Univerzita Karlova

Filozofická fakulta

Katedra pomocných věd historických a archivního studia

Bakalářská práce

Vliv a dopad GDPR na firmy a obyvatele

The influence and impact of GDPR on business and citizens

Pavlína Mladá

Praha 2020 Vedoucí bakalářské práce: PhDr. Daniela Brádlerová Ph.D.

„Prohlašuji, že bakalářkou práci na téma Vliv a dopad GDPR na firmy a obyvatele jsem vypracovala samostatně, že jsem řádně ocitovala všechny použité prameny a literaturu, které jsou uvedeny v poznámkovém aparátě a v seznamu použitých zdrojů.“

V Praze, dne 1. 8. 2020

……..

Pavlína Mladá

Poděkování:

Ráda bych tímto poděkovala paní PhDr. Daniela Brádlerová Ph.D. za vedení mé bakalářské práce, za cenné rady, odborný dohled, trpělivost a ochotu, kterou mi v průběhu zpracovávání bakalářské práce věnovala. Dále bych chtěla poděkovat svojí rodinně za podporu po celé období mého studia, nejvíce pak právě v průběhu psaní mé bakalářské práce.

Anotace:

Za cíl své bakalářské práce si kladu seznámit čtenáře s Obecným nařízením o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR), jeho dopadu jak na firmy, tak na samotné občany, a poukázat na časté chyby vznikající v souvislosti s nedodržováním platných právních ustanovení. V úvodu krátce přiblížím předcházející zákony a vládní ustanovení, na které bude navazovat analýza samotného nařízení GDPR. V souvislosti s tím také zmíním elektronický systém spisové služby a informační systém datových schránek (ISDS). Dále se budu věnovat rozdílům napříč zákonnými předpisy národní i mezinárodní povahy. Poté přiblížím samotný dopad všech nařízení na chod firem, jejich zaměstnanců a klientů.

Abstract:

The aim of my bachelor thesis is to acquaint readers with General Data Protection Regulation, its impact on businesses, citizens themselves, and to point out frequent mistakes that arise in connection with non-compliance with applicable legal provisions. In the introduction, I will briefly present the previous laws and governmental provisions, which will be followed by an analysis of the GDPR regulation itself. In connection with this, I will also mention the electronic document and records management system and the data box information system (ISDS). Furthermore, I will describe address the differences across legal regulations of a national and international nature. I will also then describe the impact of all regulations on the operation of companies, their employees, and clients.

Klíčová slova:

Archiv, dokument, Evropská Unie, firmy, GDPR, kancelář, Komise, kybernetická data, osobní údaje, Sbor, smlouvy, vládní nařízení, zaměstnanci

Key words:

Archives, document, European Union, business, GDPR, office, Commission, cybernetic data, personal data, EDPB, contracts, government regulation, staff

Obsah

1. Úvod

V dnešní době se čím dál tím víc setkáváme s nutností poskytovat naše osobní údaje různým subjektům: v rámci uzavírání smluv různého charakteru, registrací do věrnostních programů nejrůznějších firem či v zdravotnických organizací, např. přechod do péče praktického lékaře, změně pojišťovny apod. Při takovém množství citlivých osobních údajů je kladen stěžejní požadavek na ochranu a zabezpečení informací o subjektech, tak aby nemohlo dojít k jejich případnému zneužití. K řádnému zabezpečení předaných informací je tedy nezbytné uvést v platnost několik příslušných vládních nařízení, které upraví postup, zajistí ochranu a uchovávání dokumentů a dat. I přes nutnost ochrany osobních údajů nesmíme pominout právo občanů na svobodný přístup k informacím, který se však s přibývajícími opatřeními stále více omezuje a zpřístupňována mohou být pouze taková data neumožňující svým obsahem, jakkoliv poškodit práva či způsobit újmu poskytovateli. Výjimky jsou pak stanoveny zvláštním zákonem, v případě činnosti spojené s archivními účely, u podezření ze spáchání trestného činu, při ohrožení života subjektu apod.

V následujících kapitolách se budu věnovat dřívějším i stávajícím vládním nařízením tedy: zákonu č. 106/1999 Sb., o svobodném přístupu k informacím; zákonu č. 101/2000 Sb., o ochraně osobních údajů; zákonu č. 181/2014 Sb., o kybernetické bezpečnosti; nařízení EU 2016/679, o ochraně osobních údajů (GDPR); směrnici Evropského parlamentu a Rady (EU) 2016/680, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů; zákonu č. 110/2019 Sb., o zpracování osobních údajů; a jejich vlivu na české firmy a občany. Ve své práci si mimo obecného seznámení s danou tématikou kladu za cíl rozšířit povědomí o možných chybách, kterých se často dopouštějí sami pracovníci daných zařízení, v důsledku nekompetentního přístupu ať už ze strany jejich zaměstnavatelů, kteří nezajistili dostatečné proškolení, nebo jich samotných. Je až trestuhodné, jak často se setkáváme se zneužitím našich osobních dat, která by měla být v rámci zákonů a mezinárodních smluv chráněna, a přesto jsou nadále předávána. Ne vždy jsou však na vině správci či zpracovatelé dat. Tyto informace se mohly jakýmkoliv způsobem dostat k třetí osobě, ještě v době před zavedením GDPR a zákonu na ochranu osobních údajů, která nadále neoprávněně čerpá z jejich neoprávněného shromáždění.

Dále se budu věnovat analýze celkového stavu a postupu mnou oslovených firem ve srovnání s platnými právními nařízeními, vzájemnému porovnání jejich praktik a jejich celkovému přístupu. V neposlední řadě představím průzkum veřejného mínění na toto téma. S příchodem nařízení GDPR vyvstalo několik otázek a také mírná panika ze strany občanů,

jelikož si nebyli schopní představit, v jak velkém rozsahu se nařízení dotkne jejich životů. I dnes GDPR představuje pro mnohé lidi velkou neznámou. Někteří ho považují jen za nařízení, které je nutné dodržovat. Většina z nich se pak při podpisu souhlasu ani nesnaží seznámit, s čím vlastně souhlasí u potvrzování podmínek o zpracování. Berou ho jako nezbytnost, kterou musí v rámci registrace či podpisu smlouvy udělat.

V závěru se budu věnovat účinnosti vládních a mezinárodních nařízení, zhodnocení získaných poznatků, návrhu na možná řešení nedostatků pro jejich nejrychlejší odstranění v oslovených firmách, aby tak bylo možné předejít zneužití informací citlivého charakteru.

2. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Je stávajícím platným nařízením vydaným Parlamentem České republiky dne 11. května 1999. Zákon zpracovává směrnici Evropského parlamentu a Rady 2003/98/ES ze dne 17. listopadu 2003 o opakovaném použití informací veřejného sektoru a směrnici 2013/37/EU ze dne 26. června 2013, kterou se mění směrnice 2003/98/ES, a která upravuje pravidla, a podmínky pro svobodný přístup k informacím.[1] Subjekty povinné k poskytování informací v rámci jejich působnosti jsou státní orgány, územně samosprávné celky a jejich orgány, veřejné instituce, subjekty rozhodující o právech, právem chráněných zájmem a povinnostech fyzických či právnických osob v sektoru veřejné správy. V případě, že se jedná o centrální evidenci účtů, průmyslové vlastnictví nebo zvláštní zákony, informace se neposkytují. Zákon se také nevztahuje na zpřístupnění dotazů na názory, budoucí rozhodnutí či vytváření nových.[2] Za žadatele se považuje každá fyzická či právnická osoba, která o ně zažádá. Pro dálkový přístup k datům žadatel využívá sítě nebo služby elektronických komunikací. Informací se rozumí celek nebo její část v listinné, analogové či digitální podobě, uložená na jakémkoliv nosiči. Je nutné zdůraznit, že za ni nepovažujeme počítačový program. Po svém zveřejnění musí být informace dále dohledatelná s možností dalšího uschování a opětovného znovu zveřejnění. Formát datového souboru, který umožňuje snadné dohledání, rozpoznání a získávání s jednotlivými údaji, nazýváme strojově čitelným formátem. Otevřeným formátem pak formát datového souboru nezávislého na konkrétních technických či programových vybavení, který je zároveň přístupný veřejnosti bez omezení. Za otevřenou formální normu považujeme pravidlo, vydané písemně upravující specifické požadavky na zajištění programů, vzájemné poskytování služeb a spolupráci. Metadaty pak data, která popisují obsah, strukturu a souvislost s informací a její průběh v čase. Dálkový přístup v otevřené a strojově čitelném formátu bez omezení přístupu zajišťují otevřená data. Jejich evidenci je možno ověřit v národním katalogu otevřených dat.[3] K podání žádosti může dojít ústní formou, v případě že bylo ústní podání shledáno nedostačujícím, je nutné ji opakovaně podat písemně.[4] Na žádost podanou písemnou formou, je pak informace zpřístupněna ve formátech a jazycích, v nichž byla společně s příslušnými metadaty vytvořena. Poskytovatelem na základě žádostí či zveřejňování je povinný subjekt. Ten není povinen měnit jazyk, formát či metadata nebo je vyjímat z většího celku, pokud by mu to činilo nepřiměřenou zátěž. V případě nutnosti předá celý soubor nebo,

[1] § 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
[2] § 2 zákona č. 106/1999 Sb.
[3] § 3 zákona č. 106/1999 Sb.
[4] § 13 zákona č. 106/1999 Sb.

