost zůstává výhradní odpovědností každého členského státu."*[16]

Na základě výše uvedeného lze konstatovat, že článek 2 odst. 2 písm. a) GDPR způsobuje nemožnost aplikace právní úpravy GDPR na zpracování osobních údajů, které je nezbytné realizovat na úrovni členských států při dosahování národní bezpečnosti, případně při jiných činnostech spojených s nezbytností zpracování osobních údajů při realizaci jiných výlučných zbytkových pravomocí členského státu EU, které jsou na základě primárního práva EU, resp. zakládajících smluv svěřeno do výlučné působnosti členských států, jako je konkrétně daňová politika, národní bezpečnost, nebo členského státu, který si vyjednal s EU výjimky.

[15] Smlouva o Evropské unii, článek 5 a následující této smlouvy.

[16] Smlouva o Evropské unii, článek 5 a následující této smlouvy.

2. Zpracování osobních údajů členskými státy při výkonu činností spojených se společnou zahraniční a bezpečnostní politikou EU

GDPR se ve smyslu článku 2 odst. 2 písm. b) GDPR nevztahuje na zpracování osobních údajů členskými státy při provádění činností v souvislosti se společnou zahraniční a bezpečnostní politikou Unie, tedy v rozsahu zvláštních ustanovení o společné zahraniční a bezpečnostní politice podle kapitoly 2 hlavy V. Smlouvy o EU.

3. Zpracování osobních údajů orgány, úřady a agenturami EU

Úvodní ustanovení článku 17 GDPR poskytuje vysvětlení, že: *"Na zpracovávání osobních údajů orgány, jinými subjekty Unie se vztahuje nařízení Evropského parlamentu a Rady (ES) č. 45/2001. Nařízení (ES) č. 45/2001 a ostatní právní akty Unie, které se vztahují na takové zpracování osobních údajů, by měly být upraveny podle zásad a pravidel stanovených v tomto nařízení a uplatňovat s ohledem na toto nařízení. V zájmu stanovení silného a soudržného rámce ochrany údajů v Unii by po přijetí tohoto nařízení měli následovat potřebné úpravy nařízení (ES) č. 45/2001, aby se začaly uplatňovat současně s tímto nařízením."*[17]

4. Výjimka domácích nebo osobních činností

GDPR se ve smyslu úvodního ustanovení č. 18 *"nevztahuje na zpracování osobních údajů fyzickou osobou v průběhu výlučně osobní nebo domácí činnosti, a tedy bez spojení s profesní nebo obchodní činností. Osobní nebo domácí činnosti by mohly zahrnovat korespondenci a uchovávání adres či využívání sociálních sítí a online činnosti vykonávané v kontextu těchto činností. Toto nařízení se však vztahuje na provozovatele nebo zprostředkovatelů, kteří poskytují prostředky na zpracování osobních údajů pro*

[17] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 17

takové osobní nebo domácí činnosti."[18] Výjimka domácích nebo osobních činností se zdá na první pohled jasná. Avšak v aplikační praxi dozorčích orgánů se v minulosti již vyskytlo několik případů, které byly náročné na posouzení možnosti aplikace této výjimky z působnosti regulace obecně závazné regulace ochrany osobních údajů, která zůstala zachována i v GDPR. V současnosti s rozvojem digitální ekonomiky nelze zužovat výjimku osobních a domácích činností pouze na seznamy kontaktů v mobilu, soukromé databáze v domácím PC, zda domácí složky soukromých osob obsahující různé pojistné smlouvy, lékařské záznamy, potvrzení, diplomy, apod. V současnosti je třeba zohlednit i to, že soukromá osoba může mít vlastní blog, webovou stránku, zda profil na sociální síti, který může sloužit výhradně k osobním účelům, příp. může využívat i různé smart aplikace.

Právě tyto nové formy zpracování osobních údajů v intencích výjimky domácích nebo osobních činností představují zvýšené riziko pro exces z jejího rámce. Stanovení objektivních kritérií nezbytných pro rozlišení přítomnosti složky osobních činností v řízení neformální skupiny, zda osoby formálně jednající jako jednotlivec, ale fakticky jednající jako veřejně politicky, příp. obchodně činná od subjektu, který cílevědomě v kontextu předem vymezeného účelu provádí aktivity, jejichž součástí je i zpracování osobních údajů může být náročné. Při takovýchto nejasných případech je vhodné použít metodiku převažujících faktorů k určení nebo naopak k vyloučení možnosti aplikace výjimky domácích nebo osobních činností prostřednictvím pomocných otázek, které formulovala pracovní skupina zřízená podle článku 29 směrnice 95/46 / ES.

---

[18] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 18

5. Zpracování osobních údajů orgány na účelem prevence, vyšetřování, odhalování nebo stíhání nebo výkonu trestů včetně ochrany před ohrožením veřejné bezpečnosti

Tato výjimka zpod působnosti GDPR pro tzv. law-enforcement účely zachovává kontinuitu se směrnicí 95/46 / ES, která také vylučovala několik ze svých ustanovení zpod své působnosti pro tyto případy. Vzhledem k tomu, že pro zpracování osobních údajů pro účely předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání plně pokrývá tzv. Policejní směrnice o ochraně osobních údajů, která se začne aplikovat ve stejný den jako GDPR již není nutné částečné vynětí z působnosti konkrétně vybraných ustanovení, ale je možné vyloučit celkovou působnost všech ustanovení GDPR na tyto případy.

6. Možnost omezit právní účinky GDPR na soudy a jiné justiční orgány na národní úrovni

V členských státech EU je nezávislost soudní moci pozorně chráněnou součástí demokratického uspořádání společnosti, a proto je třeba poukázat na skutečnost, že GDPR na více místech vylučuje nebo vytváří prostor pro národní legislativu státu pro vyloučení aplikace několika ustanovení GDPR na zpracování osobních údajů soudy při výkonu soudnictví. Na základě tohoto přístupu lze omezit výkon určitých práv dotčené osoby přiznaných GDPR zahrnující článek 12 až 22 GDPR, zda omezit aplikaci základních zásad zpracování osobních údajů nebo povinnost oznamovat dotyčné osobě porušení její ochrany osobních údajů - článek 34 GDPR legislativním opatřením splňujícím obsahové náležitosti vyžadované v článku 23 odst. 2 GDPR na národní nebo na úrovni EU, pokud takové omezení respektuje podstatu základních práv a svobod a je nezbytným a přiměřeným

opatřením v demokratické společnosti s cílem zajistit ochranu nezávislosti soudnictví a soudních řízení.[19]

3.2.2. Pozitivní působnost

Pozitivní působnost GDPR je do značné míry totožná se základní pozitivní věcnou působností GDPR, která je vyjádřena v článku 2 odst. 1 GDPR, které stanoví, že právní úprava se vztahuje "na zpracování osobních údajů zcela nebo částečně automatizovanými prostředky a na zpracování jinými než automatizovanými prostředky v případě osobních údajů, které jsou součástí informačního systému nebo jsou určeny k tomu, aby tvořily součást informačního systému. *"Pojem informační systém je legálně definován jako" jakýkoliv uspořádaný soubor osobních údajů, které jsou přístupné podle určitých kritérií, bez ohledu na to, zda jde o systém centralizovaný, decentralizovaný nebo distribuován na funkčním nebo geografickém základě."*[20] Uvedené je možné interpretovat tak, že GDPR vztahuje na jakékoli zpracovávání osobních údajů, které se realizuje v důsledku provozovatelem autonomní vymezeného účelu zpracování osobních údajů, typicky například rozhodnutí o zřízení e-shopu nebo provozovateli direktivně stanovenému účelu zpracování osobních údajů v důsledku aplikace zákonné povinnosti, a to bez ohledu na to, zda se při zpracovávání využívají pouze technologie, kombinace technologie a lidského faktoru nebo jen lidského faktoru. GDPR se rovněž vztahuje na jakékoli zpracovávání osobních údajů, které probíhá mezi hmotněprávní definovanými a odlišenými subjekty, se kterými provozovatel může provádět jednotlivé zpracovatelské operace s osobními údaji. Primární a v největší možné míře je touto pozitivní působností GDPR zasažen provozovatel a zprostředkovatel jako obchodní partner provozovatele, ale jde také o

---

[19] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 12-23,článek 34

[20] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 2

zpracování osobních údajů od zprostředkovatele k subdodavatelům, nebo od provozovatele a / nebo zprostředkovatele k třetím stranám nebo příjemcům osobních údajů.

3.2.3. Věcná působnost

Jak již bylo uvedeno, věcná působnost GDPR se do značné míry prolíná s pozitivní působností a zároveň i negativní působností. Jednoduše řečeno věcná působnost GDPR se týká jakéhokoliv způsobu zpracování osobních údajů v informačním systému, které provádí provozovatel a nebo zprostředkovatel a netýká se okruhů zpracování osobních údajů, které jsou vymezeny v článku 2 odst. 2 GDPR. Podstatou věcné působnosti GDPR je, že se vztahuje na zpracovávání osobních údajů. Pojem "osobní údaje" je legálně definován v článku 4 bod 1 GDPR a pojem "zpracovávání" je legálně definován v článku 4 bod 2 GDPR. V této souvislosti je vhodné poznamenat, že GDPR zpřesňuje koncept osobních údajů tak, že za osobní údaje budou již považovány i různé online identifikátory osob (například IP adresa, cookies) a jiné elektronické identifikátory (například RFID technologie, či tzv. provozně lokalizační údaje), ale i tzv. pseudonymizované údaje legálně definované v článku 4 bod 5 GDPR a blíže vysvětleny v úvodním ustanovení článku 26 GDPR. Samozřejmě stále, stejně jako v minulosti, bude nutné, aby údaj nebo skupina zpracovávaných dat byla způsobilá v konkrétním případě identifikovat přímo či nepřímo dotčenou osobu. Pokud půjde o data, která budou právně kvalifikovány jako osobní údaje a subjekt s nimi bude provádět jakékoli zpracovatelské operace, jako je získávání, zaznamenávání, prohlížení, strukturování, pořádání, využívání, šíření, poskytování, zveřejňování a jiné) bude založena věcná působnost GDPR.

Kromě toho je třeba vzít na zřetel, že zpracovávání osobních údajů orgány a institucemi EU se řídí vlastním právním režimem odlišným od GDPR (Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů), jakož i zpracovávání osobních údajů orgány činnými v trestním řízení a soudy v trestním řízení (Policejní směrnice o ochraně údajů). Rovněž zpracování osobních údajů poskytovateli služeb informační společnosti (např. Různí poskytovatelé online služeb od provozovatelů sociálních sítí, přes inzertní portály, tzv. seznamky, online zprostředkování úvěru, datová úložiště až po e-shop) může být bez ohledu na GDPR dotčeny právní

úpravou transponována do národních právních řádů členských států v rámci příslušných právních předpisů daného členského státu EU.

3.2.4. Osobní působnost

GDPR se primárně týká subjekty, které zpracovávají osobní údaje jako provozovatelé včetně tzv. společných provozovatelů ve smyslu článku 26 GDPR a zprostředkovatelé včetně tzv. Subdodavatelů zapojených do procesu zpracovávání osobních údajů ze strany zprostředkovatele se souhlasem provozovatele. Regulace však také zasahuje i zástupce provozovatelů nebo zprostředkovatelů, kteří nejsou usazeni v Evropské unii (článek 27 GDPR), tedy nepřímo i subjekty, které zpracovávají osobní údaje občanů EU, aniž byly usídlené v některém členském státě. Osobní působnost GDPR zasahuje i další osoby, které zpracovávají osobní údaje na základě pověření od provozovatele nebo zprostředkovatele podle článku 29 GDPR, například současné oprávněné osoby ve smyslu zákone členského státu EU o ochraně osobních údajů.

Samozřejmě osobní působnost GDPR se vztahu i na dotčené osoby, jejichž osobní údaje jsou zpracovávány výše uvedenými subjekty a které mají vždy primárně postavení fyzické osoby - jednotlivce a nikoliv například fyzické osoby podnikatele. To však platí jen, pokud jde o identifikační údaje fyzické osoby - podnikatele používané v běžném obchodním styku, které jsou běžně zveřejněny v souladu se zákonem v příslušných registrech a ne další identifikátory, které by již mohly mít soukromou povahu a bylo by je třeba považovat ve vztahu k fyzické osobě - podnikateli za osobní údaje, a tedy i takový subjekt by se jako dotčená osoba stala subjektem osobní působnosti GDPR. Pojem dotyčná osoba paradoxně není v GDPR legálně definovaný, ačkoli v našem národním zákoně o ochraně osobních údajů je dotyčná osoba legálně definována jako *"každá fyzická osoba, které se osobní*

údaje týkají." Bližší vysvětlení toho jak vymezit dotčenou osobu pro účely GDPR poskytuje úvodní ustanovení článek 26 GDPR.[21]

V souvislosti s osobní působností GDPR je také nezbytné uvést, že právní úprava obsažená v GDPR by neměla ve smyslu úvodního ustanovení článku 27 uplatňovat na osobní údaje zemřelých osob, přičemž však členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zemřelých osob. Naše aktuální národní právní úprava v zákoně o ochraně osobních údajů obsahuje pouze stručnou zmínku o tom, že když dotyčná osoba nežije, tak souhlas se zpracováním osobních údajů může poskytnout její blízká osoba, přičemž takový souhlas není platný, pokud i jen jedna blízká osoba vyjádřila nesouhlas.

3.2.5. Časová působnost

GDPR se plně začal v praxi uplatňovat a dozorovými orgány kontrolovat od 25. května 2018, a to bez ohledu na to, zda je na národní úrovni přijat zákon o ochraně osobních údajů, který představuje právní režim GDPR s doplněním vlastní právní úpravy, která však musí být konzistentní s GDPR nebo takový národní zákon přijatý na národní úrovni členského státu nebylo možné přijmout. Časová působnost je tedy upravena jednoduše, neexistuje zde několik přechodných ustanovení na splnění jednotlivých povinností stanovených GDPR. Odpovědným subjektům plyne aktuální dvouroční přechodné ustanovení určené na celkovou konverzi svých podmínek zpracování osobních údajů na novou regulaci.

3.2.6. Územní působnost

Územní působnost GDPR je předmětném právní úpravy ustanovení článku 3 odst. 1 až 3 GDPR a blíže je také vysvětlena v bodech odůvodnění článku 23 až článku 25 GDPR.[22]

---

[21] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 26

[22] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 3, článek 23 až 25

GDPR usiluje, v porovnání se směrnicí 95/46 / ES, kterou nahrazuje, rozšířit působnost právních předpisů EU o ochraně údajů i tím, že se stane irelevantní umístění prostředků zpracování osobních údajů, které bylo podstatné dosud a prosadí se určité exteritoriální prvky s cílem zasáhnout regulací GDPR i takové podniky v postavení provozovatelů a zprostředkovatelů, které sice nemají sídlo v žádném členském státu EU, ale i přesto zpracovávají osobní údaje občanů EU. V první řadě GDPR samozřejmě platí pro provozovatele a zprostředkovatele usazených na území všech členských států Evropské unie a se sídlem v Evropském hospodářském prostoru včetně Islandu, Norska a Lichtenštejnska. V tomto směru je zajímavé vzít v úvahu brexit, který fakticky ovlivní současné postavení Spojeného království. Podle dostupných informací je možné se domnívat, že i přes dopady brexitu bude Spojené království dodržovat GDPR, protože v procesu jeho přijímání se zohlednilo mnoho připomínek britské delegace a technický-společenský vývoj vyžaduje akutní novou regulaci této oblasti. Postavení Spojeného království je aktuální i z hlediska ochrany osobních údajů předmětem politických diskusí. Jako nejpravděpodobnější alternativa se nám jeví, že Spojené království implementuje GDPR a Evropská komise jej na čas po brexitu určí rozhodnutím vydaným v souladu s článkem 45 GDPR za zemi zajišťující odpovídající úroveň ochrany osobních údajů, což zajistí kontinuitu ve volném toku osobních údajů mezi Spojeným královstvím a ostatními členskými státy EU.[23]

GDPR se vztahuje na provozovatele a zprostředkovatelů usazených v EU / EHP bez ohledu na to, zda se zpracovávání fakticky vykonává na území EU / EHP, čímž se stává irelevantním umístění prostředků zpracování osobních údajů, například cloudová infrastruktura rozmístěna v datových centrech na různých kontinentech světa, ale určující bude právní domicil organizace ve spojitosti s právním určením toho, zda jde při zpracovávání osobních údajů touto organizací o aktivity provozovatele nebo zprostředkovatele. Vzhledem k tomu, že na vnitřním trhu EU je běžné, že dochází v rámci

[23] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html, článek 3, článek 45

korporačních struktur různých obchodních společností k takovým obchodním aktivitám, které doprovází zpracování osobních údajů s přeshraničním prvkem v několika členských státech je na místě se zamyslet jak takové případy řešit. GDPR pro tyto případy stanovila princip tzv. jediného kontaktního místa, který je normativním způsbem vyjádřený v článku 60 GDPR.

Ve stručnosti je možno uvést, že principem one-stop-shop mechanismu je určení vedoucího dohlížitele podle místa hlavní provozovny správce nebo zpracovatele se zpracovatelskými aktivitami ve více členských státech, což je v podstatě země, v níž má korporace hlavní ústředí. Tento vedoucí kontrolní orgán je pak příslušný pro všechny záležitosti spojené s GDPR a ochranou osobních údajů ve vztahu ke zpracovávání osobních údajů, které je realizováno prostřednictvím spřízněných provozoven korporace ve více členských státech.

GDPR se bude tedy vztahovat na společnosti, které mají "provozovny" v EU, kde jsou osobní údaje zpracovávány "v rámci činností" takové provozovny. Pokud jsou předmětné podmínky splněny, GDPR platí bez ohledu na to, zda vlastní zpracování dat probíhá v rámci geografické teritoriality členských států EU, nebo ne. Rozhodujícím novým momentem přítomným v GDPR je explicitní rozšíření územní působnosti tohoto aktu, který odráží jednak politické ambice Evropské komise exteritoriální ochraňovat vnitřní trh a jednak to ukazuje trend rostoucího vlivu Soudního dvora EU a dozorových orgánů v oblasti ochrany osobních údajů, které budou mít uplatňovat EU regulaci ochrany osobních údajů i vůči takovým společnostem, které v minulosti nespadaly do jejich působnosti.

Společnosti zřízené mimo EU budou podle článku 3 odst. 2 podléhat GDPR, pokud zpracovávají osobní údaje o dotčených osobách v EU v souvislosti s následujícími předpoklady:

- Nabídkou zboží nebo služeb (není nutná platba);
- Sledováním jejich chování v rámci EU.

Co se týče nabídky zboží a služeb (ale ne monitorování), pouze zpřístupnění webových stránek v rámci Evropské unie není dostačující. Musí být zřejmé, že společnost své aktivity bude směřovat na dotčené osoby žijící v EU. Kontaktní adresy přístupné z EU a používání jazyka používaného v zemi provozovatele také nestačí. Avšak schopnost objednávky v

úředním jazyce dotyčné členské země EU a možnost platby v příslušné měně už budou relevantními faktory pro určení extra teritoriální působnosti GDPR. Bližší tyto úvahy rozvádí úvodní ustanovení č. 23 GDPR. V souvislosti se sledováním chování dotčených osob žijících, resp. fyzicky se nacházejících v EU je třeba zjistit ve smyslu úvodního ustanovení článku 24 GDPR, zda jsou fyzické osoby sledované na internetu včetně případného následného využití technologických řešení zpracování osobních údajů, které spočívají v profilování fyzické osoby k přijetí rozhodnutí týkajícího se této osoby nebo pro účely analýzy či předvídání osobních preferencí, chování a postojů této osoby.

Pod sledováním chování dotyčné osoby se tak myslí hlavně online tracking a behaviorální reklama generována provozovateli internetových vyhledávačů či provozovateli sociálních sítí. Prostřednictvím tohoto ustanovení GDPR realizuje svou ambici zasáhnout a donutit respektovat svoji právní úpravu i těch největších gigantů digitální ekonomiky, kteří nejvíce profitují se zpracování osobních údajů a kteří jsou převážně usídlení v USA. Právo členského státu EU, resp. GDPR se bude moci také v některých případech uplatňovat exteritoriální i na základě mezinárodního práva veřejného.

3.3 Principy ochrany OÚ dle GDPR

Hlavní principy nové ochrany OÚ podle Nařízení GDPR jsou následující:[24]

- **Rozsah regulovaných dat** - rozšíření zvláštní kategorie například o genetické údaje;
- **Jeden kontinent, jedna úprava** - nahrazení národních legislativ;
- **Jednotné místo (one-stop-shop)** - jeden kontrolní orgán;
- **Stejná pravidla pro všechny společnosti** - bez ohledu na to, kde jsou usazeny;
- **Úprava souhlasu nezletilých** - věková hranice 13 až 16 let, toto blíže stanoví členský stát;

[24] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

- **Technologická neutralita** - pokrok inovací;
- **Pseudo anonymizace** - reverzibilní anonymizace dat, konkrétní oddělení identifikačních údajů;
- **Oznamovací povinnost** - povinnost ohlásit regulátorovi porušení ochrany OÚ; • **Privacy by design** - požadavky ochrany OÚ už během vývoje resp. na začátku projektu.

