DIPLOMOVÁ PRÁCE

Implementace principů GDPR ve společnosti AF Consult s.r.o.

Implementation of GDPR Principles in AF Consult s.r.o.

STUDIJNÍ PROGRAM

Řízení rozvojových projektů

STUDIJNÍ OBOR

Projektové řízení inovací v podniku

VEDOUCÍ PRÁCE

Ing. Šikýř Martin, Ph.D.

MRÁZOVÁ

PAVLA

2019

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: Mrázová Jméno: Pavla Osobní číslo: 424184

Fakulta/ústav: Masarykův ústav vyšších studií (MÚVS)

Zadávající katedra/ústav: Oddělení manažerských studií

Studijní program: Řízení rozvojových projektů

Studijní obor: Projektové řízení inovací v podniku

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Implementace principů GDPR ve společnosti AF Consult s.r.o.

Název diplomové práce anglicky:

Implementation of GDPR Principles in AF Consult s.r.o.

Pokyny pro vypracování:

CÍL: Cílem práce je prozkoumat zavádění nového nařízení o ochraně osobních údajů (GDPR) ve společnosti AF Consult s.r.o. a představit návrh implementace jednotlivých principů GDPR z pohledu správce.
PŘÍNOS: Přínosem práce je vymezení postupu implementace principů GDPR, který může být využitelný i v jiných společnostech.
OSNOVA: 1) Úvod; 2) Teoretická část - ochrana osobních údajů, GDPR; 3) Praktická část - popis společnosti, informační systémy, zpracování materiálů, vlastní implementace; 4) Závěr.

Seznam doporučené literatury:

BARTÍK, V., JANEČKOVÁ, E. Ochrana osobních údajů v aplikační praxi: vybrané otázky. Praha: Linde Praha, 2013.
MATOUŠOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. Praha: ASPI, 2003.
NEZMAR, L. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017.
NULÍČEK, M. GDPR. Obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017.

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Šikýř Martin, Ph.D., Oddělení manažerských studií

Jméno a pracoviště konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: 4.5.2018 Termín odevzdání diplomové práce: 11.1.2019

Platnost zadání diplomové práce: 30.9.2019

Podpis vedoucí(ho) práce | Podpis vedoucí(ho) ústavu/katedry | Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

24.5.2018
Datum převzetí zadání

Podpis studenta(ky)

MRÁZOVÁ, Pavla. *Implementace principů GDPR ve společnosti AF Consult s.r.o.* Praha: ČVUT 2018. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.
Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: 07. 01. 2019 Podpis:

Poděkování

Ráda bych touto cestou poděkovala Ing. Martinu Šikýři, Ph.D., za odborné vedení při zpracování této diplomové práce, za jeho čas, podnětné připomínky a pomoc. Dále bych ráda poděkovala Ing. Vladislavě Balonové, která mi umožnila spolupracovat ve společnosti AF-Consult Czech Republic s.r.o. na praktické části této závěrečné diplomové práce a za její pomoc.

Abstrakt

Tato diplomová práce se zabývá prozkoumáním a implementací principů Obecného nařízení o ochraně osobních údajů (GDPR) ve společnosti AF-Consult Czech Republic, s.r.o. Práce nejdříve teoreticky popisuje problematiku a změny Obecného nařízení a v praktické části je vidět celý proces implementace principů GDPR od případové studie po školení zaměstnanců. Procesy implementace Obecného nařízení ve vybrané společnosti, popsané v praktické části, mohou být přínosem pro jiné společnosti.

Klíčová slova

Osobní údaj, ochrana osobních údajů, GDPR, Obecné nařízení, souhlas se zpracováním osobních údajů, zaměstnanci, správce

Abstract

The thesis deals with the exploration and implementation of the principles of General Data Protection Regulation (GDPR) in AF-Consult Czech Republic, s.r.o. The theoretical part of thesis describes the issues and changes of the General Data Protection Regulation, and in the practical part is the whole process of implementation of GDPR principles from case study to employee training. Processes for implementing the General Regulation in the defined company described in the practical part can be beneficial to other companies.

Key words

Personal data, Personal Data Protection, GDPR, General Regulation, Consent to the Processing of Personal Data, Employee, Data Controller

Obsah

Úvod

Rychlý technologický rozvoj a větší objem sdílených a shromažďovaných informací, působí na posílení ochrany osobních údajů. Žijeme v době, kde nás identifikační údaje doprovází již od narození přidělením rodného čísla a jména. Shromažďování a zpracování informací patří k definičním znakům moderní společnosti. Informace mají ale dvojí účinek. Na jedné straně jsou ty, které pomáhají, například výzkumu a lidskému pokroku, a na druhé straně jsou ty, které se dají určitým způsobem zneužít. Obzvlášť v době digitální, kdy se šíří mnohem rychleji. Tudíž je mnohem důležitější zaměřit se na oblast ochrany osobních a citlivých údajů, jako je například jméno, příjmení, datum narození, zdravotní stav i náboženské vyznání.

Zákon o ochraně osobních údajů, který byl platný do května 2018 již upravoval zacházení s těmito citlivými daty. Evropská unie však přišla s Obecným nařízením (GDPR – General Data Protection Regulation). Obecné nařízení představuje nový právní rámec ochrany osobních údajů v prostoru Evropské unie. Obecné nařízení přísněji upravuje shromažďování a zpracovávání osobních údajů. Údaje by měly být lépe chráněné před volným šířením mezi další osoby a ke každému zpracování by měl být přidělen právní účel nebo souhlas se zpracováním osobních údajů. Cílem Obecného nařízení je sjednotit legislativu upravující ochranu osobních údajů a v co největší míře hájit práva subjektů údajů proti neoprávněnému zacházení s jejich údaji. Celou změnu ochrany osobních údajů podtrhují velké pokuty za nedodržení Obecného nařízení.

Tato diplomová práce se zaměřuje na informace, které popisují fyzické osoby a které zasahují do soukromí člověka, tedy na osobní a citlivé údaje. Zaměřuje se především na osobní údaje v pracovněprávním vztahu, tedy ty, které získává, shromažďuje a zpracovává zaměstnavatel o svých zaměstnancích.

Cílem práce je prozkoumat zavádění nového Obecného nařízení o ochraně osobních údajů (GDPR) ve společnosti AF-Consult Czech Republic s.r.o. a představit návrh implementace jednotlivých principů GDPR z pohledu správce.

V teoretické části je nejdříve vymezení zákona o ochraně osobních údajů a srovnání s novým Obecným nařízením. Následuje popis Obecného nařízení, jaké jsou požadavky, principy a jaké jsou sankce za nedodržení. V praktické části je cílem ukázat implementaci nového Obecného nařízení o ochraně osobních údajů ve společnosti AF-Consult Czech Republic s.r.o. a představit implementaci jednotlivých principů GDPR z pohledu správce. Přínosem práce, který je popsán v závěru, je vymezení postupu implementace principů GDPR, který může být využitelný i v jiných společnostech.

Důvod pro výběr tématu diplomové práce „implementace principů GDPR", je jeho aktuálnost v roce 2018 a přínos pro AF-Consult Czech Republic s.r.o. Přinos pro tuto

společnost tkví v pomoci při zpracování implementace Obecného nařízení, kterou lze vidět v praktické části. Podle praktické části a závěru by se dala implementace Obecného nařízení aplikovat i do jiných společností, zejména do společností s obdobnou strukturou a velikostí.

TEORETICKÁ ČÁST

1 Ochrana osobních údajů

Dříve v České republice ochranu osobních údajů upravoval zákon č. 101/2000 Sb., o ochraně osobních údajů, který je od května 2018 nahrazen Obecným nařízením o ochraně osobních údajů, celým názvem Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (tj. Obecné nařízení o ochraně osobních údajů a dalšími právními předpisy). Nařízení je platné, jak z názvu vyplývá, v rámci Evropské Unie a dalších třech států, které nejsou státy EU. Těmito státy jsou Island, Norsko a Lichtenštejnsko. Oba předpisy upravují především povinnosti správcům a zpracovatelům a subjektům údajů upravují spíše práva.

„Právo na soukromí je chápáno jako nejuniverzálnější nebo nejrozsáhlejší ze všech takzvaných osobnostních práv, chráněných občanským právem." (Mates, 2002, s. 37). Proto by se každá organizace, nejen podniky mající zaměstnance, ale i organizace jako jsou školy, nemocnice anebo obce, měly starat o zabezpečení citlivých a osobních údajů a zabraňovat tak jejich zneužití. Ochrana osobních údajů by měla být součástí lidské slušnosti, ale lidská soutěživost a touha po moci převyšuje tuto základní lidskou vlastnost. Nejen touha po moci, ale i na základě rozvoje informačních technologií, vznikají nové a důkladnější předpisy, týkající se problematiky osobních údajů jako je například Obecné nařízení o ochraně osobních údajů – GDPR.

Osobní údaje jsou v bývalé směrnici z roku 1995 i v GDPR definovány jako „jakékoliv informace týkající se určeného nebo určitelného subjektu údajů" [ÚZ zákona o ochraně osobních údajů a GDPR, hlava 1, § 4, písmeno a)]. Jsou to jakékoliv údaje, které umožňují identifikovat konkrétní osobu. Osobním údajem může být jeden jediný údaj nebo i více údajů, které teprve dohromady umožňují určit osobu. Mezi osobní údaje patří například jméno, adresa, pohlaví, věk, datum narození, e-mailová adresa atp. Další kategorií osobních údajů, pomocí kterých můžeme identifikovat člověka, jsou citlivé osobní údaje. Jde o takové údaje, které vypovídají o politických postojích, etnickém nebo národnostním původu, filozofickém přesvědčení, trestné činnosti anebo zdravotním stavu subjektu údajů (více v kapitole 2.1 Vymezení pojmů).

Změny v České republice nebyly tak velké jako v některých ostatních členských zemích EU, jelikož zákon o ochraně osobních údajů byl z velké části podobný novému Obecnému nařízení. GDPR je více rozsáhlé nařízení a velká změna byla hlavně v oblasti pojetí odpovědnosti správce, kde je přístup tentokrát založený na riziku. „Nové obecné nařízení rozvíjí princip odpovědnosti správce za zpracování tím, že nejen výslovně stanovuje odpovědnost správce za dodržení povinností vyplývajících z Obecného nařízení, ale zároveň mu stanovuje povinnost být schopen soulad doložit." (Žůrek, 2017, s. 24). Mezi další upřesnění již platných úprav, patří povinnost správce zavést organizační opatření (např. vnitřní předpisy a školení zaměstnanců) a technická opatření

(např. pseudonymizace osobních údajů). Více k povinnostem správců v kapitole 2.3 Povinnosti správců.

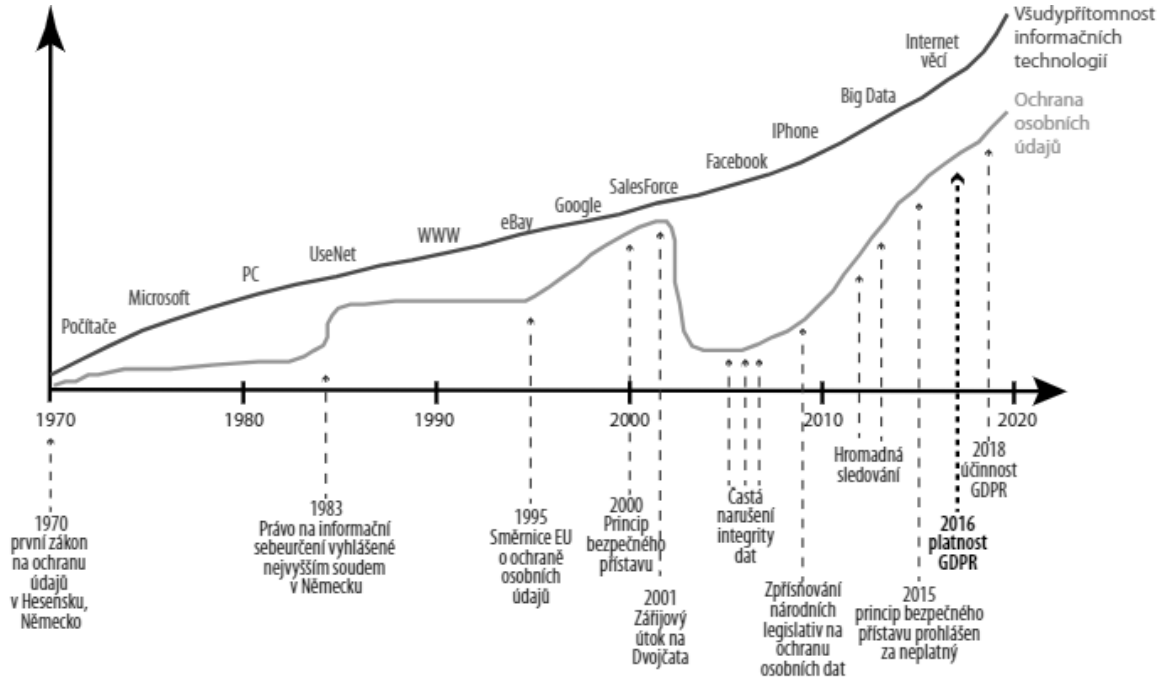
Výrazně byla rozšířena práva subjektů údajů například v oblasti informovanosti a přístupu k vlastním osobním údajům. Mezi nová práva patří například právo „být zapomenut" nebo právo na přenositelnost osobních údajů ve strukturovaném a čitelném formátu. Více o právech subjektů údajů v kapitole 2.2 Práva subjektů údajů.

1.1 Vývoj ochrany osobních údajů

Právní předpisy na ochranu osobních údajů, stejně jako jiná normativní jednání, jsou produktem společenského a technologického vývoje. U nás je zřejmé, že vývoj kopíroval s určitým zpožděním legislativu západní Evropy.

K prvnímu přijetí jakékoli úpravy ochrany osobních údajů došlo „v druhé polovině sedmdesátých let dvacátého století a důvodem pro jejich vydání byl tehdy masově nastupující technologický pokrok v podobě zavádění výpočetní techniky, který sebou přinesl nové hrozby pro soukromí občanů." (Maštalka 2008, s. 11). Další úpravy si žádal i rozvoj sociálně tržního státu, dále globalizace a technologizace životního stylu, kde se rozvíjela potřeba shromažďovat a zpracovávat osobní údaje pro ekonomické a marketingové účely.

První přijetí vnitrostátních předpisů na ochranu osobníc údajů „se opíralo o Úmluvu Rady Evropy č. 108/1981, o ochraně osob, se zřetelem na automatizované zpracování osobních dat." (Maštalka 2008, s. 11). Předchůdce zákona č. 101/2000 Sb., o ochraně osobních údajů, byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Tento zákon však nebyl moc respektován z důvodu nezřízení nezávislého dozorového orgánu nad zpracování osobních údajů. V zákoně 101/2000 Sb., o ochraně osobních údajů již byl tento problém odstraněn. Se vstupem České republiky do Evropské unie se zákon musel novelizovat, aby se vyrovnal s podmínkami Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů.



Obrázek 1 Vývoj technologií v porovnání s vývojem legislativy

Zdroj: Nezmar (2017, s. 15)

Na obrázku 1 lze vidět průběh vývoje technologií v porovnání s vývojem legislativy na ochranu osobních údajů. Například v roce 2003 s příchodem Facebooku se rapidně snížila ochrana osobních údajů, jelikož legislativa zatím neupravovala takový obsah a rozsah šíření osobních údajů. Postupem let opět nabírala legislativa vyšší bezpečnosti, ale i tak lze z grafu vidět, že pokrok sdílení informací je rychlejší než právní úprava ochrany osobních údajů.

1.2 Účel ochrany osobních údajů v pracovněprávních vztazích

Ochrana osobních údajů v pracovněprávních vztazích je oblast, kde se vzájemně prolínají dva základní zákony, a to zákoník práce a zákon o ochraně osobních údajů. Na ochranu osobních údajů mohou dále navazovat speciální právní předpisy, například z občanského zákoníku nebo listiny základních práv EU. Některé další předpisy mohou vymezovat například konkrétní sumu údajů, které správce údajů dále může zpracovávat, nebo dále vymezují zabezpečení daných údajů.

V první řadě se zaměstnavatel nebo správce musí rozhodnout, jaké informace po zaměstnanci bude požadovat. Údaje, které může zaměstnavatel získávat od zaměstnance jsou vymezeny v § 316 odst. 4. zákoníku práce. „Základní pravidlo zní, že zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí

s výkonem práce a se základním pracovněprávním vztahem." (Chládková a Bukovjan, 2015, s. 71)

„Konkrétně by mělo být právní úpravou zajištěno, aby měl zaměstnavatel právo shromažďovat a dále zpracovávat osobní údaje zaměstnance v rozsahu nezbytném pro realizaci svých práv a plnění svých povinností, které mu vyplývají ze zvláštních právních předpisů." (Morávek, 2013, s. 55) Zaměstnavatel nesmí na základě získaných údajů zaměstnance diskriminovat a osobní údaje používat k jinému zpracování, než k čemu bylo shromáždění těchto údajů určené (kapitola 2.4.2 Účel zpracování osobních údajů).

Značnější úpravě zabezpečení osobních údajů se musí věnovat ten zaměstnavatel, u kterého se o osobní údaje zaměstnanců stará větší počet lidí. Správce společně s účelem a dobou trvání zpracování osobních údajů, určuje i ke komu se zpracovávané osobní údaje dostanou a kdo s nimi může dále pracovat. Například u vypracování mezd se k určitým osobním údajům dostane minimálně personalista a mzdová účetní. Proto musí být konkrétně zaznamenáno v účelu zpracování osobních údajů, že pro účely zpracování mezd jsou potřeba osobní údaje jako například jméno, pozice a počet odpracovaných hodin. Dále je pro zpracování mezd důležité potvrzení, že tyto osobní údaje může zpracovávat personalista a mzdová účetní, případně další zainteresované strany.

2 Seznámení s problematikou GDPR

Zákonodární rámec GDPR byl přijat Evropským parlamentem v dubnu 2016 po čtyřech letech diskuzí. Nová legislativa EU, tedy Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation), která přinesla vyšší ochranu osobních údajů občanů, nabyla účinnosti 25. května 2018 a nahradila do té doby platný zákon č. 101/2000 Sb., o ochraně osobních údajů.

Toto nové nařízení vzniklo proto, „aby byla zajištěna jednotná úroveň ochrany fyzických osob v celé Unii a zamezilo se rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu" (Nařízení Evropského parlamentu a Rady [EU] 2016/679, odstavec 13). Hlavním smyslem tohoto předpisu je vyšší harmonizace úpravy ochrany osobních údajů a vytváření stále užších vztahů mezi národy Evropské unie. Nařízením byla posílena práva subjektů údajů, a tedy i kvalitnější kontrola zacházení s osobními údaji lidí. Rovněž došlo k přesnějšímu vymezení povinností správců a zvýšení sankcí za jejich porušení. Všechny dosavadní zásady ochrany a zpracování osobních údajů, na kterých unijní systém stál, přešel na Obecné nařízení (GDPR).