může soubor poskytnout v elektronické podobě pro usnadnění procesu. Zpřístupnění probíhá v digitální či listinné podobě a má různou formu: může se jednat o originál nebo kopii, datový soubor či nahlédnutí do datového souboru, sdílením dat nebo umožnění dálkového přístupu k nim. V případě nemožnosti předání zmíněnými postupy je možná dohoda s žadatelem na jiném způsobu vyřízení.[5] Zveřejňování pro veřejnost by mělo být dostupné na všeobecně přístupném místě. Subjekty pověřené zpřístupňováním jsou povinni doložit důvod a způsob svého založení včetně činnosti jimi provozované, popis své organizační struktury, způsob, jakým lze podat žádost, stížnost či návrh, postup při vyřizování žádostí, podání opravných prostředků proti rozhodnutím, přehled nejdůležitějších předpisů, sazebník úhrad, usnesení nadřízených orgánů o výši úhrad a informace o elektronické adrese podatelny. Poskytovatelé mají povinnost ve svém sídle v úředních hodinách, zpřístupňovat právní předpisy související s jejich působností a seznamy hlavních dokumentů, tak aby bylo možno pořídit si od nich kopii, opis či přepis. Dále pak musí umožnovat dálkový přístup nebo odkázat na místo, kde je již informace tímto způsobem dostupná. Dále pak zpřístupňují přístup nebo ho předávají správci portálu veřejné správy.[6] Poskytnutí žadateli není přípustné v případě, že žadatel podléhá zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Jedná se tedy o utajovanou skutečnost, dokumenty označení jako Přísně tajné nebo Tajné, kde by v případě jejich zveřejnění mohlo dojít k ohrožení utajení.[7] Tentýž postup je uplatněn v případě obchodního tajemství či stavu majetkového poměru. Omezení na poskytnutí se uplatní v případě vztahu vnitřních pokynů a personálních předpisů, věcí označených značkou „NATO UNCLASSIFIED“ nebo „LIMITE“ poskytnuté Organizací Severoatlantské smlouvy, informací vzniklých v době zveřejňování, v případě ohrožení činnosti bezpečnostních opatření pro zajištění ochrany osob, majetku a veřejného pořádku nebo výkonu zahraniční služby na obranu České republiky jejich občanů zde i v zahraničí. K zamítnutí přístupu dojde v případě: vyžaduje-li to zvláštní zákon; při ochraně práv třetí osoby ve vztahu k autorským právům; pokud by byla ohrožena stabilita finančního systému; informace nevznikly z činnosti kontrolního úřadu a byly získány od třetí osoby, při trestním či soudním řízení. Dále se nezveřejnují: přípravy, průběhy a projednávání výsledků kontrol Nejvyššího kontrolního úřadu, činnosti Finančního analytického úřadu a evidence tržeb České Národní banky.[8] Poskytnutí

[5] § 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
[6] § 5 zákona č. 106/1999 Sb.
[7] § 7 zákona č. 106/1999 Sb.
[8] § 11 zákona č. 106/1999 Sb.

informací v souladu s právně stanoveným postupem není považováno na porušení mlčenlivosti.[9]

Zákon vešel v platnost 8. 6. 1999 a účinnosti nabyl 1. 1. 2000.[10] Jeho přechodná ustanovení dále upravují zákon č. 61/2006 Sb., zákon č. 222/2015 Sb., zákon č. 298/2016 Sb., a zákon č. 111/2019 Sb.

[9] § 19 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
[10] § 22 zákona č. 106/1999 Sb.

3. Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon fungoval jako základní právní předpis, který upravoval ochranu neoprávněných zásahů do soukromí, práva a povinnosti při práci s osobními údaji; stanovoval podmínky, za nichž se uskutečňovalo předávání do jiných států.[11] Byl vyhlášen v souladu s právem Evropské Unie[12] a mezinárodními smlouvami, kterými je vázána Česká republika.[13] Upravoval zřízení a činnost nově vzniklého Úřadu pro ochranu osobních údajů, fungujícího jako dozorový úřad.[14] Působnost se vztahovala na všechny osobní údaje zpracovávané státními orgány, orgány uzemní samosprávy, jinými orgány úřední moci, fyzickými a právnickými osobami, ať už ke zpracovávání docházelo automatizovaně či v jiné formě. Nevztahovala se na fyzickou osobu, která tak činila pouze za účelem své osobní potřeby a na nahodilé shromažďování informací, které nebyly dále zpracovávány. Zpracováním se rozumí: shromažďování; ukládání na nosiče informací; zpřístupňování, úprava či pozměňování; vyhledávání; používání; předávání šíření; zveřejňování; uchovávání v takové podobě, aby byly dále použitelné; výměna; třídění nebo kombinace; blokování a likvidace. Subjektem údajů se rozumí: určitý nebo určený subjekt, který můžeme přímo či nepřímo identifikovat na základě čísla a kódu, nebo jednoho či více prvků, který je specifický pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[15] Povinností správce bylo stanovení účelu, k němuž se budou shromážděné údaje využívat, prostředky a způsob jejich zpracovávání. Dále pak musel subjekt podléhající zájmu informovat a požádat o souhlas. Správce mohl vykonávat činnost i bez souhlasu, pokud jednal na základě nezbytného dodržení právní povinnosti správce, k ochraně životně důležitých zájmů subjektu či správce, k plnění smlouvy na návrh subjektu, k zveřejnění výlučně pro archivní účely nebo na základě zvláštního zákona. Výjimky povinnosti správce dále tvořily okolnosti nezbytné k zajištění bezpečnosti a obrany České republiky; veřejného pořádku a vnitřního bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky a Evropské unie; zpřístupňování svazků bývalé státní bezpečnosti a činnosti spojené s vedením centrální evidence tržeb.[16] Subjekt musel být vždy informován v jakém rozsahu, jakému správci a na jaké časové období se budou jeho údaje zpracovávat, pokud jinak nestanovil zákon. Svůj

[11] § 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[12] § 10 odst. 1 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).
[13] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 Sb. m. s.
[14] § 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[15] § 4 zákona č. 101/2000 Sb.
[16] § 3 zákona č. 101/2000 Sb.

nesouhlas mohl učinit písemnou formou, aby tak zabránil dalšímu zpracovávání, předávání za účelem obchodu či nabízení jiných služeb.[17] V případě zmocnění zákonným předpisem mohl správce poskytnout osobní údaje ke zpracování zpracovateli, také tak mohl učinit po uzavření smlouvy, pokud k tomu nebyl předtím oprávněn zákonným nařízením.[18] Zpracovatel byl nadále povinen, v případě podezření na zneužití nebo samotnému zneužití ze strany správce na tuto skutečnost upozornit a s okamžitou platností rozvázat smlouvy o vzájemné spolupráci, jinak by na tomto činu nesl stejnou zodpovědnost jako správce.[19] Oba nadále dbali, aby subjektu zájmů nevznikla újma na jeho právech.[20] Subjekt údajů mohl požádat o informace ke zpracování, v případě podání takové žádosti mu muselo být vyhověno.

Správce mohl požadovat přiměřený poplatek za náklady spojené s poskytnutím informací.[21] Zpracovatel i správce měli za povinnost přijímat opatření taková, aby nemohlo dojít k neoprávněnému nebo nahodilému zneužití. Dále bylo nutné zajistit technologicko-organizační opatření související s přejímáním a dokumentací, aby s dokumenty pracovaly pouze osoby s oprávněnou autorizační prověrkou v nezbytně nutném rozsahu. Nutné bylo určit postup ověřování a určování osoby, které byly předány nebo zpracovány informace, tak aby je bylo možné dohledat v případě vzniku možných nesrovnalostí. Zabránit neoprávněnému čtení, kopírování či jinému přenosu, a zajištění zabezpečení datových nosičů.[22] Zaměstnanci pracující s osobními údaji subjektu, byli vázáni smlouvou stanovující rozsah a podmínky v jakých s nimi mohli nakládat. Nadále byli povinni zachovávat mlčenlivost a bezpečnostní opatření, a to i po skončení lhůty stanovené pro zpracovávání, pouze v případě zvláštního zákona mohli toto nařízení porušit (např. v případě podezření na trestný čin).[23]

Osoba, která chtěla vykonávat funkci správce, byla povinna tuto skutečnost oznámit na Úřadu, a to před začátkem výkonu této činnost, aby byla provedena registrace. Nebylo-li do 30 dnů od podání žádosti zahájeno řízení, byl správce zapsán do registru. V žádosti zaslané úřadu bylo nutné uvést všechny nezbytné informace související s následným zpracováváním. V případě chybějících náležitostí byl správce obeslán s výzvou k doplnění, které bylo nezbytné podat, a to ve stanovené lhůtě 30 dnů. Pokud tak neučinil, bylo na žádost nahlíženo, že nebyla podána. Po provedení registrace úřad na žádost správce vydával osvědčení s identifikačními

[17] § 5 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[18] § 6 zákona č. 101/2000 Sb.
[19] § 8 zákona č. 101/2000 Sb.
[20] § 10 zákona č. 101/2000 Sb.
[21] § 12 zákona č. 101/2000 Sb.
[22] § 13 zákona č. 101/2000 Sb.
[23] § 15 zákona č. 101/2000 Sb.