Nařízení č. 2016/679 (GDPR) poměrně rozsáhlé, mezi hlavní změny, které ovlivní instituce a podnikatelské subjekty nejvíce, můžeme zařadit především následující:[25]

a) Okruh osobních údajů se podle GDPR rozšíří o údaje technického charakteru

Tradiční okruh osobních údajů, mezi které řadíme například jméno, příjmení a adresu zákazníka nebo klienta určitého úřadu či instituce, v určitých případech také email či telefonní číslo, bude od 25. 5. 2018 rozšířeno o další údaje technického charakteru, jakými jsou **IP adresa nebo cookies.** Jsou tak reflektovány požadavky, které vyplývají z technologických a technických inovací ve vztahu k činnosti podnikatelských subjektů i ve vztahu k institucím a organizacím.

b) GDPR zpřísní pravidla pro udělení a prokázání souhlasu se zpracováním osobních údajů

Zatímco některé osobní údaje se zpracovávají na základě zákona nebo v rámci plnění smluvních povinností, jiné údaje podnikatelé získávají na základě souhlasu dotčené osoby. Takový souhlas **musí být podle GDPR konkrétní, svobodný, informovaný a jednoznačný,** oproti předchozí právní úpravě takový **souhlas nemůže být součástí obchodních podmínek**, přičemž podnikatel nebo instituce musí být schopen kdykoli prokázat, že souhlas se zpracováním osobních údajů mu byl skutečně udělen. Tato skutečnost bude mít významný vliv například na zpracování osobních údajů pro účely

[25] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

marketingu nebo na používání souborů cookies, které se od 25. 05. 2018 budou muset změnit. Zároveň platí, že odvolání souhlasu se zpracováním osobních údajů by mělo být stejně jednoduché jako jeho získání.

c) Podle GDPR budou zpřísněné podmínky pro zpracování osobních údajů osob mladších 16 let

V souvislosti s nabídkou služeb informační společnosti, jako je například nakupování v e-shopech, využívání sociálních sítí, registrace na různých webových stránkách, apod. GDPR zavádí podmínku, že **zpracovávání osobních údajů osoby mladší 16 let na základě souhlasu je legální jen tehdy, pokud k tomu udělil souhlas její zákonný zástupce**. Jelikož ověření věku návštěvníka webové stránky je prakticky nemožné, text při zaškrtávacím políčku pro udělení souhlasu se zpracováním osobních údajů by měl v zájmu provozovatele webové stránky obsahovat alespoň další větu typu: *"Prohlašuji, že pokud mám méně než 16 let, tak jsem požádal svého zákonného zástupce (rodiče) o souhlas se zpracováním mých osobních údajů."* Tento návrh na sdělení v elektronické podobě vyplývá z konkrétních změn, které budou v rámci ČR v kontextu GDPR zavedeny.

d) GDPR zavádí povinnost stanovit tzv. odpovědnou osobu v originálním označení jako DPO, Data Protection Officer, v českém překladu Pověřenec pro ochranu osobních údajů

Podnikatelé, kteří systematicky, pravidelně a ve velkém rozsahu monitorují dotčené osoby, například konkrétně retargeting a různých formách behaviorální reklamy, musí podle GDPR stanovit odpovědnou osobu, která bude mít na starosti kontrolu postupů při zpracovávání osobních údajů, poskytování informací či spolupráci s Úřadem na ochranu osobních údajů. Odpovědnou osobou může být externí dodavatel služeb, jakož i vlastní zaměstnanec, ovšem pouze za splnění přísných, zejména kvalifikačních podmínek. Pověřenci pro ochranu osobních údajů musí bát nominování jak u podnikatelských subjektů, tak u institucí nebo organizací, které pracují s relevantními osobními údaji. Úkolem těchto pracovníků je zajistit soulad s daným Nařízením a jeho implementace do interních dokumentů organizace, stejně jako zajištění souladu relevantních činností a procesů v těchto organizacích.

e) Podle GDPR bude zavedena povinnost vést záznamy o zpracování osobních údajů

Každý podnikatelský subjekt, instituce a organizace, která zaměstnává alespoň 250 zaměstnanců, která zpracovává osobní údaje pravidelně jako například e-shop, nebo zpracovává osobní údaje zvláštní kategorie, musí podle GDPR vést záznamy o zpracování osobních údajů, například formou provozního deníku, do kterého budou zapisovány všechny důležité informace, například o přijatých technických opatřeních, o rozsahu a účelu zpracování osobních údajů nebo jejich přenosech do třetích zemí. Právě ve vztahu k tomuto pak hlavní úlohu v plnění těchto činností má pověřenec pro ochranu osobních údajů.

f) GDPR zavede povinnost nahlašovat bezpečnostní incidenty Úřadu pro ochranu osobních údajů jako i dotčeným osobám

Podnikatelé v postavení provozovatelů i zprostředkovatelů, stejně jako instituce a organizace budou mít nově povinnost nahlásit Úřadu pro ochranu osobních údajů každé podstatnější narušení či únik osobních údajů, a to nejpozději do 72 hodin od zjištění takového bezpečnostního incidentu. Pokud by takový únik či narušení představovaly vážné riziko pro práva dotčených osob, podnikatel, instituce nebo organizace bude povinen kontaktovat i samotné dotčené osoby, jejichž údaje mohou být ohroženy.

g) Podle GDPR budou někteří podnikatelé, instituce a organizace povinni provést analýzu dopadů na ochranu osobních údajů v anglickém označení jako DPIA, Data Protection Impact Assessment – audit osobních údajů a konzultovat svou činnost s Úřadem pro ochranu osobních údajů

V případech, kdy určitý druh zpracování osobních údajů může představovat vysoké riziko pro práva a svobody fyzických osob, podnikatelé, instituce a organizace budou povinni provést analýzu dopadu plánovaných zpracovatelských operací na ochranu osobních údajů. Nejčastěji tak půjde o případy systematického monitorování veřejně přístupných prostor

nebo rozsáhlé zpracování zvláštních kategorií údajů, například údajů o rasovém nebo etnickém původu, politických názorech či zdravotním stavu. Pokud podnikatel na základě zmíněné analýzy zjistí, že jeho činnost by mohla být vyhodnocena jako riziková podle GDPR bude muset požádat Úřad pro ochranu osobních údajů o konzultaci.

h) Dotčené osoby budou mít podle GDPR právo být vymazány nebo úplně zapomenuty

Tak jak je tomu v současné právní úpravě po 25. 5. 2018 bude platit, že pokud fyzická osoba požádá o výmaz svých osobních údajů, typicky například životopisu zaslaného společnosti, instituci, která uchazeče o zaměstnání nepřijala, podnikatel či instituce bude povinna takové žádosti vyhovět. Podle GDPR bude mít každý za určitých podmínek navíc právo požadovat, aby jeho osobní údaje byly zcela vymazány z internetových vyhledávačů jako Google, Yahoo, Bing, Seznam či jiných což v rámci české právní úpravy označujeme jako *„právo být zapomenut,“*

i) Dotčené osoby budou mít podle GDPR právo na přenos svých osobních údajů

Každá fyzická osoba bude mít po novém právo na bezplatné získání svých osobních údajů, které sama poskytla provozovateli, a tyto údaje následně předat jinému provozovateli, konkrétně například při změně poskytovatele určité služby, ať už internetové nebo jiné. Původní provozovatel tak bude povinen požadované osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, konkrétně pak XML nebo CSV vydat a umožnit jejich přenos za účelem dalšího použití. Tomuto právu by měly věnovat pozornost zejména provozovatelé webových stránek, kteří by na své stránky měli včas implementovat příslušnou funkci.

j) Pokuty podle GDPR budou mnohem přísnější

Zatímco pokuty podle současného zákona o ochraně osobních údajů dosahují v maximální míře hodnotu do 200.000 EUR, GDPR za porušení povinností při ochraně osobních údajů stanoví pokuty až do výše 20.000.000 EUR, případně až do výše 4 % z celosvětového ročního obratu. Ustanovení odpovědné osoby pouze "pro forma", opomenutí rodičovského souhlasu při zpracování osobních údajů dítěte, ignorování žádosti o výmaz osobních údajů či jiné porušení GDPR tak mohou být podstatně přísněji sankcionovány. Nicméně již

v současné době mnohé pojišťovny nabízejí speciální typy pojištění, které jsou určeny pro krytí rizik spojených se zpracováním osobních údajů vyplývajících právě z GDPR.

Prvním krokem každého podnikatele nebo instituce, který zpracovává osobní údaje, by měla být důkladná analýza používaných dokumentů, konkrétně pak formulářů, smluv, obchodních podmínek, podmínek ochrany osobních údajů, apod. A nastavení vnitřních postupů v rámci podnikatelského subjektu nebo organizace, jako je konfigurace kamerového systému, objednávkového procesu v e-shopu nebo registrace na fóru či v jiných částech webové stránky nebo webové aplikace. Jelikož samostudium a pochopení některých ustanovení GDPR může být pro mnohé poměrně náročné, jednou z možností, jak vyhodnotit rizika a identifikovat potřebné změny, je konzultace s advokátem nebo s odborníkem na ochranu osobních údajů.

Podnikatelé, kteří zpracovávají osobní údaje, stejně jako relevantní instituce a organizace ve velkém rozsahu, mohou na základě takové analýzy včas odhalit potřebu ustanovení odpovědné osoby, jejíž výběr nebo zaškolení trvá i několik měsíců. Jiní podnikatelé, kteří provozují e-shopy a webové portály, mohou zas přijít na to, že jejich podmínky ochrany osobních údajů jsou zastaralé, rozesílání reklamních nabídek je protiprávní, souhlas se zpracováním osobních údajů a s použitím cookies, nebo formulace účelu zpracování osobních údajů je nesprávná atd., přičemž implementace potřebných změn jim zabere jen několik hodin. V rámci prvotní analýzy bude proto vždy záležet na tom, jaké údaje, v jakém rozsahu, jakým způsobem a za jakým účelem tyto údaje podnikatel zpracovává. To, co však mají podnikatelé společné, je potřeba seznámit se s GDPR s dostatečným předstihem. Na základě výše uvedeného můžeme konstatovat, že Nařízení GDPR je často poměrně vágní, přičemž mnohé z výše uvedených změn se vyznačují různými specifiky.

4. Vlastní práce

4.1 Problémy související s únikem dat a GDPR

Unikly vám osobní údaje nebo jste byli napadeni hackery? Pokuty nebo medializace dané případu vám rozhodně nepomůže. Porušení ochrany osobních údajů nebo tzv. bezpečnostní incident je třeba oznámit nejen Úřadu pro ochranu osobních údajů, ale ve vybraných případech i samotné dotyčné osobě, tedy člověku, jehož osobní údaje unikly nebo byly předmětem jiné formy zneužití. GDPR však nevyžaduje, abyste oznámení bezpečnostního incidentu provedli vždy. Kdy tedy oznámení třeba provést a v jakých případech tyto skutečnosti nejsou nutné.[26]

Nařízení GDPR nestanoví pouze povinnosti související se zpracováním osobních údajů a očekávání na jejich zabezpečení prostřednictvím různých bezpečnostních opatření, ale počítá i se skutečností, že i nejlepší zabezpečený systém může selhat. Bezpečnost zpracování osobních údajů byste tak měly zajistit především prostřednictvím anonymizace, šifrování, zálohování a omezování přístupu i doby zpracování osobních údajů, jakož i prostřednictvím dalších vhodných organizačních a technických bezpečnostních opatření pozitivně působících na bezpečnost zpracování osobních údajů.

Při uvedeném by to však nemělo zůstat. Pamatujte na to, že všechna pravidla ochrany osobních údajů nesmí být prověřovány pouze v okamžiku jejich přijetí. Je třeba prověřovat jejich funkčnost a implementaci po celou dobu zpracování osobních údajů a používání bezpečnostních pravidel a prostředků ochrany osobních údajů. Proto je třeba pravidelně testovat, posuzovat a hodnotit jejich účinnost s ohledem na zajištění bezpečnosti zpracování osobních údajů, přičemž bude vhodné využívat odborně způsobilé osoby se

[26] *GDPR* [online]. EU: Evropská komise, 2018 [cit. 2018-12-20]. Dostupné z: https://www.gdpr.cz/gdpr/kompletni-zneni-gdpr/

znalostí IT technologii, informační bezpečnosti a právní úpravy v oblasti ochrany osobních údajů.

Pokud používáte tzv. zprostředkovatele osobních údajů, tedy například cloudové služby, datové úložiště, externí firmu na mzdy a účetnictví, externí SBS s přístupem ke kamerovým záznamům a další je v rámci podniku vyžadovat písemné záruky o tom, že takový zprostředkovatel přijal vhodná technická a organizační opatření splňující požadavky GDPR a zajistil dostatečné organizační, personální a technické předpoklady pro ochranu práv dotčených osob. Zprostředkovatel by s tímto cílem měl kdykoliv provozovateli, což zahrnuje daný podnik s právní závazností písemně potvrdit rozsah přijatých bezpečnostních opatření a právních záruk formou podpisu kontrolního seznamu s jasnou specifikací těchto opatření. Takový seznam bude tvořit nedílnou přílohu tzv. smlouvy o zprostředkování zpracování osobních údajů, a to ve formě smluvního závazku.[27]

V případě existence bezpečnostního incidentu v rámci podniku je nutné v první řadě bude třeba zachovat tzv. "chladnou hlavu" a racionálně přistoupit k jeho řešení za pomoci podnikové GDPR dokumentace a interních směrnic, které jsou vypracované přímo pro daný podnik. Tyto incidenty by při aplikaci dostatečných technických a personálních opatření neměly nastat, avšak jsou součástí relativně běžné praxe u mnoha firem. Nařízení GDPR tedy řeší tuto situaci tím, že je třeba začít minimálně tím, že s bezpečnostním incidentem "vyjdete na povrch". Tedy nebudete ho tajit. Pokud neohlásíte bezpečnostní incident v případech, kdy vám tato povinnost z jeho povahy vyplývá, bude na tuto skutečnost přihlížet Úřad pro ochranu osobních údajů při ukládání pokuty a stanovování jejich celkové výše.[28]

---

[27] *GDPR* [online]. EU: Evropská komise, 2018 [cit. 2018-12-20]. Dostupné z: https://www.gdpr.cz/gdpr/kompletni-zneni-gdpr/

[28] *GDPR* [online]. EU: Evropská komise, 2018 [cit. 2018-12-20]. Dostupné z: https://www.gdpr.cz/gdpr/kompletni-zneni-gdpr/

Ve smyslu ustanovení čl. 83 GDPR, pojednávajícího o obecných pravidlech ukládání správních pokut, při rozhodování o uložení správní pokuty a její výši v každém jednotlivém případě Úřad náležitě zohlední i způsob, jakým se o porušení dozvěděl, a zejména to, zda provozovatel nebo zprostředkovatel porušení oznámili a pokud ano, v jakém rozsahu. Proto, pokud vám vznikne povinnost oznámit bezpečnostní incident, raději tak proveďte. Mnozí podnikatelé mají obavu z toho, že pokud oznámí bezpečnostní incident, budou čelit reputačnímu riziku a medializaci. A právě zde se dostáváme do situace, kdy vzniká o důvod víc na to, abyste správně posoudili, zda vám povinnost na oznámení bezpečnostního incidentu vznikla nebo ne. Povinnost oznámit bezpečnostní incident je stanovena v čl. 33 a 34 nařízení GDPR.[29]

1.1.1 Přístup států EU k GDPR

Pro příklad, jeden z našich nejbližších sousedů, Německo, jako nadstavbu k GDPR zavedlo povinnou pozici zmocněnce pro ochranu dat ve společnostech, které mají 20 a více zaměstnanců. Tito zmocněnci se tak ve zpracování dat angažují a celou tuto problematiku ve společnostech zastřešují.

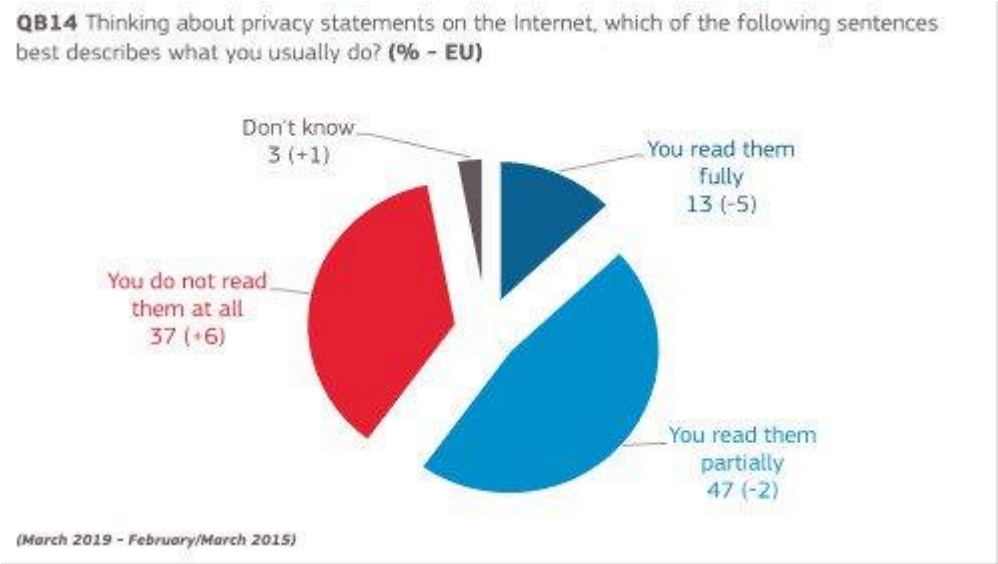
Komise ve výsledku také zpracovala informaci o procesu týkajícím se vyšetřování případných zanedbání, opomenutí a porušení daných nařízení. „Některá vyšetřování prohřešků, která začala krátce po účinnosti nařízení stále běží, protože se jedná o složitý proces," uvedla a zdůraznila, že by se úspěšnost nařízení neměla měřit počtem udělených pokut, ale výhradně na základě snahy a nápravných procesů ze strany zúčastněných aktérů. Doposud nejvyšší pokuta ve výši 50 milionů eur byla prozatím udělena francouzské společnosti - Googlu, a to pro nevyhovující podmínky týkající se získání souhlasu uživatelů tohoto vyhledávače.

---

[29] *GDPR* [online]. EU: Evropská komise, 2018 [cit. 2018-12-20]. Dostupné z: https://www.gdpr.cz/gdpr/kompletni-zneni-gdpr/

Podle Komise je v souvislosti s ochranou dat a dodržováním GDPR v tuto chvíli nezbytná a zároveň stěžejní podpora malých a středních podniků, samozřejmě neustálé a podrobné seznamování obecné veřejnosti s danou problematikou tak, aby byla zažita jako standardní a běžná součást našeho života a v neposlední řadě vytvoření systému „kultury ochrany dat“.

Obrázek 1: Eurobarometr Březen 2019



Zdroj: https://euractiv.cz/section/digitalni-agenda/news/rok-od-gdpr-nektere-staty-pravidla-stale-nedodrzuji-cesko-udeluje-prvni-pokuty/

Podle vydání Eurobarometru z května jen v tuto chvíli jen pětina Evropanů dokáže správně odpovědět, která instituce za ochranu jejich osobních dat zodpovídá. Komise proto nedávno přišla s kampaní, jejichž záměrem je motivovat evropany, aby vždy důkladně přečetli a prostudovali prohlášení o ochraně soukromí a upravili si tak osobní nastavení ochrany soukromí“ dle svého uvážení a rozhodnutí. Ovšem v opačném případě naopak 67 % dotazovaných o existenci tohoto nařízení ví a 73 % má nějaké kusé informace alespoň o jednom z práv, které nařízení občanům přináší.

Některé státy jsou pozadu

V tuto chvíli dosud tři státy Unie nařízení nezavedly do svých národních právních řádů. Jedná se o Portugalsko, Řecko a Slovinsko.

K tomu komise uvedla, že zmíněné státy musí nařízení uvést do svých národních právních řádů co nejdříve. Pokud tak nebude učiněno, komise „využije všechny nástroje, které má k dispozici včetně řízení o nesplnění povinnosti, aby zajistila, že jsou národní předpisy členských států v souladu s nařízením a zamezila tak roztříštění evropského rámce ochrany údajů."

Komplikace s implementací se objevily i u některých dalších zemí. Ve Španělsku, taktéž v Německu vydaly nedávno jejich vlastní soudy rozhodnutí, kdy došlo k anulaci některých národní předpisů. Právě kvůli jejich neslučitelnosti s GDPR.

4.2 Náklady na implementaci GDPR

Kolik přibližně vyjde implementace opatření na zohlednění GDPR středně velkou firmu působící v České republice? Níže jsou uvedeny komentáře zástupců vybraných českých firem.