Obecné nařízení se týká všech společností Evropské unie, které jakýmkoli způsobem zpracovávají a uchovávají údaje zaměstnanců a zákazníků, dále pak i obcí a organizací jako jsou školy a nemocnice. Taková společnost nebo organizace je nazývána správcem osobních údajů. Obecným nařízením se musí řídit i zpracovatel, který pro správce osobní údaje zpracovává. GDPR se týká všech činností spojených se zpracováním, uchováním a shromažďováním osobních údajů ve výše zmíněných organizacích.

Naopak se Obecné nařízení nevztahuje na zpracování osobních údajů právnických osob a netýkají se ho ani „činnosti fyzické osoby [čl. 2 odst. 2 písm. c) Obecného nařízení], při kterých jsou zpracovávány osobní údaje výlučně pro osobní či domácí činnost. Dále je z působnosti Obecného nařízení vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení." (Nezmar, 2017, s. 29)

Hlavním subjektem, kterého se nařízení týká, a který uplatňuje svěřené pravomoci za účelem plnění stanovených úkolů je Úřad pro ochranu osobních údajů. Kromě správců a zpracovatelů z Evropské unie se Obecným nařízením musí řídit i organizace z Islandu, Norska a Lichtenštejnska.

2.1 Vymezení pojmů

V této kapitole jsou popsány jednotlivé pojmy, které se týkají této diplomové práce a problematiky Obecného nařízení. Obecné nařízení je upravuje takto:

- **Osobní údaj**

Definice osobního údaje byla již krátce zmíněna v kapitole 1 Ochrana osobních údajů, kde Nařízení Evropského parlamentu říká, že „osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby; veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě." (Nařízení Evropského parlamentu a Rady [EU] 2016/679, čl. 4, odst. 1).

- **Zpracování**

Zpracováním se rozumí „jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, omezení, výmaz nebo zničení." (Žůrek, 2017, s. 30).

- **Zpracovatel**

„Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce." (Nařízení Evropského parlamentu a Rady [EU] 2016/679, čl. 4, odstavec 8). Mezi správcem a zpracovatelem musí být uzavřená písemná smlouva o účelu a povaze zpracování, o jaké osobní údaje se bude jednat a po jakou dobu se budou osobní údaje zpracovávat.

- **Správce**

Správcem je, dle Obecného nařízení „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů." (Nařízení Evropského parlamentu a Rady [EU] 2016/679, čl. 4, odstavec 7). Správce provádí zpracování a odpovídá za něj. Může také zmocnit nebo pověřit zpracovatele, aby zpracoval osobní údaje, ale předání zpracování osobních údajů správce nezbavuje odpovědnosti za zpracování.

- **Souhlas se zpracováním osobních údajů**

Souhlas se zpracováním osobních údajů udává subjekt údajů, který je dle Obecného nařízení definován jako „jakékoli vyjádření svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení." (Nařízení Evropského parlamentu a Rady [EU] 2016/679, odstavec 32).

2.2 Práva subjektu údajů

Obecné nařízení – GDPR posiluje práva subjektů údajů zejména v oblasti přístupu a informovanosti. Každý má právo na přístup k osobním údajům, opravu, smazání údajů, dále pak právo na omezení zpracování a právo vznést námitku kontrolnímu úřadu.

Každý občan má právo být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, na jaké období budou údaje uchovávány a také ke komu se osobní údaje o subjektu dostanou. Změnou mezi zákonem o ochraně osobních údajů a Obecným nařízením je právo na přenositelnost dat nebo právo tzv. být zapomenut.

- **Právo na informace**

Právo na informace zaručuje subjektu údajů být informován o zpracování jeho osobních údajů. U subjektu údajů jde o pasivní právo a u správce jde o aktivní povinnost. Správce musí informovat subjekt údajů o zpracování a účelu osobních údajů automaticky.

- **Právo na přístup k osobním údajům**

Na rozdíl od práva na informace, je právo na přístup k osobním údajům, aktivním právem subjektu údajů. Jde o právo získat od správce potvrzení, k čemu a jak zpracovává dané osobní údaje. Pokud se subjekt údajů rozhodne toto právo využít a správce údaje zpracovává, má subjekt údajů právo získat přístup k následujícím informacím (Janečková, 2018, s. 21):

- účel zpracování;
- příjemci nebo kategorie příjemců, kterým osobní údaje byly zpřístupněny;
- plánovaná doba, po kterou budou osobní údaje uloženy;
- právo požadovat od správce opravu;
- právo podat stížnost u dozorového úřadu;
- veškeré dostupné informace o zdroji osobních údajů.

- **Právo na opravu a doplnění**

Dle článku 16 Obecného nařízení i dle § 21 Zákona o ochraně osobních údajů, má právo subjekt údajů na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se týkají subjektu údajů. S přihlédnutím k účelům zpracování, má právo i na doplnění neúplných osobních údajů. Právo na opravu nebo doplnění informací navazuje na povinnost správce osobních údajů zpracovávat přesné a aktualizované údaje.

- **Přenositelnost údajů**

„Zcela novým právem je v Obecném nařízení právo na přenositelnost údajů, které umožňuje subjektu údajů získat osobní údaje, jež poskytl správci a které se ho týkají, ve strukturovaném, běžně používaném a strojově čitelném formátu a zároveň tyto

údaje předat jinému správci, a to i prostřednictvím původního správce. A to v případě, že zpracování je založeno na souhlasu subjektu údajů nebo na smlouvě a provádí se automatizovaně." (Žůrek, 2017, s. 136).

Toto nové právo občanů na přenositelnost údajů je podobné právu na přístup k osobním údajům, ale podstatným rozdílem je právě stanovený formát, ve kterém se údaje poskytují. Údaje se musí přímo týkat subjektu údajů, takže se právo na přenositelnost údajů nevztahuje na anonymní údaje (kapitola 3.1.3 Zabezpečení osobních údajů).

- **Právo na výmaz tzv. právo být „zapomenut"**

Právo subjektu údajů být „zapomenut" nebo právo na to, aby jeho osobní údaje byly vymazány. Právo, které umožňuje, aby správce vymazal osobní údaje, pokud je dán alespoň jeden z níže uvedených důvodů (Nezmar, 2017, s. 37):

- osobní údaje již nejsou potřebné pro stanovený účel, pro který byly shromažďovány nebo jinak zpracovány;
- subjekt údajů odvolá svůj souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování;
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
- osobní údaje byly zpracovány protiprávně;
- osobní údaje musí být vymazány ke splnění právní povinnosti.

Právo na výmaz se dle článku 17 odst. 3 Obecného nařízení neuskuteční, pokud je zpracování dále nezbytné:

- pro výkon práva na svobodu projevu a informace;
- pro splnění právní povinnosti;
- z důvodu veřejného zájmu v oblasti veřejného zdraví;
- pro účely archivace ve veřejném zájmu;
- pro určení, výkon nebo obhajobu právních nároků.

2.3 Povinnosti správců

Obecné nařízení ukládá povinnost zavést tzv. správce (kapitola 2.1 Vymezení pojmů – správce), který je zodpovědný za všechny změny týkající se osobních údajů. Správce je hlavní odpovědná osoba nebo více osob, která ručí, že implementace principů GDPR bude zpracována korektně a že údaje, za které nese odpovědnost, budou zpracovány pouze v souladu s požadavky Obecného nařízení. Činnosti implementace se týkají zejména těchto oblastí:

- implementace nezbytné ochrany dat,
- informovat zaměstnance, kdo a jaké osobní údaje zpracovává, k jakému účelu tak činí, zda je předává třetím osobám a kdo má k osobním údajům přístup,
- vypracování posouzení vlivu na ochranu osobních údajů,
- vedení záznamů o činnostech zpracování,

- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů.

Správce je v první řade povinen zajistit, aby všechna práva subjektů údajů byla splněna nebo byl umožněn jejich průběh, tedy aby správce nediskriminoval subjekt údajů. „Správce je povinen zavést vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, které jsou pro každý konkrétní účel daného zpracování nezbytné. (časopis IT Systems 1-2/2018, čl. GDPR od A do Z, str. 44). Dále by správce měl informovat subjekty údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Dále musí správce informovat subjekt údajů o jakékoli změně nebo výmazu tzv. oznamovací povinnost nebo také oznámení o ochraně osobních údajů. Správce musí subjekt údajů informovat o jeho právu na přístup k osobním údajům, právu na opravu osobních údajů, jakož i o právech, požádat správce nebo zpracovatele o důvodu zpracování, popř. požadovat odstranění nedostatků při rozporech při zpracování.

Pokud správce/zaměstnavatel zpracovává osobní údaje, je povinen oznámit Úřadu pro ochranu osobních údajů, že bude z pracovněprávní oblasti zpracovávat osobní údaje svých zaměstnanců. Toto oznámení musí obsahovat (Mzdy od A do Z, 2013, s. 45):

- identifikační údaje správce,
- účel nebo účely zpracování,
- kategorie subjektů údajů a osobních údajů,
- popis způsobu zpracování osobních údajů,
- místo nebo místa zpracování osobních údajů,
- příjemce,
- popis opatření k zajištění požadované ochrany osobních údajů.

„Oznamovací povinnost zaměstnavatele se nevztahuje na zpracování osobních údajů, které jsou součástí evidencí veřejně přístupných, nebo na osobní údaje, jejichž zpracování je zaměstnavateli uloženo zákonem.“ (Mzdy od A do Z, 2013, s. 46)

Správce je povinen zajistit implementaci Obecného nařízení ve své organizaci a odpovídá za všechny změny, proto je více informací o povinnostech a činnostech správců popsáno v kapitole 3.1 implementace v organizaci.

2.3.1 Odpovědnost správce

„Klíčovou složkou principu odpovědnosti je v souladu s čl. 24 odst. 1 Obecného nařízení přijímání technických a organizačních opatření pro zajištění souladu s Obecným nařízením a schopnosti soulad prokázat na základě komplexního posouzení, ve kterém správce přihlédne k povaze, rozsahu, kontextu a účelům zpracování a k různě

závažným a pravděpodobným rizikům pro práva a svobody, která zpracování představuje." (Nulíček a kol., 2017, s. 247)

Ustanovení Obecného nařízení ukládá správci povinnost odpovědnosti, za dohled nad procesem zpracování osobních údajů. Správce vždy musí vědět o tom, kdo, kde a jak zpracovává osobní údaje subjektů údajů. To platí i v případě, že správce předá zpracovateli osobní údaje ke zpracování, a ten je bez dovolení správce nesmí předat dál jinému zpracovateli.

Na základě odpovědnosti z Obecného nařízení plyne, že správce, a v omezeném rozsahu i zpracovatel, musí „posoudit rizika pro práva a svobody fyzických osob, která jsou se zpracováním spojena, a podle významu těchto rizik uplatnit některá opatření k zajištění souladu s GDPR." (Nulíček a kol., 2017, s. 248)

2.3.2 Záznamy o činnostech zpracování

Záznamy o činnostech zpracování do jisté míry představují náhradu za oznamovací povinnost, která byla zrušena Obecným nařízením. Pokud se na ně nevztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, jsou správce a zpracovatel povinni vést záznamy s určitými informacemi. Těmito záznamy může správce prokázat soulad zpracování s Obecným nařízením. (Nezmar, 2017, s. 31)

Aby správce nebo zpracovatel mohl doložit soulad s Obecným nařízením, měl by vést záznamy o činnostech zpracování osobních údajů, za které odpovídá. Správci a zpracovatelé by měli být povinni spolupracovat s dozorovým úřadem. Pokud dozorový úřad požádá, musí mu správci a zpracovatelé záznamy zpřístupnit, aby na jejich základě mohly být operace zpracování monitorovány.

Dle článku 30 odst. 1 Obecného nařízení by měl „každý správce a jeho případný zástupce vést záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace (Obecné nařízení, čl. 30, odst. 1):

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
b) účely zpracování;
c) popis kategorií subjektů údajů a kategorií osobních údajů;
d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;

g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

Záznamy o činnostech zpracování se nevztahují na podnik nebo organizaci s méně než 250 zaměstnanci. Ale „bez ohledu na počet zaměstnanců je správce nebo zpracovatel povinen vést záznamy o takovém druhu zpracování, které (Nulíček a kol., 2017, s. 310):

a) pravděpodobně představuje riziko pro práva a svobody subjektů,
b) není příležitostné nebo
c) zahrnuje
    a. zvláštní kategorii údajů, tj. citlivé údaje, nebo
    b. osobní údaje, které se vztahují k rozsudkům v trestních věcech a k trestným činům."

2.4 Hlavní principy GDPR

Obecné nařízení stanovuje základní principy ochrany osobních údajů, podle kterých by se měly spravovat osobní údaje v organizacích. Od principů se dále odvíjí veškerá činnost implementace GDPR v organizacích.

Hlavní principy Obecného nařízení nejsou žádnou novinkou, tyto zásady byly upravovány v zákoně 101/2000 Sb., o ochraně osobních údajů. Pokud se jimi organizace řídily, tak s novým nařízením šlo jen o pozvednutí úrovně ochrany zpracování. Pokud se jimi organizace neřídily, došlo u organizací k velkým změnám. V Obecném nařízení je upravuje čl. 5, písmena a-f:

d) zákonnost, korektnost a transparentnost;
e) účelové omezení;
f) minimalizace údajů;
g) přesnost;
h) omezení uložení;
i) integrita a důvěrnost.

Správce odpovídá za dodržení všech principů Obecného nařízení a musí být schopen doložit toto dodržení zpracování osobních údajů.

2.4.1 Zákonnost, korektnost a transparentnost

Správce osobních údajů, by měl poskytovat subjektu údajů stručné, srozumitelné a snadno dosažitelné informace o zpracování jeho osobních údajů. „Subjekt údajů musí být informován o tom, jaké zpracování bude probíhat – transparentnost, zpracování musí odpovídat poskytnuté informaci – korektní a zpracování údajů musí odpovídat požadavkům kladeným nařízením – zákonné." (Nezmar, 2017, s. 52).

V rámci principu transparentnosti nesmí správce zatajovat účel subjektu údajů, pro který jsou osobní údaje zpracovávány. Také by měl poskytnout subjektu údajů informace o tom, kdo a jak nebo v jakém rozsahu osobní údaje zpracovává a zda jsou předávány někomu dalšímu.

2.4.2 Účel zpracování osobních údajů

Zpracování osobních údajů je možné pouze pro jasné, výslovně vyjádřené a zákonné účely. Toto tvrzení odpovídá §5 odst.1 písm. f) zákona o ochraně osobních údajů, kde upravuje povinnosti správce. „Správce je povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení §3 odst. 6 (kapitola 2.2 Koho se GDPR týká – pozn. stejné jako čl. 2, odst. 2 Obecného nařízení), nebo pokud k tomu dal subjekt údajů předem souhlas (kapitola 3.2 Souhlas se zpracováním osobních údajů)." [Zákon o ochraně osobních údajů a GDPR 2017, § 5, odst. 1, písm. f)].

Správce může účel zpracování stanovit přímo, jako jsou doprovodné činnosti k účelu podnikání, nebo účel může představovat činnost správce, pro kterou potřebuje zpracovávat osobní údaje. „Velmi často jde o zákonem stanovenou povinnost správce, se kterou souvisí nutnost zpracování osobních údajů, nebo jde rovnou o explicitně stanovenou povinnost zpracovávat osobní údaje pro určitý účel a většinou i ve stanoveném rozsahu." (Žůrek, 2017, s. 56).

Účel zpracování musí být prokazatelný a nesmí být protizákonný. Osobní údaj může mít vícero účelů zpracování, přičemž se uplatní právní tituly jejich zpracování a shromažďování (zákonem stanovená povinnost, plnění smlouvy, souhlas). Účely mohou mít různou délku doby, po kterou se údaje mohou zpracovávat a uchovávat a pozbytím jednoho účelu nebo souhlasu nezaniká daný údaj, jelikož je údaj zpracováván ještě pro jiný účel.

2.4.3 Minimalizace údajů

Obecné nařízení v článku 5 písm. c) definuje minimalizaci údajů jako: „Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány."

Správce by měl určit minimální množství osobních údajů, které jsou potřeba k naplnění cíle podnikání. Měl by uchovávat pouze nezbytné osobní údaje o subjektu údajů, tzn. přesně tolik informací, kolik je potřeba, které jsou dané účelem zpracování. Určitě by správci neměli uchovávat informace, které jsou nadbytečné a nepotřebné nebo jakýmkoli způsobem doplňující k potřebným informacím.

Princip minimalizace údajů je považován i jako bezpečnostní prvek, jelikož čím méně osobních údajů správce shromažďuje a zpracovává, tím se snižuje riziko subjektu údajů úniku jeho údajů a následnému obvinění správce údajů a pokutám zaměstnavateli.

Tento princip je zahrnutý i v článku 25 odst. 2 Obecného nařízení, který ukládá správci povinnost „zavést vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti."

2.4.4 Přesnost údajů

Mezi další principy Obecného nařízení patří správnost a přesnost osobních údajů, které správce zpracovává. Informace o sobě mohou poskytovat samy subjekty údajů nebo je organizace získává pomocí třetích stran. Aby byly údaje přesné měl by správce údajů (Nezmar, 2017, s. 63):

- realizovat přiměřené kroky k zajištění přesnosti všech osobních údajů, které získá a zpracovává;
- zajistit, aby byl zdroj osobních údajů jasný a nezpochybnitelný;
- pečlivě zvážit veškeré problémy či nejasnosti ohledně přesností informací;
- zvážit, zda je nutné a jak často informace aktualizovat.

Tento princip ale neukládá povinnost správci údajů, „aby aktivně vyhledával nepřesné údaje nebo aby se opakovaně obracel na subjekt údajů s žádostí o aktualizaci osobních údajů. Správce však předně musí v případě žádosti subjektu údajů, nebo pokud sám narazí na zjevně nepřesné údaje, přijmout rozumné opatření k tomu, aby byly nepřesné osobní údaje s přihlédnutím k účelům, pro které se zpracovávají, vymazány nebo opraveny." (Žůrek, 2017, s. 61)

2.4.5 Omezení uložení údajů

Omezení uložení údajů znamená v jednoduchosti, aby správce osobních údajů neshromažďoval osobní údaje déle, než je potřebné pro stanovený účel a stanovenou dobu zpracování osobních údajů. Toto pravidlo ovšem neplatí, pokud zákon stanovuje delší lhůty archivace některých dokumentů.

Obecné nařízení konkrétní lhůty neukládá, jen ukládá povinnost správci údajů nejdříve stanovit na jak dlouho a za jakým účelem uchovávat informace a následně kontrolovat dobu uchovávání osobních údajů. Po uplynutí stanoveného účelu a uplynutí doby, po kterou se údaje mohly zpracovávat, musí správce údajů bezpečně smazat či jinak zlikvidovat nebo archivovat zastaralé osobní údaje.