údaji správce a s účelem registrace.[24] V případě vzniku obavy z porušení pravomocí, bylo z podnětu zahájeno řízení. Pokud osoby pověřené řízením došly k závěru, že nebyly porušeny žádné zákony či nařízení, řízení bylo zastaveno. Při zjištění nesplňujících podmínek, byla činnost zastavena a následně zrušena registrace.[25] Oznamovací povinnost se neuplatňovala v případě přítomnosti zvláštního zákona, na politické, filozofické, náboženské a odborové cíle sledované sdruženími v rámci jejich oprávněné činnosti, které se týkalo jejich členů či osob se kterými byla v častém kontaktu souvisejícím se zajištěním chodu jejich organizace. Osobní údaje však nadále nemohly být zpřístupňovány bez souhlasu subjektů organizace. Správce měl nadále za povinnost zajistit možnost poskytnutí na dálku či jinou vhodnou formou.[26] Rozhodnutí o ukončení činnost bylo rovněž nutné oznámit úřadu, jelikož bylo nezbytné informovat o postupu, jak naložil se svěřenými dokumenty.[27] Po uplynutí lhůty pro zpracovávání byl správce, popřípadě zpracovatel povinen provést likvidaci. Mohlo k tomu dojít i na přání subjektu. Výjimku tvořily archivní potřeby a uplatňování práv v civilním soudním řízení, správním a trestním řízení stanovené zvláštním zákonem.[28] Subjekt údajů mohl v případě domněnky či zjištění, že nebyla zajištěna dostatečná ochrana nebo zpracování, mohl požádat o vysvětlení a o okamžité odstranění vzniklého stavu. V případě že subjektu vznikla jiná újma, než majetková postupovalo se podle § 13 občanského zákoníku č. 40/1964 Sb., později podle občanského zákoníku č. 89/2012 Sb. Správce spolu se zpracovatelem pak bez rozdílu nesli stejnou odpovědnost.[29] Obecná náprava za škodu pak byla upravena dřívějším občanským zákoníkem č. 40/1964 Sb. a stávajícím obchodním zákoníku č. 513/1991 Sb.[30]

Předání údajů do států Evropské unie nemůže být omezen. U zemí třetího světa je omezení předávání vázáno na základě mezinárodních smluv nebo rozhodnutím orgánu Evropské unie. Informace mohly být poskytnuty do dalších zemí se souhlasem subjektu, v případě záruky, že dané země disponují dostatečnými bezpečnostními podmínky pro přijetí a zpracovávání, pokud se projevil zvláštní právní záměr, při uplatnění veřejného zájmu, při tvorbě, změně nebo plnění smlouvy, v případě ochrany práv či života subjektu. Před předáním je správce nucený oznámit tuto skutečnost úřadu a počkat na povolení o předání, obsahující

[24] § 16 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[25] § 17 zákona č. 101/2000 Sb.
[26] § 18 zákona č. 101/2000 Sb.
[27] § 19 zákona č. 101/2000 Sb.
[28] § 20 zákona č. 101/2000 Sb.
[29] § 21 zákona č. 101/2000 Sb.
[30] § 25 zákona č. 101/2000 Sb.

okolnosti, účel a dobu zpracovávání. Úřad může změnit či zrušit povolení v důsledku změny podmínek, pro které bylo povolení vydání, zejména z rozhodnutí Evropské unie.[31]

Úřad na ochranu osobních údajů je nezávislý orgán, postupující nezávisle, řídící se zákony a jinými platnými nařízeními, do jehož činnosti lze zasahovat pouze z nařízení zvláštního zákona.[32] Provádí dozor nad dodržováním povinností stanoveným zákonem, vede registr, přijímá podněty a stížnosti na nedodržování nařízení, zpracovává a zpřístupňuje výroční zprávu veřejnosti, projednává přestupky a uděluje pokuty, plní požadavky mezinárodních smluv, poskytuje konzultace, spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a jiných mezinárodních organizací. V případě kontroly se dříve postupovalo podle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů, nyní podle zákona č. 255/2012 Sb. U výkonu dozoru zpravodajskou službou je použit § 12 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, novelizovaný zákonem č. 325/2017 Sb. Ministerstvo vnitra a Policie České republiky poskytuje úřadu referenční údaje z registru obyvatel, ze systému evidence obyvatel a cizinců. Z předaných informací bylo možné využít jen nezbytně nutné ke splnění daného úkolu.[33] Pracovníky úřadu se rozumí předseda, inspektoři a další zaměstnanci. Kontroly provádí inspektoři nebo zaměstnanci k tomu pověření.[34] Kontrolní činnost se pak provádí na základě stanoveného plánu, podnětu nebo stížnosti.[35] Předseda je jmenován prezidentem republiky na dobu 5 let, maximálně na dvě funkční období. Je bezúhonný, způsobilý k právním úkonům, jeho znalosti, zkušenosti a morální hodnoty jsou předpokladem k řádnému vykonávání činnosti a má ukončené vysokoškolské vzdělání. Nesmí být členem politické strany ani hnutí, vykonávat funkci poslance, senátora, soudce či pracovat ve veřejné správě nebo územní samosprávě. Tato funkce je až na výjimky neslučitelná s výkonem ostatních zaměstnání, a to pouze pokud tato činnost nenarušuje důvěryhodnost, důstojnost, nezaujatost a nezávislost spojenou s úřadem (např. pedagogická, vědecká, literární, publicistická činnost, výdělečná činnost spjatá se správou osobního majetku). K odvolání dochází v důsledku nesplňování podmínek nutných pro jeho jmenování nebo v případě nečinnosti delší 6 měsíců.[36] Inspektor je jmenován a odvoláván prezidentem republiky. Funkční období je na dobu 10 let s možností opakovaného zvolení. Řídí a provádí další kontroly v působnosti úřadu, činnost řízení a kontroly pak celkově provádí sedm inspektorů. Výkon této

[31] § 27 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[32] § 28 zákona č. 101/2000 Sb.
[33] § 29 zákona č. 101/2000 Sb.
[34] § 30 zákona č. 101/2000 Sb.
[35] § 31 zákona č. 101/2000 Sb.
[36] § 32 zákona č. 101/2000 Sb.

činnosti je obdobný s podmínkami pro činnost předsedy úřadu. V případě nesplnění podmínek stanovených pro výkon funkce dochází k jeho odvolání.[37] Oprávnění kontrolující osoby se vztahuje na seznámení se s údaji v takovém rozsahu, který je nezbytně nutný pro řádné provedení kontroly, a to včetně citlivých.[38] Dále je povinen prokázat se průkazem, kterým je oprávněn k provádění kontroly.[39]

Inspektor je oprávněn nařídit nápravu zjištěných nedostatků plynoucích z porušení povinnosti stanovené zákonem a je oprávněn určit lhůty pro jejich odstranění. Úřad může dále upustit od uložené pokuty v případě nápravy protiprávního stavu.[40] V případě, že se fyzická osoba v zaměstnaneckém poměru se správcem nebo zpracovávatelem dopustí porušení povinnosti mlčenlivosti, dopouští se tak přestupku. Správce či zpracovatel se dopouští přestupku, pokud nestanový účel, prostředky a postup; údaje jemu svěřené zpracovává nepřesně nebo shromažďuje mimo účelu, který mu byl stanoven; překročuje dobu nutnou k uchovávání; činnost vykonává bez souhlasu; neposkytuje nebo odmítá poskytnout informace subjektu; nezajišťuje dostatečná bezpečnostní opatření; nesplňuje oznamovací povinnost; neprovedl ve stanovené lhůtě nápravná opatření; ohrozil větší počet osob svým neoprávněným zásahem do jejich soukromého a osobního života; porušil povinnost při zpracování citlivých osobních údajů. Pokuta se odvíjí podle závažnosti přečinu nejvýše však do výše 5 000 000 Kč.[41] Toto ustanovení dále platí pro právnické a podnikatelské osoby.[42] Přestupky podle toho zákona projednává a pokuty vybírá úřad.[43]

Tento zákon zrušil dosavadní zákon č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech,[44] dále novelizoval dosavadní zákon na svobodný přístup k informacím, který se nevztahuje na poskytnutí podle zvláštního právního předpisu.[45] Zákon byl schválen Parlamentem České republiky dne 4. 4. 2000, platnosti nabyl 24. 4. 2000, účinnosti pak dne 1. 6. 2000.[46] Novelizován byl na základě zákona č. 439/2004 Sb. Zrušen a nahrazen zákonem č. 110/2019 Sb., o zpracování osobních údajů dne 24. 4. 2019.[47]

[37] § 33 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení.
[38] § 37 zákona č. 101/2000 Sb.
[39] § 38 zákona č. 101/2000 Sb.
[40] § 40 zákona č. 101/2000 Sb.
[41] § 44 zákona č. 101/2000 Sb.
[42] § 45 zákona č. 101/2000 Sb.
[43] § 46 zákona č. 101/2000 Sb.
[44] § 48 zákona č. 101/2000 Sb.
[45] § 50 zákona č. 101/2000 Sb.
[46] § 51 zákona č. 101/2000 Sb.
[47] § 64 zákona č. 110/2019 Sb., o zpracování osobních údajů.

4. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Je platný právní předpis vydaným parlamentem České republiky dne 23. 7. 2014, upravující práva povinnosti a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zajišťuje úpravu bezpečnosti sítí elektronických komunikací a informačních systémů podle směrnice EU 2016/1148. Nevztahuje se na systémy utajovaných informací.[48] Pod pojmem kybernetický prostor bychom si měli být schopni představit prostředí, ve kterém je uživateli umožněno vytvářet a zpracovávat kybernetická data navzájem propojená v systému sítí, služeb a elektronických komunikací, podléhající zákonu č. 127/2005 Sb. Dále zde pracujeme s kritickým prvkem infrastruktury upravované vládním nařízením č. 432/2010 Sb. Za správce považujeme osobu či orgán určující podmínky zpracovávání, provozování a komunikace, poskytovatelem pak osobu či orgán určený Národním úřadem pro kybernetickou a informační bezpečnost.[49] Nezbytné je zajištění důvěrnosti, integrity a samotná dostupnost. Nutnost vzájemného propojení veřejných komunikačních sítí a zajištění chodu základní služby, jelikož při jejím výpadku by mohl být ohrožen chod energetiky, dopravy, bankovnictví, finanční trh, zdravotnictví, vodní hospodářství, digitální infrastruktura či chemický průmysl. Provozováním digitální služby míníme zajištění internetového vyhledávače, cloud computingu (virtuálního úložiště) a on-line tržiště mezi spotřebitelem a prodávajícím, kteří mezi sebou mohou uzavírat on-line smlouvy upravené § 2 zákona č. 634/2012 Sb. a § 419 a 420 zákona č. 89/2012 Sb.[50] Správci a provozovatele jsou dále povinni zajistit taková bezpečností opatření (organizační a technická), aby zajistili bezpečnost informací, dostupnost a spolehlivost služeb a sítí v kybernetickém prostoru.[51] Za organizační opatření považujeme: systém řízení bezpečnosti informací; řízení rizik; bezpečnostní politiku; organizační bezpečnost; stanovení bezpečnostních požadavků pro dodavatele; řízení aktiv; bezpečnost lidských zdrojů; řízení provozu a komunikací; řízení přístupu osob; akvizici; vývoj; údržbu; zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů; řízení kontinuity činností a kontrolu a audit. Technickými pak fyzickou bezpečnost; nástroje pro ochranu integrity komunikačních sítí; nástroje pro ověřování identity uživatelů; nástroje pro řízení přístupových oprávnění; nástroje pro ochranu před škodlivým kódem; nástroje pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů; nástroje pro

[48] § 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[49] Čl. 5 odst. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
[50] § 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[51] § 4 zákona č. 181/2014 Sb.

detekci kybernetických bezpečnostních událostí; nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí; aplikační bezpečnost; kryptografické prostředky; nástroje pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů.[52] V prováděcím právním předpise je nutné stanovit obsah a rozsah opatření a pravidel; obsah a strukturu dokumentace a významné informační systémy spolu s jejich kritérii.[53] Dalšími úkoly správců a provozovatelů jsou detekce kybernetických bezpečnostních událostí, jejichž vznik by měl za následek tzv. incident narušující bezpečnost informací, služeb a integrity sítí.[54] Nadále jsou povinni po detekci neprodleně incidenty nahlásit provozovateli národního CERT, nebo Úřadu,[55] kteří je evidují, vytvářejí opatření a vydávají varování.

Národní CERT je organizace zajišťující sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti. Přijímá oznámení kontaktních údajů a hlášení od orgánů a osob; eviduje a vyhodnocuje incidenty; poskytuje metodickou pomoc; podporu a součinnost; provádí hodnocení zranitelnosti; předává Úřadu údaje o incidentech; plní roli týmu CSIRT[56] a spolupracuje s ním. Provozovateli je povoleno nadále provozovat i jinou hospodářskou činnost vlastním jménem, na svoji zodpovědnost, pouze pokud tím nenaruší plnění stanovených povinnosti. Dále pak musí koordinovat svoji činnost s Úřadem a vždy postupovat nestraně.[57] Může se jím stát fyzická osoba, se kterou Úřad uzavřel veřejnoprávní smlouvu, nebo právnická osoba splňující následující požadavky: nevyvíjí a nevyvíjela činnost proti zájmům České republiky; provozuje, spravuje informační systémy, sítě, služby nebo se nejméně po období 5 let na nich podílí; má technické předpoklady v daném oboru; je členem národní organizace v dané oblasti; v evidenci daní nemá žádný záznam o nedoplatcích; nebyla stíhána za trestnou činnost; není zahraniční osobou podle jiného právního předpisu; nebyla zřízena či založena za výlučným účelem zisku. Splnění podmínek se prokazuje čestným prohlášením a potvrzením od Finanční a Celního správy České republiky. Na vyžádání se také předkládá výpis z Rejstříku trestů. Činnost jemu svěřenou vykonává bezúplatně, vynakládá

[52] § 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[53] § 6 zákona č. 181/2014 Sb.
[54] § 7 zákona č. 181/2014 Sb.
[55] § 8 zákona č. 181/2014 Sb.
[56] Čl. 9 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
[57] § 17 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

nezbytné výdaje spojené s výkonem jemu svěřených pravomocí. Údaje o provozovateli na svých stránkách zveřejní Úřad.[58]

Vládní CERT funguje jako součást Úřadu. Přijímá oznámení kontaktních údajů; hlášení o incidentech; vyhodnocuje údaje; poskytuje metodickou pomoc a součinnost; přijímá podněty a údaje, které dále zpracovává; poskytuje provozovateli národního CERT bezpečnostní údaje z evidence incidentů; vyhodnocuje zranitelnost v oblasti kybernetické bezpečnosti; informuje orgány jiného členského státu; plní roli týmu CSIRT a spolupracuje s týmy CSIRT členských států.[59]

Jako ústřední správní orgán byl zřízen Úřad pro oblast kybernetické bezpečnosti se sídlem v Brně. V čele stojí ředitel, zvolený Poslaneckou sněmovnou, který je nadále odpovědný předsedovi vlády nebo pověřenému členovi vlády. Úřad dále stanovuje a vykonává opatření; vede evidence; ukládá správní tresty za nedodržení povinností; působí jako koordinační orgán ve stavu kybernetického nebezpečí; zajišťuje mezinárodní spolupráci; sjednává a uzavírá mezinárodní smlouvy; zajišťuje prevenci; vzdělání a metodickou podporu; provádí výzkum a vývoj; uzavírá veřejnoprávní smlouvy s provozovatelem CERT; zasílá Ministerstvu vnitra návrhy prvků kritické infrastruktury, které určuje podle krizového zákona č. 240/2000Sb.; každé 2 roky ověřuje aktuální určení prvků kritické infrastruktury; určuje provozovatele a informační systém základních služeb; zpracovává a vládě předává návrh na národní strategie kybernetické bezpečnosti[60] a akční plán aktualizovaný každých 5 let; je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v rámci EU; je příslušný orgán České republiky; plní informační povinnost vůči Evropské komisi;[61] informuje veřejnost o kybernetickém incidentu; provádí analýzu a monitoring hrozeb a služeb; vykonává působnost v Evropském programu družicových navigací Galileo; vydává Věstník Úřadu následně zveřejněný na webových stránkách; plní další úkoly spojené s tímto zákonem a zákonem o utajovaných informacích č. 412/2005 Sb. Pro výkon činnosti jsou mu dále poskytovány referenční údaje z registru obyvatel; z agendového systému evidence obyvatel o státních občanech České republiky; ze systému cizinců; z registru rodných čísel fyzických osob; z registru právnických osob; podnikajících fyzických osob a orgánů veřejné moci. Z poskytnutých informací lze použít jen takové, které jsou nezbytné pro splnění stanoveného úkolu. Zpracovávání osobních údajů

[58] § 18 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[59] § 20 zákona č. 181/2014 Sb.
[60] Čl. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
[61] Čl. 5 odst. 3, čl. 7 odst. 3 a čl. 8 směrnice Evropského parlamentu a Rady (EU) 2016/1148.

probíhá podle nařízení EU 2016/679, a to i za jinými účely, než pro které byly shromážděny. V případě řešení kybernetického incidentu; události; při prevenci rizik či hrozeb nemusí obdržené osobní údaje, pokud je zpracovává za stanoveným úkolem, subjektu poskytovat informace o výmazech, omezení či opravách; zajišťovat k nim přístup; opravovat nebo je jinak doplňovat.[62] Kontrolu vykonávají zaměstnanci úřadu postupující podle kontrolního řádu. V případě zjištění nedostatků je stanovena lhůta pro jejich odstranění. Pokud zde existuje bezprostřední ohrožení kybernetickým incidentem, může být kontrolovanému zakázáno používání ohroženého systému nebo jeho části, a to do doby, než se odstraní nedostatky. Poslanecká sněmovna pak vykonává kontrolu nad Úřadem prostřednictvím zvláštního kontrolního orgánu. Počet členů orgánu je stanoven, aby v něm byly obsaženy všechny politické kluby, nejméně však 7 jednajících orgánů, jejichž práva a povinnosti jsou stanoveny v souladu se zákonem č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů, pokud není stanoveno jinak zákonem č. 181/2014 Sb. Ředitel Úřadu předává orgánu zprávu o činnosti; návrh rozpočtu; podklady potřebné při plnění rozpočtu; vnitřní předpisy; na vyžádání pak zprávy o kybernetických incidentech. Dále je povinen podat vysvětlení v případě zjištění nezákonného omezování či poškozování práv a svobod občanů. Poslanecká sněmovna spolu s ředitelem je dále informována při zjištění porušení povinností zaměstnancem úřadu.[63] V případě přestupku lze uložit pokutu do výše 5 000 000 Kč podle rozsahu provinění,[64] projednávání přestupků a vybírání pokut spadá do kompetence Úřadu.[65]

Zákon dále změnil některá ustanovení zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. [66] Zákon nabyl účinnosti 1. 1. 2015,[67] a byl dále upraven zákony č. 104/2017 Sb. a č. 205/2017 Sb.