Společnost White & Case

Podle zástupců této firmy není klíčová velikost společnosti, jako spíš to, čím se podnik zabývá a v jakém rozsahu s osobními údaji pracuje a manipuluje. U společnosti, která spolupracuje se zaměstnaneckou a smluvní agendou, se může jednat o náklady v řádech desítek tisíc korun; u firmy, která musí ustanovit pověřené osoby pro osobní údaje, implementovat nutné směrnice a technické úpravy ve vlastních systémech, se částky za GDPR pohybují v rozmezí od několika set tisíc korun až po miliony.

Deloitte Legal

Firma tvrdí, že výše nákladů na zavedení GDPR se hlavně odvíjí od úrovně ochrany osobních údajů v dané firmě, od její velikosti, povahy a rozsahu zpracovávání osobních údajů. Na tchto aspektech také závisí nutnost externí asistence e zavedením, jejíž nabídku na dnešním trhu může reprezentovat klasické právní poradenství, ale také inovativní metody rozboru skrze automatizované nástroje na uskutečnění prvotní analýzy. Náklady pro středně velké firmy se tak mohou pohybovat okolo několika set tisíc korun.

Kinstellar

Zástupce firmy Kinstellar říká, že firma s 50 zaměstnanci prodávající výrobky na internetu a zpracovávající především osobní údaje klientů, by měla počítat s cenou za zavedení kompletního systému GDPR přibližně na úrovni půl milionu korun. Na trhu se bohužel objevují nejrůznější standardizované balíčky za několik desítek tisíc korun, deklarující kompletní řešení pro střední firmy, nicméně v praxi jsou nepoužitelné.

Rowan Legal

Firma tvrdí, že náklady na zavedení GDPR záleží na velké spoustě nejrůznějších okolností – především jde o to, do jaké míry taková firma doposud respektovala platný zákon, jaký je předmět její činnosti a jak velká zpracování osobních údajů provádí. Odvíjí se to rovněž od toho, zda taková firma umí GDPR zavést vlastními prostředky, nebo s využitím externích sil. Středně velký, výrobně-obchodní podnik, který doposud respektoval platnou legislativu (a tomu odpovídaly jeho informačně-technologické systémy), by za transfer na GDPR nemusel vynaložit více, než několik desítek tisíc korun. Naopak třeba středně velký poskytovatel cloudových služeb, který platnou legislativou dodržoval jenom okrajově a jehož informačně-technologické systémy na GDPR nejsou nachystané, může za zavedení GDPR utratit i několik set tisíc korun.

Legalité

Zástupce firmy na to, kolik středně velký podnik stojí implementace GDPR, neumí odpovědět. Náklady se totiž mohou odlišovat – záleží na odvětví, v němž firma působí, a také na tom, nakolik podnik splňoval nároky na tehdejší právní úpravy (zákona o ochraně

osobních údajů). Stavební firma zaměstnávající mnoho pracovníků z různých stavebních profesí může mít podstatně menší náklady na splnění nároků GDPR než firma s pár pracovníky, která se ovšem orientuje např. na směnárenskou činností a musí o svých klientech uchovávat mnoho osobních údajů - zda jsou „politicky exponovanou osobou“, odkud sehnali potřebné finanční prostředky apod.

4.3 Požadavky na zajištění shody s GDPR

Jedná se o první krok, který provedeme pro dosažení shody s GDPR. Na základě analýzy zjistíme nedostatky v plnění nařízení. Analýza se zabývá porovnáním stavu ochrany osobních údajů zadávajícího s požadavky nařízení. Stanovíme oblasti ochrany údajů, které je třeba zlepšit, protože nedosahují potřebnou úroveň. Zjištěné poznatky nám poskytují informace o slabinách a nedostatcích ochrany osobních údajů klienta. Výstupní dokumenty obsahují detailní i souhrnný přehled hodnocení pro jednotlivé požadavky GDPR.[30] Postup při specifikaci požadavků zajištění shody s GDPR ve firemní praxi je uveden níže.

Sestavení plánu shody

V návaznosti na analýze je zpracován detailní návrh změn. Plán shody organizaci přivede až do cíle naplnění obsahových požadavků nařízení. Cílem je podrobné definování dílčích úkolů a postupů realizace k dosažení souladu s GDPR.

Posouzení dopadů na ochranu osobních údajů

Druhým krokem, který umožňuje posoudit zpracování osobních údajů a plánovaná opatření z pohledu skutečných rizik je posouzení dopadů na ochranu osobních údajů. GDPR požaduje provádět posouzení přiměřenosti a nezbytnosti operací při zpracování údajů z hlediska účelu a posouzení rizik. Půjde o nejvíce kontrolovanou povinnost a GDPR přímo stanoví odpovědnost za takové posouzení v rámci organizace. Zpracování hodnocení

[30] DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8, s. 168

obsahuje zpracování formuláře, identifikaci respondentů, zajištění potřeby a hodnocení rizik nakládání s osobními údaji klienta, dopad na soukromí a zpracování záznamu z hodnocení rizik práce s osobními údaji a předání tohoto záznamu klientovi.[31]

Implementace GDPR do firemní praxe

Posledním krokem k dosažení shody s GDPR jsou změny procesů. Vycházíme z analytické fáze a informací o neshodách. Implementace představuje úpravy, nasazení technologií, upgrade systému, doplnění procesů a definování pravidel ochrany osobních údajů.

Změna procesů organizace v souvislosti se zavedením GDPR do firemní praxe

Cílem je zajistit zefektivnění práce s osobními údaji a minimalizování uloženého, zpracovávaného a přenášeného množství. Výhodou je zmenšení rozsahu, ve kterém je nutné přijímat opatření pro jejich ochranu a celkové snížení a optimalizaci nákladů na dosažení shody. Jde především o zřízení, odstranění, změny, předávání osobních údajů, hlášení incidentů a řízení kontinuity systémů.[32]

Návrh ICT opatření v kontextu zavedení GDPR

Jde o významnou fázi, jejímž cílem je změnit infrastrukturu IS organizace, aby byla schopna provádět technická opatření v souladu s požadavky GDPR. Klíčové oblasti jsou řízení přístupu, zálohování dat, monitorování a logování, IDS / IPS, kryptografie, sítě, mobilní zařízení, antivirová ochrana a další individuální oblasti s ohledem dosavadní podnikatelské činnosti firmy.

---

[31] IAPP. 2018. GDPR. [online]. [2018-01-11]. Dostupné z: https://iapp.org/search?q=gdpr

[32] IAPP. 2018. GDPR. [online]. [2018-01-11]. Dostupné z: https://iapp.org/search?q=gdpr

Právní aspekty související s GDPR

Změny nastávají rovněž ve vztazích v organizací a jejich klienty, dodavateli nebo kontrolními subjekty. Změny ve smluvních a právních vztazích mohou obsahovat souhlas subjektů, zaměstnanecké smlouvy, smlouvy s dodavateli, smlouvy o zachování důvěrnosti informací a další.

Definování rolí

Je třeba definovat roli, kdo bude řídit ochranu osobních údajů a ponese odpovědnost. Pověřenec pro ochranu osobních údajů musí být jmenován, pokud zpracování provádí orgán veřejné moci či veřejný subjekt, jeho činnost vyžaduje rozsáhlé pravidelné a systematické sledování subjektů údajů nebo zpracování speciálních kategorií údajů.

Klíčové vlastnosti k dodržování GDPR

Z hlediska nařízení je třeba se zaměřit na pět hlavních klíčových oblastí, které nám pomůže k získání shody s GDPR. Tyto klíčové oblasti jsou specifikovány níže.[33]

Oblast 1 – řízení

Je důležité definovat, jak přenést GDPR do norem, hodnot a akcí. Zjistit, jaká opatření je třeba provést, zda jsou účinné a jako jejich víme dále zefektivnit.

Oblast 2 - lidé a komunikace

Zaměstnanci potřebují znát rizika a důsledky nesprávného využívání dat. Proto je důležité zajistit pracovníkům školení v oblasti požadavků GDPR.

---

[33] IBM. 2018. [online]. [2018-01-11]. Dostupné z: https://www.ibm.com/

Oblast 3 – procesy

Součástí analýzy je zaměření se na procesy, jakým způsobem jejich GDPR ovlivní, jaké budou dopady a jak se budou řešit požadované změny.

Oblast 4 – data

Zjistíme, jaká data máme a k čemu jejich využíváme. Je třeba zajistit kvalitu a řízení údajů i interakci s klienty a třetími stranami. Je to nezbytnou součástí pro zajištění důvěryhodnosti a transparentnosti.

Oblast 5 – zabezpečení

Musíme zajistit ochranu a důvěrnost osobních údajů jakož i zajistit jejich řádné použití zahrnující možnosti volby, souhlasu, upozornění, přístupu, nápravy nebo odstranění dalších aspektů.

4.4 Řízení procesů z hlediska interního auditu v souvislosti s GDPR

Cílem interních auditů je definování účinnosti a spolehlivosti celého systému, zabránění neshodám a jeho stále zlepšování. Interní audity stanoví stávající nedostatky, slabá místa, hledají jejich příčiny a navrhují nápravná a preventivní opatření pro zlepšení systému.[34] Cílem interního auditu je přesvědčení se, že se řešily stávající i nově vznikající rizika související se zabezpečením ochrany dat. Interní audit formuluje vhodná doporučení, jak předejít újmě a efektivně využít zdroje pro přípravu na nové povinnosti. Interní audit GDPR klade značné požadavky na složení a odbornost auditorského týmu. Členové týmu by měli mít přinejmenším dobrý přehled o informačních a komunikačních technologiích, řízení bezpečnosti informací, řízení procesů a o právu ochrany osobních údajů.[35] Výstupem

[34] DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8, s. 174

[35] TECHBIT. 2018. *Interný audit GDPR*. [online]. [2018-01-10]. Dostupné z: https://www.bdo.cz/

auditu je záznam auditu informačního systému o události, která může ovlivnit bezpečnost informačního systému.[36]

Audit je nezávislý, systematický a dokumentovaný proces získání důkazů z auditu a jejich hodnocení. Cílem je definovat rozsah splnění kritérií. Poskytuje důležité informace pro zlepšování systému řízení, jde o efektivní a spolehlivý nástroj pro podporu úspěšného řízení a sladění zpracování osobních údajů se závaznými předpisy. V kontextu výše uvedeného je možné uvést následující typy auditů, konkrétně:[37]

- **Audity první stranou** - jsou označovány jako interní audity. Firmy si tyto audity vykonávají samy pro sebe. Organizace si volí pravidla, kterými se audit řídí a výsledky využívá výhradně pro vlastní vylepšování. Rozhoduje o prioritách, cílech, rozsahu a určuje oblasti, které potřebuje nejvíce prověřit. Tento typ auditu může být prováděn interními pracovníky i externími subjekty.
- **Audity druhou stranou** - jsou známé jako odběratelské audity. Provádějí je převážně externí subjekty, které mají vůči firmě konkrétní zájmy. Může jít o audity vyplývající ze vzájemných smluvních vztahů. Odběratel může prověřit míru zabezpečení údajů u dodavatelů a na základě auditu provést opatření a příslušné rozhodnutí. Využívá se hlavně v automobilovém průmyslu.
- **Audity třetí stranou** - jsou prováděny externí organizací. Pravidla, kterými se řídí, schvaluje regulační nebo akreditační orgán. Třetí strana může rozhodovat o vydání nebo odebrání certifikátu a na základě objektivních informací také o stavu auditované oblasti. Úkolem auditu je na základě předem definovaných požadavků zjistit soulad v organizací. Požadavky definuje firma interně vlastními předpisy,

[36] 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 pozdějších předpisů

[37] 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 pozdějších předpisů

legislativa, která je závazná nebo pomocí zvoleného standardu například příslušnou ISO normou. Prioritou je zvolit správný způsob a použité nástroje pro ověření subjektu na základě zaměření daného auditu. Při bezpečnostním auditu se zaměřujeme na zabezpečení, při procesním budou sledovány interní postupy. Vzhledem na ochranu osobních údajů se provádí kombinace těchto druhů. GDPR vyžaduje nejen odpovídající technická opatření, ale i vhodné organizační řešení. Právě prostřednictvím auditu dokážeme skutečně zajistit správnost dokumentovaných a zavedených opatření.[38]

4.4.1 Průběh auditu a jeho vymezení

Audit je proces skládající se ze vstupních a výstupních informací. Mezi vstupní data patří vše, co se spojuje s výskytem a způsobem zpracování osobních údajů. Ověření současného stavu s definovanými požadavky nám dává výsledek výstupu. Pokud nebyla stanovena shoda, výstupem může být doporučení auditora jak efektivně řešit nebo zlepšit stávající opatření. Výsledkem může být rovněž stav "shoda" nebo "neshoda". GDPR upravuje požadavky na ochranu osobních údajů fyzických osob. Tyto požadavky jsou určeny:[39]

- **v procesní rovině** - potřeba dokumentování a zavedení interních metod zpracovatele a správce při získávání osobních dat. Samozřejmostí je potřeba zajistit práva subjektů,
- **v administrativně - organizační rovině** - jde o zajištění organizačních opatření spojených s bezpečným používáním OÚ oprávněnými, poučenými a vyškolenými osobami,

[38] AUTOCONT. 2018. *Nové pravidlá v oblasti ochrany osobných údajov.* [online]. [2018-01-10]. Dostupné z: http://www.autocont.cz

[39] AUTOCONT. 2018. *Nové pravidlá v oblasti ochrany osobných údajov.* [online]. [2018-01-10]. Dostupné z: http://www.autocont.cz

- **v technické rovině** - jako požadavky na zavedení technických a technologických opatření, které zajistí bezpečnost zpracovávaných osobních údajů ve všech fázích jejich životního cyklu.

Připravenost k plnění kritérií nařízení mohou auditoři ověřit především z těchto hledisek:[40]

- plnění pravidel právních předpisů pro zpracování osobních dat a připravenost na nová pravidla,
- zpracovávání dokumentace systému řízení osobních údajů,
- nastavení a fungování technických a organizačních opatření a kontrol,
- řízení lidských zdrojů v rámci bezpečnosti osobních dat.

4.3.2. Postup prováděného auditu

Cílem auditorských postupů je získání důkazů, na základě kterých auditor dospěje k přiměřeným závěrům pro vyjádření konkrétních doporučení a opatření.

Porozumění organizaci v rámci dané firmy

Auditor definuje všechny informace o charakteru a o předmětu činnosti organizace firmy a organizačních jednotek, její struktuře, používaných IS, kategoriích zpracovávaných osobních dat a o zpracovávajících. Na základě těchto údajů auditor Předběžně identifikuje oblasti a procesy, v rámci kterých se zpracovávají osobní údaje. Dále navrhne strategii ověřovacího auditu.

Předběžné vyšetřování

V této části auditor komunikuje se zástupci organizace firmy, zhodnotí vnitřní předpisy a metodiky a další podklady týkající se zpracování osobních údajů. Pokračuje předběžného

[40] TECHBIT. 2018. *Interný audit GDPR*. [online]. [2018-01-10]. Dostupné z: https://www.bdo.cz/

klasifikací rizik pro firmu a pro subjekty osobních údajů. Upřesní vymezení oblastí, kde se pracuje s osobními údaji. Předběžné vyšetřováním upřesní cíle a předmět auditu tak, aby byly významné z hlediska ochrany ověřovány klíčové procesy zpracování osobních údajů a skutečností. Může jít například o zajištění personální činnosti a mezd, zajištění fyzické bezpečnosti prostřednictvím kamerových systémů, účetnictví, obchodní a marketingové aktivity. Auditor rovněž posoudí nezbytnost použití sofistikovaných nástrojů datové analýzy a přidanou hodnotu případného penetračního testování. Výstupem tohoto vyšetřování je program interního auditu.

Audit na místě

Auditor získává a shromažďuje všechny potřebné dokumenty a informace jako formuláře, žádosti nebo smlouvy. Provádí rozhovory s pracovníky společnosti, jako jsou bezpečnostní pracovníci, vlastníci aktiv a IT celků, správci provozních postupů a aplikací, personalisté, účetní nebo marketingoví zaměstnanci a provádí plánované testy. Auditor může provést i fyzickou prověrku prostorů, ve kterých se osobní údaje nacházejí nebo zařízení, které je zpracovává. Získané informace vyhodnotí a posoudí správnost stávajících postupů a dokumentace a rizika procesů zpracování osobních údajů.

Reporting

Auditor vytvoří návrh zprávy na základě vyhodnocených informací, která obsahuje všechny závěry z auditu. Její součástí jsou doporučení k odstranění nedostatků a pro snížení identifikovaných rizik. Vytvořený návrh zprávy projedná s příslušnými zástupci společnosti a na základě výsledků projednání auditor připraví konečnou verzi zprávy.

V kontextu výše uvedených skutečností je možné formulovat předpoklady kvalitního auditora z hlediska implementace GDPR v rámci firemní praxe. Konkrétně jsou to následující předpoklady:[41]

[41] TECHBIT. 2018. *Interný audit GDPR*. [online]. [2018-01-10]. Dostupné z: https://www.bdo.cz/

1. Je úprava odpovědnosti dostatečná v rámci zpracování osobních údajů?

2. Je dostatečná úprava pravidel v oblasti IT, zejména politiky přístupů, správy hesel, zavedení a uplatňování technických opatření?

3. Jsou plněny povinnosti vůči subjektům údajů, povinnost poskytovat informace o kategoriích zpracovávaných osobních údajů, účelech zpracování, příjemcích údajů, právech dotčených osob?

4. Existuje rejstřík zpracovávaných osobních údajů? Musí obsahovat alespoň kategorie takových osobních údajů, kategorie dotčených osob, povahu a účel zpracování. Dále místo, kde jsou osobní data shromažďovaná, zodpovědnost za jednotlivé fáze zpracování, lhůty, po které mají být osobní údaje zpracovávány a právní tituly opravňující správce k jejich zpracování.

5. Je práce a souhlasy se zpracováním osobních údajů prováděna správně? Zahrnuje vymezení, kde je souhlas nezbytný ke zpracování osobních údajů, a kde je zpracování osobních údajů odůvodněné jiným právním titulem. Je nezbytné jasné odlišení souhlasu od smluvních podmínek, plnění informační povinnosti a konkrétní vymezení účelu.

6. Je úprava smluv mezi správcem a zpracovateli osobních údajů dostatečná? Například konkrétně ujednání o zárukách součinnosti zpracovatele v souvislosti s vyřízením požadavků dotčených osob uplatněných u správce těchto údajů.

7. Je zajištěno zvyšování povědomí zaměstnanců v oblasti ochrany osobních údajů a s tímto souvisejících školení?

8. Je dostatečné nastavení postupů pro uchování a likvidaci osobních údajů s ohledem na zásadu minimalizace osobních údajů a omezení uložení osobních údajů?

9. Existují postupy v případě narušení ochrany osobních údajů?

10. Existují postupy pro komunikaci s Úřadem pro ochranu osobních údajů?

5. Případová studie

5.1 Předpoklady implementace GDPR ve společnosti Alza

Nařízení zavádí nové definice pojmů a povinnosti týkající se ochrany osobních údajů. Tato část popisuje nejdůležitější povinnosti společností a podnikatelů, práva dotčených osob i změny v oblasti zpracování osobních údajů na praktických příkladech. Definuje bezpečnost, možnosti zálohování z hlediska GDPR, technická opatření a nové technologie. Detailně popisuje zavedení GDPR nařízení v konkrétní společnosti, včetně postupů a opatření v tomto zařízení obsažených z hlediska jednotlivých ustanovení.

Povinnosti podnikatele a firmy obecně

GDPR zavádí povinnost stanovit odpovědnou osobu. (dále jen DPO) Podnikatelé musí zvolit v organizací odpovědnou osobu, pokud ve velkém rozsahu a pravidelně monitorují fyzické osoby. Bude mít pod dohledem poskytování informací, kontrolu postupů zpracování osobních údajů a komunikaci s Úřadem pro ochranu osobních údajů. Odpovědná osoba musí splňovat kvalifikační podmínky, může jít o vlastního zaměstnance i externího dodavatele. Uvedená povinnost se týká následujících subjektů, které zpracovávají osobní údaje:[42]

- **orgánů veřejné moci** (ministerstva, úřady) a veřejnoprávních subjektů (obce, školy, nemocnice) s výjimkou soudů při výkonu jejich pravomocí,
- **provozovatele a zprostředkovatele**, jejichž hlavní činností jsou zpracovatelské operace, které si vzhledem ke své povaze, rozsahu nebo účely vyžadují pravidelné a systematické sledování dotčených osob ve velkém rozsahu,

[42] IRWIN, L. 2018. *The GDPR: What technical measures do you need to conduct? [*online]. [2018-01-12]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-what-technical-measures-do-you-need-to-conduct/

- **provozovatele a zprostředkovatele**, jejichž hlavní činností je zpracování zvláštních kategorií údajů ve velkém rozsahu nebo zpracovávání osobních údajů týkajících se uznání viny za trestné činy a přestupky,
- **provozovatele**, u kterých to stanoví zvláštní právní předpis.