Účelem stanovení doby zpracovávání osobních údajů je, aby se organizace vyvarovala riziku, že informace budou zastaralé a budou používány chybně, což je v rozporu s principem přesnosti. „Délka doby uchování osobních údajů závisí na účelu, pro který byly získány, a na jejich povaze. Pokud je nezbytné uchovávat údaje z důvodů existence zákonného nařízení, jakým je například zákon o archivnictví, účetnictví atd., měla by organizace informace uchovat tak dlouho, dokud je tento důvod platný a relevantní. Na druhou stranu, informace s pouze krátkodobou hodnotou by měly být během několika dnů smazány." (Nezmar, 2017, s. 67)

2.4.6 Integrita a důvěrnost

Posledním principem je integrita a důvěrnost. „Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením." [Zákon o ochraně osobních údajů a GDPR 2017, čl. 5, písm. f)].

Nařízení opět neukládá přesné povinnosti správců, jak zabezpečit zpracování osobních údajů před neoprávněným zneužitím. Jelikož opatření, které jsou vhodné pro organizaci závisí na mnoha faktorech, například na firemní kultuře, pravidlech organizace, náhledu na bezpečnost, povaze informací atp.

Pro soulad s posledním principem GDPR musí organizace (Nezmar, 2017, s. 74):

- navrhnout a uspořádat svou bezpečnost tak, aby odpovídala povaze osobních údajů, které uchovává, a zabránit nebo minimalizovat škody, které mohou vzniknout v důsledku porušení bezpečnosti;
- jasně stanovit, kdo v organizaci odpovídá za zajištění bezpečnosti informací;
- ověřit, zda má správné fyzické a technické zabezpečení, včetně spolehlivého a dobře vyškoleného personálu;
- být připravena reagovat na jakékoli narušení bezpečnosti rychle a efektivně, tedy mít zpracovány náležité procesy a postupy pro tyto případy.

„Zabezpečení osobních údajů při jejich zpracování musí vždy odpovídat povaze, rozsahu, kontextu a účelům zpracování." (Žůrek, 2017, s. 63)

2.5 Dozorový orgán a sankce

Kontrolu uplatňování GDPR v organizacích má na starosti dozorový úřad. Jeho cílem je chránit základní práva a svobody subjektů údajů v souvislosti se zpracováním jejich osobních údajů. Každý dozorový úřad je kompetentní k výkonu pravomocí udělených Obecným nařízením na území příslušného státu.

Dozorový úřad musí zajistit, aby „ukládání správních pokut bylo účinné, přiměřené, ale zároveň odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu, a to kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j) obecného nařízení. Podstatné tedy je, že nikoli za každé porušení Obecného nařízení musí být udělena pokuta, ale správce může být například nejprve upozorněn, že zamýšlené operace zpracování pravděpodobně porušují Obecné nařízení, nebo může být správci, jehož operace zpracování porušily Obecné nařízení, uděleno napomenutí nebo mu může být nařízeno, aby vyhověl žádosti subjektu údajů. Správci může být mezi dalšími též nařízeno uvést zpracování do souladu s obecným nařízením atd." (www.uoou.cz online 7.11.2018)

Nejvyšší možné pokuty jsou rozděleny do dvou kategorií, a to na pokuty pro orgány veřejné moci a pro ostatní subjekty. Pro orgány veřejné moci je maximální výše pokuty nižší než u ostatních, jelikož placení udělených pokut plyne zpravidla z veřejných rozpočtů. Maximální výše pokuty pro tyto orgány je 10 000 000 EUR a pokud jde o podnik, jsou to až 2 % z celkového celosvětového ročního obratu (podle toho, která hodnota je vyšší).

Porušení, která budou pro správce připadat v úvahu v první kategorii jsou (Žůrek, 2017, s. 183):

- povinnosti při zabezpečení ochrany osobních údajů;
- podmínky pro najmutí a spolupráci se zpracovatelem;
- povinnosti vyhotovit záznamy o činnostech zpracování;
- povinnosti při ohlašování, resp. Oznamování případu porušení zabezpečení osobních údajů dozorovému úřadu a subjektu údajů;
- povinnosti posoudit vliv na ochranu osobních údajů atd.

Dle Žůrka obsahuje druhá kategorie závažnější porušení, za které lze udělit pokutu do výše 20 000 000 EUR a jde-li o podnik, tak až do výše 4 % celkového celosvětového ročního obratu (podle toho, která hodnota je vyšší).

Porušení, za která mohou být správci pokutováni v druhé kategorii jsou (Žůrek, 2017, s. 184):

- zásady a zákonnosti zpracování;
- podmínky vyjádření souhlasu;
- podmínky pro zpracování zvláštních kategorií osobních údajů;
- práva subjektů údajů;
- podmínky pro předávání osobních údajů do třetí země;
- povinnosti vyplývající z právních předpisů členského státu;
- povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem;
- nesplnění správy dozorového úřadu.

Pokuty se nebudou udělovat vždy v nejvyšší možné hodnotě, budou se udělovat postupně „např. společnosti může být udělena pokuta ve výši 2 % z ročního obratu za to,

že její záznamy nejsou v pořádku, neoznámí dohlížejícímu orgánu a subjektu údajů porušení nebo nevykonává posouzení dopadů." (DPO4U.cz online 7.11.2018). Na pokuty bude dozorový orgán přistupovat k přihlédnutí ke stavu vybavení, nákladům na provedení, charakteru, rozsahu a účelům zpracování.

Na druhou stranu maximální výše pokuty může být udělena velkým nadnárodním organizacím i malým soukromým firmám. Stejně tak je důležité si uvědomit, že pravidla Obecného nařízení a podrobování kontrole dozorovým úřadem se musí řídit jak správce, tak i zpracovatel.

3 GDPR v organizacích

Implementace GDPR do organizací je velký krok pro všechny určené správce, kteří jsou povinni zajistit soulad se všemi principy Obecného nařízení ve své organizaci a jsou zodpovědní tento soulad dokázat. Informace lze čerpat z různých zdrojů, ale všechny jsou jen obecnou formou postupu, jak by implementace měla v daném podniku vypadat. Proto každý správce musí zvolit jedinečný postup implementace, která bude šitá na míru prostředí, kultuře a předpisům dané společnosti. V této kapitole jsou popsány jednotlivé kroky implementace GDPR od případové analýzy po školení.

3.1 Implementace v organizaci

Prvním krokem implementace je mapování osobních údajů, to znamená, v jakých oblastech se v organizaci zpracovávají osobní údaje, těmito oblastmi může být personalistika, mzdová agenda, obchodní agenda, přístupy do objektu, bezpečnost, vlastní realizace činnosti – poskytování zboží, služeb a oblast ICT. Je potřeba identifikovat všechny tyto oblasti, kde dochází ke zpracování osobních údajů, a to nejen v elektronické podobě na cloudových úložištích, ale i ve fyzické podobě např. v kartotékách a pořadačích.

Každý osobní údaj, který společnost zpracovává, musí být odůvodněný a mít určený právní titul zpracování a lhůtu, po kterou se údaj bude moci zpracovávat. Dále pak musí organizace určit konkrétní zaměstnance, kteří s danými údaji budou moci pracovat.

Hlavním cílem takové analýzy je identifikovat, jaké osobní údaje organizace zpracovává nad rámec, a které se ze zpracování musí vyřadit. Pravidlem Obecného nařízení je zpracovávat pouze nezbytné množství údajů, po nezbytně nutnou dobu. V tomto kroku jsou obsaženy všechny principy GDPR popsané v kapitole 2.4 Hlavní principy GDPR. V dalších podkapitolách jsou popsány jednotlivé kroky implementace v organizaci.

3.1.1 Analýza

Po zmapování zpracování osobních údajů následuje analýza současného stavu zajištění osobních údajů neboli posouzení míry shody současného stavu organizace s požadavky GDPR. K takovému rozboru je nejlepší GAP analýza (doslova analýza mezer), která se „používá k definování rozdílu mezi současným stavem a stavem požadovaným." (Nezmar, 2017, s. 96)

GAP analýzou, která je implementovaná na zavedení GDPR, se zjistí rozdíly (mezery) porovnáním současného stavu, který je dán vnitřními předpisy a managementem společnosti s pravidly danými Obecným nařízením.

Výstupem GAP analýzy by měly být zjištěné nálezy a návrh úprav vnitřních procesů v návaznosti na GDPR. Výstup pomůže organizaci identifikovat rizika spojená se změnami, dále by měla ukázat všechny oblasti, kde je zapotřebí změna k dosažení souladu s Obecným nařízením a určí úroveň IT zabezpečení osobních údajů.

3.1.2 Posouzení vlivu

Posouzení vlivu zpracování osobních údajů (anglicky Data Protection Impact Assessment – DPIA) je nová povinnost, kterou upravuje Obecné nařízení. Posouzení vlivu rizik je „proces, jehož cílem je popsat zpracování, posoudit nezbytnost a přiměřenost zpracování a napomoci zvládnutí rizik pro práva a svobody fyzických osob vyplývající ze zpracování osobních údajů." (Nezmar, 2017, str. 99)

„Posouzení vlivu se provádí pro zamýšlené operace zpracování před jejich provedením. Podle čl. 35 odst. 1 Obecného nařízení může pro více operací zpracování, které jsou si podobné a představují podobné riziko, stačit pouze jedno posouzení. Povinnost provádět posouzení vlivu na ochranu osobních údajů ve stanoveném rozsahu dle čl. 35 odst. 7 Obecného nařízení se vztahuje pouze na (Nulíček a kol., 2017, s. 341):

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

c) rozsáhlé systematické monitorování veřejně přístupných prostorů; (Zákon o ochraně osobních údajů a GDPR 2017, čl. 35, odst. 1)

d) zpracování, které označil za rizikové dozorový úřad;

e) zpracování, u kterého existuje pravděpodobnost, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

„Posouzení vlivu na ochranu osobních údajů poslouží i jako nástroj pro plnění souladu a jeho prokazování, protože si správce bude vědom vysokého rizika, které jeho zpracování pro subjekty údajů představuje, a proti těmto vysokým rizikům, resp. pro jejich zmírnění přijme adekvátní prostředky. Ostatně i samotné vypracování posouzení vlivu na ochranu osobních údajů a uskutečnění předchozí konzultace bude plněním a prokazováním souladu zpracování." (Žůrek, 2017, s. 116)

3.1.3 Zabezpečení osobních údajů

Zabezpečení osobních údajů upravoval již zákon č. 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů, tudíž toto pravidlo není úplně nové, v Obecném nařízení je jen lehce upraveno. Správce musí zpočátku zhodnotit rizika, která při zpracování osobních údajů hrozí, následně „musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením." (Nezmar, 2017, s. 40)

Rizika, která mohou osobním údajům hrozit, jsou dle čl. 32 Obecného nařízení hrozby narušení důvěrnosti a integrity zpracování. Dle čl. 32 odst. 2 Obecného nařízení je nutné zohlednit následující rizika:

- náhodné nebo protiprávní zničení,
- ztráta,
- pozměňování,
- neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo
- neoprávněný přístup k nim.

„Při posuzování rizik by správce neměl myslet pouze na rizika, která představují porušení zabezpečení IT systémů. Důkladně by měl zvážit i rizika, která představují lidský faktor, fyzické prostředí, a nakonec i bezpečnost, kterou poskytují při zpracování subdodavatelé a obchodní partneři." (Nulíček a kol., 2017, s. 315)

Pro snížení rizik by měl správce přijmout některá opatření, které upravuje čl. 32 odst. 1 Obecného nařízení – Zabezpečení zpracování.

- **Pseudonymizace a šifrování údajů.**
  „Pseudonymizace je bezpečnostní opatření, při kterém jsou odděleny přímé identifikátory fyzických osob, jako je např. jejich jméno nebo rodné číslo, od ostatních údajů, které se jich týkají.

  Šifrování je opatření, při jehož implementaci jsou osobní údaje převedeny do podoby, která není čitelná bez znalosti speciálního šifrovacího klíče." (Nulíček a kol., 2017, s. 316)

- **Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování.**
  Opatření důvěrnosti je nepostradatelná úroveň míry utajení v každém momentu, kdy dochází ke zpracování údajů a je zaručena prevence jejich vyzrazení mimo subjekt údajů a zpracovatele.

  Opatřením integrity je zabezpečeno, že data jsou správná, s korektním obsahem a jsou realizována opatření proti jejich změně.

Opatření dostupnosti cílí na to, aby byly k dispozici záložní zdroje při výpadku nějakého systému.

Posledním opatřením tohoto bodu je opatření k zajištění odolnosti systémů zpracování. „Odolností se rozumí schopnost jednotlivých prvků systémů či služeb zpracování odolávat různým selháním a zachovat funkcionalitu a bezpečnost celku v případě selhání." (Nulíček a kol., 2017, s. 318)

- **Schopnost včas obnovit dostupnost osobních údajů a přístup k nim, v případě fyzických či technických problémů.**
  Opatření schopnosti včas obnovit dostupnost osobních údajů, se vztahuje na případy, kdy dojde k fyzickému či technickému incidentu znemožňující přístup k osobním údajům. A toto opatření má urychlit pozdější obnovení dostupnosti osobních údajů. (Nulíček a kol., 2017, s. 318)

- **Pravidelné testování a hodnocení účinnosti zavedených technických opatření.**
  K pravidelnému testování účinnosti bezpečnostních systémů, mohou sloužit zavedené pravidelné simulace incidentů nebo pravidelné prověřování IT systémů. Pravidelné testování může být prováděno interními systémy, ale mohou být prováděny i audity ze strany externích společností.

3.1.4 Dokumentace schopnosti prokázat soulad s požadavky

Schopnost prokázat soulad s požadavky GDPR je novým prvkem, který musí správce zajistit. Prokázat soulad s požadavky patří k povinnostem správce a dá se označit jako další zásada principů Obecného nařízení – princip odpovědnosti (kapitola 2.4 – Hlavní principy GDPR). Správce musí zajistit, aby principy Obecného nařízení byly splněny všude, kde dochází ke zpracování osobních údajů.

K zajištění všech principů a práv subjektů údajů bude muset správce vytvořit opatření tvorby některých dokumentů. Takové opatření může obsahovat dokumentaci týkající se:

- řízení;
- struktur managementu a odpovědností;
- šablony odpovědí;
- řízení rizik;
- školení;
- správy záznamů;
- dohody o sdílení údajů;
- ověřování zabezpečení;
- hlášení porušení zabezpečení.

„Organizace by měly v praxi zavést celou řadu politik, zásad a postupů, které zajistí a prokážou dodržování nařízení a dalších příslušných zákonů. Organizace bude muset prokázat celou svou činností, že má dokumentaci a záznamy, které prokazují, že ve skutečnosti dělá to, co teoreticky říká v papírových pravidlech. Musí reálně dojít k prokázání, že principy a související chování jsou plně začleněny do činnosti organizace." (Nezmar, 2017, s. 83)

3.1.5 Směrnice a příručky

Za odpovědnost správce se považuje také zařadit do interních směrnic příručky, resp. politiky, které se týkají ochrany osobních údajů. V těchto příručkách by měl být dostačující popis procesů zpracování osobních údajů a opatření k nim. Dle Nulíčka a kol. (2017, s. 279), by měly tyto politiky splňovat několik kritérií pro zajištění souladu zpracování s Obecným nařízením:

- **Podrobné a srozumitelné**. Sepsané politiky musí jasně vyjádřit povinnosti a postupy při zpracování. V různých oblastech organizace se mohou povinnosti lišit, a proto by měla být daná příručka napsaná z pohledu určité pozice – jiné pro IT oddělení, jiné pro lidské zdroje atd.

- **Možnost posouzení plnění**. Musí být zjistitelné, zda se postupy shodují s politikami společnosti.

- **Proveditelnost**. Politiky musí být napsané tak, aby byly v budoucnu proveditelné, nesmí být napsané obecnou formou, ale měly by být nastavené přímo na procesy v organizaci.

- **Aktuálnost**. Správce by měl dle procesů a technologií v organizaci aktualizovat směrnice a tyto politiky.

3.2 Souhlas se zpracováním osobních údajů

Do zákonného zpracování patří právní tituly, které byly popsány v kapitole 2.4.2 Účel zpracování osobních údajů, a souhlas se zpracováním osobních údajů, kterému se věnuje tato kapitola. „Definice souhlasu je přísnější, než byla u Zákona o ochraně osobních údajů – podle definice GDPR musí být souhlas subjektu údajů svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterou subjekt údajů vyjádří prohlášením nebo jiným potvrzujícím způsobem své svolení se zpracováním osobních údajů. Takže podmínek pro zákonnost zpracování údajů na základě uděleného souhlasu je více než v předchozí úpravě." (Sdělovací technika 12/2017, čl. GDPR změní některé dosavadní zvyklosti, str. 10)

Subjekt údajů by měl mít svobodnou vůli a rozhodnout se, zda souhlas se zpracováním osobních údajů podepíše nebo ne, zaměstnavatel nesmí, dle předchozí definice, nutit k podpisu subjekt údajů. Další částí, kterou správci musí nově stanovit nejen v souhlasu, je konkrétní doba, po kterou budou osobní údaje zpracovávány. V neposlední řadě musí být informace v souhlasu konkrétní a jednoznačné.

Souhlas by měl obsahovat informace jaké údaje subjekt poskytuje a k čemu, po jakou dobu budou osobní údaje zpracovávány, kým budou zpracovávány, poučení o odvolání se dozorčímu orgánu a možnost zrušení souhlasu.

Zrušením souhlasu není dotčena právnost zpracování vycházejícího ze souhlasu, který byl udělen před jeho odvoláním. Souhlas byl dán k daným účelům a odvolání souhlasu nemusí pro správce představovat povinnost osobní údaje zlikvidovat, jelikož zde již nastává právní účel pro archivaci (např. archivace mzdových listů). Pro správce nastává povinnost přestat osobní údaje zpracovávat pro daný účel, pro který byl souhlas udělen.

„Pokud je souhlas součástí obsáhlejšího textu (např. v obchodních podmínkách), pak musí být jasně odlišen od textu popisujícího jiné skutečnosti. Text souhlasu musí být pro subjekt údajů srozumitelný, dobře čitelný a umožnit mu právo volby." (časopis Sdělovací technika 12/2017, čl. GDPR změní některé dosavadní zvyklosti, str. 11)

„Souhlas může subjekt údajů vyjádřit jakoukoliv formou. Zvolená forma udělení souhlasu však musí vykazovat prvky jednoznačného potvrzení, že subjekt údajů dává svolení ke zpracování osobních údajů, které se jej týkají. Souhlas tedy může být poskytnut také elektronickou cestou (např. prostřednictvím internetové stránky, nastavením technického zařízení pro poskytování služby informační společnosti apod.). Podstatné ovšem je, že správce musí být schopen udělení souhlasu prokázat po celou dobu zpracování údajů." (časopis Sdělovací technika 12/2017, čl. GDPR změní některé dosavadní zvyklosti, str. 11)

3.3 Školení

Školení zaměstnanců o interních pravidlech ochrany osobních údajů je poslední částí implementace Obecného nařízení. Od května 2018 je školení nutná součást opatření, které vedou k ochraně osobních údajů.