[62] § 22 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[63] § 24 zákona č. 181/2014 Sb.
[64] § 25 zákona č. 181/2014 Sb.
[65] § 27 zákona č. 181/2014 Sb.
[66] § 35 zákona č. 181/2014 Sb.
[67] § 38 zákona č. 181/2014 Sb.

5. Nařízení Evropského parlamentu a Rady EU č. 679/2016

Vzniklo za účelem efektivnější ochrany osobních údajů, základních práv a svobod občanů Evropské unie podle Listiny základních práv a svobod. Stanovuje pravidla pro práci se zpracováváním a volného pohybu osobních údajů v rámci EU. Nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracovávání těch údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Dále se působnost vztahuje na údaje související se subjektem údajů, jehož údaje se nachází v Unii; činností správce nebo zpracovatele bez ohledu, jestli se nacházejí na území EU nebo mimo něj; na zpravování údajů správce nacházejícím se v EU nebo mimo ni, pokud se v právu státu uplatňuje mezinárodní právo veřejné. Nevztahuje se na zpracování, které nespadá do působnosti práva EU; výkonu činností členských států v působnosti V. hlavy kapitoly 2 smlouvy o EU;[68] fyzickou osobou v průběhu osobní nebo domácí činnosti; příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Článek 4 nám dále přesně stanovuje termíny jako osobní údaj, omezení zpracování, profilování, pseudonymizace, apod.[69] Zásady zpracování osobních údajů probíhají zákonným a transparentním způsobem; jsou shromažďovány za konkrétním účelem, přiměřeně, relevantně a omezeně v nezbytném rozsahu; jsou uloženy ve formě umožňující identifikaci subjektů po nezbytně nutnou dobu s náležitým zabezpečením a zákonností.[70] Členskému státu se ponechává možnost zachování nebo zavedení konkrétnějších ustanovení vyvozených z tohoto nařízení. Podmínky vyjádření souhlasu jsou založeny na souhlasu subjektu, který je zpracovatel povinen doložit. Subjekt může kdykoliv svůj souhlas odvolat. V souvislosti se službami informačních společností jsou podmínky použitelné na souhlas dítěte stanoveny hranicí 16 let, v případě osob mladších je zapotřebí souhlasu zákonného zástupce. Členské státy mohou stanovit hranici nižší, nesmí však být nižší než 13 let.[71] Dále je zakázáno zpracovávat osobní údaje, které vypovídají o rasovém či etnickém původu; politických názorech; náboženském vyznání; filozofickém přesvědčení nebo členských odborech; zpracování genetických údajů; biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu; sexuální orientaci nebo životě fyzické osoby. Zpracování je přípustné pokud subjekt udělil výslovný souhlas; je nezbytné pro účely plnění povinností správce nebo zpracovatele v oblasti pracovního práva nebo sociálního

[68] Smlouva o Evropské Unii, Úřední věstní Evropské Unie C 326/30, str. 18.
[69] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 48.
[70] Tamtéž, s. 50.
[71] Tamtéž, s. 51.

zabezpečení či ochrany; v případě životně důležitých zájmů subjektu údajů nebo jiné osoby pokud on sám není způsobilý k udělení souhlasu; v rámci činností nadací, sdružení nebo jiných neziskových subjektů, sledující politické, filozofické, náboženské nebo odborové cíle; údajů zveřejněných subjektem; pro určení, výkon nebo obhajobu právních nároků nebo soudních pravomocí; nezbytně z důvodu významného veřejného zájmu na základě práva EU nebo členského státu; pro účely preventivního nebo pracovního lékařství, posouzení pro pracovní uschopnění zaměstnance, lékařské diagnostiky, poskytování zdravotní či sociální péče nebo léčby, řízení systémů a služeb zdravotnictví a sociální péče; z důvodu veřejného zájmu v oblasti veřejného zdraví; a pro účely archivace, vědeckého či historického výzkumu nebo pro statistické účely. V případě rozsudků v trestních věcech a činech se zpracovávání může provádět pouze pod dozorem orgánu veřejné moci, pod oprávněním EU nebo členského státu.[72]

Subjekt údajů při poskytnutí svých údajů obdrží od správce informace o totožnosti a kontaktní údaje na správce, popřípadě pověřence; účely zpracování; oprávněné zájmy správce, případné příjemce nebo úmysl předat tyto informace do třetí zemně nebo mezinárodní Komise. Dále je obeznámen s dobou, po kterou budou údaje uloženy; seznámen s právem na přístup k osobním údajům; na odvolání souhlasu; podání stížnosti u dozorového úřadu; na skutečnost, že poskytování je zákonným nebo smluvním požadavkem, a že dochází k automatizovanému rozhodování a profilování. Pokud správce hodlá dále údaje zpracovávat za jiným účelem, musí o tom neprodleně subjekt informovat.[73] Ten má rovněž právo na opravu nepřesných údajů, doplnění neúplných údajů, které může učinit prostřednictvím dodatečného prohlášení. Právo na výmaz se použije, pokud již osobní údaje nejsou potřebné pro účely, za kterými byly shromážděny; subjekt odvolá souhlas, podle něhož byly zpracovávány; vznese námitku proti zpracovávání; údaje byly zpracovávány protiprávně; musí být vymazány ke splnění právní povinnosti stanové v právu EU nebo členského státu; byly shromážděny v souvislosti s nabídkou služeb společnosti podle čl. 8 (souhlas dítěte). V případě již zveřejněných informací je nutné odstranit veškeré odkazy na tyto údaje, kopie nebo repliky.[74] K výmazu nedojde v případě práva na svobodu projevu a informace; při uskutečňování právních povinností; z důvodu veřejného zájmu v oblasti veřejného zdraví; pro účely archivace ve veřejném zájmu; pro vědecké či historické výzkumy nebo statistické úřady; a pro určení, výkon nebo obhajobu právních výkonů. V případě, že subjekt popírá přesnost údajů; zpracovávání je protiprávní; subjekt žádá omezení zpracovávání nebo proti němu vznesl námitku; nebo správce, již údaje

[72] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 52.
[73] Tamtéž, s. 54.
[74] Tamtéž, s. 55.

nepotřebuje, může subjekt požadovat omezení práva správce na jejich zpracovávání. Ten tak může činit pouze se souhlasem subjektu, nebo z důvodů určení, výkonu nebo obhajoby právních nároků; z důvodu ochrany práv fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu EU nebo členského státu. Správce je dále povinen oznámit subjektu jakékoliv opravy nebo výmaz údajů či omezení zpracování. Také předává údaje druhému správci v případě žádosti subjektu podle práva na přenositelnost údajů.[75] Při automatizovaném individuálním rozhodování nebo profilování se subjekt může rozhodnout nebýt předmětem žádného takového rozhodnutí. Nestane se tak v případě uzavření nebo plnění smlouvy mezi subjektem a správcem, při povolení ze strany EU nebo členského státu nebo v případě výslovného souhlasu subjektu.[76]

K odpovědnostem správce náleží zajistit vhodná technická a organizační opatření, aby byl schopen doložit, že zpracovávání probíhá v souladu s tímto nařízením (např. kodex chování nebo vydávání osvědčení). Opatření musí být průběžně revidována a aktualizována. V případě, že jsou dva nebo více správců, musí si mezi sebou vymezit své podíly odpovědnosti na povinnostech plnění stanovených úkolů. Rovněž je možné určit zástupce správce nebo zpracovatele, který vystupuje v jednom z členských států, kde se zpracovávají údaje subjektu. Na zástupce se pak mohou obracet dozorové orgány nebo subjekty údajů. Správce je oprávněn pověřit zpracovatele, kterým se může stát ten, kdo je schopen dostatečně zabezpečit svěřené údaje a který nesmí do zpracovávání zapojit nikoho jiného bez předchozího souhlasu správce. Zpracování se řídí podle smlouvy nebo jiným právním aktem podle práva EU nebo právo některého členského státu.[77] Zpracovatel nebo jiná osoba mohou zpracovávat údaje pouze na základě pověření správcem, nebo v případě ukládá-li to právo EU nebo členského státu.[78] Každý správce, popřípadě zpracovatel je povinen vést záznamy o činnostech zpracování, na požádání také spolupracují s dozorovým úřadem. Dále je nutné zajištění ochrany údajů jako pseudonymizace a šifrování; zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb; schopnosti obnovení dostupnosti; procesu pravidelného testování; posuzování a účinnosti zavedených zabezpečení. V případě porušení zabezpečení ochrany údajů je správce povinen bez odkladu tuto skutečnost nahlásit dozorovému orgánu, nejpozději pak do 72 hodin od zjištění incidentu.[79] Pro pozdní ohlášení je nutné uvést důvody zpoždění. Hlášení by mělo obsahovat popis povahy daného případu; jméno a kontaktní údaje pověřence

[75] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 56.
[76] Tamtéž, s. 57.
[77] Tamtéž, s. 58.
[78] Tamtéž, s. 59.
[79] Tamtéž, s. 60.