Povinnost nahlašování bezpečnostní incidentů v rámci organizace firmy

Každé narušení, ale také únik osobních údajů musí společnosti nahlásit Úřadu na ochranu osobních údajů. Tuto povinnost musí provést do 72 hodin od vzniku bezpečnostního incidentu. Podnikatelé jsou povinni narušení nebo únik hlásit i dotčeným osobám, pokud situace představuje vážné riziko a ohrožuje údaje těchto osob. Pokud by to však vyžadovalo nadměrné úsilí, může zvolit organizace i informování veřejnosti. Oznamovací povinnost se vyhodnocuje na základě vážnosti daného problému a konkrétních okolností. Za porušení ochrany se rozumí ztráta nosiče s nekódující klientskými daty, nedovolené vniknutí do sítě a zásah do uchovávaných dat. Může nastat i situace, kdy hacker kontaktuje provozovatele a žádá o výkupné za zpřístupnění databáze, do které neoprávněně vnikl.[43]

Zrušení bezpečnostních projektů

Bezpečnostní projekt je v podstatě nepoužitelný pro legislativu podle GDPR. Dochází k zániku povinnosti vypracovat bezpečnostní projekt. Důležitým diferenciačním prvkem je, že při bezpečnostním projektu je třeba se zaměřit na rizika bezpečnosti a zájmy firmy, při DPIA se zaměřujeme na rizika práv a svobody dotčených osob. I přes některé podobnosti a identické povinnosti zpracovávat přijatá bezpečnostní opatření bezpečnostní projekty a DPIA nemůžeme ztotožňovat, jak je k dispozic a výkladu aktuální účinné právo. Někteří podnikatelé musí provést analýzu dopadů na ochranu osobních údajů (dále jen DPIA) a konzultovat své aktivity s Úřadem pro ochranu osobních údajů Firmy musí vypracovat analýzu dopadu plánovaných zpracovatelských operací týkajících se ochrany osobních údajů, pokud nějaký druh zpracování dat může znamenat riziko pro

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

svobody a práva dotčených osob. Týká se zvláštních kategorií údajů o etnickém nebo rasovém původu, zdravotním stavu nebo politických názorech. Rovněž situací systematického monitorování veřejně přístupných prostor. Pokud společnost zjistí, že její aktivity by mohly být hodnoceny jako rizikové, musí podle nařízení požádat o konzultaci Úřad pro ochranu osobních údajů.[44]

Bezpečné zpracování osobních údajů

Firmy musí provést opatření pro bezpečné zpracování dat. Mohou údaje anonymizovat, například šifrovat. To znamená, že až po dešifrování jsme schopni osobu identifikovat. Za vhodné opatření můžeme považovat v případě incidentu schopnost včas obnovit dostupnost údajů, periodické testování a jiné. Důležitá je také minimalizace údajů. Firmy by neměly zpracovávat zbytečné údaje o klientovi. Výhodné je, aby firmy zapracovaly nové požadavky pro vývoji nových produktů nebo služeb pro jednotlivé skupiny zákazníků. V době, kdy dotyčná osoba poskytuje provozovateli své údaje, musí být upozorněna na jaký účel a na základě čehož budou její data zpracovávána. Komu jsou tato data poskytovány, jak dlouho jejich provozovatel bude uchovávat a zda budou přenášeny do zahraničí.[45]

Dotčené osoby mají podle GDPR právo na přístup a poskytnutí osobních údajů. Pokud dotyčná osoba požádá o kopie osobních údajů, které o ní zpracovávají, kdo k nim má přístup a za jakým účelem, společnost je povinna jí tyto údaje poskytnout. Tyto požadavky si většinou vyžadují zásadní zásah do stávajících informačních systémů. Systémy takové funkcionality běžně neobsahují. Firma však může takovou požadavek odmítnout nebo zpoplatnit, pokud půjde o opakované nebo nepodstatné žádosti. Je možné poskytnout

---

[44] IRWIN, L. 2018. *The GDPR: What technical measures do you need to conduct? [*online]. [2018-01-12]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-what-technical-measures-do-you-need-to-conduct/

[45] IRWIN, L. 2018. *The GDPR: What technical measures do you need to conduct? [*online]. [2018-01-12]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-what-technical-measures-do-you-need-to-conduct/

přímý vzdálený přístup k údajům, které si bude moci sama upravit nebo doplnit. Samozřejmě takový přístup nesmí ohrozit vlastnictví provozovatele ani údaje třetích osob.[46]

Dotčené osoby mají právo na přenos svých osobních údajů. Právo na portability dat je novým právem, které má podpořit konkurenci provozovatelů. Lidé budou mít právo na bezplatné nabytí svých osobních údajů. Tyto údaje svobodně poskytují provozovateli a ten je povinen kdykoli tato data poskytnout a s cílem dalšího použití umožnit jejich bezpečný přenos například při změně poskytovatele internetové služby. Dotčené osoby mají právo být vymazány nebo úplně zapomenuté. Pokud je zpracování dat v rozporu s oprávněnými zájmy dotčené osoby, má právu být zapomenuta. Pokud fyzická osoba požádá o výmaz svých osobních údajů, společnost je povinna tyto údaje vymazat a informovat provozovatele, kteří tato data zpracovávají. Firma však nemusí žádosti vyhovět, pokud by vymazání stálo nepřiměřeně mnoho peněz nebo by se musely použít složité technické prostředky. Podle GDPR bude mít každý za určitých podmínek navíc právo požadovat, aby jeho osobní údaje byly zcela vymazány z internetových vyhledávačů jako Google, Yahoo, Bing či Seznam.[47]

GDPR má však i výjimky, pokud půjde o povinné uchovávání údajů například pro daňové účely nebo uchovávání dat pro obhajobu právních nároků. Provozovatel tehdy žádosti nemusí vyhovět. Občané mohou vznést proti zpracování osobních údajů. Provozovatel je povinen o této možnosti osobu výslovně informovat. Dotyčná osoba si sama vybírá formu komunikace ústně, písemně, telefonicky nebo elektronicky. Provozovatel má být schopen v těchto formách žádost zpracovat a zpřístupnit občanům případnou telefonickou hot linku, zpřístupnění dotazníků nebo formulářů. Tedy určitým způsobem usnadnit výkon práv dotčených osob. Pro vyřízení žádosti má provozovatel lhůtu jeden měsíc, v případě náročných žádostí může tuto dobu prodloužit o dva měsíce od doručení. Přijaté žádosti

---

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

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

musí vyřešit neprodleně a bezplatně. Poplatek však může požadovat, pokud jde o neopodstatněnou, nepřiměřenou nebo opakovanou žádost a požadavek zákazníka.

Podnikatelé, kteří vlastní webové portály nebo e-shopy se musí rovněž seznámit s nařízením GDPR. Implementace žádoucích změn nicméně nemusí být pro ně až tak náročná, a to proto, že se na tyto změny postupně připravovali. Nejdůležitější je zajistit správnost souhlasu a souladu se zpracováním údajů a používáním cookies i formulaci účelu zpracování osobních údajů. Zkontrolovat aktuálnost podmínek ochrany údajů a zajistit, aby posílání marketingových nabídek nebylo protiprávní. I když je Nařízení č. 2016/679 (GDPR) poměrně rozsáhlé, mezi hlavní změny, které podnikatele ovlivní nejvíce, je možné zařadit především následující oblasti:[48]

- firmy, e-shopy nebo provozovatelé kamerových systémů musí vést zápisy o zpracování osobních údajů,
- firmy zaměstnávající více než 250 zaměstnanců mají povinnost mít speciální evidenci o zpracování osobních údajů. Tuto povinnost mají rovněž podnikatelé zabývající se specifickou kategorií dat. Jde například o zdravotní údaje nebo takové, které se nezpracovávají příležitostně. Nařízení obsahuje výjimku pro společnosti s méně než 250 zaměstnanci, například pokud zpracování dat nevede k riziku nebo je příležitostí pro práva a svobody občanů,
- na webové stránce nemůže být předem označen souhlas se zpracováním osobních údajů. Pokud je ikona pro udělení souhlasu na e-shopu nebo webu předem zaškrtnutá, musíme ji změnit na neoznačenou. Souhlas s marketingovým zpracováním osobních údajů musí být svobodný, jednoznačný a konkrétní,
- v obchodních podmínkách nemůže být automaticky uveden souhlas se zpracováním osobních údajů pro marketingové účely. Pokud se souhlas se zpracováním údajů provádí automaticky podepsáním smlouvy, jde o neplatný a nesvobodný úkon a marketingové zpracování dat se považuje za protizákonné. Reklamní nabídky

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

nemohou být součástí smlouvy, obchodních podmínek ani formulářů určených pro objednávku,

- firma musí umět prokázat udělení souhlasu se zpracováním osobních údajů. Společnost musí umět kdykoli prokázat souhlas fyzické osoby se zpracováním osobních údajů. Pokud podnikatel nebude schopen tuto skutečnost prokázat, hrozí mu vysoké sankce. Vhodné je používat tzv. double opt-in nástroje zejména pro provozovatele e-shopů nebo internetových obchodů. Jde o poslání potvrzujícího emailu o zpracování dat. Zákazník tento email dostane a následně ho potvrdí, čímž potvrzuje svůj souhlas. Cookies můžeme sbírat, jen pokud návštěvník webové stránky udělí svůj souhlas Soubory cookies jsou považovány za osobní údaj, a proto je můžeme používat až tehdy, pokud návštěvník web stránky udělí svůj svobodný souhlas. Pokud v současnosti webová stránka využívá cookies ukládající se u zákazníka před vyjádřením jeho souhlasu, na základě nařízení toto nastavení systému bude muset změnit do začátku platnosti GDPR,
- při zpracování osobních údajů dětí a mladistvých, které mají méně než 16 let, je nutný rodičovský souhlas. Provozovatel musí ověřit, že zákazníkovi, který nedovršil 16 let, je udělen souhlas zákonného zástupce s předáním jeho osobních údajů. Podle nařízení tak musí udělat každý, kdo zpracovává osobní údaje na základě souhlasu nebo provozuje web nebo e-shop s online služby. Při zaškrtávací ikonce by měla být doplněna formulka o větu: *"Prohlašuji, že pokud mám méně než 16 let, tak jsem požádal svého zákonného zástupce (rodiče) o souhlas se zpracováním mých osobních údajů."* Je to důležité z toho důvodu, že ověření věku návštěvníka webu je téměř nemožné,
- Předávání osobních údajů ze služby ke konkurenci musí být bezplatný a v meta datech. Uživatel může požádat o zpřístupnění osobních údajů konkurenční aplikací nebo webové stránce. Tyto údaje poskytneme z databáze naší aplikace nebo webové stránky, pouze pokud jsou splněny nezbytné podmínky:[49]

[49] MEKYŇOVÁ, J. *Osobní údaje?* Profil. 2016, 22, s. 12-14. ISSN 1335-4620

- a) Sám uživatel poskytl osobní údaje provozovateli aplikace nebo webu,
- b) Na základě splnění smlouvy, může být v zájmu poskytnutí určité služby nebo souhlasu zpracování osobních údajů,
- c) Automatizovaně zpracované osobní údaje, může jít o kliknutí na tlačítko "zaregistrovat se."

5.2 Bezpečnostní a technická opatření ve společnosti Alza za účelem GDPR

V rámci nařízení GDPR mluvíme o ochraně osobních údajů. Jednou z nejdůležitějších věcí je proto bezpečnost a zálohování osobních údajů. Zálohování dat je podstatné pro zajištění nepřetržitého informačního systému firmy Alza. V malých a středních společnostech se využívají jednoduché způsoby zálohování dat. Ukládání dat bývá zejména dle potřeby, a to na disky, resp. NAS servery. V menších firmách bývá rovněž zálohování často řešeno nevhodným způsobem nebo zanedbáváno, hlavně z pohledu nařízení GDPR. Osobní údaje mají být uchovávány ve formě, která poskytuje identifikaci dotyčné osoby, dokud je to nezbytné pro potřebný zpracovávaný účel. Na jedné straně jde o jednoduché znění zákona založena na nařízení GDPR, na druhé straně jde o poměrně problematickou implementaci. V každém případě je třeba definovat způsob zálohování.

Za nevhodné považuje zálohování v nešifrované podobě z hlediska velkého rizika ztráty dat. Rovněž využívání veřejně dostupných a bezplatných cloudových úložišť v nešifrované podobě. Kvůli rozsahu zpracovávání množství informací ve společnosti včetně osobních údajů bývá řešení zálohování poměrně složité. Dosud stačilo prokázat zálohy a zabezpečené úložiště záloh v rámci bezpečnostního projektu. Data se zálohovala i na tzv. block - chains úložištích. Z pohledu bezpečnosti představují decentralizovaný model ukládání dat a z pohledu ochrany údajů výborné řešení. Z pohledu GDPR a ochrany osobních údajů jde však o nevhodné řešení, zvláště pokud jde o bezodkladný výmaz osobních údajů dotčené osoby. Problém je také ve virtualizovaných informačních systémech. Znamenají přínos ve pro informační systém firmy Alza obecně. Pokud však někdo zálohuje počítač, který virtualizuje společně s virtualizovanými počítači, ty obsahují osobní data, a tedy i záloha obsahuje osobní údaje. Žádost o vymazání osobních údajů

znamená vymazat data ve virtualizovaném počítači, tak i v podkladové záloze virtualizačního počítače.[50]

Vymazat údaje z takové zálohy je v podstatě nemožné. Firma Alza by se pak mohla dostat do konfliktu s nařízením GDPR a porušit práva a svobodu osob. Reálné bychom měli ukládat osobní údaje samostatně na jedno místo, databázi, disk, takovým způsobem, aby na osobní údaje mohl být aplikován plán záloh nezávislý na obvyklém zálohovacím postupu. Z toho vyplývá minimalizovat množství zpracovávaných osobních dat, data ukládat pseudonymizovaně, případně anonymizované. Používat co nejméně databází a souborů, aby v případě potřeby bylo možné dotčeným osobám vyhovět. V jednoduchém příkladu by se dalo uvést, že pokud organizace má osobní data v souborové databázi, je možné uvažovat nad tím, že bude na samostatném disku ukládána, tento disk bude samostatně zálohován na šifrovaném zástavního zařízení, například BitLocker šifrování.[51]

Zbylý systém mimo osobních údajů na jiném disku bude zálohovaný běžným způsobem. V případně komplexnějších systémů to bude výrazně složitější. Podle mého názoru jedním z nejlepších a nejjednodušších řešení je mít cloudové úložiště, které má smluvně ošetřeno převzetí záruk v rámci nařízení GDPR. Existuje několik specializovaných řešení pro organizaci firmy Alza. Toto řešení je založeno na šifrovaných kanálech, šifrovaných technologiích a nejnovějších technologiích autentifikace uživatele. Při přechodu na cloud je častou překážkou bezpečnost, protože firmy chtějí mít údaje pod kontrolou, avšak častokrát mají zabezpečení dat mnohem horší neţ jakýkoliv poskytovatel tohoto řešení. Základní myšlenkou je efektivita, tedy k údajům se dostaneme odkudkoliv a prakticky z čehokoliv, například z mobilního telefonu. Cloudové řešení vědí přispět k naplnění agendy GDPR.[52]

---

[50] MEKYŇOVÁ, J. *Osobní údaje?* Profil. 2016, 22, s. 12-14. ISSN 1335-4620.

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

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

GDPR nařizuje společnostem provádět potřebné organizační a technická opatření pro řízení rizik. Popisuje vzory opatření, ale neposkytuje podrobné informace o tom, proč jsou nezbytné nebo z čeho se skládají. V této souvislosti můžeme specifikovat kontroly zranitelnosti, penetrační testy a jejich způsob spolupráce.

Chyby zabezpečení

Mnoho společností zajišťuje ochranu sítí prostřednictvím antivirového softwaru a správy patchů. Jsou zásadní, ale zkoumá se konfigurace, aplikace a hardware třetích stran. To je to, co ověřuje zranitelnost. Skenování zranitelností může být interní nebo externí. Jde o proces automatizovaný, hledá a upozorňuje společnost na slabiny v systému. Vnitřní skeny zjišťují hrozby uvnitř firmy, například potenciál zneužívání uživatelských privilegií a externí skenování hledá, jakým způsobem mohou potencionální útočníci napadnout informační systém firmy. Je třeba zajistit pravidelné kontroly zranitelnosti, zabránit narušení dat zabezpečením nejběžnějších bezpečnostních nedostatků a rovněž se správně naučit interpretovat výsledky vyhledávání zranitelností. Mnohokrát se stává, že rizika jsou označována jako "nízká" nebo "střední" a odborníci označí zabezpečení organizace jako přiměřeně účinné. Všechny slabiny však mohou být zneužívány hackery pro protiprávní činnosti. Pro zabránění takové situace se provádějí pravidelné penetrační testy.[53]

Penetrační testy

Provádění penetračního testování vyžaduje určitou úroveň praktické práce a odbornosti. Tester dokáže vytvářet skripty, ladit nastavení nástrojů a měnit parametry útoku. Profesionální tester jménem organizace používá stejné praktiky jako hacker a hledá zranitelnosti v aplikacích nebo sítích společnosti. Testy dokáží zkontrolovat celou infrastrukturu a všechny aplikace a rozsah testování můžeme upravit na základě funkcí, oddělení nebo určitých aktiv.

---

[53] TECHBIT. 2017. *Nařízení GDPR z pohledu IT – úvod do problematiky nařízení GDPR.* [online]. [citováno 12-22- 2018].

Testování podle rozpočtových požadavků

V minulosti bylo penetrační testování chybně interpretovány jako nákladný způsob pro zjištění, kde je potřeba vynaložit více finančních prostředků. Organizace se bez potřebného testování vystavuje útokům a narušení dat, což představuje vyšší náklady než je cena penetračního testu. Využívají se rovněž způsoby, jak snížit náklady na penetrační testování. Není třeba vždy testovat všechny části sítě nebo aplikace. To se provádí pouze při uchovávání vysoce citlivých údajů, nebo pokud máme důvod myslet si, že jsme cílení hackery.[54]

Sítě ve velké většině hotelů, restaurací či nákupních center nejsou dostatečně zabezpečeny. Provozovatelé firem, škol, barů nebo restaurací by měli mít přehled o každém člověku připojeném do sítě a o tom, kde všude je k dispozici jejich heslo. Je to ale reálné téměř nemožné. Firma, která poskytuje firmě Alza internet, monitoruje pouze činnost ve své síti. Pokud jsme tedy například majitelem hotelu a dojde k útoku prostřednictvím free Wi-fi, tak hotel je zodpovědný za tuto nezabezpečenou Wi-fi a případné problémy nebo žaloby od poškozených. Proto je nezbytné znát osobu, která pošle přes Wi-fi nelegální obsah nebo poplašnou zprávu. Ve světě je zabezpečení sítě standardem a podle nového nařízení GDPR nutností. Chráněné musí být zejména jméno, příjmení, email, data narození i IP adresa. Na základě těchto údajů dokážeme přímo či nepřímo identifikovat osoby. Zabezpečení přenosu můžeme vyřešit dvěma způsoby.[55]

Prvním způsobem je důvěra k poskytovateli internetového připojení. Druhým a lepším způsobem je vytvořit vlastní VPN server v případě, že má společnost k dispozici veřejnou IP adresu a router. Případným negativem tohoto řešení může být rychlost. Je závislá na

[54] TECHBIT. 2017. *Nařízení GDPR z pohledu IT – úvod do problematiky nařízení GDPR.* [online]. [citováno 12-22- 2018].

[55] TECHBIT. 2017. *Nařízení GDPR z pohledu IT – úvod do problematiky nařízení GDPR.* [online]. [citováno 12-22- 2018].

propustnosti serveru a počtem uživatelů připojených v daném okamžiku na server.[56] Ve firemní praxi je při tvorbě bezpečnostních opatření nutné zaměřit se na eliminaci jednotlivých bezpečnostních rizik, a na základě tohoto pak zpracovat návrh síťového řešení, stejně jako pravidel. Bezdrátové technologie jsou v současnosti poměrně dostupné, ale jejich jednotlivé řešení je individuální. Firemní wireless síť je možné vystavit z celkem dvaceti přístupových bodů, a to v částce například do třiceti tisíc korun, ale také v částce pohybující se ve statisících korun. Levnější řešení zahrnuje nasazení přístupových bodů, které jsou připojeny d stávajících switchů LAN infrastruktury. V případě, že existují stávající volné porty, tak je nutné, každé AP nastavit samostatně, konkrétně:[57]

- způsob a řešení autentizace
- konfigurace kanálu, na kterém je AP vysíláno a vyzařovacího výkonu

S ohledem na to, že AP spolu nijak nekomunikují, tak celkové nastavení spoléhá na zručnost a schopnosti administrátora a dochází ke zvýšenému riziku, že při větším počtu AP vzniká riziko, že bude docházet k větší interferenci. K tomuto je nutné aplikovat profesionální měřící metody, protože pak následně v tomto spočívá problém nerovnoměrného pokrytí. Decentralizace konfigurace je pro administrátora problematická z hlediska repetitivně práce, která souvisí s chybovostí celého systému a tím také zvýšeného rizika.