Ke školení by mělo dojít až po dopsání všech vnitřních předpisů, týkajících se zabezpečení osobních údajů. Předpisy by měly být tvořeny v průběhu celé implementace Obecného nařízení, jelikož je jejich sepsání rozsáhlý a časově náročný proces. Vnitřní předpisy slouží jako podklady pro školení a pro budoucí zacházení s osobními údaji.

Školení musí být jak pro vedoucí pracovníky, tak pro ostatní zaměstnance. Zaměstnanci musí být schopni pochopit, co je Obecné nařízení, k čemu slouží, dále pak práci s osobními údaji, jejich zabezpečení a shromažďování. Při školení se správce musí zaměřit i na možná rizika porušení zabezpečení osobních údajů a možné sankce, které by organizaci poté hrozily. „Zaměstnanci musí pochopit, že ochrana osobních údajů úzce souvisí s každodenními pracovními postupy, procesy a návyky, které má organizace nastaveny a zavedeny v oblasti dodržováním ochrany osobních údajů." (Nezmar, 2017, s. 181)

Do školení musí být zařazena oblast rozpoznávání porušení ochrany osobních údajů, jelikož je každý, kdo si porušení všimne, povinen hlásit jej do 72 hodin Úřadu pro ochranu osobních údajů. Zaměstnanci pak budou schopni rozpoznat včas porušení zabezpečení a budou schopni hlásit jej s minimálním časovým rozestupem příslušnému orgánu, tím se částečně vymezí riziko nesouladu s Obecným nařízením a následného postihu.

PRAKTICKÁ ČÁST

4 Charakteristika vybrané společnosti

Předmětem praktické části této diplomové práce je implementace principů GDPR ve společnosti AF-Consult Czech Republic, s.r.o. (dále jen AF CZ) v Pražské pobočce a divizi energetiky. AF v České republice se skládá ze tří divizí, kde se nachází tým inženýrů a specialistů, kteří se zabývají inženýrskými a poradenskými činnostmi v oblasti průmyslu, infrastruktury a energetiky. V následujících kapitolách je popsán předmět činnosti celé společnosti a její náznak vývoje v letech a popis činnosti pobočky AF-Consult Czech Republic, s.r.o.

Zkratky společnosti, které se objevují v praktické části
ÅF – mateřská základna ve Švédsku
AF CZ – pobočka v České republice

4.1 Společnost ÅF

Společnost byla založena již v roce 1895 pod názvem "The Southern Swedish Steam Generator Association", jako první švédské průmyslové sdružení, které se staralo o zájmy vlastníků parních generátorů a jiných tlakových nádob. Až v roce 1964 se spojily dvě společnosti do Ångpanneförening (zkratka „ÅF"), kde se specializovali hlavně na kontroly bezpečnosti parních generátorů a konzultace bezpečnostních opatření. Od té doby prošlo ÅF vývojem od parních elektráren, elektřiny jako takové, jaderné energie a digitalizace. Má několik dceřiných společností a nyní patří společnost ÅF k celosvětově vedoucím poradenským společnostem. Zaměřuje se na inženýrské a projekční poradenství v oblasti energetiky, projekty pro průmysl a infrastrukturu. Vytváří udržitelná řešení pro novou generaci prostřednictvím technologií. Hlavní sídlo je ve Švédsku, ale pobočky má po celé Evropě a klienty po celém světě. Koncem roku 2018 oznámila společnost ÅF fúzi se společností Pöyry, přední evropskou inženýrskou a poradenskou společností.

Hlavním cílem společnosti je soustředit se na udržitelná řešení, jako jsou chytrá města („smart cities"), bezpečnější doprava, průmyslová digitalizace a změny energetických trhů – přejít na udržitelné zdroje a možnost skladování energie.

4.2 AF Consult Czech Republic s.r.o.

AF-Consult Czech Republic, s.r.o. je jedna z poboček nadnárodní skupiny ÅF. AF v České republice vzniklo v roce 2010 akvizicí firem MEACONT Praha spol. s r.o. a jejich dceřiných společností REGULA a. s. a TODO spol. s r.o. švédskou firmou ÅF. Při sloučení firem a vzniku AF-Consult Czech Republic s.r.o. převzala ÅF z těchto firem zejména know-how, kvalifikovaný tým a reference. Stejně jako celá skupina ÅF, poskytuje společnost AF CZ projektové a inženýrské činnosti v oblasti průmyslu, infrastruktury a energetiky.

V Praze jsou zastoupeny prostřednictvím společnosti AF-Consult Czech Republic s.r.o. a její sesterské společnosti AF-CITYPLAN s.r.o. dvě ze čtyř divizí skupiny ÅF, a to divize energetiky a divize infrastruktury.

AF-Consult Czech Republic s.r.o. se zaměřuje především na klasickou a jadernou energetiku, dalšími činnostmi je oblast teplárenství, obnovitelných zdrojů energie a v oblasti podpůrných služeb pro přenosovou soustavu. AF-Consult Czech Republic s.r.o. je autorizovanou společností Energetického regulačního úřadu ČR pro certifikační měření podpůrných služeb. Aby služby byly v souladu s požadavky Energetického regulačního úřadu ČR, je společnost držitelem certifikátů ISO-9001, ISO-14001 a OHSAS 18001.

Služby, které AF-Consult Czech Republic, s.r.o. poskytuje v projektovém řízení jsou:

- studie proveditelnosti,
- technologické posouzení,
- koncepční stude a analýzy,
- podnikatelské záměry staveb,
- Basic a Detail Design.

Další licencované služby, které AF-Consult Czech Republic, s.r.o. poskytuje, jsou:

- technické audity vč. hodnocení životního cyklu (due dilligence),
- dokumentace pro územní a stavební řízení,
- inženýrské služby pro jednání s dotčenými orgány státní správy,
- management kvality,
- plán organizace výstavby,
- autorský dozor,
- technický dozor investora.

Provozní a servisní služby poskytuje zejména v rozsahu:

- zhotovení dokumentace pro provoz a údržbu,
- zhotovení průvodně-technické dokumentace,
- plánování údržbových prací,
- bezpečnostního posouzení,
- školení a tréninku,
- modernizace, prodlužování životnosti a tzv. "backfitting",
- ostatních expertních služeb (např. energetické audity).

Všechny tyto služby poskytuje AF-Consult Czech Republic s.r.o. v oborech: stavební, strojní, elektro, a slaboproudé systémy, ASŘTP a podpůrné služby pro přenosovou soustavu.

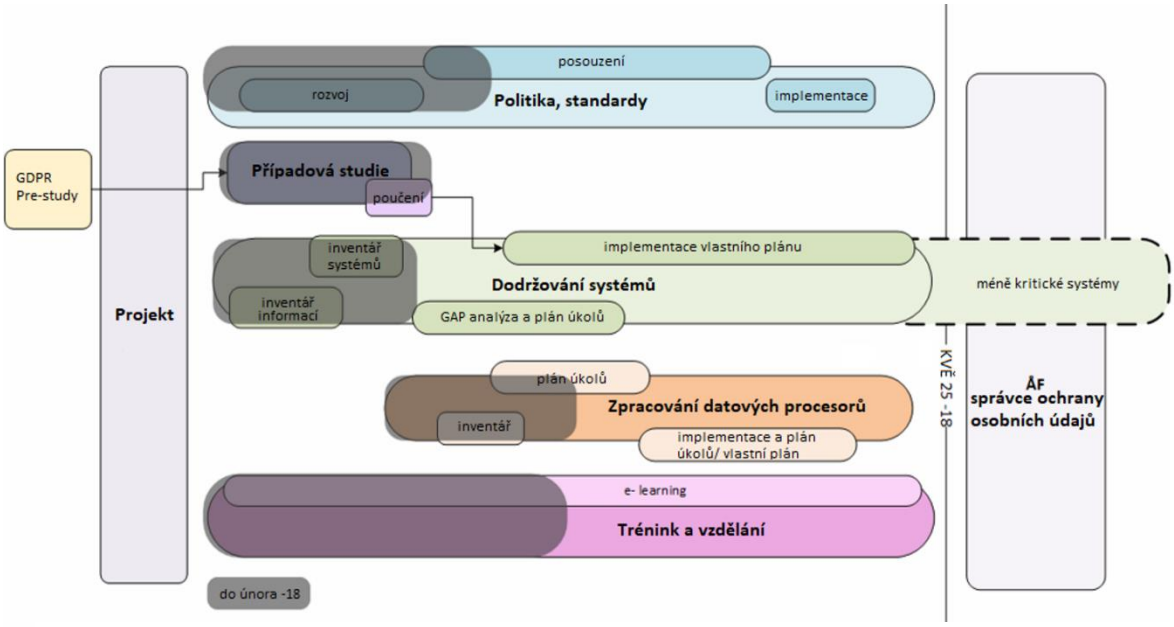
5 Implementace GDPR v AF-Consult Czech Republic s.r.o.

Hlavním smyslem praktické části této diplomové práce je popis implementace GDPR ve společnosti AF-Consult Czech Republic s.r.o. Obecné nařízení je navrhnuto tak, jak již název vypovídá, aby se dalo obecně implementovat na každou organizaci, které se ochrana zpracování osobních údajů týká, a proto není žádný jedinečný postup zavedení pro jednotlivé organizace.

Všechny kroky, které byly v AF-Consult Czech Republic s.r.o. k implementaci GDPR podstoupeny, vedly k tomu, aby veškeré zpracování a shromažďování osobních údajů bylo v souladu s Obecným nařízením k 25. květnu 2018, kdy Obecné nařízení vyšlo v platnost. V praktické části je popsán celý proces od případové studie po závěrečná školení vedoucích pracovníků a zaměstnanců.

Případová studie a počáteční fáze analýz byly vypracovány mateřskou základnou skupiny ÅF ve Švédsku. Tato obecná příprava zajistila všem ostatním pobočkám hladší průběh implementace GDPR a také zajistila, aby zpracování bylo v souladu s kulturou a zásadami společnosti. Mateřská základna ÅF také vypracovala postup implementace GDPR pro všechny společné informační systémy, které jsou sdíleny všemi pobočkami ÅF po světě. Praktická část se týká implementace principů GDPR ve společnosti AF-Consult Czech Republic s.r.o. v České republice, konkrétně v pražské divizi energetiky.

Časový harmonogram, který lze vidět na obrázku 2 – Harmonogram činností, byl stanoven na základě náročnosti jednotlivých úkonů a s ohledem na termín platnosti GDPR.



Obrázek 2 Harmonogram činností
Zdroj: ÅF

Cílem bylo rozvržení dílčích oblastí Obecného nařízení, zvážení, jaká opatření jsou rozumná přijmout a do jakého časového rámce činnost zařadit. Šedivý stín u každé oblasti označuje činnost mateřské základny ÅF a její přípravné činnosti. Ta zajistila počáteční průzkum a vzdělávání v oblasti GDPR pro všechny pobočky. Samotnou implementaci na lokální podmínky a další vzdělávání měla na starost každá jednotlivá pobočka.

Obrázek 3 Postup implementace
Zdroj: AF-Consult Czech Republic s.r.o.

Proces na obrázku 3 ukazuje postup implementace, který byl nastaven v AF-Consult Czech Republic s.r.o. Prvním krokem implementace bylo seznámení se s požadavky GDPR, tedy projít školením od mateřské základny ÅF. Jaké informace si pročíst a definovat stávající stav, tzn. na jakém disku interní databáze nebo případně jiných zdrojích jsou informace o osobních údajích k dohledání.

Druhým krokem byla analýza stavu před implementací GDPR, do které patřilo vytvoření seznamu osobních údajů a systémů, které údaje zpracovávají a jejich náležitosti:

- kdo je zodpovědný za osobní údaje,
- typ údajů,
- legálnost,
- účel osobních údajů,
- minimalizace, přesnost a aktuálnost údajů,
- zabezpečení,
- možná rizika a opatření rizik.

Třetím krokem bylo vytvoření pravidel zpracování osobních údajů a přidělení zodpovědnosti. Do tohoto kroku patří jádro implementace principů Obecného nařízení ve společnosti. Dále i vytvoření všech podkladů, které s osobními údaji souvisí:

- Zásady ochrany osobních údajů,
- Interní směrnice GDPR,
- Standardy ochrany osobních údajů,
- Postupy ochrany osobních údajů,
- příp. modifikace stávajících postupů.

Další tři kroky jsou potřebné k používání a dodržování zásad ochrany osobních údajů v souladu s GDPR, tedy nejdříve zaškolení všech zaměstnanců, vlastní dodržování zásad a následná kontrola postupů a zabezpečení.

5.1 Případová studie

Případová studie v této kapitole, se věnuje analýze stavu zpracování údajů a analýze vnitřních předpisů před implementací GDPR. Analýza stavu v období, kdy ochrana osobních údajů byla upravována zákonem č. 101/2000 Sb. zákon o ochraně osobních údajů, tedy před Obecným nařízením – GDPR. Jak společnost zabezpečovala osobní údaje před nezákonným zpracováním a jak osobní údaje charakterizovala.

AF-Consult Czech Republic s.r.o. je součástí nadnárodní společnosti, která již měla některé principy ochrany osobních údajů automatizované pro všechny společnosti celé skupiny, vždy s přihlédnutím k zákonným úpravám země, ve které společnost sídlí. Osobní údaje byly ukládány jak ve fyzické, tak i v elektronické formě v interních úložištích a některé informace na globálních cloudových úložištích společnosti.

Případová studie s analýzou stavu zpracování osobních údajů je prvním krokem implementace Obecného nařízení a slouží k zjištění a vyhodnocení rozsahu zpracovávaných osobních údajů a úrovně jejich ochrany. Pomohla nalézt odpovědi na to, jakým způsobem byly plněny povinnosti vůči zákonu o ochraně osobních údajů, a tím se vytvořily podmínky pro implementaci Obecného nařízení.

Případová studie se uskutečnila během přípravných fází na implementaci GDPR na jaře v roce 2017 mateřskou základnou, s cílem prověřit a inventarizovat vzorek systémů skupiny ÅF. Případová studie sloužila k zjištění připravenosti skupiny ÅF na implementaci principů GDPR. Skupina ÅF si nechala přezkoumat firmou Legal Works osmnáct systémů společnosti formou GAP analýzy, ve které se mělo zjistit, zda jsou systémy kompatibilní se standardy GDPR. Tyto informační systémy patřily mateřské společnosti ÅF sídlící ve Stockholmu, část z nich se používá interně a část z nich jsou informační systémy, které se používají napříč všemi pobočkami po celé Evropě. Systémy, které slouží jako databáze údajů a umožňují práci s údaji mezi všemi pobočkami AF v Evropě je systém Lime Recruiter a Aditro Personec. V kapitolách 5.3.1 Lime Recruiter a 5.3.2 Aditro Personec níže jsou k nalezení mimo jiné aplikace změn z analýzy těchto dvou systémů.

Případová studie obsahuje nejen informace o tom, zda jsou informační systémy kompatibilní s GDPR, ale pokud nejsou, tak jsou zde uvedeny návrhy řešení úprav. Dále případová studie rozvíjí metodu adaptace všech systémů AF na GDPR a jejich navrhované úkony.

5.1.1 Analýza vnitřních předpisů

Před samotnou analýzou vnitřních předpisů, bylo potřeba identifikovat osobní údaje. V jakých oblastech se osobní údaje zpracovávají a jaké standardy zpracování vytvořit.

V rámci případové studie a analýzy předpokladů souladu s principy Obecného nařízení, se zjišťoval stav předpisů, které před implementací Obecného nařízení upravovaly standardy chování při shromažďování, zpracování a skladování osobních údajů. V interní GAP analýze bylo zjištěno, že ve skupině ÅF nebyly sepsány žádné předpisy, které by chování při zpracování osobních údajů upravovaly. Zaměstnanci se řídili nastavenou interní politikou na pracovišti a svým nejlepším uvážením.

Návrhem na zlepšení stavu interních předpisů bylo, že ve skupině ÅF je k dosažení souladu s GDPR potřeba zajistit vnitřní předpisy jako jsou:

- Interní předpis pro zabezpečení osobních i citlivých údajů. V oblasti náboru zaměstnanců je mimo jiné zpracováván a uchováván u některých zaměstnanců výpis z rejstříku trestů, se kterým by se mělo zacházet jako s citlivým údajem;
- Předpis pro shromažďování osobních údajů, včetně nevyžádaných osobních údajů. Nevyžádané osobní údaje se ke zpracování dostanou například při získání životopisů uchazečů;
- Norma pro informační povinnost a další povinnosti správce;
- Metodika pro zpracování osobních údajů zákazníků, při získání nových zakázek fyzických osob;
- Standardy pro zpracování osobních údajů třetí stranou (lékařské zprávy, daně, mzdy atp.);
- Úprava interní směrnice v oblasti ochrany osobních údajů.

Jediný zavedený dokument pro možnost zpracování osobních údajů byl souhlas se pracováním osobních údajů. Tento souhlas byl určený pro nově příchozí zaměstnance. Součástí souhlasu byl osobní dotazník, který přijatý uchazeč o zaměstnání vyplnil a podepsal. Dotazník sloužil pro účely sepsání smlouvy, pro přihlášení zaměstnance na finančních úřadech, pro přidělení přihlašovacích údajů atd. V samotném souhlasu byla vypsaná práva a povinnosti zaměstnavatele i zaměstnance.

Níže je vidět tabulka – osobní dotazník, jaký byl před implementací Obecného nařízení. Z takového dotazníku se utvořil záznam všech potřebných osobních údajů ke zpracování různých činností popsaných výše.

Tabulka 1 Osobní dotazník

Jméno	**Příjmení**	**Rodné příjmení**	**Titul**
Rodné číslo	**Datum narození**	**Místo narození**	**Pohlaví**
Rodinný stav	**Druh dokladu (OP, pas)**	**Číslo dokladu**	**Státní příslušnost**
Řidičský průkaz - skupina	**Zdravotní pojišťovna**	**Telefon/Mobil**	**E-mail**

Trvalé bydliště			
Ulice, č.p.	**PSČ**	**Město**	**Stát**
Kontaktní adresa			
Ulice, č.p.	**PSČ**	**Město**	**Stát**

Kontaktní osoba v případě závažné události			
Jméno, příjmení		**Mobil**	

Bankovní spojení	Číslo účtu	Kód banky
Souhlasím se zasíláním mzdy na účet		

Typ důchodu				
Datum přiznání důchodu				
Nejvyšší dosažené vzdělání				
Student	ANO (doložte potvrzení)		NE	
Vyživované osoby/ děti	ANO (doložte kopii RL)		NE	
Jste současně veden(a) na úřadu práce	ANO (doložte potvrzení)		NE	
Ostatní srážky, exekuce	ANO (doložte jaké)		NE	

Zdroj: AF-Consult Czech Republic s.r.o.