pro ochranu údajů nebo jiné kontaktní místo; popis pravděpodobného důsledku narušení zabezpečení; opatření přijatá k vyřešení dané situace. Pokud informace nemohou být poskytnuty najednou, je možné je poskytnout postupně bez zbytečného odkladu. Správce dále vede dokumentaci o všech nastalých incidentech, podle které je dozorovému orgánu umožněno ověření v souladu s čl. 33. Oznámení vzniklých případů provede také za účelem informování subjektu údajů. V případě pravděpodobnosti vzniku ohrožení práv a svobod fyzických osob je nejprve provedeno posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů subjektu. Správce si vyžádá posudek pověřence pro ochranu údajů, který provádí posuzování vlivu. Nutnost posuzování vlivu je zejména v případech systematického a rozsáhlého vyhodnocování aspektů fyzických osob na základě automatizovaném zpracovávání včetně profilování; zvláštních kategorií údajů; v trestných činech a jejich rozsudků nebo při rozsáhlém systematickém monitorování veřejně přístupných prostorů. Seznam druhů operací podléhajících požadavkům na posouzení sestavuje dozorový orgán.[80] Posouzení by mělo obsahovat systematický popis zamýšlených operací; posuzování nezbytnosti, přiměřenosti, rizik pro práva a svobody subjektů; plánování opatření k řešení těchto rizik, záruk, bezpečnostních opatření a mechanismů k zajištění ochrany. Pokud z posouzení vyplývá vysoké riziko, konzultuje správce před zpracováním tuto skutečnost s dozorovým orgánem. Ten danou situaci zhodnotí, popřípadě upozorní na nedostatečné určení nebo zlehčení rizika. Správce při konzultaci poskytuje informace o rozdělení odpovědnosti správce; společných správců a zpracovatelů; účely a způsoby zpracování; opatření a záruky za účelem ochrany práv a svobod subjektu; kontaktní údaje pověřence; posouzení vlivu na ochranu, a další informace o které úřad požádá. Během přípravy legislativního nařízení se zpracováváním konzultují rovněž členské státy s dozorovým úřadem návrh opatření.

Pověřenec pro ochranu údajů je jmenován správcem nebo zpracovatelem pokaždé, když zpracovávání provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů; hlavní činnosti v operacích vyžadují rozsáhlé pravidelné a systematické monitorování subjektů nebo spočívající v rozsáhlém zpracovávání zvláštních kategorií uvedených v čl. 9 nebo v případě trestných činů čl. 10. Lze jmenovat jednoho pověřence pro vícero podniků nebo orgánů a subjektů veřejné moci, ten však musí být snadno dosažitelný.[81] On sám je jmenován na základě profesních kvalit, odborných znalostech práva a praxe v oblasti ochrany údajů. Pro výkon jeho práce je nezbytné náležité a včasné zapojení do veškerých záležitostí ze strany správce či

[80] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 61.
[81] Tamtéž, s. 62.

zpracovatele; jeho podpora při plnění úkolů; zajištění absence pokynů k výkonu těchto úkolů. Subjekty se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním. Je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele. Dále je vázán tajemstvím nebo důvěrností v souvislosti s výkonem úkolů; může plnit i jiné úkoly a povinnosti, pouze pokud to nepovede ke střetu zájmů. Do jeho kompetencí spadá poskytování informací a poradenství správcům, zpracovatelům nebo zaměstnancům; monitorování souladu s tímto nařízení; poskytování poradenství na požádání; spolupráce s dozorovým orgánem; působení jako kontaktní místo pro dozorový úřad v záležitosti zpracovávání.

Jednou z nezbytných součástí tohoto nařízení jsou kodexy chování, jejichž vypracování vzniká za pomoci členských států, dozorových úřadů, Sboru a Komise podporující vypracování kodexů chovaní. Jejich cílem je přispět k řádnému dodržování tohoto nařízení s ohledem na povahu různých odvětví a podniků. Dozorový orgán vydává stanovisko k návrhu, popřípadě navrhuje úpravu či rozšíření. Kodexy mohou být upravovány sdruženími nebo subjekty zastupujícími správce nebo zpracovatele, popřípadě rozšiřovány pro upřesnění tohoto ustanovení jako spravedlivé a transparentní zpracovávání; shromažďování a pseudonymizace údajů; informace poskytované veřejnosti apod.[82] Schválení kodexu podléhá do kompetencí Komise, která tak činí prostřednictvím prováděcích aktů. Po schválení je nutné zajistit odpovídající zveřejnění a Sbor dále všechny schválené kodexy shromažďuje v registru a zajišťuje k nim přístup pro veřejnost. V rámci tohoto nařízení se zde rovněž uplatňují mechanismy monitorování pro kontrolu jejich dodržování. Kontrolu může mimo dozorový úřad provádět i subjekt, který má příslušnou úroveň odborných znalostí a je akreditován dozorovým úřadem. Příslušný úřad předkládá návrh požadavků na akreditaci takového subjektu.[83] Členské státy, dozorové úřady, Sbor a Komise dále podporují zavádění mechanismů pro vydávání osvědčení, zavádění pečetí a známek. Mohou být rovněž zavedeny za účelem prokazování vhodných záruk ze strany správce nebo zpracovatele, které však nesnižují jejich zodpovědnosti. Osvědčení vydávají subjekty tím pověřené nebo příslušný dozorový úřad na základě schválených kritérií. Je vydáváno na dobu nejvýše 3 let, lze je obnovit za stejných podmínek při plnění stanovených kritérií. V případě nedodržení je osvědčení odebráno. Subjekt vydávající osvědčení musí být akreditován dozorovým úřadem, vnitrostátním akreditačním orgánem určeným v souladu s nařízení Evropského parlamentu a Rady (ES) č. 765/2008 nebo oběma.[84]

[82] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 63.
[83] Tamtéž, s. 64.
[84] Tamtéž, s. 65.

Předávání osobních údajů do třetích zemí nebo mezinárodních organizací je uskutečněno na základě rozhodnutí nebo je založeno na vhodných zárukách. Komise posuzuje a rozhoduje o vydání údajů, jestliže země nebo organizace zajišťuje dostatečnou úroveň ochrany. Samotné předání nevyžaduje žádné speciální povolení. Jako prvky k posuzování se používají: listina základních práv a svobod; příslušné právní předpisy týkající se bezpečnosti, obrany, národní bezpečnosti, trestního práva a přístupu orgánů veřejné moci k osobním údajům, existenci a fungování dozorových orgánů, mezinárodních závazků, která země nebo organizace přijala.[85] Dále je stanoven prováděcí akt, podle kterého probíhá pravidelný přezkum nejméně každé 4 roky. Komise dále sleduje vývoj v zemích a organizacích, který by mohl narušit fungování přijatých rozhodnutí. V případě zjištění nedostatečné ochrany jsou prováděcí akty bez zpětné působnosti zrušeny, změněny nebo je pozastavena jejich působnost. Je zajištěna konzultace se zemí nebo organizací s cílem napravit daný stav. S tímto ustanovením rovněž souvisí činnost dozorového orgánu ve věcech závazných podnikových pravidel.[86] Ta jsou závazná a platná pro všechny členy nebo skupiny podniků vykonávající hospodářskou činnost; subjektu údajů přiznávají vymahatelná práva v souvislosti s jejich údaji. Pravidla vymezují sktrukturu a kontaktní údaje; předání souboru nebo údajů; použití obecných zásad pro ochranu údajů; účelové omezení; minimalizaci; dobu uložení; kvalitu údajů; mechanismus spolupráce s dozorovým úřadem apod.[87] V případě, že zde neexistuje rozhodnutí o odpovídající ochraně (vhodné záruky) a to včetně závazných podnikových pravidel, je předání uskutečněno pouze při splnění např. informování subjektu údajů o možných rizicích; předání je nezbytné pro splnění smlouvy mezi subjektem a správcem; z důvodu veřejného zájmu; pro určení, výkon nebo obhajobu právních nároků; k ochraně životně důležitých zájmů subjektu nebo jiné osoby. Rovněž se můžeme setkat s jednorázovým převodem informací, pokud je to nezbytně nutné, týká se to pouze omezeného počtu subjektů a nelze zde uplatnit předání založené na rozhodnutí ani na vhodných zárukách. Při mezinárodní spolupráci v zájmu ochrany údajů, realizuje Komise s dozorovými orgány vhodná opatření pro rozvoj mechanismů pro spolupráci; poskytnou vzájemnou pomoc na mezinárodní úrovni při prosazování právních předpisů na ochranu údajů; zapojí příslušné strany do diskuse a činností pro prohlubování spolupráce; podpoří výměny a dokumentace v souvislosti s právními předpisy a praxi.[88]

[85] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 66.
[86] Tamtéž, s. 67.
[87] Tamtéž, s. 68.
[88] Tamtéž, s. 69.