Při uvádění rizik, se wireless sítě stávají velmi často terčem útoků, tzv. typu „man in the middle." Princip spočívá v tom, že útočník podstrčí do firemní sítě své vlastní pirátské AP a nastaví jej takovým způsobem, aby působilo jako ostatní systém, kdy následně pro tohoto útočníka již je snadné získat od napadaného potřebné informace, které jsou posílány

---

[56] CIO. *CIO - analýzy a statistické údaje* [online]. 2019 [cit. 2019-01-17]. Dostupné z: http://businessworld.cz/analyzy?offset=80

[57] CIO. *CIO - analýzy a statistické údaje* [online]. 2019 [cit. 2019-01-17]. Dostupné z: http://businessworld.cz/analyzy?offset=80

z konkrétního PC mimo wireless síť, konkrétně jsou zasílány informace týkající se e-mailové komunikace, přístupových údajů a hesel, což je pro firmu velmi riziková situace. Pirátské AP je možné identifikovat v síti bez centrální správy a monitoringu jen velmi obtížně, až náhodně. V případech, kdy na wireless síť někdo útočí ad hoc připojením přímo přes autentizovaného klienta, tak se odhalují jednotlivé problémy ještě hůře.[58]

Mezi další bezpečnostní rizika patří levnější řešení s použitím méně výkonných AP, které jsou určeny pro domácí užití. Optimální připojení, tímto levnějším způsobem, představuje okolo 15 uživatelů, nad rámec této hodnoty je připojení rizikovější. V okamžiku přetížení AP, opětovně dochází k poklesu kvality a stability služeb a v této souvislosti lze doporučit dvě možné varianty řešení, a to:[59]

- úspora vstupních nákladů pořízením levné bezdrátové sítě, s absencí hromadného managementu IT bezpečnosti, a také s rizikem, že data nejsou zcela zabezpečena
- druhým případem je řešení založené na wireless switching

Zaměřme se na druhé uvedené řešení, kdy wireless switch v sobě zahrnuje dvě zařízení, kdy jedním jen L2 + switch s PoE Porty, případně 10 GbE konektivitou pro uplink například, druhá funkce je pak wireless kontroler. Při zapojení speciálních řiditelných AP do wireless switch, nebo minimálně do stejné topologie, jsou AP kontrolérem automaticky rozpoznána nebo také napájena, takže je dostačující pouze ethernetový kabel. Všechna AP se pak následně konfigurují dávkovým nahráním profilu s nastavením, což je jednak rychlé, a také to minimalizuje možnost rizika a chybného nastavení v rámci zabezpečení wireless sítě.

---

[58] CIO. *CIO - analýzy a statistické údaje* [online]. 2019 [cit. 2019-01-17]. Dostupné z: http://businessworld.cz/analyzy?offset=80

[59] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-18]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

Jednotlivé profily mohou být různé, kdy wireless kontroler po zapojení celou síť proskenuje a automaticky se u všech AP nastaví vyzařovací výkon a kanál, na kterém se AP vysílají. Skenovat síť je možné i periodicky, takovým způsobem, aby switch reagoval úpravou nastavení na případné změny v prostředí, takže funguje vždy spolehlivě. Konkrétně při výpadku AP z důvodu krádeže a dalších negativních jevů, mají tzv. samoléčící schopnost.

Switch zahrnuje metody, které umožňují identifikovat a lokalizovat, a také blacklistovat pirátské AP nebo AP ze sousedních sítí, které bývá jednou ze součástí WIDS.[60] Mezi další funkce, v rámci zabezpečení bezdrátové sítě, patří identifikace a zamítnutí útoku přes bezdrátovou síť na jednotlivé klienty. Autorizaci do sítě je možné poměrně snadno řešit, a to formou databáze uživatelů, která je uložena přímo v kontroléru, nebo formou externího RADIUS serveru, na který může být například navázáno konkrétní zpoplatnění služeb, apod. Za pomoci WAC je možné, aby autentizace proběhla také přes webový formulář, součástí zabezpečení je účinné šifrování provozu pro bezpečnost dat.

Výše uvedené řešení je jednou z možností a řešení toho, jak wireless síť je velmi sofistikovaným systémem. Její bezpečnost je samozřejmě odvislá od toho, jak jsou nastaveny individuální korporátní standardy ve firmě. V posledních týdnech, z pohledu bezpečnosti bezdrátových sítí, byla představena nová platforma Connected Mobile Experiences, jež nabízí nové služby, které jsou zaměřeny na vyhodnocení polohy uživatele WiFi sítě, na analýzu získaných dat a vývoj souvisejících mobilních aplikací. Tuto platformu vyvíjí společnosti Cisco, s tím, že dle jejich analýz WiFi sítě mohou částečným způsobem nahradit v oblasti datových přenosů tradiční sítě mobilních operátorů, konkrétně na veřejně přístupných místech jako jsou hotely, obchody, apod., kde je potenciál této platformy velmi zajímavý.[61]

---

[60] Z anglické zkratky označení Wireless Instrusion Detection System.

[61] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-18]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

Potenciál nových řešení překonává dosavadní limity bezdrátových sítí a za pomoci zajistit jejich provozovatelům nový zdroj příjmu. Nové systémy, založené na těchto moderních aplikacích poskytují analytická data o chování uživatelů, díky nimž je možné optimalizovat jednotlivé procesy a související činnosti firem. Podle studií, které byly vypracovány, se předpokládá, že v roce 2016 bude produkováno až 130 exabajtů dat, a více než pětina těchto dat, okolo 22 % bude posílána přes WiFi sítě, které se budou podílet na snižování datové zátěže mobilních sítí. Proto lze konstatovat, že investice a technologický rozvoj v této oblasti představují určitý potenciál dalšího rozvoje.[62]

Limitujícím faktorem je nutnost opakovaného přihlašování, což je také určitá bezpečnostní hrozba, toto souvisí také se zadáváním vstupního hesla nebo výběru vhodné sítě. Všechna tato omezení odstraňuje například nový standard Hotspot 2.0., kdy rozvoj tohoto standardu byl podporován specializovanými IT firmami, v rámci WiFi Alliance. Kdy WiFi sítě budované podle tohoto standardu mimo jiné zajišťují:

- **automatické připojení k WiFi síti**, kdy mobilní zařízení samostatně vyhledá a automaticky zvolí správnou a vhodnou síť, která je v daném místě dostupná
- **přístup bez nutnosti zadávání hesla**, zahrnuje identifikaci uživatele v síti, je založena na příklad na informacích o zařízení, nebude tedy nutné zadávat žádná další hesla
- **vysoký stupeň bezpečnosti**, představuje všechny přenosy dat v bezdrátové síti, které jsou automaticky šifrovány a uživatelům nehrozí jejich zachycení jinou osobou

Mezi konkrétní příklady aplikace nových WiFi technologií můžeme přiřadit jejich využití například ve formě platformy Location Based Services, která je využívána v letišti

[62] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-18]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

v Kodani. Zajišťuje konkrétně pohyb lidí a optimalizuje vyřízení personálu letiště nebo ještě zvyšuje bezpečnost. Přínosem je také, mimo připojení k internetu, vysoká míra zabezpečení a doplňující služby a servis pro zákazníky, v souvislosti s internetovými službami. Příkladem aplikace technologie WiFi jsou prostory Masarykova onkologického ústavu v Brně v rámci ČR. V tomto institutu byl nasazený systém, který za využití technologie RFID čipů a bezdrátové sítě WiFi umožňuje ujistit aktuální polohu vybraných zdravotnických přístrojů a zařízení, ale také hospitalizovaných pacientů, kteří jsou pro tento případ vybaveni speciálními náramky. Tyto osoby si tak mohou, v případě problémů, přivolat pomoc zdravotnického personálu, který pacienta lokalizuje v případech, kdy se nachází mimo prostory nemocnice, resp. mimo zdravotní lůžko.

Konkrétní útočník pak může využít připojení do vzdálené bezdrátové sítě za pomoci například směrové antény, a protože se jednotlivé ochranné a zabezpečovací systémy vyvíjely postupně, je vhodné, zejména u starších zařízení, použít zabezpečení na vyšší síťové vrstvě, ve formě virtuální privátní sítě, apod.

Z praktického hlediska je tak bezpečnost bezdrátových sítí členěna do dvou hlavních skupin, a to:[63]

šifrování, zahrnující zabezpečení přenášených dat před odposlechem

autorizace, řízení přístupu oprávněných uživatelů

Jednotlivé formy zabezpečení bezdrátových sítí je možné v souhrnu uvést následovně, s tím, že jednotlivě budou některé z nich specifikovány samostatně. Nejprve se zaměříme na zablokování vysílání SSID, které obecně porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě formou jejího zdánlivého skrytí. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID. Při

[63] CIO. *CIO - analýzy a statistické údaje* [online]. 2019 [cit. 2019-01-18]. Dostupné z: http://businessworld.cz/analyzy?offset=80

připojování klienta k přípojnému bodu je SSID přenášen v otevřené formě, je možné jej tak snadno zachytit. Zejména pak při zachytávání SSID při asociaci klienta s přípojným bodem se užívá k aplikaci, kdy útočník do bezdrátové sítě vysílá rámce, které přinutí klienty, aby se opětovně asociovaly.

Kontrola jednotlivých MAC adres, spočívá v tom, že přípojný bod bezdrátové sítě má k dispozici seznam MAC adres klientů, kterým je dovoleno se připojit. Úročník se tak může vydávat za stanici, která je již do bezdrátové sítě připojena, a to za pomoci nastavení totožné MAC adresy, v případě, že je na AP tato funkce aktivní. Protokol 802.1X je užíván v rámci přístupového bodu k autentizaci. Pro konkrétní ověření je používán na straně klienta program, označovaný jako suplikant, kterému přístupový bod zprostředkovává komunikaci se třetí stranou, která konkrétní ověření provede, protokol 802.1X také odstraňuje nedostatky, které souvisejí se zabezpečením pomocí WEP klíčů.

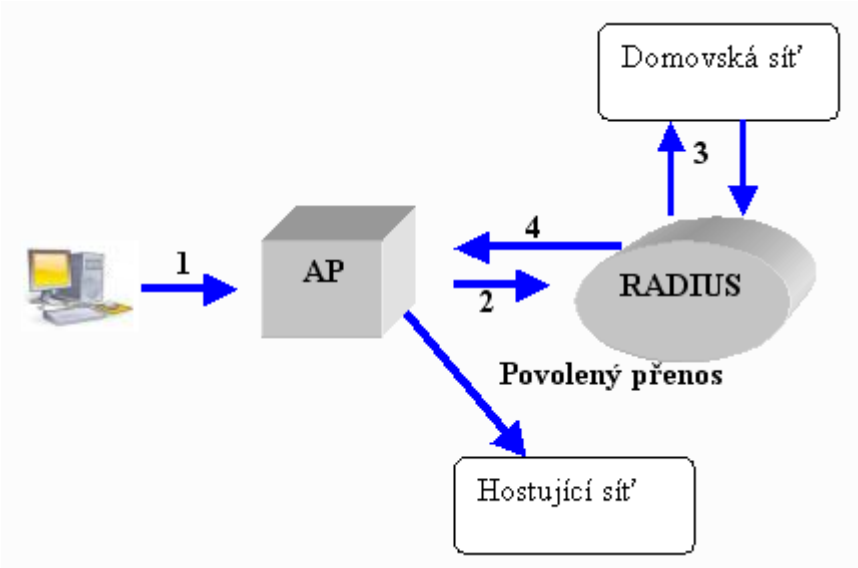
Protokol IEEE 802.1X je informačním protokolem, který taktéž umožňuje jednoduché a efektivní zabezpečení fyzického přístupu do počítačové sítě, v tomto případě v rámci bezdrátových sítí. V případě, že je do síťového portu, například do switche, připojeno nové zařízení, je port zablokován, kdy neumožňuje ani přenos dat, a to do okamžiku, dokud nejsou poskytnuté autentizační údaje, nejčastěji uživatelské jméno a heslo. 802.1X je dostupné na switchi, obsahující tzv. management a umožňující proto konfiguraci autentizaci připojených zařízení, které jsou vybaveny softwarem umožňujícím autentizaci.[64]

Informační protokol zabraňuje neautorizovaným osobám v přístupu síťové komunikaci, aniž by bylo nezbytné všechna připojená zařízení fyzicky autorizovat. Jeho uplatnění v bezdrátových sítích, kde fyzické zabezpečení není možné, volné připojení by mohlo být lehce zneužitelné. Princip činnosti a schéma protokolu 802.1X je uvedeno na obrázku níže.

---

[64] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-19]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

Obrázek 1: Informační protokol 802.1X



Zdroj: http://www.ieee802.org/1/pages/802.1x.html

V případě, že se uživatel připojí na síťový port, je blokována kompletní komunikace mimo EAP protokolu, který zohledňuje autentizaci, což v praxi probíhá následně:[65]

klient musí mít aktivní speciální autorizační program, který vyšle přes EAP protokol žádost o autentizaci na AP server

switch, případně jednotlivá AP přepošle žádost RADIUS serveru

proběhne autorizace uživatele, kdy se může jednat o lokálního uživatele, kdy je autorizace prováděna přímo na RADIUS serveru, pokud není uživatel lokální, tak probíhá autorizace přes strukturu RADIUS serverů až k uživatelově domovské síti

výsledek autentizace obdrží switch nebo konkrétní AP, jež buď další síťový provoz dále povolí, nebo jej zakáže

---

[65] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-19]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

Právě v souvislosti na některé nedostatky protokolu WEP, jsou prosazovány některými výrobci 802.1X pro bezdrátové přístupové body. Autentizaci většinou provádí třetí strana, jak už bylo zmíněno například RADIUS server, což s sebou přináší i specifická pozitiva a negativa v rámci bezpečnosti. Mezi hlavní pozitiva náleží možnost blokování neautorizovaných osob v síti, nebo osob, které mají z určitých důvodů přístup k síti zakázaný, z důvodu virové hrozby, spamu, atd.

Pokud budeme bezpečnostní opatření kombinovat s dalšími technologickými řešeními, tak je možné včlenit nežádoucí uživatele do tzv. VLAN, kde uživatel může využívat minimum síťových zdrojů, stále má také přístup k nástrojům na případné řešení bezpečnostních hrozeb. Mezi negativa patří skutečnost, že PC, které je připojena na neautorizovaný port nemá k síti přístup. Toto je značná nevýhoda pro vzdálenou správu PC, i když je možné nastavit opatření bezpečnosti v PC tak, aby bylo možné je eliminovat. Z hlediska implementace, jednotlivé typy operačních systémů jako je Windows XP, nebo Windows Vista, Windows 8, podporují protokol 802.1X pro všechna síťová připojení. Pro Linux byl vytvořený projekt Open 1X open source client, který je aplikovatelný pro bezdrátové připojení IEEE 802.11. Stejně tak Mac OS X umožňuje podporu pro 802.1X od verze 10.3.[66]

WEP[67] statistické klíče představují šifrování komunikace na základě symetrických šifer, které jsou ručně nastaveny na obou stranách bezdrátového spojení. Na základě nedostatků v protokolu lze zachycením specifických rámců a jejich následnou analýzou klíč vytvořit Pro vygenerování jednotlivých klíčů existují specializované programy. WPA[68] klíč se užívá kvůli zpětné kompatibilitě, jsou dynamicky bezpečným způsobem měněny. K tomuto je určeny doprovodný program, který má autorizační charakter, proto je WPA klíč

---

[66] K tomuto například: *Bezpečnost WiFI sítí* [online]. 2019 [cit. 2019-01-19]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

[67] Z anglického originálu Wired Equivalent Privacy

[68] Z anglického originálu Wi-FI Protected Access

aplikovatelný i na starších zařízeních. Autentizace přístupu do WPA sítě je realizována ve formě PSK[69], kdy je oběma stranami používána dostatečně dlouhá heslová fáze, nebo RADIUS serveru, kde je ověřování přihlašovacím jménem a heslem. Novější verze klíče WPA2 poskytuje kvalitnější šifrování, a to šifrou AES, jež vyžaduje větší výkon, není možné jej uplatnit na starších zařízeních. Zhodnocení WPA klíče je uvedeno na obrázku níže.

Obrázek 2: Srovnání WEP a WPA klíčů

	WEP	WPA	802.11i (WPA2)
autentizace	otevřená	EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) nebo PEAP (Protected EAP)	EAP-TLS nebo PEAP
šifrování	statický WEP	TKIP/CKIP (Cisco Key Integrity Protocol)	AES
útok:		**odolnost**	
na integritu, důvěrnost dat	dobrá	lepší	nejlepší
falešná autentizace	nic moc	nejlepší	nejlepší
na slabý klíč	nic moc	nejlepší	nejlepší
falšované pakety	minimální	nejlepší	nejlepší
falešný přístupový bod	minimální	lepší	lepší
úroveň šifrování	pro domácí síť (40- nebo 104bitový klíč; 24bitový vektor IV)	pro podnikovou síť (128bitový klíč; 48bitový vektor IV)	pro podniky i vládu (128+bitový klíč; 48bitový vektor IV)

Zdroj: http://www.odbornecasopisy.cz/index.php?id_document=32563

Dalším rizikem při bezpečnosti bezdrátových sítí je potenciálně možný únik dat, která nejsou dostatečným způsobem chráněna. Příkladným bezpečnostním problémem je případ společnosti Google, která při tvorbě svých internetových map nechala katalogizovat bezdrátové sítě, s cílem jejich účelu pro určení polohy. Při zachycování potřených dat byla zachycena i data z bezdrátových sítí. Jejich rozsah a obsah byl různý, ovšem kritická byla například data, která se vztahují k internetovému bankovnictví. I když v této souvislosti

[69] Z anglického organizační Pre-Shared Key

jsou data elektronického bankovnictví automaticky šifrována, ale i tak je uvedený případ obecnou ukázkou rizik bezdrátových sítí.

Nařízení GDPR je rozsáhlou reformou a přináší různé konsekvence. Problémem může být část zabývající se vymazáním osobních údajů. Do rozporu s kompatibilitou nařízení se mohou dostat strojové učení nebo neuronové sítě. Například analýzou osobních údajů milionů návštěvníků sociální sítě vytvoří neuronová síť znalostní model. Ten je statistickým otiskem dat každého subjektu a ve vnitřní struktuře vše spolu souvisí. Proto je nemožné, abychom vymazali údaje popisující osobu X, protože by se smazal celý model. Stejným případem je například databázová struktura blockchain. Bývá spojován s Bitcoiny a jinými kryptoměnami. Je velmi odolný vůči nelegálním změnám. Je charakteristický tím, že jedna hodnota matematicky navazuje na následující hodnotu jako řetěz. Pokud by někdo změnil záznam blockchainu, celý by se zhroutil, protože návaznost záznamů by přestala fungovat. Bylo by nutné začít znovu v bodě nelegálního zásahu, protože záznamy by již nepředstavovaly správné kontrolní součty. Znamená to, že daná technologie pravděpodobně nemůže být s napadením validní. Záznam nemůžeme zpětně smazat nebo upravit.

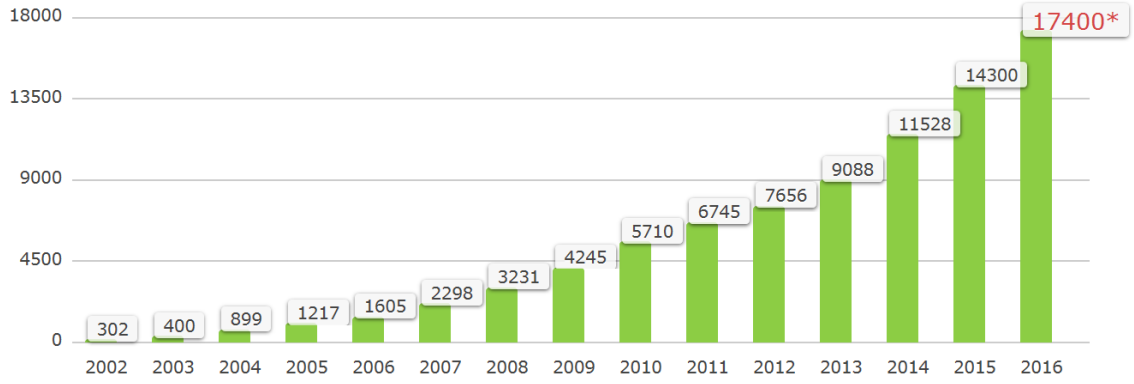
5.3 Současná strategická pozice společnosti Alza

Společnost Alza se zabývá prodejem spotřebního zboží, zejména elektroniky pro zákazníky skrze silné webové platformy a internetového marketingu. Nová obchodní strategie společnosti Alza byla přijata v roce 2015 a je pro všechny prodejny společnosti Alza společná zahrnuje nyní provozní dobu 24/7, tedy během celého týdne. Toto umožňuje zákazníkům využít možnosti takto široké otevírací doby, která je v pracovních dnech od 9 do 21 hod. Návštěvnost na uvedených prodejnách je nejvyšší zejména v odpoledních hodinách, podle interních informací společnosti Alza je nejvyšší návštěvnost v časovém rozmezí mezi 15 – 18 hod, v ostatních časových úsecích je pak návštěvnost nižší. Co se týká současného stavu, je možné konstatovat jednotlivé části webových stránek i sociální

sítě, stejně jako všechny pobočky společnosti Alza mají jednotný firemní design, který je dán interními předpisy a řídí se jimi každá nově vzniklá pobočka společnosti. Toto posiluje vnímání značky společnosti Alza u zákazníků a nelze předpokládat, že by se grafický a firemní design společnosti Alza v dohledné době nějakým způsobem zásadně změnil.[70]

Podle dostupných informací společnosti Alza jsou na kamenných pobočkách podle jejich velikosti zaměstnanci v počtu několika osob až desítek osob. Celkově má společnost Alza okolo 500 zaměstnanců a průměrný obrat byl v posledních dvou letech v rozsahu okolo 11 miliard korun. Vývoj celkového obratu společnosti ke konci listopadu 2017 je uveden na grafu níže, nicméně není zde započítáno nejsilnější období roku, a to jsou Vánoce.