Doporučení změny osobního dotazníku a souhlasu zaměstnance bylo oddělit osobní dotazník a do souhlasu vypsat, v souladu s Obecným nařízením, konkrétní osobní údaje, k jakému účelu jsou zpracovávány a po jak dlouhou dobu jsou uchovávány. Dále pak, že souhlas je udělován dobrovolně, může být kdykoliv odvolán a při jakékoli změně osobních údajů musí zaměstnanec změnu ohlásit. Z dotazníku by také měly být odstraněny údaje, které nejsou ke zpracování potřebné (např. rodinný stav nebo rodné příjmení).

5.1.2 Zabezpečení osobních dat před implementací GDPR

Zaměstnanci ve společnosti AF ukládají osobní údaje jak v elektronické, tak v tištěné podobě a před implementací GDPR byla příslušně chráněná, přístup byl omezený, ale

s vynaložením snahy, by se k fyzicky uloženým osobním údajům dalo dostat. Elektronické uchovávání dat bylo zabezpečeno na různých discích a zálohované na cloudových úložištích společnosti. K osobním údajům, jak v interních, tak i ve vzdálených systémech, byly vytvořeny odstupňované přístupy pracovníků, s tím, že přístup přiřazuje jen vedoucí pracovník. Přístupy do aplikací a informačních systémů byly zpřístupněny pod heslem.

Fyzické ukládání dokumentů bylo zajištěno v kancelářích u příslušných vedoucích pracovníků. Dokumenty byly uloženy v těch kancelářích, ke kterému pracovnímu oboru se vztahují. Některé skříně se složkami se zamykaly, některé byly volně přístupné. Obecně je vniknutí cizích osob do prostor parkoviště u sídla firmy zamezeno bránou na přístupové heslo a v budově, ve které společnost sídlí, je recepce, kde se musí každý cizí člověk po příchodu ohlásit.

Doporučení na opatření, které se ve společnosti AF-Consult Czech Republic s.r.o. muselo zavést, bylo opatření přístupů k fyzickému uložení dokumentů. Dále se mělo zavést u všech systémů ohlášení porušení zabezpečení osobních údajů Dozorovému orgánu a subjektům údajů.

Mimo návrhy na upravení stavu ochrany osobních údajů uvedené v textech předchozích kapitol, byly společnosti poskytnuty návrhy spojené s novými úpravami Obecného nařízení. Mezi tyto návrhy na nové procesy patřilo zavedení záznamů o zpracování osobních údajů, formuláře žádosti o přenos a výmaz nebo hlášení incidentů.

5.2 Vlastní implementace principů GDPR

V této kapitole je popsaná druhá, třetí i čtvrtá fáze z obrázku 3. Je zde popsán celý proces implementace GDPR v AF-Consult Czech Republic s.r.o. Některé procesy se týkají celé skupiny ÅF, aby standardy chování při získávání, zpracování a shromažďování osobních údajů byly u všech poboček stejné. Některé procesy jsou implementovány jen v AF-Consult Czech Republic s.r.o.

5.2.1 Vnitřní předpisy GDPR

Z analýzy vnitřních předpisů (kapitola 5.1.1 Analýza vnitřních předpisů) vyšlo, že se musí zpracovat nové vnitřní předpisy. Pro zajištění shody s Obecným nařízením byl v AF-Consult Czech Republic s.r.o. vytvořen rámec na ochranu osobních údajů, kterými se společnost ÅF řídí. Rámec se skládá ze tří kategorií řídících dokumentů, které jsou zde uvedeny od nejvyšší priority po nejnižší:

1. Zásady ochrany osobních údajů / Data Privacy Policy;
2. Standardy ochrany osobních údajů / Data Privacy Standards;
3. Postupy ochrany osobních údajů / Data Privacy Procedure.

Dokument s nejvyšší prioritou, z kterého vycházejí tři výše uvedené dokumenty, je Směrnice ochrany osobních údajů. Tato Směrnice definuje, jak se mají zaměstnanci chovat při získávání, zpracování a shromažďování osobních údajů. Zásady chování se vztahují na veškeré informace zpracovávané společností ÅF, a které nejsou veřejně dostupné.

Směrnice vymezuje základní pojmy Obecného nařízení, práva a povinnosti správce a práva subjektu údajů. Obsahuje popis osobních údajů, formu souhlasu se zpracováním osobních údajů, formu záznamů o činnostech zpracování, způsob využívání kamerových systémů, jakým způsobem musí být osobní údaje zabezpečené a čím se řídí porušení zabezpečení.

1. Zásady ochrany osobních údajů

Zásady ochrany osobních údajů stanovují rámec ÅF pro ochranu osobních údajů a zajištění shody ÅF s platnými pravidly a předpisy upravujícími ochranu soukromí, zejména s Obecným nařízením. Dokument Zásady ochrany osobních údajů je určen spíše pro manažery celé skupiny ÅF a uděluje jim zodpovědnost za to, aby veškeré zpracování osobních údajů v oblasti odpovědnosti správce bylo provedeno zákonně a bezpečně v souladu s těmito zásadami. (Data Privacy Policy, ÅF 2018)

Stanovuje Radu pro ochranu osobních údajů, která se skládá z generálního advokáta, ředitele CIO, vedoucího personálního oddělení a dalších manažerů. Rada pro ochranu osobních údajů by měla (Data Privacy Policy, ÅF 2018):

a) dohlížet na provádění a dodržování této politiky,
b) předkládat návrhy na nezbytné změny politiky, které musí přijmout generální ředitel skupiny,
c) přijímat standardy ochrany osobních údajů a
d) mít pravomoc delegovat odpovědnost osobám na plnění úkolů Vlastníka systému v rámci těchto zásad v případě potřeby.

Generální ředitel skupiny ÅF zajistil jmenování Správce ochrany osobních údajů. Správce ochrany osobních údajů by měl (Data Privacy Policy, ÅF 2018):

a) dohlížet na každodenní provádění a dodržování těchto zásad,
b) předkládat návrhy na nezbytné změny politiky, které předloží Rada pro ochranu osobních údajů k přijetí generálním ředitelem skupiny,
c) vytvářet nezbytné standardy ochrany osobních údajů k přijetí Radou pro ochranu osobních údajů,
d) poskytovat doporučení a šablony, které se používají pro postupy ochrany osobních údajů,
e) systematicky a pravidelně provádět vnitřní kontrolu a monitorování dodržování rámce ochrany soukromí společnosti ÅF,
f) sledovat vývoj právních předpisů a osvědčených postupů v oblasti ochrany osobních údajů,

g) oznamovat Radě pro ochranu osobních údajů, pokud jde o její práci s výše uvedenými skutečnostmi,
h) sdělovat nezpochybnitelná rizika v oblasti ochrany osobních údajů a incidenty spojené s ochranou soukromí Výboru pro ochranu osobních údajů.

2. Standardy ochrany osobních údajů

Dokument Standardy ochrany osobních údajů je více podrobným rozpisem Zásad ochrany osobních údajů. Popisuje standardy chování při zabezpečení, zpracování a přenosu osobních údajů. Vymezuje přesná práva subjektů údajů, jak teoreticky, tak i prakticky nebo jak práva v případě potřeby využít.

3. Postupy ochrany osobních údajů

Dokument postupy ochrany osobních údajů je obecná šablona, vytvořená společností ÅF, která má za úkol standardizovat úpravu postupů všech procesů ve společnosti. Uvádí, jak a proč jsou data spravována, a je dokladem o tom, že zpracování probíhá v souladu s GDPR. Nesplnění GDPR může vést k silným sankcím a vážně poškozenému pověsti společnosti ÅF a jejích zákazníků.

Dokument dělí postupy na čtyři fáze, a to na:
1. právní základ pro zpracování – účel zpracování osobních údajů
2. základní pojmy (vlastník systému, účel zpracování, osobní a citlivé údaje, práva a svobody subjektů údajů),
3. vlastní postup (výměna informací s jinými systémy, vizualizace, vstupy, výstupy, smlouvy o zpracování dat atp.),
4. hlavní principy GDPR (časový rámec zpracování osobních údajů, aktualizace údajů, informovanost, vymazání dat a určení přístupových práv).

Ke každému systému je vytvořen takový dokument, kde je popsaný postup činnosti daného systému v souladu s Obecným nařízením.

5.2.2 Posouzení dopadu rizik

Implementace principů GDPR probíhala ve sledované společnosti AF-Consult Czech Republic s.r.o. postupně, a jednotlivé principy se zapisovaly do jedné rozsáhlé tabulky. Jednalo se o posouzení dopadu rizik, minimalizace osobních údajů, zda se můžou některé osobní údaje odstranit, určení účelu osobních údajů, dobu zpracování osobních údajů, aktuálnost osobních údajů, zabezpečení, přístup do systému a zda se objevuje riziko při zpracování osobních údajů. Pro účely této diplomové práce byla tabulka rozdělena dle konkrétních principů zmíněných výše. Každý princip má svou část tabulky, a ta je vložena do jednotlivých kapitol, kterých se daná část týká.

Do souhrnné tabulky byly zapisovány osobní údaje zaměstnanců, které ÅF zpracovává k tomu, aby byly splněny zákonné povinnosti, a ty jsou například:

- jména a příjmení,
- trvalý pobyt a kontaktní adresa,
- pohlaví,
- datum narození, věk, rodné číslo,
- rodinný stav,
- zdravotní způsobilost a zdravotní znevýhodnění,
- e-mailová adresa (soukromá i pracovní),
- telefonní číslo (soukromé i pracovní),
- číslo a platnost řidičského průkazu,
- číslo a platnost občanského průkazu,
- číslo a platnost cestovního pasu,
- údaje o dosaženém vzdělání a dalších kvalifikačních oprávněních nutných pro výkon dané profese (titul),
- údaje o příjmu (na mzdových listech),
- údaje o vyživovaných osobách,
- údaje o exekučních srážkách,
- údaje o srážkách na základě dohody o srážce ze mzdy,
- údaje o přiznání důchodu,
- údaje o přípravě na budoucí povolání,
- údaje o zdravotní pojišťovně, u které je zaměstnanec přihlášen,
- údaje o soukromém životním pojištění, o penzijním připojištění se státním příspěvkem, o doplňkovém penzijním spoření,
- identifikační číslo zaměstnance,
- podpis,
- výpis z rejstříku trestů.

Poslední tři osobní údaje uvedené výše, jsou jen pro některé pozice, které tyto osobní údaje vyžadují, např. výpis z rejstříku trestů je požadován jen pro jednatele společnosti.

V první řade bylo potřeba zjistit, jaké informační systémy zpracovávají osobní údaje a vypsat konkrétní zpracovávané osobní údaje. Ve společnosti AF-Consult Czech Republic s.r.o. bylo zjištěno padesát devět informačních systému, které zaznamenávají nebo pracují s osobními údaji. Od takto rozdělených osobních údajů se odvíjí posouzení dopadu rizik, minimalizace údajů a určení účelu údajů.

Posouzení dopadu rizik musí být dokumentováno v písemném výkazu, který obsahuje (Data Privacy Standards, ÅF 2018):

- Popis operací zpracování a účelů, včetně případných oprávněných zájmů sledovaných správcem;
- Posouzení nutnosti a přiměřenosti zpracování ve vztahu k účelu;
- Posouzení rizik práv a svobod subjektů údajů;

- Opatření zavedená k řešení rizik a prokazování souladu s politikou ochrany osobních údajů společnosti ÅF a platnými zákony o ochraně osobních údajů.

Posouzení dopadu rizik porušení zabezpečení osobních údajů se určovalo po zavedení nutných opatření. V tabulce 2 jsou tato opatření nazvaná jako „další nutná opatření".

Tabulka 2 Posouzení dopadu rizik

Zdroje			Rizika					Další nutná opatření
Subjekt údajů	**Úložiště / umístění osobních údajů / Systém / SW**	**Typ osobních údajů**	**Rizika spojená se zpracováním údajů**	**U**	**P**	**Z**	**Vyhodnocení rizika [Nízké, Střední, Vysoké]**	
Dodavatelé, Zákazníci	Lotus Notes	Jméno a příjmení kontaktní osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Je nutné mít souhlas, pokud není Smlouva	+	+	+	Nízké	Je třeba získat souhlas od subjektu ke zpracování OÚ, pokud s ním není platná smlouva nebo údaje odstranit nebo zarchivovat omezením přístupu. Omezit přístup k těmto kontaktům!
Privátní osoby	Lotus Notes	Jméno a příjmení osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Je nutné mít souhlas, pokud není Smlouva	+	+	+	Nízké	Je třeba získat souhlas od subjektu ke zpracování OÚ, pokud s ním není platná smlouva nebo údaje odstranit nebo zarchivovat omezením přístupu. Omezit přístup k těmto kontaktům!
Zaměstnanci	Lotus Notes	Jméno a příjmení osoby a absolvované školení		+	+	+	Nízké	Je třeba zarchivovat a omezit přístup.
Zaměstnanci	W:\01_Administrace Lime, Reference, Podpisový vzor, Marketing	Jméno a příjmení, adresa zaměstnání, email-zaměstnání, Tel. číslo-zaměstnání, Mobil. tel. číslo-zaměstnání	Přístup mají všichni zaměstnanci	+	+	+	Nízké	Omezen přístup do vybraných složek viz záložka disk W

Zdroj: Ing. Radek Jambor a Ing. Vladislava Balonová

V tabulce 2 jsou vidět jen čtyři systémy jako ukázka analyzovaných systémů, které zpracovávají osobní údaje, se analyzují pro posouzení dopadu rizik a dalších principů. Rizika spojená se zpracováním dat, jsou ta, u kterých hrozí porušení zabezpečení údajů. Písmena U, P, Z jsou počáteční písmena slov Užití, Přístup a Zabezpečení, tyto tři faktory se posuzovaly a přiřadil se k nim znak *plus* (+) v případě, že k nim již nejsou potřeba zavést žádná nutná opatření nebo *mínus* (-), pokud je možnost nějakého dalšího rizika. Vyhodnocení rizika nízké znamená třikrát znak *plus.* U středního by bylo potřeba udělat menší dodatečná opatření, kdyby se v políčkách U, P, Z objevilo *plus* jen dvakrát. A vysoké riziko by bylo v případě, že by se *plus* neobjevilo ani jednou nebo jen jednou. V případě, že by zhodnocení zpracování vyplynulo jako velice rizikové a nešla by tato rizika zmírnit, musela by organizace konzultovat zabezpečení s Úřadem pro ochranu osobních údajů (ÚOOÚ).

Tímto způsobem se posoudily všechny systémy a všechny zpracovávané osobní údaje. Například je jasné, že u uchazečů a osobních údajů, které se zpracovávají při nástupu pro účely finančního a personálního oddělení, je mnohem více shromažďovaných

osobních údajů, než které jsou uvedeny v tabulce u systému Lotus Notes, tím i možné větší riziko a aplikovaná opatření.

5.2.3 Minimalizace údajů

Aby bylo zpracování osobních údajů v souladu s Obecným nařízením a platnými právními požadavky, musí se osobní údaje zpracovávat dle platných principů Obecného nařízení, do nichž patří minimalizace zpracovávaných osobních údajů.

Dle principů uvedených v kapitole 2.4 Hlavní principy GDPR bylo potřeba zpracovat, vymazat nebo odůvodnit osobní údaje, které již společnost AF-Consult Czech Republic s.r.o. měla ve své databázi. K tomuto účelu byly vydané Zásady ochrany osobních údajů, aby se určil standardní postup pro získávání nových údajů v součinnosti s Obecným nařízením.

V procesu minimalizace osobních údajů byla doplněna celková tabulka procesu implementace jednotlivých principů, o údaje minimalizace a ukládání údajů a o přesnost osobních údajů.

Tabulka 3 Minimalizace údajů

Zdroje			Minimalizace dat	Minimalizace ukládání	Přesnost
Subjekt údajů	**Úložiště / umístění osobních údajů / Systém / SW**	**Typ osobních údajů**	**Potřebujeme k naplnění účelu všechna získaná data ?**	**Jak dlouho budeme data zpracovávat?**	**Jsou údaje, které jsme shromáždili správné a aktuální?**
Dodavatelé, Zákazníci	Lotus Notes	Jméno a příjmení kontaktní osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	ne		neaktuální
Privátní osoby	Lotus Notes	Jméno a příjmení osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	ne		neaktuální
Zaměstnanci	Lotus Notes	Jméno a příjmení osoby a absolvované školení	ne		neaktuální
Zaměstnanci	W:\01_Administrace Lime, Reference, Podpisový vzor, Marketing	Jméno a příjmení, adresa zaměstnání, email-zaměstnání, Tel. číslo-zaměstnání, Mobil. tel. číslo-zaměstnání	ne	Po dobu trvání PPV a poté dle archivační lhůty jednotlivých dokumentů	ano

Zdroj: Ing. Radek Jambor a Ing. Vladislava Balonová

V tabulce 3 je vybraný stejný vzorek zdrojů, jako u posouzení dopadu rizik. Tato tabulka je jen jako ukázka průběhu implementace principů GDPR. Ve sloupci minimalizace osobních údajů, je specifikace, zda je potřeba jednotlivé osobní údaje zpracovávat, u všech uvedených je odpověď „ne". Pro účely zpracování byly některé údaje nadbytečné, a proto byly některé údaje smazány, případně archivovány. U některých zdrojů osobních údajů bylo v políčku „ano" tzn. že všechny osobní údaje jsou potřebné pro stanovený účel zpracování. V tabulce je dále specifikace určení doby, po kterou

se osobní údaje budou zpracovávat. U každého zdroje záleží na jiných kritériích, a proto se u každého subjektu údajů bude dále každá doba specifikovat. V posledním sloupci tabulky je uvedeno, zda jsou všechny získané osobní údaje aktuální. V případě aplikace Lotus Notes nebyly údaje aktuální, a proto proběhla, na základě tohoto zjištění, aktualizace údajů. Údaje na disku W byly při implementaci GDPR aktuální.

V celé skupině ÅF včetně AF-Consult Czech Republic, s.r.o. byly jednotlivé osobní údaje tímto způsobem zhodnoceny. Zda je potřeba údaje zpracovávat a v jakém rozsahu pro jednotlivé útvary nebo procesy. Osobní údaje, které byly vyhodnoceny jako nepotřebné, byly smazány. Osobní údaje, které již nebyly potřebné pro aktuální činnost, ale nesmí se smazat, byly archivované a přístup k nim je omezený. Jedná se např. o:

- evidenci privátních kontaktů a firem v aplikaci Lotus Notes,
- evidenci kontaktů dodavatelů a zákazníků (přechod na systém Navigo),
- údaje na disku W: Reference, marketingové informace pro zaměstnance, životopisy osob, které pro společnost pracují na základě živnostenského oprávnění atd.