Dozorový úřad je zprostředkován v každém členském státě Unie, kdy má za úkol, jak monitorovat uplatnění tohoto nařízení, tak přispívat k jeho jednotnému uplatňování. Ve státě může být zřízeno více takových úřadů, z nichž je vybrán jeden zástupce, který stanoví mechanismus pro dodržování jednotnosti. Každý dozorový úřad postupuje při plnění povinností nezávisle, rovněž tak musí postupovat i jeho členové, kteří nesmí vykonávat výdělečnou ani nevýdělečnou pracovní činnost s tímto neslučitelnou. Úřad musí být vybaven: lidskými, finančními a technickými zdroji; prostorami a infrastrukturou nezbytnou pro plnění úkolů; dále podléhá finanční kontrole, která nesmí ovlivňovat jeho nezávislost. Každý člen úřadu je jmenován transparentním způsobem: parlamentem, vládou, hlavou státu nebo nezávislým subjektem, jemuž tato pravomoc byla svěřena právem členského státu. Rovněž musí mít potřebnou kvalifikaci, zkušenosti, dovednosti a jeho povinnosti končí uplynutím jeho funkčního období. Jeho odvolání je možné v případě závažného pochybení, nebo pokud přestane splňovat podmínky pro plnění povinností. Právní předpisy úřadu jsou upraveny každým členským státem, tedy samotné zřízení úřadu; kvalifikace a podmínky způsobilosti členů; pravidla a postupy pro jejich jmenování; délka funkčního období a otázka znovuzvolení; a v neposlední řadě podmínky, kterými se řídí povinnosti člena. Během stanoveného funkčního období jsou vázáni mlčenlivostí, a to i po uplynutí stanovené lhůty ve vztahu ke zpracovávaným údajům. Příslušnost plnění úkolů a vykonávání pravomocí, náleží každému úřadu na území svého státu.[89] Toto stanovisko se nepoužije při zpracovávání údajů soudy v rámci soudních pravomocí. V případě přeshraničních zpracování náleží příslušnost vedoucímu dozorovému úřadu, stejně tak i zabývání se stížnostmi, možnostmi porušení tohoto nařízení. Každý dozorový úřad se bez rozdílu zabývá monitorováním a vymáháním plnění nařízení; zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech; poskytuje poradenství; podporuje povědomí správců a zpracovatelů; zabývá se stížnostmi; spolupracuje s dalšími dozorovými úřady; provádí šetření o uplatňování nařízení; monitoruje vývoj v relevantních oblastech; přijímá standardní smluvní doložky; připravuje seznam na posouzení vlivu na ochranu; poskytuje poradenství o operacích zpracovávání; podporuje vypracovávání kodexů chování; nabádá k zavádění mechanismů pro vydávání osvědčení; provádí jejich pravidelný přezkum; navrhuje a zveřejňuje požadavky pro akreditaci subjektů pro monitorování kodexů;[90] provádí schvalování takových to subjektů; schvaluje smluvní doložky, závazná podniková pravidla; přispívá k činnostem Sboru; vede záznamy o porušení nařízení a plní další úkoly spjaté s ochranou údajů. Pro usnadnění podání stížností je zavedena možnost podání v elektronické

[89] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 70.
[90] Tamtéž, s. 71.

podobě. Subjekty údajů se mohou bezplatně obracet na pověřence a členy úřadu. V případě nedůvodného nebo nepřiměřeného požadavku, může být požadován přiměřený poplatek. Kategorie pravomocí úřadu rozdělujeme do tří skupin: vyšetřovací (např. možnost nařídit poskytnutí veškerých informací o správce, vyšetřování formou auditu, provádění přezkumu osvědčení …); nápravné (udělení napomenutí, nařízení o vyhovění žádosti, dočasné nebo trvalé omezení, odebrání osvědčení …); povolovací a poradní (poskytnutí poradenství, vydávání stanoviska, schvalování návrhů kodexu, povolání správního ujednání …).[91] Výkon stanovených pravomocí nesmí ohrožovat subjekty na právech uvedených v Listině základních práv a svobod, na právu EU, nebo porušovat soudní ochranu či spravedlivý proces. Kompetence mohou být dále rozšiřovány podle uvážení členského státu, nesmí však narušovat spolupráci a jednotnost mezi úřady. V případě porušení pravomocí je uvědoměn justiční orgán, popřípadě zahájeno soudní řízení. K řádnému chodu je také nutná nezbytná spolupráce, vzájemná pomoc a jednotnost napříč úřady. Při zavádění opatření (jako přijímání seznamů operací zpracovávání návrhů kodexů chování schvalování požadavků na akreditaci apod.) vydává Sbor stanovisko k posouzení záležitosti. V případě nesplnění povinností úřadů ve věcech vzájemné spolupráce a společných postupech, posuzuje záležitosti za získáním stanoviska. Sboru jsou dále od úřadů a Komise předávány veškeré relevantní informace elektronickými prostředky. Předseda tyto informace bezodkladně přednáší členům Sboru, Komisi a dozorovému úřadu spolu se zaujatým stanoviskem. Úřad zohlední stanovisko Sboru a poté sdělí předsedovi rozhodnutí o zachování nebo změně, popřípadě zašle pozměněný návrh.[92] Sbor zavádí závažná rozhodnutí v případech, že dozorový úřad vznesl relevantní a odůvodněnou námitku vůči návrhu rozhodnutí vedoucího dozorového úřadu; pokud vedoucí úřad tuto námitku nezohlednil nebo ji zamítl jako relevantní či nedůvodnou; existují-li protikladné názory ohledně příslušnosti úřadu pro hlavní provozovnu; pokud úřad nepožádal o stanovisko Sboru nebo se neřídí vydaným stanoviskem. Ve výjimečných situacích se může dozorový úřad uchýlit k přijetí opatření a odchýlení se od mechanismu jednoty nebo vzájemné spolupráce; tato opaření jsou však časově omezená a proveditelná pouze na území daného úřadu. O této situaci musí být bez prodlení informovány ostatní dotčené úřady, Sbor a Komise. Dále je nezbytné stanovit konečné opatření, při čemž může požádat Sbor o naléhavé stanovisko nebo naléhavé závažné rozhodnutí. Průběh elektronické výměny informací mezi úřady navzájem, a úřady a Sborem je pod správou

[91] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 72.
[92] Tamtéž, s. 75.

Komise, která může přijímat prováděcí akty za účelem průběhu výměny, zejména pak určení standardizovaného formátu.

Nově je zřízen Evropský Sbor pro ochranu osobních údajů jako subjekt EU s právní subjektivitou. Zastupuje ho předseda, je tvořen vedoucími jednotlivých dozorových úřadů ze všech členských států a evropský inspektor ochrany údajů. Komise má právo účastnit se činností a schůzek Sboru, bez hlasovacího práva. Předseda informuje Komisi o činnostech Sboru. Evropský inspektor má hlasovací právo pouze pro rozhodnutí týkající se zásad a pravidel použitelných pro orgány, instituce a jiné subjekty Unie.[93] Sbor při plnění svých úkolů nebo výkonů postupuje nezávisle, od nikoho nevyžaduje ani nepřijímá pokyny. Zajišťuje jednotné uplatňování tohoto nařízení, poskytuje Komisi poradenství ohledně ochrany osobních údajů; ohledně formy a postupů výměny informací pro závazná podniková pravidla; vydává pokyny, doporučení a osvědčené postupy pro výmaz odkazů, kopií nebo replik z veřejně dostupných komunikačních služeb; prošetřuje zvláštní podněty; vydává pokyny, doporučení a postupy za účelem vymezení dalších kritérií a podmínek, pro zajištění případů porušení zabezpečení; stanovuje správní pokuty; přezkoumává praktické uplatňování pokynů, doporučení a postupů; zavádí společné postupy pro podávání zpráv fyzickým osobám v případě porušení nařízení; podporuje vypracovávání kodexů chování a zavedených mechanismů pro vydávání osvědčených mechanismů, schvaluje kritéria pro vydávání osvědčení; vede registr mechanismů pro vydávání osvědčení a příslušných pečetí a známek; schvaluje požadavky pro účely akreditace subjektů pro vydávání osvědčení; poskytuje Komisi stanovisko k požadavkům na vydávání osvědčení, k posuzování úrovně ochrany ve třetích zemích a mezinárodních organizací,[94] vydává stanoviska k návrhům rozhodnutí dozorových úřadů; podporuje spolupráci a účinnou dvoustrannou i vícestrannou výměnu informací a osvědčených postupů; společné školící programy a usnadnění výměny pracovníků mezi úřady; výměnu znalostí a dokumentů o právních předpisech; veřejně přístupný elektronický registr rozhodnutí přijatých úřady; vydává stanoviska ke kodexům chování. Sbor zasílá stanoviska, pokyny, doporučení a postupy Komisi a výboru. Rozhodnutí jsou přijímána prostou většinou členů. Pro schválení jednacího řádu a připravení provozních opatření je nutná dvoutřetinová většina. Předseda je volen spolu s dvěma místopředsedy na dobu pěti let, svolává zasedání a připravuje pořad k projednání, oznamuje rozhodnutí, zajišťuje plnění úkolů Sborem. Nedílnou součástí je sekretariát, který poskytuje evropský inspektor pro ochranu údajů. Sekretariát pracuje výlučně

[93] ÚZ 1319, Zpracování osobních údajů, GDPR: Sagit, 2019, s. 76.
[94] Tamtéž, s. 77.

s pokyny předsedy; podílí se na plnění pokynů nařízení; zajišťuje analytickou, administrativní a logistickou podporu. V případě potřeby sekretariát vypracuje se Sborem memorandum o porozumění. Dále odpovídá za každodenní fungování; komunikace mezi členy a jinými institucemi nebo veřejnosti; využití elektronických prostředků pro interní a externí komunikaci; překládá relevantní informace; připravuje zasedání a navazující opatření; návrhy a zveřejnění stanovisek a rozhodnutí o urovnání sporů mezi dozorovými úřady.[95] V případě nezbytnosti jsou jednání Sboru důvěrná.