Obrázek 3: Vývoj celkového obratu společnosti



Zdroj: www.alza.cz

Na pobočkách společnosti jsou zaměstnáni zaměstnanci v počtu od dvou do 10 zaměstnanců, případně podle období, jako jsou například Vánoce, tak v tomto období jsou

[70] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

najímány další pracovní síly, které zde pracují ve formě brigády většinou na DPP. Zaměstnanci pobočky z hlediska zákaznického servisu pro zákazníky poskytují jak informace pro zákazníky ohledně služeb nebo zboží, ale také vyřizují objednávky, které si zákazníci objednají přímo na danou prodejnu. V tomto ohledu jsou prodejny jednotně vybaveny prodejním automatem, kde po zadání finanční částky neb kódu je pak možné na základě kuponu si od zaměstnanců prodejny vyzvednout své zboží. Podle našeho názoru by bylo toto možné změnit přímo na vyzvednutí zboží u přepážky v případě, že jsou v prodejně k dispozici zaměstnanci.[71]

Co se týká architektonického řešení každé prodejny, jejich design je totožný, jak z hlediska interního řešení prodejny, tak z hlediska externího vzhledu prodejny. Nabídka služeb společnosti Alza je v každé prodejně prezentována zaměstnanci, jejich chování je celkově příjemné a je možné konstatovat, že jsou znalí dané problematiky. Produkty na pobočce jsou také prezentovány, ale jejich rozsah je spíše dekorační, což by se mohlo změnit a mohly by se například střídat prezentace nových výrobků každý měsíc pro zákazníky na pobočce společnosti Alza.

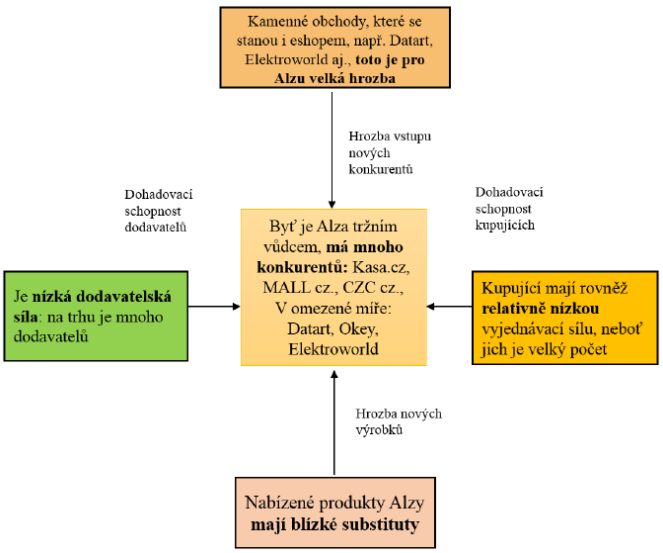
Z hlediska dalšího rozvoje jednotlivých poboček společnosti Alza je možné uvést následující zjištění, které můžeme vyjádřit z hlediska konkurenčního postavení společnosti Alza na trhu Porterovým pětifaktorovým modelem v grafickém řešení níže. Toto grafické řešení poukazuje na hlavní faktory, které ovlivňují konkurenční pozici společnosti Alza i jejich kamenných prodejen a budou tak do budoucna představovat součást obchodní strategie společnosti Alza.[72]

---

[71] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

[72] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

Obrázek 4: Porterův model Alza



Zdroj: www.alza.cz

Z hlediska dalšího vývoje společnosti Alza je nutné zhodnotit zejména vývoj celé společnosti Alza na českém trhu. Jak už bylo uvedeno, tak společnost má průměrný obrat okolo 11 miliard Kč, pravidelně vyřizuje ročně okolo tří milionů objednávek a jak už bylo uvedeno má v současné době více jak 500 zaměstnanců. Na trhu má společnost pozici největšího internetového prodejce s počítači a elektronikou. Nabídka jejich produktů je velmi široká, silná společnost podporuje aktivně všechny své pobočky, z hlediska podnikatelské činnosti je kladen důraz na inovace, jak v rámci společnosti, tak u jednotlivých poboček společnosti. Obchodní strategie Alzy je celkově poměrně agresivní, je kreativní a pravidelně přichází z novými přístupy z hlediska obchodní nebo marketingové strategie, jako je Alza Kredit a další. Společnost Alza je také velmi aktivní v komunikaci, a to hlavně prostřednictvím svého maskota a v neposlední řadě má společnost stabilní distribuční síť a na některých svých pobočkách pro své zákazníky

prezentuje Alza showroomy, kde jsou aktuálně prezentovány například nejnověji nabízené elektromobily.[73]

Z hlediska budoucího vývoje je možné otevřít další showroomy v některých velkých městech pro zákazníky společnosti. Problémem společnosti Alza je to, že její obchodní a podnikatelská činnost má nízkou přidanou hodnotu, což je dáno tím, že se společnost Alza orientuje na prodej výrobků. I proto by se měla společnost Alza zaměřovat mimo prodeje produktů také na poskytování služeb k produktu, což by mohl zvýšit marže společnosti, a to také u kamenných prodejen společnosti Alza. Jako určitá slabina se jeví, že masivní komunikace je sice silnou stránkou společnosti, ale komunikace není cílená, oslovuje hlavně široký okruh zákazníků, a proto efektivnost některých reklamních sdělení není již natolik efektivní. Je nutné také uvést, že společnost Alza je primárně elektronickým obchodem, i když má již společnost dostatek kamenných prodejen, je nutné v rámci budoucího vývoje zajistit vhodné rozložení jednotlivých činností mezi centrálu společnosti a jednotlivé kamenné prodejny společnosti Alza.[74]

Z hlediska příležitostí pro společnost Alza je možné uvést poměrně stálý růst objemů internetových prodejů, což je hlavní devíza společnosti Alza. Mimo toho také díky kamenným prodejnám si společnost buduje u zákazníků povědomí a posiluje se tak firemní identita společnosti na trhu. Vzhledem k tomu, jak je společnost Alza vnímána veřejností, je možné konstatovat, že je zákazníky vnímána jako důvěryhodná a na základě tohoto zde zákazníci s větší důvěrou nakupují zboží.[75]

---

[73] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

[74] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

[75] *Alza* [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

1. **Jaké je povědomí v organizaci společnosti Alza o GDPR? Jaký je stav přípravných prací? Probíhá nebo připravuje se proškolení zaměstnanců? Příprava aktualizace dokumentů a další přípravné práce. Využití externích dodavatelů (IT firem) pro zabezpečení ochrany osobních údajů.**

Z hlediska přípravy společnosti na účinnost GDPR si společnost Alza uvědomuje význam ochrany osobních údajů i možné sankce za nedodržení požadovaných zákonných požadavků. Na základě tohoto tedy připravuje poslední rok přípravné práce, které se týkají procesních i technických řešení směrem k naplnění požadavků vyplývajících z právní úpravy.

Společnost Alza za tímto účelem sestavila projektový tým, který je základním předpokladem pro úspěšnou implementaci GDPR do praxe organizace společnosti Alza. Společnost sestavila efektivní a vyvážený pracovní tým, kdy do přípravy a zavádění interních pravidel ochrany osobních údajů jsou zapojeni jak zaměstnanci, IT specialisté a technici, ale také management jednotlivých oddělení společnosti Alza. Neméně důležití jsou jednotliví zaměstnanci společnosti Alza, stejně jako právníci společnosti Alza, a také zaměstnanci personálního oddělení. V souvislosti se zavedením a prosazováním GDPR v organizaci společnosti Alza byl přijat do pracovního poměru zaměstnanec na **pracovní pozici Pověřence pro ochranu osobních údajů**, který má právní vzdělávání a byl na tuto pozici proškolen specializovaným odborným externím školícím subjektem.[76]

V souvislosti s tímto projektový tým stanovil konkrétní cíle a úkoly, které bude nutné do května roku 2018 realizovat. Celkově je **cílem činnosti projektového týmu implementovat GDPR do praxe společnosti Alza.** Jedná se tak o naplnění požadavků nařízení 2016/679. V návaznosti na toto jsou stanoveny dílčí číle, které konkrétně stanovují nezbytné aktivity, které budou harmonizovat současnou ochranu osobních údajů zákazníků

[76] Interní dokumenty společnosti Alza ke GDPR a její implementaci, v tištěné podobě, upraveno.

s novými doplňujícími požadavky GDPR. Pro naplnění jednotlivých projektových požadavků a stanovených cílů je nutné realizovat následující činnosti:[77]

- Zhodnocení analýzy dopadů GDPR – tato analýza již byla ze strany společnosti Alza provedena,
- Provést jednotlivé kroky k implementaci požadavků GDPR – tento krok probíhá a momentálně probíhají technické úpravy, a také proškolování zaměstnanců společnosti Alza,
- Jmenování pověřence pro ochranu osobních údajů – tento krok již byl realizován,
- Zpracování metodik pro nakládání s osobními údaji zaměstnanců i zákazníků společnosti v rámci činnosti společnosti Alza – tento krok probíhá v rámci činnosti projektového týmu, očekává se dokončení v prvním čtvrtletí 2018,
- Úprava a případné zavedení procesů a postupů zpracování osobních údajů - tento krok realizují vedoucí pracovníci oddělení společnosti Alza a IT pracovníci společnosti, očekávané dokončení v prvním čtvrtletí 2018,
- Nastavení pravidel vedení záznamů o zpracování osobních údajů – tento krok realizuje IT oddělení a IT zaměstnanci společnosti Alza,
- Zpracování a odsouhlasení dopadů jednotlivých činností na ochranu osobních údajů ve společnosti Alza – toto již bylo realizováno.

K realizaci projektových etap a jednotlivých cílů v rámci společnosti Alza budou využity ve většině případů interní zdroje, i s ohledem na ochranu všech interních informací, ale také proto, že společnost Alza má dostatečné odborné kapacity k naplnění požadavků nařízení. Společnost Alza využije externě některé školící aktivity pro management, a také využije externě některé vysoce odborné právní poradenství.[78]

[77] Interní dokumenty společnosti Alza ke GDPR a její implementaci, v tištěné podobě, upraveno.

[78] Interní dokumenty společnosti Alza ke GDPR a její implementaci, v tištěné podobě, upraveno.

2. **Jak se promítne implementace GDPR do nákladů a do vývoje počtu a struktury pracovních míst?**

Na vývoj počtu zaměstnanců nebude mít požadavek nařízení GDPR žádný vliv. Zůstane zachován stávající počet zaměstnanců, spíše je možné očekávat jejich nárůst s ohledem na zvyšující se podnikatelské činnosti společnosti Alza.

Rozpočet projektu implementace GDPR do praxe společnosti Alza zahrnuje dvě samostatné položky uvedené níže. Rozpočet na přípravnou fázi a implementaci GDPR, a to na základě vstupných a rozdílových analýz, na základě zhodnocení změn a nastavení procesů, stejně jako školení, metodiky, konzultací projektového týmu a spolupráce jednotlivých zainteresovaných subjektů. Jednotlivé výstupy z analýz je moné prakticky využít při zavádění konkrétních pravidel GDPR a v návaznosti na to při certifikaci ISO normy 27001. Na základě tohoto se tak sestavuje:

- Přípravný rozpočet společnosti Alza,
- Implementační rozpočet společnosti Alza.

Celkové finanční náklady a finanční požadavky rozpočtu na implementaci GDPR nejsou veřejně dostupné a jsou součástí obchodného tajemství. Harmonogram má nastaveny termíny plnění výše stanovených projektových úkolů a jednotlivých cílů i proces kompletní realizace, ale tento harmonogram také není veřejně k dispozici.

3. **Celkové hodnocení připravenosti společnosti Alza na zvládnutí uvedeného nařízení EU.**

Současný stav implementace nařízení je možné hodnotit pozitivně. Jak bylo výše uvedeno, společnost Alza se na požadavky vyplývající z nařízení připravuje již poslední rok, a to sestavením projektového týmu a vytvořením předpokladů pro realizaci jednotlivých projektových úkolů a cílů projektového týmu, které je nutné do budoucna realizovat. Nicméně procesy i činnosti jsou náročné a rozsáhlé a je možné očekávat, že dokončení celého procesu implementace bude i tak dokončeno až v období dubna 2018.

4. Jak hodnotit dopady GDPR? Shrnutí.

V roce 2016 Evropský parlament a Rada (EU) přijaly tzv. Balík reforem ochrany osobních údajů. Reforma obsahuje Nařízení 2016/679 o ochraně fyzických osob při zpracování osobních údajů a o volném pohybu těchto údajů (GDPR) a Směrnici 2016/680 / ES o ochraně osobních údajů pro policii a orgány činné v trestním řízení. Důležitou poznámkou je, že nařízení je přímo vykonatelné na celém území EU a má přednost před lokální legislativou. Reforma byla odstartována Evropskou komisí už na počátku roku 2012. Celkově čtyři tisíce změn provedlo z tohoto nařízení nejvíce komentovaný právní úpravu v historii EU. Ve srovnání s předchozí Směrnicí 95/46 / ES narostl počet článků nařízení z původně navrhovaných 33 na 91.[79]

Cílem nařízení především je:[80]

- sjednocení právní úpravy ochrany osobních údajů v členských státech Evropské unie;
- zvýšení práv dotčených osob;
- zjednodušení pravidel zpracování osobních údajů.

Nařízení vstoupilo v platnost 24. května 2016 a v jednotlivých členských státech se začne aplikovat od 25. května 2018. Jde o obecnou právní úpravu, tedy podléhají jí všechny komerční i nekomerční činnosti organizací, při kterých dochází ke zpracování osobních údajů, kromě aktivit taxativně vyjmenovaných. Právní úprava se dotýká nejen organizací se sídlem v členských státech EU, ale všech organizací, které monitorují aktivity nebo zpracovávají osobní údaje rezidentů EU.

Právní úprava se v praxi dotýká zejména dvou skupin dotčených osob - **zaměstnanců a zákazníků v maloobchodě.** Specificky se úprava dotýká oblastí jako například:[81]

---

[79] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[80] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

- Big Data a Business Intelligence;
- Biometrické, kamerové a přístupové systémy;
- Lokalizační služby;
- Marketing, spotřebitelské soutěže, věrnostní programy, apod.;
- Profilování a automatizované rozhodování;
- Další individualizované oblasti.

GDPR s sebou přináší nové principy ochrany osobních údajů. Mezi ty nejvýznamnější je možné uvést tyto:[82]

- Rozsah regulovaných dat - rozšíření zvláštní kategorie například o genetické údaje;
- Jeden kontinent, jedna úprava - nahrazení národních legislativ;
- Jednotné místo (one-stop-shop) - jeden kontrolní orgán;
- Stejná pravidla pro všechny společnosti - bez ohledu na to, kde jsou usazeny;
- Úprava souhlasu nezletilých - věková hranice 13 až 16 let (stanoví členský stát);
- Technologická neutralita - pokrok inovací;
- Pseudo anonymizace - reverzibilní anonymizace dat (oddělení identifikačních údajů);
- Oznamovací povinnost - povinnost ohlásit regulátorovi porušení ochrany osobních údajů;
- Privacy by design - požadavky ochrany osobních údajů už během vývoje resp. na začátku projektu.

Česká republika patří v regulaci ochrany osobních údajů k přísnějším z členských zemí EU, nové nařízení obsahuje změny, které současný právní stav zpřísňují, respektive zdůrazňují některé již v současnosti platná práva dotčených osob.[83]

---

[81] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[82] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

Právo na zapomnění

Dotyčná osoba má právo dosáhnout u provozovatele bez zbytečného odkladu vymazání svých osobních údajů, pokud je splněn některý z těchto důvodů: osobní údaje již nejsou potřebné pro účely, pro které se získávaly nebo dotčená osoba odvolá souhlas a neexistuje jiný právní základ.

Právo na přenos

Subjekt údajů má právo získat osobní údaje, které se jí týkají, a které poskytla provozovateli, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo přenést tyto údaje dalšímu provozovateli, pokud zpracovávání zakládá na souhlasu nebo na smlouvě, a pokud se zpracování provádí automatizovaně.

Profilování

Dotyčná osoba má právo na to, aby se na ni nevztahovalo rozhodnutí, které je založeno výlučně na automatizovaném zpracování, jako je například automatické vypočítání výše slevy na základě profilu zákazníka nebo zamítnutí online žádosti o úvěr nebo elektronické postupy přijímání pracovníků bez jakéhokoliv lidského zásahu.

One-stop-shop

Každý dohlížitel má přispívat k jednotnému výkladu a uplatňování nařízení v celé EU. Kontrolní úřad hlavní, resp. jediné provozovny, je příslušný jednat jako vedoucí dohlížitel pro přeshraniční zpracovávání prováděné provozovatelem nebo zprostředkovatelem. Z výše uvedeného například vyplývá, že kontrolu ní nemusí provádět na území ČR jen český úřad.

---

[83] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

Pseudo anonymizace dat

Identita dotčené osoby je uchovávána pouze v jedné databázi a ostatní informační systémy uchovávají data v anonymizované podobě. Jde o reverzibilní anonymizaci, přičemž jako reference se nejčastěji používá bezvýznamový identifikátor, pomocí kterého lze opětovně určit, ke které identitě data patří. Tento princip snižuje riziko porušení důvěrnosti osobních údajů.

Oznámení resp. zveřejnění bezpečnostních incidentů[84]

V případě porušení ochrany osobních údajů provozovatel bez zbytečného odkladu a nejlépe do 72 hodin od zjištění oznámí incident příslušnému kontrolnímu orgánu s výjimkou případů, kdy není pravděpodobné, že porušení ochrany OÚ povede k riziku pro práva a svobody fyzických osob. Pokud může incident vést k vysokému riziku pro práva a svobody fyzických osob, provozovatel bez zbytečného odkladu oznámí porušení ochrany osobních údajů i dotyčné osobě.

Účinné, přiměřené a odrazující pokuty

Nařízení přináší výrazné zvýšení pokut, které mají být "účinné, přiměřené a odrazující". Pokuty ve smyslu nařízení jsou následující:[85]

- správní pokuta až do výše 10 mil. € nebo 2 % celkového světového ročního obratu skupiny, například za porušení ustanovení o specificky navržené a standardní osobních údajů, společných provozovatelích, zprostředkovatelích, bezpečnosti osobních údajů, apod.;

---

[84] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

[85] *GDPR* [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

- správní pokuta až do výše 20 mil. € nebo 4 % celkového světového ročního obratu skupiny, například za porušení základních zásad zpracování, práv dotčených osob, přenosu osobních údajů příjemci ve třetí zemi bez splnění záruk, apod.

5.4 Formulace interního předpisu GDPR ve společnosti Alza

Tento interní předpis pro ochranu osobních údajů, včetně postupů v něm obsažených, je určen pro organizaci firmy Alza a její jednotlivé pobočky, které neprovádí rizikové zpracování. Popisuje faktický stav a opatření zavedené ve společnosti v rámci přípravy na GDPR. Tomuto předpisu předcházela analýza, mapující účely zpracování údajů a odpovídající procesy.[86]

Úvodní ustanovení

Tento interní předpis upravuje zpracování osobních údajů pro zajištění ochrany osobních údajů v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob při zpracování osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46 / ES (GDPR). Cílem tohoto interního předpisu je zajistit dodržování povinností vyplývajících z GDPR ve společnosti a umožnit dotyčným osobám výkon jejich práv.