5.2.4 Určení účelu údajů

Stejně jako u minimalizace údajů je potřeba zajistit soulad s Obecným nařízením v určení účelu osobních údajů či zajištění souhlasu se zpracováním osobních údajů, který je popsán v následující kapitole.

Společnost AF-Consult Czech Republic s.r.o. shromažďuje a zpracovává osobní údaje zaměstnanců pro oprávněné obchodní účely, včetně uzavírání a provádění obchodních smluv se zákazníky, jednání s obchodními partnery, marketingu a jejich služeb, a jestliže je to jinak nezbytné pro splnění příslušných práv a povinností pracovní smlouvy a jak je vyžadováno zákonem.

Do souhrnné tabulky všech principů GDPR byly doplněny údaje, které jsou potřebné k určení účelu osobních údajů anebo zda je potřeba doplnit souhlas se zpracováním osobních údajů.

Tabulka 4 Určení účelu osobních údajů

Zdroje			Účel	Útvar	Právní důvody ke zpracování	
Subjekt údajů	**Úložiště / umístění osobních údajů / Systém / SW**	**Typ osobních údajů**	**Za jakým účelem jsou data zpracovávány?**		**Na základě jakého právního důvodu se data zpracovávají?**	**Je souhlas?**
Dodavatelé, Zákazníci	Lotus Notes	Jméno a příjmení kontaktní osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Evidence kontaktů dodavatelů a zákazníků	IT	Souhlas	zatím ne
Privátní osoby	Lotus Notes	Jméno a příjmení osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Evidence privátních kontaktů a firem	IT	Souhlas	zatím ne
Zaměstnanci	Lotus Notes	Jméno a příjmení osoby a absolvované školení	Školení na Lotus Notes - evidence školení	IT	Nepodléhá souhlasu/oprávněný zájem	n/a
Zaměstnanci	W:\01_Administrace Lime, Reference, Podpisový vzor, Marketing	Jméno a příjmení, adresa zaměstnání, email-zaměstnání, Tel. číslo-zaměstnání, Mobil. tel. číslo-zaměstnání	Reference, marketingové informace pro zaměstnance	Administrace	Nepodléhá souhlasu/oprávněný zájem	Dle GDPR směrnice, uložen na finančním oddělení

Zdroj: Ing. Radek Jambor a Ing. Vladislava Balonová

V tabulce 4 jsou uvedené základní údaje o systému a typ zpracovávaných osobních údajů, v celkové verzi je v tabulce uveden i správce systému, který je zodpovědný za systém, zde nahrazen pouze útvarem (IT, Administrace). V dalších sloupcích je již samotné určení účelu. Jedná se o přesné určení účelu zpracovávaných osobních údajů, jak jsou zajištěny, zda souhlasem nebo oprávněným zájmem a v posledním sloupci je určení, zda jsou údaje založené na souhlasu zajištěné souhlasem nebo zatím ne.

Tabulka 4 je jen ukázkou, jaké údaje byly potřeba k určení účelu osobních údajů, a také jen ukázkou, jakým způsobem se zkoumaly systémy, které zpracovávají osobní údaje. Informace, které byly do tabulky vyplněny jsou interní informací společnosti AF-Consult Czech Republic s.r.o. Kolonky pro vyplnění údajů obsahují veškeré informace o daném údaji, aby byly všechny požadavky Obecného nařízení v souladu s procesem určení účelu osobních údajů.

5.2.5 Souhlas se zpracováním osobních údajů

Jak již bylo uvedeno v teoretické části, souhlas se zpracováním osobních údajů je jen jeden ze zákonných důvodů, které Obecné nařízení upravuje k možnosti zpracovávat osobní údaje.

U zavedení nových souhlasů bylo nejprve potřeba projít staré souhlasy se zpracováním osobních údajů, zda jsou aktuální, zda jsou souhlasy účelné a zda jsou v souladu

s Obecným nařízením. Po zjištění, že souhlasy již aktuální nejsou, byly některé odstraněny a některé zarchivovány.

V předchozí kapitole 5.2.4 Určení účelu údajů je v tabulce 3 vidět, že k některým činnostem zpracování osobních údajů jsou přiřazeny právní tituly zpracování a pokud ke zpracování není žádný právní důvod, je potřeba získat souhlas se zpracováním osobních údajů od subjektu údajů. Subjekt údajů, ať jde o zaměstnance nebo dodavatele, musí vždy znát účel zpracování a musí jej podepsat dobrovolně.

Na základě neaktuálnosti souhlasů se zpracováním osobních údajů, byly v AF-Consult Czech Republic s.r.o. vytvořeny 3 nové. Souhlas se zpracováním osobních údajů se v AF CZ zaváděl v souvislosti s přijímáním nových zaměstnanců, pro stávající zaměstnance a pro fyzickou osobu či subdodavatele. K udělení Souhlasu se zpracováním slouží následující formuláře:

1. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro zaměstnance,
2. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro fyzické osoby a subdodavatele,
3. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro osoby ucházející se o zaměstnání.

Obsah souhlasu se zpracováním osobních údajů se na každém z uvedených souhlasů liší, a to ve zdůvodnění, proč daný subjekt údajů souhlas dává a podle toho, komu je souhlas určený. Součástí souhlasu je poučení, že subjekty údajů mohou svůj souhlas kdykoli odvolat. Udělení souhlasu musí být oddělené od smlouvy nebo obchodních podmínek, a proto se souhlas subjektu údajů dává zvlášť.

První Souhlas se zpracováním osobních údajů je určen pro stávající zaměstnance, u kterých již nebyl aktuální předchozí souhlas. Slouží pro zpracování osobních údajů, pro které AF-Consult Czech Republic s.r.o. jako správce a zaměstnavatel nemá právní titul, například osobní údaje pro přihlašování na vzdělávací akce související s funkcí zaměstnance nebo zajištění cestovního pojištění v případě vyslání na služební cestu atp.

Druhý souhlas je určený pro fyzické osoby a subdodavatele. Platí například pro marketingové zasílání obchodních nabídek nebo pro osobní údaje, které jsou v evidenci v databázi AF-Consult Czech Republic s.r.o.

Třetí a poslední souhlas je určený pro nově příchozí zaměstnance. Uchazeč dává souhlas se zpracováním osobních údajů pro účely účasti ve výběrovém řízení na danou pozici. Uchazeč o zaměstnání nejdříve podepíše tento souhlas, poté vyplní osobní dotazník a na základě těchto dvou dokumentů se sjedná pracovní smlouva. Celý proces

náboru nových zaměstnanců je v kapitole 5.4 Dopady implementace v oblastech organizace.

Ve všech souhlasech je uvedená doba, po kterou může AF-Consult Czech Republic s.r.o. jako správce osobní údaje zpracovávat a po jakou dobu budou dané údaje archivovány po skončení doby zpracování. Ve všech souhlasech je uvedeno poučení o právech subjektu údajů v souladu s článkem 15 a článkem 22 Obecného nařízení. Dále je ve všech souhlasech poučení o odvolání souhlasu a o odvolání se Dozorovému orgánu.

5.2.6 Zabezpečení osobních údajů

Zabezpečení osobních údajů v AF-Consult Czech Republic s.r.o. probíhalo nejdříve doplněním informací do souhrnné tabulky, která již byla zmiňovaná v předchozích kapitolách a obsahuje všechny principy implementace Obecného nařízení.

Tabulka 5 Zabezpečení osobních údajů

Zdroje			Zabezpečení			
Subjekt údajů	**Úložiště / umístění osobních údajů / Systém / SW**	**Typ osobních údajů**	**Kdo má přístup k těmto údajům?**	**Jak jsou data zabezpečena?**	**Jakým kategoriím zaměstnanců mohou být udělena přístupová práva a s jakým účelem?**	**Jaké jsou běžné postupy pro udělení a zrušení přístupových práv?**
Dodavatelé, Zákazníci	Lotus Notes	Jméno a příjmení kontaktní osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Všichni zaměstnanci	Heslem do LN	Všichni zaměstnanci	Nastavení práv dle pozice a funkce ve společnosti
Privátní osoby	Lotus Notes	Jméno a příjmení osoby, název společnosti, adresa společnosti, telefon, fax, email společnosti	Všichni zaměstnanci	Heslem do LN	Všichni zaměstnanci	
Zaměstnanci	Lotus Notes	Jméno a příjmení osoby a absolvované školení	Všichni zaměstnanci	Heslem do LN	Všichni zaměstnanci	
Zaměstnanci	W:\01_Administrace Lime, Reference, Podpisový vzor, Marketing	Jméno a příjmení, adresa zaměstnání, email-zaměstnání, Tel. číslo-zaměstnání, Mobil. tel. číslo-zaměstnání	viz záložka disk W	Omezen přístup viz záložka disk W	viz záložka disk W	Po dohodě na poradě vedení

Zdroj: Ing. Radek Jambor a Ing. Vladislava Balonová

Tabulka 5 popisuje jakým způsobem ošetřit zabezpečení daných osobních údajů k vybraným čtyřem systémům (Lotus Notes – dodavatelé a zákazníci, Lotus Notes – privátní osoby, Lotus Notes – zaměstnanci a Disk W pro zaměstnance). K určení zabezpečení všech osobních údajů jsou v tabulce informace o tom, kdo má přístup k daným osobním údajům, jak jsou data nyní nově zabezpečena, komu mohou být udělena přístupová práva a jakým způsobem se mohou udělit nebo zrušit přístupová práva. V souhrnné tabulce pro všechny systémy, jsou dále informace o tom, kdo odpovídá za udělení přístupových práv.

IT zabezpečení osobních údajů upravuje dokument ÅF Corporate IT Policy, který má za cíl vyjasnit základní principy a pokyn skupiny pro vývoj a využití IT. Stanovuje základní zásady a pokyny pro strategická rozhodnutí a základ pro rozvoj strategie IT a základních politik, jsou zde popsané všechny aktivity a zaměstnanci skupiny ÅF. Tyto IT zásady mají povinnost dodržovat všichni uživatelé IT systémů. Z korporátní politiky IT byl vyvinut na lokální úrovni Řídící postup IT, který vešel v platnost v listopadu 2018.

Přístupy k osobním údajům jsou dány na základě určených právních titulů zpracování. Každý přístup, který je zaměstnanci přidělen, musí být oprávněný, tedy že ke zpracování určitých údajů musí mít právní důvod. Různé právní tituly či oprávněné důvody jsou popsané v kapitole 5.2.4 Určení účelu údajů. Z právního účelu je pak jasné, kdo jaké osobní údaje může zpracovávat. Zpracování osobních údajů se tedy rozděluje mezi jednotlivá oddělení. Přístup k nejvíce osobním údajům bude mít HR a Finanční oddělení společnosti. Někteří pracovníci těchto oddělení mohou zpracovávat jen část osobních údajů mimo citlivých osobních údajů.

Přístup do cloudového úložiště interní databáze, je dán dle účelu zpracování a na základě unikátního hesla k jednotlivým přístupům. Jednotlivé přístupy se liší dle pozice a osobních údajů, které mohou zpracovávat. U personálního oddělení budou jiné přístupy než u projektového manažera, projektový manažer nemá přístup ke složkám personalistů a naopak. Pokud je více zaměstnanců na stejné pozici, je dán přístup do sdíleného úložiště pro danou pozici pod unikátním heslem.

Dostupnost dokumentů fyzicky ukládaných v kancelářích, byla upravena povolením přístupu do kanceláří vedení, jen s povolením vedení. Všechny dokumenty, které obsahují osobní údaje a mají být zabezpečeny, musí být zamčeny ve skříních příslušného oddělení.

5.2.7 Záznamy o činnostech zpracování

Zpracování daných osobních údajů, které správce musí zaznamenávat jsou uvedené v teoretické části v kapitole 2.3.2 Záznamy o činnostech zpracování. Jelikož má skupina ÅF včetně všech společností více jak 250 zaměstnanců, musí vést záznamy o činnostech zpracování.

V ÅF jsou nastavené dvě oblasti záznamů, a to Řídící záznam a Procesní záznamy. Řídící záznam vede záznamy o všech zpracovatelských činnostech prováděných v rámci odpovědnosti ÅF jako správce, tj. pokud ÅF, samostatně nebo společně s ostatními, určuje účel a prostředky zpracování osobních údajů.

Procesní záznamy vedou údaje o zpracovatelských činnostech prováděných v rámci odpovědnosti ÅF jako zpracovatele, tj. v případech kdy ÅF jako správce zpracovává osobní údaje. Zpracovatelské činnosti musí být pokryty a probíhat v souladu s Řídícími

záznamy. Procesní záznam musí obsahovat alespoň tyto informace (Data Privacy Standards, ÅF 2018):

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, jímž jménem zpracovatel jedná, a případně zástupce správce nebo zpracovatele a úředníka pro ochranu údajů;
- kategorie zpracování prováděné jménem každého správce;
- případně předávání osobních údajů do třetí země nebo mezinárodní organizace včetně identifikace této třetí země nebo mezinárodní organizace a v případě převodů uvedených v čl. 49 odst. 1 druhém pododstavci Obecného nařízení, dokumentace vhodných ochranných opatření;
- pokud je to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v normě ochrany osobních údajů společnosti ÅF týkající se ochrany osobních údajů.

5.3 Informační systémy

V kapitole Informační systémy jsou popsané některé aplikace a elektronické systémy, které ÅF využívá k uchovávání a zpracovávání osobních údajů. Ke každému informačnímu systému je stručný popis účelu, kdo ho ke své práci využívá, jaké osobní či citlivé údaje shromažďuje a jaké změny byly provedeny k přizpůsobení principů Obecnému nařízení.

Dokument Zásady ochrany osobních údajů upravuje povinnost vlastníka informačního systému. Pro každý informační systém, v němž jsou zpracovávány osobní údaje, je odpovědný vlastník systému, který v souladu s těmito zásadami a všemi platnými standardy ochrany osobních údajů a ochranou osobních údajů (Data Privacy Policy, ÅF 2018):

a) vypracovává, přijímá a udržuje postupy ochrany osobních údajů pro informační systém v rámci odpovědnosti vlastníka systému a
b) pracuje na nepřetržitém zlepšování a implementaci funkčnosti a postupů v rámci informačního systému, aby pomohla svým uživatelům při dodržování těchto zásad a platných standardů ochrany osobních údajů a postupů ochrany osobních údajů.

5.3.1 Lime Recruiter

Systém Lime Recruiter používá společnost ÅF pro náborový proces za účelem nalezení správného kandidáta na danou pozici strukturovaným procesem. Systém je celosvětově využíván lovci hlav (headhunter) i HR manažery. Systém má funkce pro vyhledávání zaměstnanců se statusem Partner (osoba, která pro společnost pracuje a není zaměstnanec, pracující pod pracovní smlouvou), Future (budoucí zaměstnanec, uchazeč o práci např. studenti) a Emeritus (dřívější zaměstnanci). V AF-Consult Czech Republic

s.r.o. nejvíce využívá Lime Recruiter HR specialista, který vybírá uchazeče a dělá náborový proces.

Osobní údaje jsou v tomto systému zpracovávány na základě souhlasu dle článku 6.1 písm. a) Obecného nařízení. Životopisy a průvodní dopisy, které posílají uchazeči, se vkládají do systému, ale mohou obsahovat citlivé údaje. Pro vyhodnocování nejsou tyto údaje relevantní, a proto nejsou pro účel zpracování důležité. Pokud jsou tyto údaje zpracovávány, tak se souhlasem dle článku 9.2 písm. a) Obecného nařízení.

K informacím je možný přístup pouze pod heslem a využívá je pouze personální oddělení. Postup mazání osobních údajů ze systému je písemně zdokumentován a jsou nastaveny standardy pro smazání.

Změny, které byly provedeny na systému Lime Recruiter v souvislosti s implementací GDPR, jsou:

a) písemné potvrzení všech účelů zpracování osobních údajů, které systém zaznamenává;
b) minimalizace údajů v systému a mazání osobních údajů zaměstnanců, s kterými se již nepracuje;
c) zavedení náhodných kontrol;
d) zavedení dokumentace přístupů do systému;
e) zavedení platných pokynů pro vyplňování volných textových polí;
f) zavedení evidence mazání osobních údajů v případě, že kandidát nereaguje na zprávu;
g) aktualizování a specifikace souhlasu se zpracováním osobních údajů, kandidát může a nemusí dát souhlas se zpracováním osobních údajů v zemích EU a v zemích třetí světa;
h) přepracování smlouvy se zpracovateli Lundalogik a ostatními subdodavateli podílející se na zpracování údajů, kteří museli potvrdit shodu se standardem GDPR;
i) zavedení dokumentace veškerého přenosu osobních údajů do třetích zemí.

Výsledky změn byly opět předloženy společnosti Legal Works k ověření shody s Obecným nařízením a systém Lime Recruiter je v souladu s principy GPDR.

5.3.2 Aditro Personec HR

Systém Aditro Personec HR je využíván personálním oddělením k registraci všech potřebných údajů o svých zaměstnancích. Společnosti skupiny ÅF využívají Aditro Personec HR jako hlavní datový systém podporující ostatní informační systémy. Hlavním účelem tohoto systému je zvládnout velké spektrum záležitostí týkajících se zaměstnanosti a jaké aby ÅF mohla splňovat požadavky podle právních předpisů, kolektivních smluv a individuálních pracovních smluv ve vztahu ke svým zaměstnancům.

Informace pocházejí především z pracovních smluv, počínaje podpisem pracovní smlouvy, nebo při změně některých podmínek v pracovní smlouvě. Ve Švédsku se o tento systém starají čtyři lidé ze správy lidských zdrojů a mimo Švédsko je za každou jednotlivou zemi určena jedna osoba, a jen tito zaměstnanci mohou měnit osobní údaje uvedené v systému. Údaje se mění vždy na základě doložených podkladů.

Aditro Personec HR se využívá nejen jako datové úložiště informací, ale i jako prostředek pro hlášení incidentů v rámci Švédského pracovního prostředí. V České republice a jiných státech musí každý jednotlivý správce nebo subjekt údajů hlásit incidenty příslušnému dozorovému orgánu. Systém se také používá pro tvoření statistik porozumění pracovní síle ve společnosti ÅF.

Přístup do systému Aditro Personec HR je rozdělen dle rolí a úrovní přístupu. Všechny přístupy do systému zajišťuje personální oddělení, skupina odpovědná za správu lidských zdrojů. Odlišné úrovně přístupu manažerů jsou uvedeny podle toho, jakou roli má osoba v Personec HR (tj. v sekci manažer, market area manager, business area manager).

Změny, které byly provedeny v systému Aditro Personec HR v souvislosti s implementací GDPR, jsou:

a) minimalizace údajů v systému a mazání osobních údajů zaměstnanců, s kterými se již nepracuje;
b) písemné potvrzení všech účelů zpracování osobních údajů, které systém zaznamenává;
c) určení správců systému, kteří jsou zodpovědní za soulad systému s principy GDPR;
d) zavedení regulace přístupů k osobním údajům třetích stran;

5.3.3 Navigo

Navigo je lokální interní CRM systém používaný pouze zaměstnanci AF-Consult Czech Republic s.r.o. v různých úrovních přístupů, nejvíce systém Navigo využívají manažeři, obchodní specialisti a projektanti. Je vhodný pro sledování a řízení průběhu zakázek a projektů. Systém zobrazuje seznam aktuálních i hotových úkolů, informace o zakázkách, obchodních příležitostech, neschválených fakturách a kapacitách přihlášeného uživatele. Také eviduje seznam kontaktů a seznam záznamů z jednání a ostatní komunikaci se zákazníkem, pokud ji tam uživatel přidá. Systém chytře zobrazuje všem zainteresovaným plán celého projektu a všech výdajů.

AF-Consult Czech Republic s.r.o. pracuje převážně na B2B trhu, tudíž v kontaktech a zakázkách se nezpracovávají osobní údaje fyzických osob, jen údaje právnických osob, na které se Obecné nařízení nevztahuje. Pokud se zakázka vykonává pro soukromou

fyzickou osobu, osobní údaje jsou ošetřeny právním účelem dle článku 6 odst. 1 Obecného nařízení, dále by byly ošetřeny speciálním přístupem zaměstnanců, kteří s údaji mohou pracovat. Citlivé údaje systém nezpracovává.

Do systému Navigo mají přístup pouze zaměstnanci společnosti AF-Consult Czech Republic s.r.o. a není umožněn přístup třetím stranám ani nejsou osobní údaje převáděny do třetích zemí.

U systému jsou nastaveny pravidelné kontroly, které zaznamenává správce a pokud kontrola najde nějakou neshodu s příručkou zpracování osobních údajů pro systém Navigo, správce pak neshodu opraví nebo daný údaj smaže. K postupu smazání osobních údajů existuje písemný postup.

Změny, které byly provedeny na systému Navigo v souvislosti s implementací GDPR, jsou:

a) potvrzení účelů všech osobních údajů, které systém zaznamenává;
b) zavedení bezpečnostního IT opatření proti útokům třetích stran;
c) zavedení souhlasu se zpracováním osobních údajů na webovém portále Navigo;
d) zavedení dokumentace přístupů do systému;
e) zavedení platných pokynů pro vyplňování volných textových polí;
f) zamezení duplikací zanášení údajů, jak osobních, tak veřejných.

5.3.4 DUEL

Informační systém DUEL se ve společnosti AF-Consult Czech Republic s.r.o. používá pro zpracování účetnictví a mezd. Finanční účetnictví zahrnuje vystavené a přijaté faktury, DPH, daň z příjmů, výpisy z bankovních účtů, bankovní převody, platební příkazy, podpůrné doklady pro účely DPH, adresy zákazníků, bankovní účty, ID atd. Pro výplatní listy DUEL zpracovává měsíční platy, prémie, sociální zabezpečení a zdravotní pojištění, výpočet daně z přidané hodnoty, podpora zpracování pro orgány sociálního zabezpečení a zdravotního pojištění, podpora zpracování pro daňový úřad a roční výpočet daně z přidané hodnoty.

V systému DUEL je zpracování osobních údajů založeno na smluvní situaci, právním závazku a oprávněném zájmu dle článku 6.1 písm. b), c) a f) Obecného nařízení. V systému jsou také evidovány citlivé údaje, jako jsou informace o zdravotním stavu a výpis z rejstříku trestů. Údaje o zdravotním stavu jsou v systému zpracovávány s výjimkou čl. 9.2 písm. b) Obecného nařízení, na základě pracovního práva. Výpis z rejstříku trestů je v systému evidován kvůli české legislativě. Všechny zpracovávané údaje jsou pro tyto účely zpracování relevantní.

Oznámení systému o ochraně osobních údajů je aktualizováno dle standardů Obecného nařízení. A pro odstranění osobních údajů existuje písemný postup pro odstranění. K osobním údajům zpracovávaným účetním systémem DUEL nemá přístup ani není možné zveřejnění žádným třetím stranám a ani nejsou převáděna do třetího světa.

Změny, které byly provedeny v systému DUEL v souvislosti s implementací GDPR, jsou:

a) písemné potvrzení účelu zpracování osobních údajů;
b) zavedení bezpečnostního IT opatření proti útokům třetích stran;
c) zavedení písemného oznámení o ochraně osobních údajů v systému DUEL a na intranetu společnosti;
d) zavedení dokumentace přístupů.

5.4 Dopady implementace v oblastech organizace

V této kapitole jsou sepsány doplněné i nově vzniklé procesy, které se objevily s implementací nového Obecného nařízení o ochraně osobních údajů. Níže je popsaný proces přijímání nových zaměstnanců, který je obohacen o nové procesy, jinak celý proces náboru zaměstnanců zůstává stejný.

Přijímání nových zaměstnanců

Postup přijímání zaměstnanců je:

a) Souhlas o zpracování osobních údajů uchazečů;
b) Osobní dotazník;
c) Sjednání pracovních podmínek a check-list;
d) Směrnice GDPR, Etický kodex, kurz o seznámení s GDPR;
e) Souhlas o zpracování osobních údajů zaměstnanců;
f) Pracovní smlouva a mzdový výměr.

Souhlas o zpracování osobních údajů uchazečů je určený pro nově příchozí zaměstnance. Uchazeč dává souhlas se zpracováním osobních údajů pro účely účasti ve výběrovém řízení na danou pozici. Uchazeč o zaměstnání nejdříve podepíše tento souhlas, poté vyplní osobní dotazník a na základě těchto dvou dokumentů se sjednají pracovní podmínky. Jakmile se sjednají pracovní podmínky, dostane vybraný uchazeč tzv. „check-list", ve kterém jsou všechny náležitosti nástupu na pozici a slouží jako kontrola pro obě strany. Je rozdělen na dvě oblasti úkolů, a to na úkoly před nástupem do zaměstnání a na úkoly po nástupu do zaměstnání.

Těsně před nástupem dostane nový zaměstnanec uvítací email s odkazem z aplikace eMarketeer, kde se na intranetu dozví o Divizi Energy. Dále jsou v emailu přílohy jako jsou Směrnice o ochraně osobních údajů, Etický kodex a Oznámení o ochraně osobních údajů. Projde školením o ochraně osobních údajů a podepíše další Souhlas o zpracování osobních údajů, tentokrát již zaměstnanecký. Následuje Pracovní smlouva a zhotovení mzdového výměru. V den nástupu do zaměstnání jsou každému zaměstnanci

přiděleny unikátní přihlašovací údaje a jsou mu dány přístupy do aplikací. Zaměstnanec pak projde adaptací na pozici a prakticky se seznámí se všemi procesy.

5.4.1 Nově vzniklé procesy

V této podkapitole jsou popsány nové činnosti, které musí správce údajů zajistit na korporátní úrovni. Činnosti, které jsou v procesu ochrany osobních údajů navíc oproti minulé legislativě ochrany osobních údajů. Mezi nově vzniklé procesy patří:

- oznámení o ochraně osobních údajů;
- žádost o výmaz;
- žádost o přenos;
- hlášení incidentů;
- záznamy o činnostech zpracování;
- smlouva o zpracování osobních údajů;
- interní kontrola.

Oznámení o ochraně osobních údajů

Dokument Oznámení o ochraně osobních údajů poskytuje informace týkající se shromažďování, zpracování, uchovávání a sdílení osobních údajů pro individuálně identifikovatelné zaměstnance.

Oznámení o ochraně osobních údajů se zaměstnancům ÅF dává po sjednání pracovních podmínek, kdy se uchazeč stává zaměstnancem společnosti nebo již zaměstnaným osobám v rámci školení.

Obsahuje základní údaje o tom, jaké osobní údaje lze shromažďovat v souvislosti s náborovým procesem, počátkem zaměstnání nebo během zaměstnání v ÅF. Jaké jsou možné účely zpracování osobních údajů zaměstnanců. Jaké jsou běžné postupy pro uložení nebo vymazání osobních údajů nebo běžné postupy pro sdílení údajů. A samozřejmě obsahuje práva zaměstnanců, některé jsou uvedené níže.

Žádost o výmaz

Jedním z práv subjektů údajů je žádost o výmaz svých osobních a citlivých údajů. Povinností správce je tomuto požadavku vyhovět, ale jen za předpokladu, že osobní údaje:

- data již nejsou potřebná pro jejich účely;
- zákonným základem zpracování je pouze souhlas subjektu údajů;
- subjekt údajů uplatňuje své právo vznést námitky v souladu s čl. 21 odst. 1 GDPR a ÅF nemá žádné naléhavé důvody pro pokračování zpracování;
- údaje byly protiprávně zpracovány;
- vymazání je nezbytné pro dodržování práva EU nebo práva členských států EU.

Ve Standardech ochrany osobních údajů ÅF je vymezeno, že veškeré vymazání musí ÅF sdělit každému příjemci, kterému byly osobní údaje zveřejněny, pokud se sdělení neukáže jako nemožné nebo nevyžaduje nepřiměřené úsilí. Pokud subjekt údajů požádá, musí ÅF informovat subjekt údajů o těchto příjemcích.

Žádost o přenos

Mezi další práva subjektů údajů patří právo na přístup a přenositelnost údajů. Subjekt údajů může požadovat, aby společnost ÅF převedla osobní údaje na jiného správce, pokud existují technické možnosti, aby mohla AF vyhovět takové žádosti. Taková situace může nastat, pokud se například zaměstnanec rozhodně jít z ÅF do jiné společnosti a požaduje převod zpracování všech svých údajů, využije toto právo. Ve Standardech ochrany osobních údajů jsou stanoveny podmínky žádosti o přenos údajů, kde ÅF (Data Privacy Standards, ÅF 2018):

- zpracovává osobní údaje automatizovanými prostředky;
- zpracovatelské činnosti jsou založeny buď na (i) souhlasu subjektu údajů nebo (ii) na smlouvě, kterou je subjekt údajů smluvní stranou;
- zpracovatelské činnosti nejsou prováděny ve veřejném zájmu nebo při výkonu veřejné moci svěřené ÅF.

U žádosti o přenositelnost údajů má subjekt údajů právo požádat o kopii osobních údajů, které subjekt údajů poskytl ÅF (mimo osobní údaje shromážděné z jiných zdrojů) v strukturovaném, běžně používaném a strojově čitelném formátu, jako jsou CSV, JSON, XML nebo jiné běžně používané otevřené formáty.

Společnost ÅF musí reagovat na žádost přenositelnosti dat bez zbytečného odkladu. (Data Privacy Standards, ÅF 2018)

Hlášení incidentů

Rada pro ochranu osobních údajů jmenovala tým pro řízení incidentů, který se skládá z vedoucího ochrany osobních údajů, hlavního bezpečnostního úředníka ÅF a zástupců dalších příslušných funkcí, aby vedl práci v tomto ohledu. Tým pro řízení incidentů reaguje na incidenty v oblasti ochrany soukromí a koordinuje veškerá nezbytná opatření, včetně komunikace, v rámci skupiny ÅF. Správce ochrany osobních údajů provádí nezbytné kontakty s orgánem dozoru a subjekty údajů, které se dotýkají incidentu s ochranou soukromí. (Data Privacy Policy, ÅF 2018)

Účelem řízení incidentů v rámci ochrany soukromí ÅF je mít připravené prostředky a umět reagovat na incidenty soukromí. V případě potřeby ohlásit takové případy dozorovému orgánu do 72 hodin poté, co zjistí, že došlo k incidentu, který by mohl vést k ohrožení práv a svobod fyzických osob.

Úkolem týmu pro řízení incidentů je spolu s postiženou jednotkou (nejlépe vlastníkem informací) dosáhnout následujících závěrů při zjištění narušení údajů (Data Privacy Standards, ÅF 2018):

- typ porušení nebo incidentu;
- typ dotčených osobních údajů a jejich citlivost;
- objem osobních údajů;
- počet dotčených osob, kterých se incident týká;
- pravděpodobná úroveň / typ poškození, která by mohla být předmětem údajů;
- možná újma ÅF nebo třetích stran (reputace, mediální zájem atd.);
- již zavedená bezpečnostní opatření;
- podrobnosti o jakýchkoli krocích, které již byly podniknuty po incidentu;
- dosavadní časový plán událostí.

Bylo zavedeno, že pokud někdo mimo tým řízení incidentů zjistí incident soukromí, musí je hlásit prostřednictvím e-mailu na adresu GDPRProjectTeam@afconsult.com, nebo voláním na interní linku pod speciálním číslem. E-mailová zpráva musí obsahovat předmět "incident v oblasti ochrany soukromí" a musí obsahovat kontaktní informace oznamující osoby, aby tým pro řízení incidentů mohl kontaktovat tuto osobu pro podobnější informace. Podrobnosti o incidentu v oblasti ochrany osobních údajů nesmí být uvedeny v e-mailu.

Záznamy o činnostech zpracování

Blíže je tento nově vzniklý proces popsán v kapitole 5.2.7 Záznamy o činnostech zpracování. ÅF má zavedené dva dokumenty, které zaznamenávají činnost zpracování, a to Řídící záznam a Procesní záznamy.

Řídící záznam vede záznamy o všech zpracovatelských činnostech prováděných v rámci odpovědnosti ÅF jako správce, tj. pokud ÅF, samostatně nebo společně s ostatními, určuje účel a prostředky zpracování osobních údajů.

Procesní záznamy vedou údaje o zpracovatelských činnostech prováděných v rámci odpovědnosti ÅF jako zpracovatele, tj. v případech kdy ÅF jako správce zpracovává osobní údaje. Zpracovatelské činnosti musí být pokryty a probíhat v souladu s Řídícími záznamy.

Smlouva o zpracování osobních údajů

Pokud osobní údaje zpracovává jiný zpracovatel než správce osobních údajů, je potřeba zajistit smlouvu o zpracování osobních údajů. Ve smlouvě musí být uveden důvod a podmínky zpracování, povinnosti smluvních stran a osobní údaje, kterých se zpracování týká, stejně tak jako doba, po kterou bude zpracovatel údaje zpracovávat.

Zpracování jiným zpracovatelem než správcem osobních údajů, je zahrnuto i do dokumentu Postupy ochrany osobních údajů (Data Privacy Procedure), kde jsou uvedeny základní informace ze Smlouvy o zpracování osobních údajů.

Při potenciální revizi nebo auditu provedeném správcem ÅF Data Privacy Manager je důležité, aby se všechny související dokumenty mohly snadno dohledat. A proto v dokumentu Postupy ochrany osobních údajů musí být uvedeno, kde je Smlouva o zpracování osobních údajů uložena.

Interní kontrola
Pravidelný audit procesů upravuje dokument Zásady ochrany osobních údajů ÅF (Data Privacy Policy). Kontroly se provádí pravidelně nebo se provádí i tzv. ad hoc audity. Vedoucí oddělení ochrany osobních údajů vede auditorské činnosti a je v případě potřeby podporován organizací interního auditu ÅF.

5.5 Školení

Školení probíhalo v celé skupině ÅF na dvě etapy, počáteční školení a zasvěcení do problematiky GDPR zabezpečila mateřská základna ve Švédsku pro všechny ostatní pobočky. Druhá etapa školení probíhala v každé jednotlivé divizi zvlášť, po implementaci GDPR a seznámení s jeho principy mezi zaměstnanci. Průběh obou etap školení je popsán v následujících kapitolách.

Cílem školení bylo seznámit všechny zaměstnance s principy Obecného nařízení, s jeho účelem a ovlivnit chování zaměstnanců tak, aby se zacházelo s osobními a citlivými údaji v souladu s Obecným nařízením a vyvarovat se tak případným chybám při zpracování.

5.5.1 Školení vedoucích zaměstnanců

Nejdříve školení probíhalo na jaře a v létě roku 2017, kdy se mateřská základna ÅF zabývala případovou studií a nastavením standardů pro všechny ostatní pobočky. Pro nastavení standardů využila služeb firmy Legal Works, která právně zajišťovala správnost implementace Obecného nařízení v ÅF.

Školení probíhalo formou e-learningu i praktických přednášek, které byly určeny pouze pro správce dané divize, ty, kteří měli implementovat GDPR ve své divizi. E-learning obsahoval průběžné rozposlání prezentací o GDPR a obecné implementaci na systémy v ÅF. Některé e-learningové prezentace byly mezi správce systémů rozposlány a upraveny pomocí aplikace eMarketeer.

V rámci e-learningu museli správci jednotlivých systému projít školením skrze internetový portál ÅF Academy ve 4 modulech. Každý modul obsahoval jednu oblast Obecného nařízení. Pro důkaz úspěšného projití tímto školením bylo, že každý modul obsahoval otázky, na které musel správce systému odpovědět. Pokud nedostal alespoň 80 %, tak školením neprošel.

Přednášky a workshopy probíhaly každý druhý týden, kde se účastnili správci systémů a určený GDPR koordinátor. Byly zde projednávány všechny body z případové studie a GAP analýzy. Na těchto praktických přednáškách se rozebíraly a vyvíjely všechny plánované řešení implementace principů GDPR v interních systémech a standardech chování zaměstnanců.

Přednášky a školení na sebe navazovaly, s tím, že nejdříve proběhlo seznámení s Obecným nařízením a dále postupné body implementace a úprav, které vyplynuly z GAP analýzy. Každá jednotlivá řešení úprav byla řádně dokumentována.

5.5.2 Školení zaměstnanců

Po implementaci principů GDPR a sepsání všech vnitřních předpisů, které upravují ochranu osobních údajů, bylo potřeba zaškolit všechny zaměstnance o nových interních pravidlech. Seznámit je se změnami legislativy, tedy Zákona o ochraně osobních údajů a Obecného nařízení (GDPR). Cílem školení bylo seznámit zaměstnance s pravidly chování při zpracování a zabezpečení ochrany osobních údajů a vymezit nebo odstranit možné chybování a následné incidenty.

Zaměstnanci byli školeni pomocí e-learningu v aplikaci eMarketeer (popis systému a školení níže) a praktických přednášek. Školení probíhalo na základě třech dokumentů zmíněných v kapitole 5.2.1 Vnitřní předpisy GDPR – Zásady ochrany osobních údajů, Standardy ochrany osobních údajů, Postupy ochrany osobních údajů.

Prvním krokem školení bylo seznámení zaměstnanců s Obecným nařízením a se změnami, které přineslo. Seznámení s Obecným nařízením proběhlo pomocí zmíněného e-learningu. V druhé části školení byly praktické přednášky, kde byli zaměstnanci seznámeni s konkrétními změnami a byli seznámeni s novými postupy při shromažďování, zpracování a uchovávání osobních údajů. Dále jim byla definována a přidělena přístupová práva do jednotlivých aplikací, systémů a úložišť. A dále jim bylo vysvětleno chování na pracovišti včetně práce s novými standardy zabezpečení osobních údajů na počítačích.