Interpretace hlavních pojmů

Pro účely tohoto interního předpisu jsou interpretovány následující pojmy:

1. "osobní údaje" veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tj. osobě, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, typicky například jméno, identifikační číslo, lokalizační údaje, síťový identifikátor nebo jeden nebo více specifických prvků, fyzické, fyziologické, genetickou, mentální, ekonomické, kulturní nebo společenskou identitu této fyzické osoby;

[86] Interní dokumenty společnosti Alza ke GDPR a její implementaci, v tištěné podobě, upraveno.

2. "zvláštní kategorie osobních údajů" osobní údaje, které odhalují rasový nebo etnický původ, politické názory, náboženské vyznání nebo filozofické přesvědčení, členství v odborech, a zpracování genetických dat, biometrických údajů s cílem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

3. "zpracováním" jakýkoli úkon nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí nebo bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uloţení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, používání, zpřístupnění šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, odstranění nebo zničení;

4. "omezení zpracování" označení uložených osobních údajů za účelem omezit jejich zpracování v budoucnu;

5. "správcem" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů;

6. "zpracovatel" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

7. "příjemcem" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuté, ať už se jedná o třetí stranu, nebo ne. Avšak veřejné orgány, které mohou získávat osobní údaje v rámci zvláštního vyšetřování v souladu s právem členského státu, se za příjemce nepovažují;

8. "třetí strana" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo povinnou správci nebo zpracovateli, která je oprávněna ke zpracování osobních údajů;

9. "souhlas" subjektu údajů znamená svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým dotyčná osoba dává prohlášením či jiným zjevným potvrzením svůj souhlas ke zpracování svých osobních údajů;

10. "porušením zabezpečení osobních údajů" porušení zabezpečení, které má za následek náhodné nebo nezákonné zničení, ztrátu, změnu nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

11. "kontrolní úřad" Úřad pro ochranu osobních údajů České republiky

12. "likvidací" osobních údajů se rozumí fyzické zničení jejich nosičů nebo jejich vymazání.

Interní předpisy

Organizační řád, předpisy personálního oddělení, předpisy fyzické bezpečnosti, předpis pro práci s kreditní kartou, předpis na ochranu informací, předpis pro řízení rizik, předpis pro řízení bezpečnostních incidentů, předpis pro řízení uživatelského přístupů, skartační a archivační řád, systém vnitřních zásad pro chod administrativních oddělení společnosti Alza.

Role a odpovědnosti

Zaměstnanci

Každý zaměstnanec odpovídá za to, že zpracování osobních údajů provádí v souladu s právními předpisy a tímto interním předpisům a dalšími předpisy a dokumenty společnosti Alza. Každý zaměstnanec je povinen zachovávat mlčenlivost o osobních údajích a opatřeních přijatých na jejich ochranu, o kterých se v souvislosti s výkonem svého zaměstnání dozvěděl, a to i po skončení pracovního poměru. Pokud poruší povinnost mlčenlivosti, bude to zaměstnavatel považovat za porušení pracovní kázně zvlášť hrubým způsobem a může se zaměstnancem okamžitě rozvázat pracovní poměr podle § 55 odst. 1 písm. b) zákoníku práce.

Odpovědná osoba za ochranu osobních údajů

V závislosti na organizační struktuře identifikujeme osobu nebo roli v společnosti odpovědnou za agendu ochrany osobních údajů a zajištění plnění tohoto předpisu. Upravíme odpovědnosti dalších osob v souvislosti se zpracováním osobních údajů a plněním povinností podle tohoto předpisu. V případě, že je ve společnosti IT manažer

bezpečnosti nebo samostatně manažer HR, může být odpovědnost rozdělena mezi tyto, případné další role.

Zásady zpracování osobních údajů

Při zpracování osobních údajů ve společnosti je nezbytné dodržovat následující zásady:

a) ve vztahu k dotyčné osobě musí být osobní údaje zpracovávány korektně, zákonně a transparentním způsobem (tři principy - zákonnost, korektnost a transparentnost);

b) osobní údaje se musí shromažďovat pro určité, jasné a zákonné účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný (účelové omezení);

c) zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány (minimalizace údajů);

d) osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny (přesnost);

e) osobní údaje musí být uloženy ve formě, která umožňuje identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (omezení uložení);

f) osobní údaje se musí zpracovávat způsobem, který zajistí nálety zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (integrita a důvěrnost).

Technické - organizační opatření k zajištění ochrany osobních údajů

Systém ochrany osobních údajů je tvořen komplexem organizačních a technických opatření, které jsou ve společnosti realizovány za účelem zajištění ochrany a bezpečnosti osobních údajů.

Bezpečnostní opatření

A. Řízení rizik

Popisuje, jakým způsobem jsou ve společnosti identifikovány a hodnoceny různé závažné a pravděpodobné rizika a následně navrhují a přijímají opatření ke snížení vlivu těchto rizik. Revize vyhodnocení rizik je ve společnosti prováděna pravidelně jedenkrát ročně. Následná revize rizik je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. Za provedení revize odpovídá odpovědná osoba. Vyhodnocení rizik uvažuje následující:

a) Riziko vůči právům a svobodám dotčených osob z následujících pohledů:

1. Porušení principů přiměřenosti a nezbytnosti zpracování,

2. Porušení práv dotčených osob,

3. Neoprávněný přístup k osobním údajům,

4. Neoprávněná změna osobních údajů,

5. Nedostupnost nebo vymazání osobních údajů.

b) Možným vliv v případě realizace rizik například zpracování osobních údajů bez právního titulu může vést k zasílání nevyžádaných obchodních zpráv nebo neschopnosti zajistit výkon práva dotyčné osoby a následnému způsobení hmotné nebo nehmotné újmy neoprávněný přístup k citlivým osobním údajům může vést k odcizení identity a další.

c) Hodnocení závažnosti dopadu: Na základě definice možných vlivů v bodě b) je určena jedna z následujících kategorií.

1. Zanedbatelné: Subjekty údajů nebudou dotčeny, nebo budou dotčeny minimální bez jakýchkoliv větších problémů. Ve společnosti Alza je to opětovné zadávání informací do systému, obtěžování při opětovném propagačním sdělení.

2. Omezené: Subjekty údajů se mohou setkat s nepříjemnostmi, které budou schopné relativně snadno vyřešit, dodatečné náklady, popření přístupu k obchodním službám, strach, nedostatek porozumění, stres a další.

3. Významné: Událost může mít významný důsledek pro dotčené osoby. Tyto důsledky by subjekty měly být schopny překonat, ačkoli s většími obtížemi, typicky zneužití dostupných prostředků, škody na majetku, ztráta zaměstnání, zhoršení zdravotního stavu a další.

4. Vysoké: Událost může mít vysoké nebo nezvratné důsledky pro dotčené osoby, které nemusí být možné překonat, například finanční problémy, značný dluh, pracovní neschopnost, dlouhodobé fyzické nebo psychické nemoci, smrt a další.

d) Hodnocení pravděpodobnosti výskytu události, které mohou mít negativní vliv na dotčené osoby. Tato metodika uvažuje následující kategorie:

1. Zanedbatelné: Ve společnosti Alza ani v odvětví se událost ještě nevyskytla, její výskyt však není vyloučen.

2. Omezené: Ve společnosti Alza se událost v minulosti ještě nevyskytla, její výskyt však byl již zaznamenán v rámci odvětví.

3. Významné: Ve společnosti Alza se událost v minulosti již vyskytla.

4. Vysoké: Ve společnosti Alza se událost již vyskytla opakovaně.

e) Zavedené a plánované ochranné resp. nápravná opatření

Vyhodnocení rizik - na základě analýzy ve společnosti Alza.

B. Fyzická bezpečnost

Popisuje technická opatření, která slouží k zajištění bezpečnosti osobních údajů. Zaměřuje se na využití kamerových systémů, zámků, zábran, mříží, uzavřených objektů, trezorů a podobných prostředků fyzického zabezpečení. Pro kontrolu fyzického přístupu do prostor společnosti Alza je využívání recepce. Vstup je umožněn pouze oprávněným osobám, a to

na všech centrálních pobočkách společnosti Alza, netýká se běžných obchodních poboček a výdejních míst společnosti Alza.

Fyzické bariéry jsou tam, kde je to použitelné, postavené tak, aby chránily před neoprávněným vstupem.

Požární dveře jsou v definovaném bezpečnostním perimetru opatřeny elektronickým zabezpečovacím systémem a jsou monitorovány.

Vnější dveře a dosažitelná okna jsou chráněny vhodným detekčním systémem, který odpovídá místním, národním a mezinárodním normám a je pravidelně testován a kontrolován.

Zařízení na zpracování informací spravované organizací jsou fyzicky odděleny od prostředků neoprávněných osob.

Není dovoleno nechávat osobní údaje volně k dispozici bez dohledu. Platí, že písemnosti a jiné nosiče osobních údajů je dovoleno uchovávat samostatné pouze v uzamykatelných místnostech, případně pouze v uzamykatelných skříních.

Přístup do kanceláří nebo archivů, kde jsou tyto osobní údaje uložené, je umožněn pouze oprávněným zaměstnancům společnosti, a to pomocí přístupové karty / fyzického klíče.

Prostory společnosti Alza, v nichž jsou uloženy osobní údaje, jsou pod 24 hodinovým kamerovým dohledem. Zpracování formou kamerového systému je upraveno v samostatném interním předpisu.

Fyzický přístup do serverovny je umožněn pouze pracovníkům IT s oprávněním prostřednictvím přístupové karty / fyzického klíče.

Je vyžadováno dodržovat zásady prázdného stolu a zamčené obrazovky při opuštění pracoviště zaměstnance časově dočasného nebo po skončení pracovní doby.

C. IT bezpečnost

Popisuje přijatá technická opatření ve společnosti Alza, které slouží k zajištění bezpečnosti osobních údajů v elektronické formě. Zaměřuje se na to, jak jsou nastaveny přístupová oprávnění do informačního systému zpracovávajícího osobní a citlivé údaje, aby bylo zajištěno přistupování pouze oprávněných osob k údajům odpovídajícím právě tímto oprávněním. Dále jakým způsobem se pořizují elektronické záznamy (logy), které umožní určit a ověřit, kdy a kým se nakládalo s údaji. Jak je zabráněno neoprávněnému přístupu k datovým nosičem a jako je s nimi nakládáno v případě nepředvídatelné události – hlavně požár, povodeň, stěhování, výpadek proudu a další.

Řízení přístupů se řídí interním předpisem na řízení přístupů společnosti Alza a stanovuje pravidla pro řízení přístupů běžných i privilegovaných uživatelů do systémů společnosti Alza.

Přístup k osobním údajům je přidělován pouze v rozsahu nezbytně nutném pro výkon funkce a revizi těchto přidělených přístupů probíhá pravidelně. V případě zjištění neoprávněného přístupu se tento přístup následně odebírá. Dále je zajištěna kontrola neslučitelných oprávnění.

Je zavedena a zachováním evidence jednotlivých rolí týkajících se bezpečnosti IT, u nichž je jednoznačně stanovena odpovědnost a pracovní náplň s cílem snížit rizika vyplývající z lidského faktoru, neúmyslných chyb, krádeže, podvodu nebo zneužití.

Pokud provoz IT, zpracování účetnictví či jiné externě zpracovávané agendy vyžadují přístup dodavatelů, musí být tento přístup řešen smluvně, v souladu s bezpečnostní dokumentací tak, aby byla zajištěna bezpečnost osobních údajů uvnitř i vně společnosti Alza.

Uživatelé, IT administrátoři i dodavatelé mohou využívat vzdálené přístupy k IT prostředí společnosti pouze na základě jejich pracovních a smluvně převzatých povinností a kompetencí, a to jen s využitím schválených komunikačních prostředků. Možnost využívání vzdáleného přístupu musí podléhat pravidelné revizi.

O jednotlivých přístupech na úrovni domény jsou automaticky zhotovovány logy s kapacitou v rozsahu 30 dní.

Hlavní PMS systém automaticky vyhotovuje logy všech aktivitách uživatelů s kapacitou v rozsahu 30 dní.

Je zajištěno pravidelné vyhodnocování logovaných aktivit a ochrana logů, tzv. zajištění nepopiratelnosti vytvořených logů, ověření možnosti jejich modifikace vnějšími vlivy, jako je škodlivý software různého druhu a malware, lidský faktor.

Přidělování hesel se řídí interním předpisem.

Je povoleno provozovat pouze schválený, legálně nabytý a evidován SW a HW ve shodě s licenční dohodou výrobce a způsobů využití. Tento SW a HW majetek je evidován v evidenci informačních aktiv a jejich nákup je vždy diskutován a schválen IT oddělením.

Je zajištěna správa opravných a aktualizačních balíků programového vybavení.

Informační aktiva musí být chráněna před počítačovými viry, spamem, spyware a jiným škodlivým kódem správným nastavením bezpečnostních mechanismů a použitím vhodného SW aplikovaného na relevantní komponenty počítačové sítě společnosti Alza, jako jsou servery, firewally i jednotlivé pracovní stanice a mobilní zařízení ve správě společnosti Alza.

IT oddělení musí definovat a udržovat plán obnovy po infiltraci IT prostředí škodlivým kódem. Tento plán musí být pravidelně jednou za rok aktualizován na základě aktuálních potřeb.

Zálohování osobních údajů se řídí interním předpisem pro zálohování dat společnosti. Zálohy jsou uchovávány v trezoru společnosti umístěném v jiném prostoru, než je serverová místnost.

Pouţití USB klíčů, kromě USB klíče poskytnutého IT oddělením, je blokováno. USB klíče poskytnuté IT oddělením jsou příslušným způsobem zašifrovány.

Použití veřejných úložišť, služeb a nástrojů, jako je Dropbox, Google Drive, uloz.to, uschovna.cz, leteckaposta.cz, torrents, P2P, Basecamp, Slack, a další **je zakázáno.**

Osobní a citlivé údaje nesmí opustit chráněné IT prostředí společnosti Alza v nezašifrované formě. K jejich zajištění zajišťuje IT oddělení kryptografické prostředky a pravidla řízení šifrovacích klíčů.

Komunikační rozhraní se systémy společnosti Alza musí být zajištěno.

Informační aktiva, která sloužila k uchovávání nebo přenosu osobních údajů a již nejsou dále nezbytné nebo dosáhli konce své životnosti, jsou bezpečně zlikvidovány a je uchován záznam o jejich likvidaci.

V případě interního vývoje a změn v informačních systémech jsou stanoveny zásady a pravidla pro evidenci a řízení vývoje nového a změn stávajícího informačního systému společnosti Alza.

D. Narušení zabezpečení osobních údajů

Jde o řešení zjištění a posouzení narušení zabezpečení osobních údajů, tzn. postup, pokud nastane událost, která může mít za následek vznik bezpečnostního incidentu. Popisuje odpovědnost za řešení incidentu, kam je zaznamenán a jaké kroky následují po zjištění incidentu. Povinností je přijmout opatření k zamezení opakování bezpečnostního incidentu.

V případě zjištění porušení zabezpečení osobních údajů je nezbytné dodržet následující postup podle této interní směrnice:

1. Oznámit zjištění odpovědné osobě,

2. Zamezit dalšímu úniku - fyzickým zamknutím dokumentů nebo v případě elektronické formy zamezením přístupu nebo vypnutím IT systémů,

3. Případ narušení zabezpečení posoudit a zdokumentovat, tedy co se stalo, jaké a čí osobní údaje unikly, možné následky, popis opatření s cílem vyřešit daný případ, identifikace rizika / vysokého rizika podle specifikace rizik v interní směrnici výše,

4. Nahlásit porušení zabezpečení kontrolnímu úřadu bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm společnost Alza dozvěděla,

5. Oznámit porušení zabezpečení bez zbytečného odkladu subjektu údajů, pokud je pravděpodobné, že daný případ bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

E. Kontrolní činnost

Kontrola přístupu a práce s osobními údaji, a to včetně periodicity kontrol odpovědnou osobou, výstupy kontrol a další oblasti. Osoby odpovědné za jednotlivé oblasti podle katalogu zpracování osobních údajů zajistí kontrolu plnění povinností vyplývajících z tohoto interního předpisu. Kontroly jsou v následujícím rozsahu:

a) jedenkrát ročně důkladná kontrola celé společnosti Alza odpovědnou osobou,

b) jedenkrát měsíčně náhodná kontrola vybraného informačního systému nebo úseku odpovědnou osobou,

c) každodenní kontrola fyzické ochrany rizikových míst odpovědnou osobou,

d) kontrola po změně a následném školení ke změnám zákonů nebo interních předpisů, včetně tohoto interního předpisu,

e) mimořádná kontrola po řešení narušení zabezpečení osobních údajů.

O pravidelných kontrolách je proveden záznam a ten je uložen. V případě nálezů kontroly probíhá konzultace, případně dodatečné odborné proškolení.

F. Školení zaměstnanců

Zahrnuje proces vzdělávání zaměstnanců v souvislosti s ochranou osobních údajů, periody školení, výstupy ze školení. Dále postup proškolení v případě přijetí nového zaměstnance nebo přeřazení zaměstnance na jinou pozici. Proškolování zaměstnanců probíhá formou e-learningu zaměřeného na informační bezpečnost a ochranu osobních údajů a to jak při nástupu, tak pravidelně alespoň jedenkrát ročně. Evidence o absolvování školení je zpracovávána personálním oddělením společnosti. Za proškolení zaměstnanců odpovídá odpovědná osoba.

Ostatní opatření

Pravidelná revize a aktualizace interních předpisů

Popisuje způsob zajištění pravidelné revize ve společnosti a aktualizaci interních předpisů, včetně těch týkajících se ochrany osobních údajů. Všechny interní předpisy společnosti, včetně těch, které se týkají ochrany osobních údajů, jsou revidovány pravidelně jedenkrát ročně. Následná revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

Vedení a aktualizace katalogu zpracování

Obsahuje postup pro vedení a aktualizaci katalogu zpracování, osobu odpovědnou za vedení a aktualizaci a místo zaznamenání. Katalog zpracování je součástí pravidelné revize a aktualizace interních předpisů. Revize kompletnosti a přesnosti katalogu zpracování je prováděna pravidelně jedenkrát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve společnosti s možným dopadem na ochranu osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá odpovědná osoba.

Zpracovatelské vztahy

Popisují postup pro řízení vztahů s dodavateli, kteří v rámci své činnosti zpracovávají osobní údaje. Popisují, kdo schvaluje výběr zpracovatelů a na základě jakých kritérií. Výběr zpracovatele schvaluje odpovědná osoba. Při výběru zpracovatelů hodnotí zejména následující faktory:

- Schopnost dodavatele uzavřít a dodržovat povinnosti stanovené zpracovatelskou smlouvou,
- Dostatečné zabezpečení osobních údajů,
- Dobrá pověst dodavatele v rámci ochrany osobních údajů,
- Relevantní certifikace ochrany osobních údajů nebo ochrany informací obecně,
- Další relevantní faktory ve vztahu ke konkrétnímu účelu zpracování.

O splnění kritérií výběru dodavatele je vedena evidence.

Řízení projektů a změn

Popisuje postup pro zohlednění aspektů ochrany osobních údajů v rámci nových projektů a řízení změn podle principu záměrné a standardní ochrany. Uvádí osoby, které jsou v rámci tohoto postupu zapojeny a výstupy vyplývající z posouzení aspektů ochrany osobních údajů. V případě významnějších změn ve společnosti s vlivem na ochranu osobních údajů, konkrétně například nový IT systém, nový účel zpracování, včetně nové služby nebo produktu a další. Je do těchto aktivit zapojena odpovědná osoba, která identifikuje případná rizika pro ochranu osobních údajů a pomůže navrhnout adekvátní opatření ke snížení těchto rizik. V případě potřeby provede revizi a aktualizaci tohoto interního předpisu, včetně analýzy rizik nebo aktualizace katalogu zpracování, případně dalších relevantních interních předpisů.

Předávání osobních údajů třetím stranám

Obsahuje postup, podle kterého je ve společnosti Alza postupováno v případě předávání osobních údajů do třetích zemí. Skládá se ze seznamu smluv a případných dohod s obchodními partnery, například s cestovními kancelářemi, agenturami a dalšími, kde je zachyceno předávání osobních údajů do třetích zemí. V rámci činnosti společnosti Alza nedochází k předávání osobních údajů do třetích zemí.

Výkon práv dotčených osob

Skládá se z postupu a kontaktního místa, kde mohou dotčené osoby kontaktovat společnost s požadavky na realizaci níže uvedených práv. Tyto informace je možné uvést v rámci oznámení na splnění informační povinnosti.

Poskytování informací

Postupy, v rámci kterých poskytujeme subjektům údajů informace o zpracování. Informace o zpracování osobních údajů zaměstnanců či uchazeče o zaměstnání mohou být součástí pracovní smlouvy, osobního dotazníku nebo samostatného formuláře nebo interního dokumentu, se kterým se musí zaměstnanec při nástupu seznámit. Informace o zpracování osobních údajů klientů je možné provést v rámci registrační karty, webových stránek nebo

ubytovacího řádu společnosti Alza. Společnost Alza poskytuje subjektům údajů informace v souladu s GDPR, a to v požadovaném rozsahu, čímž zajišťuje transparentnost zpracování.