Noví zaměstnanci absolvují školení o ochraně osobních údajů jako součást procesu adaptace na pracovní pozici. Přičemž proces přijímání nových zaměstnanců je pospán v kapitole 5.4 Dopady implementace v oblastech organizace.

Aplikace eMarketeer

E-learning zaměstnanců probíhal ve společnosti AF-Consult Czech Republic s.r.o. pomocí aplikace eMarketeer. Aplikace eMarketeer umožňuje uživatelům přehledně, snadně a účelně tvořit marketingovou kampaň. Je všestranný model aplikace, který umožňuje snadné kombinování e-mailů, formulářů, sms zpráv a webových stránek pro

usnadnění marketingového zacílení. eMarketeer v jedné platformě zjednodušuje způsob vytváření potenciálních zákazníků nebo jednodušší komunikaci uvnitř společnosti se svými zaměstnanci.

Společnost ÅF využívá tuto platformu především pro interní komunikaci. V eMarketeeru tvoří pozvánky na společenské akce, formuláře pro personální i jiné účely, různé marketingové letáky, školení nebo informační letáky, ale hlavně emailovou komunikaci propojenou se zmíněnými výběry.

V první fázi školení ve společnosti AF-Consult Czech Republic s.r.o. bylo potřeba seznámit všechny zaměstnance s Obecným nařízením a rozposlat jim Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance – GDPR, s tím, že byli seznámeni se základy GDPR.

V informačním emailu z aplikace eMarketeer, se v rámci školení zaměstnanci dozvěděli, co obnáší Obecné nařízení a jaké změny přináší ve společnosti AF-Consult Czech Republic s.r.o. Součástí emailu byl odkaz na informativní leták tzv. zjednodušenou formu směrnice o ochraně osobních údajů a odkaz na Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance – GDPR.

Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance si zaměstnanci z emailu vytisknou a podepíší. V tomto záznamu jsou uvedena oprávnění zaměstnavatele zpracovávat osobní údaje v souvislostech pracovněprávního vztahu a poskytovat některé osobní údaje třetím stranám, jiným zpracovatelům, například poskytovateli zpracování mezd, příslušné zdravotní pojišťovně, správě sociálního pojištění, plátci důchodu atp.

V tomto dokumentu je uvedeno oznámení o omezení zpracování osobních údajů po určitou nezbytně nutnou dobu. Zpracovávat osobní údaje může zaměstnavatel ode dne uzavření pracovněprávního vztahu po dobu trvání pracovního poměru. Po jeho ukončení jen po dobu určenou právními důvody a českou legislativou.

V Záznamu o instruktáži je jediná uvedená povinnost zaměstnanců, a tou je „povinnost předávat zaměstnavateli osobní údaje pravdivé, přesné a aktuální. V případě jejich změny je povinen změnu neprodleně zaměstnavateli oznámit.

Zaměstnanec potvrzuje svým podpisem (Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance – GDPR, ÅF 2018):

- že byl zaměstnavatelem seznámen se skutečností, že poskytování osobních údajů pro plnění povinností zaměstnavatele vyplývajících z pracovněprávních vztahů je povinné,
- že byl seznámen s právem na přístup ke svým osobním údajům, právem na jejich opravu, výmaz, vysvětlení od zaměstnavatel v případě, že pojme podezření,

že zpracováním osobních údajů je narušena ochrana soukromého a osobního života nebo že osobní údaje jsou zpracovávány v rozporu s právními předpisy,

- že byl informován o právu na nápravu s nakládáním s jeho osobními údaji, je-li v rozporu s právními předpisy, zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním, či odstraněním,
- že byl upozorněn na právo kontaktovat dozorový orgán – Úřad pro ochranu osobních údajů v případě podezření, že dochází k neoprávněnému nakládání s jeho osobními údaji, nebo že bylo odmítnuto zajištění nápravy situace, která je v rozporu s právními předpisy,
- že byl ke dni, seznámen/a se směrnicí Ochrana osobních údajů – GDPR.

Závěr

Cílem této diplomové práce bylo prozkoumat zavádění nového Nařízení o ochraně osobních údajů (GDPR) ve společnosti AF-Consult Czech Republic s.r.o. a představit návrh implementace jednotlivých principů GDPR z pohledu správce. K naplnění těchto cílů vedla celá řada kroků, od seznámení se s principy a požadavky Obecného nařízení, po zkoumání procesů ve sledované společností až po praktické využití znalostí a navrhování řešení implementace ve společnosti.

Popis implementace GDPR v diplomové práci byl zhotoven až po implementaci principů GDPR, proto jsou jednotlivé návrhy na implementaci principů GDPR psané v případové studii praktické části (5.1 Případová studie). Další kapitoly vlastní implementace principů GDPR jsou psané již dle zmíněných návrhů a dle konkrétních proběhlých změn ve společnosti AF-Consult Czech Republic s.r.o.

Nejprve byla provedena případová studie externí společnosti Legal Works začátkem roku 2017, kterou zajišťovala mateřská základna ÅF. Tato případová studie sloužila jako vstupní analýza stavu před implementací Obecného nařízení všech společných systémů a systémů mateřské základny ÅF. Tato případová studie sloužila pro všechny pobočky skupiny ÅF jako vzor pro vlastní případovou studii a GAP analýzu, každé jednotlivé pobočky.

V době, kdy byla Případová studie poslána jako vzor pro ostatní pobočky skupiny ÅF, bylo zajištěno také vstupní školení, pro správce ostatních poboček, formou e-learningu i praktických přednášek. Správci jednotlivých poboček pak měli k dispozici dostatek informací a standardizovaných vzorů pro zpracování případové studie a následnou implementaci principů GDPR do jednotlivých poboček.

V případové studii ve vybrané společnosti AF-Consult Czech Republic s.r.o., byly zkoumány všechny procesy, které jsou jakýmkoli způsobem spojeny s osobními údaji subjektů údajů. Z této analýzy byly zjištěny neshody s Obecným nařízením a k jednotlivým neshodám byl přiřazen návrh na implementaci principů GDPR. Na základě přehledu neshod a návrhů byl stanoven časový harmonogram činností k naplnění souladu procesů s Obecným nařízením k 25. květnu 2018.

Na základě zjištěného stavu ve společnosti AF-Consult Czech Republic s.r.o. se v průběhu implementace principů GDPR sepisovali všechny potřebné dokumenty a směrnice. Sepsání takových dokumentů je jedním z úkolů správné implementace GDPR v organizaci. Mezi nejdůležitější patří interní Směrnice společnosti, která stanovuje základní požadavky, povinnosti a práva v souvislosti se zpracováním osobních údajů fyzických osob ve společnosti AF-Consult Czech Republic, s.r.o. Dále pak dokumenty Zásady ochrany osobních údajů, Standardy ochrany osobních údajů a Postupy ochrany osobních údajů (viz kapitola 5.2.1 Vnitřní předpisy GDPR).

Hlavní částí této diplomové práce je vlastní implementace principů GDPR ve společnosti AF-Consult Czech Republic, s.r.o. Teoreticky jsou hlavní principy Obecného nařízení popsány v kapitole 2.4 Hlavní principy GDPR a popis praktické implementace je v kapitole 5.2 Vlastní implementace principů GDPR. V teoretické části jsou popsány jednotlivé principy a v praktické části jsou rozděleny do jednotlivých procesů, které se v podniku uskutečnily při implementaci Obecného nařízení.

Při implementaci principů bylo v první řade potřeba zjistit, jaké informační systémy zpracovávají osobní údaje a vypsat konkrétní zpracovávané osobní údaje. Ve společnosti AF-Consult Czech Republic s.r.o. bylo zjištěno padesát devět informačních systému, které zaznamenávají nebo pracují s osobními údaji. Od takto rozdělených osobních údajů se odvíjelo posouzení dopadu rizik, minimalizace údajů, určení účelu údajů nebo souhlas se zpracováním osobních údajů a zabezpečení osobních údajů. Pro účely diplomové práce byly vybrány pouze čtyři informační systémy, které jsou vidět v tabulkách 2 Posouzení dopadu rizik, 3 Minimalizace údajů, 4 Určení účelu údajů a 5 Zabezpečení osobních údajů.

Při posouzení dopadu rizik, bylo u systémů společnosti AF-Consult Czech Republic s.r.o. zjištěno, že většina systémů již nepotřebuje další nutná zabezpečení, jelikož mají nízké riziko. Ale u některých informačních systémů vyšla střední úroveň rizika a bylo potřeba udělat menší dodatečná opatření k zabezpečení osobních údajů v konkrétních systémech.

Minimalizace zpracovávaných osobních údajů a omezení uložení lze vidět v kapitole 5.2.3 Minimalizace údajů, kde byly jednotlivé osobní údaje zhodnoceny. Ve vzorku zkoumaných systémů bylo zjištěno, že některé údaje nejsou pro stanovený účel potřebné. Osobní údaje, které byly vyhodnoceny jako nepotřebné, byly smazány a osobní údaje, které již nebyly potřebné pro aktuální činnost, ale musí se uchovat, byly archivovány a přístup k nim je omezen heslem. Některé osobní údaje v informačních systémech nebyly aktuální, a proto proběhla, na základě tohoto zjištění, aktualizace údajů.

Dalším krokem implementace Obecného nařízení do společnosti bylo určení účelu neboli přiřazení právního titulu osobním údajům. Ke každému systému byl přiřazený účel zpracování osobních údajů a zda je potřebný souhlas se zpracováním osobních údajů. Dále pak zda má správce souhlas k dispozici a kde je uložen. K zabezpečení všech mezer právních účelů byly vytvořeny tři souhlasy o zpracování osobních údajů, a těmi jsou:

1. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro zaměstnance,
2. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro fyzické osoby a subdodavatele,
3. Souhlas se zpracováním osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 pro osoby ucházející se o zaměstnání.

Posledním krokem vlastní implementace je zabezpečení osobních údajů (kapitola 5.2.6 Zabezpečení osobních údajů). K určení zabezpečení všech osobních údajů, aby bylo v souladu s Obecným nařízením, bylo potřeba udělat přehled o tom, jaké osobní údaje se zpracovávají a v jakých systémech (toto již bylo určeno v předchozích krocích). Dále pak kdo má přístup k daným osobním údajům, jak jsou data zabezpečena, komu mohou být udělena přístupová práva a jakým způsobem se mohou udělit nebo zrušit přístupová práva a kdo odpovídá za udělení přístupových práv.

Se změnou právní legislativy, která upravuje ochranu osobních údajů v celé Evropské unii, se nejen ve společnosti ÅF změnily anebo přidaly nové procesy týkající se zpracování a ochrany osobních údajů. Procesy, které byly do společnosti zařazeny a jsou v souladu s Obecným nařízením, jsou např. změna přijímání nových zaměstnanců, která má nyní šest kroků, včetně podepsání dvou souhlasů o zpracování osobních údajů. Proces přijímání zaměstnanců je popsán v kapitole 5.4 Dopady implementace v oblastech organizace.

Mezi další nově vzniklé procesy patří Oznámení o ochraně osobních údajů, Žádost o výmaz, Žádost o přenos, hlášení incidentů, povinnost dělat záznamy o činnostech zpracování osobních údajů, Smlouva o zpracování osobních údajů v případě jiného zpracovatele a interní kontrola. Popis všech těchto nových procesů je v kapitole 5.4.1 Nově vzniklé procesy.

Ve společnosti AF-Consult Czech Republic s.r.o. nebyl jmenován Pověřenec pro ochranu osobních údajů (DPO), neboť ke jmenování nevznikla povinnost. Společnost AF-Consult Czech Republic s.r.o. nemá povinnost jmenovat pověřence, jelikož není orgánem veřejné moci, ani pravidelně nemonitoruje občany státu a ani nezpracovává zvláštní kategorii osobních údajů (citlivé údaje).

Po veškeré implementaci principů GDPR proběhlo školení všech zaměstnanců. Školení probíhalo nejprve formou e-learningu přes interní aplikaci eMarketeer, kde se zaměstnanci seznámili s Obecným nařízením, se svými právy, povinnostmi správců a se sankcemi za porušení podmínek GDPR. Dalším krokem byly praktické přednášky, kde se zaměstnanci seznámili s konkrétními změnami a s novými procesy v praxi.

Stanovené cíle diplomové práce byly splněny, neboť prozkoumání zavádění nového Nařízení o ochraně osobních údajů je popsán v praktické části. V rámci implementace Obecného nařízení do společnosti AF-Consult Czech Republic s.r.o. byly navrhnuty některá opatření, které jsou v souladu s Obecným nařízením. Prozkoumání, návrhy a popis celé implementace principů GDPR z pohledu správce ve společnosti AF-Consult Czech Republic s.r.o. jsou vidět v celé praktické části.

Přínosem práce je vymezení postupu implementace principů GDPR, který může být využitelný i v jiných společnostech. Postup implementace v praktické části a závěry jsou přínosné pro velké, střední i malé podniky, které podléhají nové legislativě upravující

ochranu osobních údajů. Střední a malé podniky mohou absolvovat celý postup implementace v menším rozsahu. Zjištěné skutečnosti z teoretické i praktické části mohou být přínosem i pro subjekty údajů, kteří chtějí znát svá práva v souvislosti se zpracováním osobních údajů v praxi. Největším přínosem této diplomové práce je pro konkrétní společnost AF-Consult Czech Republic s.r.o., které poslouží jako dokumentace celého postupu implementace principů GDPR.

Seznam použité literatury

Odborná literatura

BARTÍK, Václav; JANEČKOVÁ Eva, 2013. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vyd. Praha: Linde. 311 s. brož. ISBN:978-80-86131-96-2

BOLOGNINI, Luca, Camilla BISTOLFI, 2017. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review [online]. ISSN: 0267-3649.

CALDER, Alan, 2016. *EU GDPR: A Pocket Guide. United Kingdom*: IT Governance Publishing. ISBN 978-1-84928-833-0.

DOHNAL, J. POUR, J, 2016. *IT v řízení podniku MBI*. Praha: Professional Publishing. ISBN 978-80-7431-160-4.

GODDARD, Michelle, 2017. *The EU Data Protection Regulation (GDPR): European re-gulation that has a global impact*. International Journal of Market Research [online]. ISSN: 1470-7853.

HŮRKA, Petr, 2009. *Ochrana zaměstnance a flexibilita zaměstnávání: princip flexijistoty v českém pracovním právu*. Praha: Auditorium. ISBN 978-80-87284-04-9.

CHLÁDKOVÁ, Alena a BUKOVJAN, Petr, 2015. *Personalistika – dvanáctero správného vedení personální agendy podle zákoníku práce v roce 2015*. Wolters Kluwer, 528 stran ISBN: 978-80-7478-692-1

JANEČKOVÁ, Eva a Václav BARTÍK, 2016. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika. ISBN 978-80-7552-145-3.

JANEČKOVÁ, Eva, 2018. *GDPR: praktická příručka implementace.* Vydání první. Praha: Wolters Kluwer. xiii, 119 stran ISBN:978-80-7552-248-1

JOUZA, Ladislav, 2004. *Předpisy z pracovního práva, které vydává zaměstnavatel*. Praha: Polygon. ISBN 80-7273-096-7.

KUČEROVÁ, Alena a František NONNEMANN, 2013. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON. ISBN 978-80-7273-173-2.

MATES, Pavel, 2002. *Ochrana osobních údajů*. Praha: Karolinum. ISBN 80-246-0469-8.

MORÁVEK, Jakub, 2013. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer. 435 s. brož. (Právní rukověť) ISBN:978-80-7478-139-1

Mzdy od A do Z: výklad je zpracován k právnímu stavu ke dni .. 10. vyd. Praha: ASPI, 2013. Meritum (ASPI). ISBN 978-80-7357-998-2.

NEZMAR, Luděk, 2017. *GDPR: praktický průvodce implementací* / Luděk Nezmar. První vydání. Praha: Grada Publishing. 301 stran: ilustrace; (Právo pro praxi) [Terminologický slovník] ISBN:978-80-271-0668-4

NULÍČEK, Michal, 2017. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2. vydání. ISBN 978-80-7598-068-7.

WAGNEROVÁ, Irena, 2011. *Legislativní kontext personální psychologie*. Praha: I. Wagnerová. ISBN 978-80-254-9039-6.

ŽŮREK, Jiří, 2017. *Praktický průvodce GDPR*. 1. vydání. Olomouc: Anag. 223 stran (Právo) [Autorská uzávěrka 9. října 2017] ISBN:978-80-7554-097-3

Právní předpisy

Nařízení Evropské Parlamentu a Rady (EU) č. 679/2016 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2018-04-12].

Ochrana osobních údajů; GDPR [ÚZ 2017 č. 1209] Ostrava: Sagit, 2017. 111 stran; (ÚZ: úplné znění; číslo 1209) ISBN:978-80-7488-241-8

Zákon o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

Zákoník práce: 2014: redakční uzávěrka 14.10.2013. Ostrava: Sagit, 2013. ÚZ. ISBN 978-80-7488-010-0.

Interní předpisy společnosti AF-Consult Czech Republic, s.r.o.

ÅF AB, 2018. *Data Privacy Policy.* Stockholm, Sweden.

ÅF AB, 2018. *Data Privacy Procedure.* Stockholm, Sweden.

ÅF AB, 2018. *Data Privacy Standards.* Stockholm, Sweden.

AF-Consult Czech Republic s.r.o., 2018. *Záznam o instruktáži týkající se zpracování osobních údajů zaměstnance – GDPR.* Praha.

Odborné články

GDPR od A do Z. *IT Systems*. 2018, 1-2/2018 (1), 43–47.

GDPR změní některé dosavadní zvyklosti. *Sdělovací technika*. 2017, 12/2017 (12), 10–11.

Internetové zdroje

About AF Consult. *Afconsult* [online]. [cit. 2018-11-14]. Dostupné z: http://www.afconsult.com/en/about-af/

Implementace GDPR. SPMO [online]. Praha: CATANIA GROUP, 2017 [07.11.2018]. Dostupné z: https://spmo.cz/wp-content/uploads/2017/07/Implementace-GDPR-e-kniha.pdf

Jaké jsou sankce za nedodržení GDPR? *GDPR | Pověřenec pro ochranu osobních údajů* [online]. DPO4U.cz [cit. 07.11.2018]. Dostupné z: https://www.dpo4u.cz/l/jake-jsou-sankce-za-nedodrzeni-gdpr/

11. Sankce, pokuty: Základní příručka k GDPR: Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Úřad pro ochranu osobních údajů. [cit. 07.11.2018]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287/p1=4744

Seznam obrázků

Seznam tabulek

Evidence výpůjček

Prohlášení:
Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Bc. Pavla Mrázová
V Praze dne: Klikněte nebo klepněte sem aPodpis:
zadejte datum.

Jméno	Oddělení/ Pracoviště	Datum	Podpis