Právo subjektů údajů na přístup k osobním údajům

Popisuje postup, jak je řešeno právo na přístup k osobním údajům, a to jak v případě zaměstnanců, tak i v případě zákazníků. V případě, že o to dotčená osoba požádá, společnost Alza poskytne subjektu údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je to tak, umožní dotyčným osobám získat přístup k těmto osobním údajům a informacím způsobem a v daném rozsahu podle GDPR.

Právo na opravu

Popisuje postup, jak je řešeno právo na opravu k osobním údajům, a to jak v případě zaměstnanců, tak i v případě zákazníků. V případě, že o to dotčená osoba požádá, případně se o nepřesných osobních údajích dozví společnost jinak, opraví bez zbytečného odkladu nepřesné osobní údaje. V případě, kdy si to účel zpracování vyžaduje, zajistí společnost Alza doplnění neúplných osobních údajů podle GDPR.

Právo na výmaz

Popisuje postup, jak je řešeno právo na vymazání osobních údajů, a to jak v případě zaměstnanců, tak i v případě zákazníků. V této souvislosti je zřízen zvláštní emailový účet nebo formulář na webové prezentaci, na který mohou zákazníci klást své požadavky a uplatňovat v tomto interním předpisu uvedená práva. Nezapomeňte na případné napojení na archivační a skartační řád společnosti. V případech a), d) a e) by měly být zavedeny postupy pro výmaz osobních údajů bez ohledu na to, zda o to subjekt údajů požádá. V případě, že je dán jeden z následujících důvodů, zajistí společnost na základě uplatnění práva subjektům údajů bez zbytečného odkladu vymazání osobních údajů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracované;

b) dotyčná osoba odvolá souhlas, na jehož základě byly osobní údaje zpracovávány a neexistuje žádný další právní důvod pro zpracování;

c) dotyčná osoba vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;

d) osobní údaje byly zpracovány nezákonně;

e) osobní údaje musí být vymazány na splnění zákonné povinnosti, která se na společnost vztahuje;

f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Právo na omezení zpracování

Popisuje postup, jak je řešeno právo na omezení zpracování osobních údajů, a to jak v případě zaměstnanců, tak v případě zákazníků. V případě, že je dán jeden z následujících důvodů, zajistí společnost omezení zpracování osobních údajů:

a) subjekt údajů popírá přesnost osobních údajů;

b) zpracování je nedovolené a subjekt údajů odmítá výmazu osobních údajů a žádá namísto toho omezení jejich použití;

c) společnost již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) dotyčná osoba vznesla námitku proti zpracování.

Právo na přenositelnost údajů

Definuje postup, jak je řešeno právo na přenositelnost osobních údajů. V případě, že o to subjekt údajů požádá a zároveň je zpracování založeny na souhlasu nebo smlouvě, a zároveň se zpracování provádí automatizovaně, umožní společnost subjektu údajů výkon práva na přenositelnost. Osobní údaje, které subjekt údajů společnosti poskytl, a které se ho týkají, poskytne společnost v strukturovaném, běžném používání a strojově čitelném formátu. Součástí tohoto práva je zajištění možnosti přenesení předmětných osobních údajů k jinému správci podle požadavky subjektu údajů. Definuje postup, jak je řešeno právo na přenositelnost osobních údajů.

Archivace osobních údajů

Obsahuje postup, případně vypsané dokumenty, které upravují archivace osobních údajů ve společnosti Alza. Definuje účel archivace a dobu archivace. Archiv je provozován samotným správcem. Rozsah údajů k archivaci a archivační doba vyplývá z katalogu zpracování osobních údajů. Přístup do archivu mají pouze osoby v konkrétních pracovních pozicích za předem daných důvodů a pro naplnění některého z účelů předvídaných GDPR.

Archivace osobních údajů klientů

Archivace osobních údajů klientů se řídí také ustanovením § 101 zákona č. 326/1999 Sb. o pobytu cizinců na území České republiky, který ukládá povinnost ubytovateli vést domovní knihu a uchovávat ji po dobu 6 let od posledního zápisu. Podle zákona č. 565/1990 Sb. o místních poplatcích, vede organizace v písemné podobě evidenční knihu, do které zapisuje dobu ubytování, účel pobytu, jméno, příjmení, adresu místa trvalého pobytu nebo místa trvalého bydliště v zahraničí a číslo občanského průkazu nebo cestovního dokladu fyzické osoby, které ubytování poskytl. Zápisy do evidenční knihy jsou vedeny přehledně a srozumitelně a jsou uspořádány chronologicky. Evidenční kniha se uchovává po dobu šesti let od provedení posledního zápisu.

Archivace osobních údajů dalších subjektů údajů – zaměstnanců

Osobní spisy se archivují 10 let s výjimkou dokladu o délce zaměstnání, kde archivační lhůta je 20 let, protože tento doklad může sloužit pro účely důchodového pojištění. Mzdový list musí organizace archivovat po dobu 20 let následujících po roce, kterého se poslední účetní záznamy v mzdovém listě týkají. Účetní závěrka a výroční zpráva se uchovává po dobu 10 let počínajících koncem účetního období, kterého se týkají, a účetní záznamy, konkrétně pro účely sociálního zabezpečení, veřejného zdravotního pojištění po dobu 5 let počínajících koncem účetního období, kterého se týkají.

Likvidace osobních údajů

Společnost Alza provádí likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovávány, případně na základě žádosti subjektu. Při likvidaci jsou dodržovány zákonné výjimky týkající se uchovávání osobních údajů pro účely archivnictví

a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení. Likvidace osobních údajů je prováděna certifikovanou externí společností na základě smlouvy o zpracování osobních údajů. O skartaci je vydáno potvrzení.

6. Výsledky a diskuse

Závěrečná ustanovení

Každé řešení podle nařízení GDPR je individuálně nastaveno podle potřeb konkrétní organizace společnosti. Univerzální řešení neexistuje a pro každou společnost znamená něco jiného. Mnoho firem poskytuje typizované produkty, audity, školení či balíkové software. To však vylučuje rozsáhlou možnost jeho aplikace. Zvolené řešení popisuje příklad faktického stavu a zvolené opatření zavedené ve společnosti Alza v rámci přípravy na GDPR a následné zavedení GDPR do praxe společnosti Alza. Definuje jasně a srozumitelně nastavení procesů, které se vztahují k životnímu cyklu zpracování osobních údajů. Seznamuje organizace s problematikou ochrany osobních údajů, objasňuje hlavní pojmy, pomáhá zajistit dodržování povinností vyplývajících z GDPR ve společnosti Alza a obecně posoudit důsledky nařízení na prostředí a rozhodnout se, jakým způsobem dále postupovat.

Poskytuje návrh vhodného postupu na řízení procesu při interním datovém auditu organizace, popisuje povinnosti společností a podnikatelů, práva dotčených osob a změny v oblasti zpracování osobních údajů na praktických příkladech a aplikování vlastního návrhu v zvolené organizací z hlediska odpovědných osob, zásad zpracování údajů, fyzické jako i IT bezpečnosti, archivace, kontrolní činnosti, likvidace a další zavedené v zařízení v rámci přípravy na GDPR. GDPR vzniklo pro to, aby si některé subjekty uvědomily, že osobní údaje jsou vlastnictvím a součástí soukromí občana. Digitalizace prudce narůstá a ochranu soukromí je třeba v online světě nějakým způsobem ukotvit, alespoň na úrovni EU, pokud to nejde globálně. Myslím si, že nařízení je formulováno nejasně a pokuty jsou vysoké. Mnoho věcí bude sporných. GDPR se netýká fyzických osob, nepodnikatele, kteří používají osobní údaje pro domácí použití, například kontakty v mobilním telefonu. Tedy netýká se zcela každého subjektu, ale primárně komerčních subjektů a veřejné správy. Jinak kromě pokut obsahoval donedávna platný zákon mnohé z toho, co je nařízením vyžadované, jen to nikdo prakticky nedodržoval.

GDPR nesmíme vnímat jako nutné zlo zbytečných nákladů. Nařízení je pro organizaci velkým přínosem z hlediska automatizace procesů, vyšší bezpečnosti, lepšímu využití dat vzájemným propojením a lepší organizací práce. Kvalitní manažer má náklady na GDPR vědět co nejlépe využít a dokázat najít návratnost vložených investic do implementace GDPR. Malé firmy se mohou spokojit s tzv. "GAP" analýzou a zaváděním nezbytných požadavků. Je možné je koupit od různých dodavatelů na trhu. Velké korporace a společnosti musí podle mého názoru rozpracovány komplexní implementační mapy a jejich řešení v rámci organizace dané společnosti a platí to i pro společnost Alza. Ta musí reflektovat na existující strategii řízení dat v dané organizací. Důležité je uvažovat ve střednědobém horizontu a zvolit strategii s ohledem na aktuální stav společnosti Alza i očekávaný vývoj. Třeba si rovněž rozmyslet zavádění nových technologií, čímž můžeme značně ovlivnit životnost navržených prováděcích opatření a také celkový výsledek. 100 % soulad s GDPR nám nedá nikdo. Samotný zákon je navržen nedokonale s právními kuriozitami a technickými omezeními. Z tohoto důvodu bude nezbytné akceptovat trhliny a rozplánovat s ohledem na vývoj legislativy do následujících období.

Hlavní klady GDPR ve společnosti Alza

Úspora a náklady

Splnění pravidel nemají na starosti národní úřady, ale jeden evropský orgán. Stejně ochranu osobních dat bude upravovat jedna evropská norma místo 28 národních. Přínosem pro firmy bude omezení byrokracie a možnost rychleji se rozhodovat. Harmonizace pravidel získávání a uchovávání osobních údajů. Zásadní je zejména sjednocení právního rámce. Společnosti musí však brát v úvahu i legislativu platnou na národní úrovni. Může jít například o zajištění ochrany svobod a práv při zpracovávání osobních údajů pracovníků v rámci zaměstnání, kde jsou důležité ustanovení kolektivní smlouvy nebo národní legislativy. Zavedení nařízení může poměrně zjednodušit přeshraniční dosah společností.

Ochrana zájmů

Nařízení povolí širší uplatnění principu zpracovávat osobní údaje pouze v souladu se zájmy fyzických osob a na zpracování dat musí společnosti získávat souhlas. Důvodem pro zpracování dat bude kromě ochrany dotčených osob i ochrana lidí v blízkém vztahu s

danou osobou. Nové podmínky zpracování dat a zvyšování povědomí o bezpečnosti údajů. Firmy budou mít volnější ruce. Vzniká nová situace vytvářející právní základ pro zpracování dat s ohledem na veřejný zájem. Údaje můžeme zpracovávat i v zájmu ochrany veřejného zdraví. Důvodem pro zpracování osobních dat jsou i vědecké, statistické nebo historické důvody.

Není nutná identifikace

Při práci s osobními údaji, které nevyžadují získání totožnosti osoby, společnost nemusí doplňkové informace získávat, uchovávat nebo zpracovávat.

Identita

Lidé získávají určité dodatečné práva a provozovatel má právo vyžádat si potvrzení identity spíše než práva přizná. Zvýšení bezpečnosti a svoboda ve výběru prostředků pro zvýšení ochrany údajů V rámci nařízení GDPR je třeba přijmout postupy pro bezpečnost dat. Zamezit únik dat a záznamů případně ztrátu zařízení (mobil, laptop).

Ochrana dobrého jména a osobní pověsti

Občané chtějí být informováni o případné ztrátě osobních údajů. Pokud nemají úplnou kontrolu nad daty poskytujícími online, jsou znepokojeni. Největším rizikem je pro dotčené osoby zneužití jejich online identity. Jen 20 % lidí je obeznámených s privacy policy jednotlivých webových stránek nebo elektronických obchodů se zbožím a službami.

Orientace na zákazníka (občana)

GDPR přináší transparentní a lepší vztah s klientem založený na důvěře. Firma získá více údajů od zákazníka a bude se umět rozhodnout se na základě kvalitnějších dat. Výhodou bude lepší pochopení chování zákazníka.

<u>Hlavní zápory GDPR ve společnosti Alza</u>

Vstupní souhlas

Při zpracování osobních údajů musí dotčená osoba souhlasit se zpracováním jejích údajů a může tento souhlas kdykoliv odvolat. Získání povolení je ve firemní praxi náročnější a

společnost Alza musí umět prokázat, že souhlas dostala. Nařízení zpřísňuje ochranu mladistvých. Zkomplikovat situaci může firmám fakt, že za mladistvé osoby do šestnácti let vyjadřuje souhlas zákonný zástupce. Hranice věku se může v členských státech lišit.

Minimalizace údajů

Firmy mohou data používat pro zpracování pouze v nezbytném období a jen ty, které skutečně potřebují pro svou činnost.

Přehledné zpracovávání

Provozovatelé musí informovat osoby o používání jejich údajů a umožnit jim přístup k těmto datům. Zákonné, spravedlivé a transparentní zpracování dat výrazně zatěžuje provozovatele. Je potřebná dodatečná administrativní práce, čímž je i prohloubení "práva být zapomenut."

Principy "protection by design" a "by default"

Společnosti musí klást doraz již při vývoji svých produktů a služeb na dodatečné kroky ochrany osobních údajů. To může způsobit zatěžující a náročné změny ve výrobě nebo v poskytování služeb. Každý musí provádět specifickou ochranu soukromí a myslet vedle ochraně dat i na způsob pracování s údaji.

Územní platnost

Dodržování nařízení GDPR sahá i za hranice mimo EU a zahrnuje mnoho dodatečných nákladů. Týká se firem poskytujících služby nebo zboží dotčeným osobám v EU nebo kontrolují jejich chování.

Formulace doporučení pro podniky

Při zpracování osobních údajů ve společnosti je nezbytné dodržovat následující zásady:

a) ve vztahu k dotyčné osobě musí být osobní údaje zpracovávány korektně, zákonně a transparentním způsobem (tři principy - zákonnost, korektnost a transparentnost);

b) osobní údaje se musí shromažďovat pro určité, jasné a zákonné účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný (účelové omezení);

c) zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány (minimalizace údajů);

d) osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny (přesnost);

e) osobní údaje musí být uloženy ve formě, která umožňuje identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (omezení uložení);

f) osobní údaje se musí zpracovávat způsobem, který zajistí nálety zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (integrita a důvěrnost).

Pro splnění výše uvedených zásad dle výsledků této práce doporučuji zajistit minimálně tyto kroky, které do podniku přinesou žádanou shodu s nařízením GDPR.

- Vytvoření a zhodnocení analýzy dopadů GDPR – tedy provézt analýzu jakým způsobem jsou data zpracovávána a jestli jsou aktuálně zpracovávaná data nezbytně nutná,
- Provést jednotlivé kroky k implementaci požadavků GDPR – technické úpravy, a také proškolování zaměstnanců společnosti,
- Jmenování pověřence pro ochranu osobních údajů,
- Zpracování metodik pro nakládání s osobními údaji zaměstnanců i zákazníků společnosti v rámci činnosti společnosti – tento krok probíhá v rámci činnosti projektového týmu,
- Úprava a případné zavedení procesů a postupů zpracování osobních údajů - tento krok realizují vedoucí pracovníci oddělení společnosti a IT pracovníci společnosti,
- Nastavení pravidel vedení záznamů o zpracování osobních údajů – tento krok realizuje IT oddělení
- Zpracování a odsouhlasení dopadů jednotlivých činností na ochranu osobních údajů ve společnosti.

Důležité je však nepodcenit přípravu a nařízení o ochraně osobních údajů věnovat patřičnou pozornost. Tedy udělat si čas a všechny kroky si nejdříve rozplánovat.

Závěr

Obecným a hlavním cílem nařízení o ochraně osobních údajů je vytvořit harmonizovaný právní rámec ochrany dat pro celou EU. Vrátit kontrolu nad osobními daty zpět do rukou občanů a zároveň zavést striktní pravidla pro osoby, které zajišťují hostování a zpracování těchto dat kdekoliv na světě. Zároveň zavádí pravidla týkající se volného pohybu osobních údajů v rámci EU i mimo ni. Cílem diplomové práce bylo definovat požadavky na klíčové procesy a navrhnout postup pro zajištění shody s podmínkami GDPR v rámci společnosti Alza. Práce je obecným podkladem pro konkrétní organizaci společnosti Alza a zároveň přínosem a pomůckou pro ostatní organizace pro zajištění jednotných pravidel pro zpracování dat. Poskytuje ucelený postup pro zajištění shody s podmínkami GDPR Jednotlivci mají mnohem lepší přehled o významu dat, rozumějí, jako obchodní značky využívají jejich data při prodeji a marketingu a uvědomují si svá práva ve vztahu ke svým osobním datům.

Implementace GDPR ve firmě proto přináší následující pozitiva:

- omezení byrokracie a možnost rychleji se rozhodovat.
- harmonizace pravidel získávání a uchovávání osobních údajů, sjednocení právního rámce
- zjednodušení přeshraničního dosahu společností
- širší uplatnění principu zpracovávat osobní údaje pouze v souladu se zájmy fyzických osob
- právní základ pro zpracování dat s ohledem na veřejný zájem.
- není nutná identifikace
- společnost nemusí doplňkové informace získávat, uchovávat nebo zpracovávat.
- zvýšení bezpečnosti a svoboda ve výběru prostředků pro zvýšení ochrany údajů

- transparentní a lepší vztah s klientem založený na důvěře.
- lepší pochopení chování zákazníka.

Díky GDPR mají jednotlivci mnohem lepší přehled o významu dat, rozumějí, jako obchodní značky využívají jejich data při prodeji a marketingu a uvědomují si svá práva ve vztahu ke svým osobním datům. Každý z výše uvedených kroků zabere určitý čas, proto je vhodné připravit se na GDPR s dostatečným předstihem a ve spolupráci s kvalifikovaným odborníkem. Příprava totiž nemusí spočívat pouze ve vypracování a aktualizaci potřebné dokumentace, ale také v podstatných změnách nastavení IT systémů či v přijetí různých jiných opatření.

Někomu se může zdát, že jde o regulaci, která se snaží vzít kousek naší svobody. Opravdu však jde o skutečné zajištění základní svobody občanů, protože je zjevné monitorování osob korporacemi a vládou. Jakákoli data a informace, které vedou k identifikaci osobních údajů jednotlivců (v oblasti zdraví, genetiky, ekonomické, sociální, kulturní situace) budou pod ochranou.

Požadavky a zásady GDPR musí dodržovat každá společnost i mimo Unii, která pracuje s údaji občanů. Evropská legislativa poprvé prosazuje zásady ochrany osobních údajů pro zbytek světa.

Důležité je však nepodcenit přípravu a nařízení o ochraně osobních údajů věnovat patřičnou pozornost.

Seznam použitých zdrojů

CALDER, Alan. Eu Gdpr. It Governance, 2017. ISBN 9781849288552.

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

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

ŽŮREK, Jiří. 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. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.

Úmluva o ochraně lidských práv a svobod [online]. USA: USA, 1950 [cit. 2018-12-01]. Dostupné z: https://www.ustrcr.cz/data/pdf/projekty/usmrceni-hranice/umluva.pdf

Evropská úmluva o ochraně lidských práv [online]. EU: EU, 2018 [cit. 2018-12-01]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

GDPR [online]. EU: EU, 2018 [cit. 2018-11-30]. Dostupné z: https://www.eugdpr.org/the-regulation.html

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

IAPP. 2018. GDPR. [online]. [2018-01-11]. Dostupné z: https://iapp.org/search?q=gdpr

IBM. 2018. [online]. [2018-01-11]. Dostupné z: https://www.ibm.com/

TECHBIT. 2018. *Interný audit GDPR*. [online]. [2018-01-10]. Dostupné z: https://www.bdo.cz/

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 pozdějších předpisů

AUTOCONT. 2018. *Nové pravidlá v oblasti ochrany osobných údajov.* [online]. [2018-01-10]. Dostupné z: http://www.autocont.cz

IRWIN, L. 2018. *The GDPR: What technical measures do you need to conduct? [*online]. [2018-01-12]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-what-technical-measures-do-you-need-to-conduct/

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

MEKYŇOVÁ, J. *Osobní údaje?* Profil. 2016, 22, s. 12-14. ISSN 1335-4620.

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

TECHBIT. 2017. *Nařízení GDPR z pohledu IT – úvod do problematiky nařízení GDPR.* [online]. [citováno 12-22- 2018].

CIO. *CIO - analýzy a statistické údaje* [online]. 2019 [cit. 2019-01-17]. Dostupné z: http://businessworld.cz/analyzy?offset=80

Bezpečnost WiFI sítí [online]. 2019 [cit. 2019-01-18]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-bezpecnost-wifi-siti.html

Alza [online]. ČR: ČR, 2018 [cit. 2018-11-30]. Dostupné z: https://www.alza.cz/historie-a-soucasnost-art141.htm

Info.cz [online]. [cit. 2019-04-11]. Dostupné z: Kolik GDPR stálo firmy? Ty středně velké i stovky tisíc korun, říkají právníci