Každý subjekt má právo podat stížnost dozorovému úřadu, pokud si myslí, že byla dotčena jeho práva. Úřad dále informuje subjekt o průběhu řešení a výsledku stížnosti, může také nabídnout možnost soudní ochrany.[96] Každá fyzická nebo právnická osoba má právo na účinnou soudní ochranu proti rozhodnutí dozorového úřadu, v případě že byla porušena jeho práva v důsledku zpracovávání údajů správcem nebo zpracovatelem. Subjekt údajů má dále právo stanovit svého zástupce (neziskový subjekt, organizaci, sdružení), který bude jeho jménem uplatňovat nároky na zmíněná práva ochrany a práva na odškodnění. V případě existence probíhajícího řízení ohledně totožné záležitosti zpracovávání jedním správcem v jiném státě může dojít k přerušení v státě druhém.[97] Pokud někdo v důsledku porušení nařízení utrpěl hmotnou nebo nehmotnou újmu má právo od správce nebo zpracovatele obdržet náhradu. Dozorový úřad zajištuje přiměřenost a účinnost pokut, tak aby současně plnil odrazující funkci.[98] Za porušení nařízení lze uložit pokutu, a to až do 20 000 000 EUR, nebo až 4 % z celkového ročního obrazu celosvětově z předchozího roku podle toho, která hodnota je větší.[99] V případě sankcí, na které se nevztahují správní pokuty, vydá každý stát pravidla a stanoví opatření, aby byla dodržována. Přijaté předpisy stát oznámí Komisi.

Toto nařízení je ustanoveno v souladu s právem na svobodu projevu a informací. V případě nutnosti pro účely: novinářské, akademické, umělecké či literární, jsou stanoveny odchylky od zásad zpracování práv subjektu údajů; od povinností správce a zpracovatele; předávání osobních údajů do třetích zemí a mezinárodních organizací, nezávislých dozorových orgánů; spolupráce a jednoty; zvláštních situací pro nutnost pro spojení práva na ochranu údajů a práva na svobodu projevu. Každý členský stát ohlásí Komisi ustanovení, která pro tento případ

[95] ÚZ 1319, Zpracování osobních údajů, GDPR: Sagit, 2019, s. 78.
[96] NULÍČEK, M.; DONÁT, J.; NONNEMANN, F.; LICHNOVSKÝ, B.; TOMÍŠEK, J. *GDPR / Obecné nařízení o ochraně osobních údajů*: Wolters Kluwer, 2017, s. 470.
[97] ÚZ 1319, Zpracování osobních údajů, GDPR: Sagit, 2019, s. 79.
[98] Tamtéž, s. 80.
[99] NULÍČEK, M.; DONÁT, J.; NONNEMANN, F.; LICHNOVSKÝ, B.; TOMÍŠEK, J. *GDPR / Obecné nařízení o ochraně osobních údajů*: Wolters Kluwer, 2017, s. 488.

přijal. Státy dále mohou stanovit zvláštní podmínky pro zpracovávání národních identifikačních čísel nebo jakýchkoliv jiných všeobecně uplatňovaných identifikátorů, které se použijí pouze pro záruky práv a svobod daného subjektu údajů.[100] Dále mohou stanovit konkrétnější pravidla k zajištění ochrany práv a svobod zapracovávaných údajů zaměstnanců v souvislosti s jejich zaměstnáním. Vhodným zárukám pro zajištění práv a svobod subjektu podléhá zpracovávání pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo statické účely. Je nutné zavedení technických a organizačních opatření, minimalizace údajů nebo pseudonymizace. Členské státy mohou stanovit pravomoci dozorových úřadů, aby dohlížely na zachovávání mlčenlivosti správců nebo zpracovatelů ve vztahu k osobním údajům. Církevní a náboženská sdružení mohou uplatňovat pravidla pro ochranu fyzických osob za předpokladu, že je uvedou v soulad s tímto nařízením.

Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 12 odst. 8 a čl. 43 odst. 8 je svěřena Komisi na dobu neurčitou. Evropský parlament nebo Rada mohou přenesení pravomoci kdykoliv zrušit.[101] Komisi je dále nápomocen výbor ve smyslu nařízení EU č. 182/2011. Nařízení č. 2016/679 dále zrušilo směrnici 95/46/ES o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a volného pohybu. Do 25. 5. 2020 a poté každé čtyři roky předkládá Komise Evropského parlamentu a Radě správu o hodnocení a přezkumu tohoto nařízení, objektem přezkumu jsou pak zejména kapitoly V (předávání údajů do třetích zemí nebo mezinárodních organizací) a VII (spolupráce a jednotnost). Vstoupení v platnost proběhlo 24. 5. 2016, používáno je od 25. 5. 2018. Nařízení je závazné pro všechny členské státy.[102]

[100] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 81.
[101] Tamtéž, s. 82.
[102] Tamtéž, s. 83.

6. Zákon č. 110/2019 Sb., o zpracování osobních údajů

Tento zákon vznikl na základě nařízení EU č. 2016/679 a směrnice EU 2016/680 o ochraně fyzických osob se zpracováním osobních údajů. Upravuje zpracování osobních údajů příslušnými orgány pro zajištění veřejného pořádku a vnitřní bezpečnosti České republiky; k předcházení, vyhledávání odhalování, stíhání trestných činů; výkonů trestů a ochranných opatření; zajišťování obrany a bezpečnosti zájmů ČR; zpracování údajů, které se mají stát předmětem evidence nebo jí již podléhající, a pravomoc Úřadu pro ochranu osobních údajů. Setkáváme se s vymezením oprávnění správce, který zpracovává jemu svěřené údaje při plnění právních povinností, ve výkonu veřejné moci nebo ve veřejném zájmu.[103] Dále zde narazíme na chráněný zájmem, který tvoří tzv. výjimku z povinnosti posuzování slučitelnosti účelů zpracovávaných dat. Nově máme zmíněnou hranici způsobilosti dětí k udílení souhlasu se zpracováním, stanovenou na dovršení 15 let dítěte. Správce je nadále povinen zpřístupňovat informace dálkovým přístupem, oznamovat změnu, omezení nebo výmaz. V případě existence chráněného zájmu může dojít k omezení některých práv a povinností správce nebo zpracovatele podle článků 5, 12 až 22 nařízení EU 2016/679, správce je povinen tuto situaci bez prodlení nahlásit Úřadu se zdůvodněním podle čl. 23. V případě zajištění chráněného zájmu je pro správce stanovena výjimka z povinnosti oznámení porušení zabezpečení osobních údajů subjektu. Při práci s údaji s omezeným zpracováním podle čl. 18 není správci či zpracovateli zamezeno jejich předání nebo zpřístupnění, je však povinen upozornit, že podléhají článku 18, a řádně označit je.[104] Podle čl. 37 mají orgány veřejné moci a orgány zřízené zákonem plnící zákonem stanovené úkoly ve veřejném zájmu povinnost jmenovat pověřence pro ochranu osobních údajů. S tím je spjaté také osvědčení vydávané akreditovanou osobou upravenou zákonem č. 22/1997 Sb. § 11 písm. a) a b). Při zpracování osobních údajů za účelem vědeckého či historického výzkumu nebo pro statistické účely je správce, popřípadě zpracovatel, povinen zajistit opatření k ochraně údajů subjektu, jako jsou např. technická a operační opatření; informování osob o zpracovávání; jmenování pověřence; zvláštní omezení přístupu k informacím; pseudonymizace a šifrování údajů atd. Správce dále zpracovává tyto údaje podle čl. 9, nečiní tak pouze v případě oprávněného bránění zájmu subjektu. Údaje lze také zpracovávat pro novinářské a akademické účely, nebo pro umělecké a literární projevy, dle čl. 9 a 10. Dále je zpracování podmíněno souhlasem Úřadu a dodržováním práva na ochranu zdrojů a obsahu informací. [105] Informování subjektu o identitě správce je možno vhodným přihlášením

[103] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 4.
[104] Tamtéž, s. 5.
[105] Tamtéž, s. 6.

se k identitě správce např. grafickým označením, ústně či jiným vhodným způsobem. Poskytnutí informace o identitě nedojde v případě, že to není možné nebo by bylo vynaloženo nepřiměřené úsilí; subjekt údajů může zpracovávání očekávat; již o něm ví nebo by poskytnutí ohrozilo či zmařilo účel zpracování. Povinnost informovat lze také splnit pomocí dálkového přístupu. V případě správcem nezveřejněný osobních údajů není možno zpřístupnit osobní údaje. Pokud by došlo k porušení zabezpečení zdroje nebo obsahu informací není správce povinen oznámit poruchu zabezpečení osobních údajů podle čl. 33 a č. 34 nařízení EU 2016/679. Při uplatnění práva na výmaz nebo opravu údajů se postupuje podle § 82 zákona č. 89/2012 Sb., občanského zákoníku. Subjekt údajů dále může požádat o omezení zpracování podle č. 17, pokud údaje potřebuje pro určení, výkon nebo obhajobu právních nároků a správce je již pro účely zpracování nepotřebuje. Informování subjektu o opravě výmazu a omezení probíhá podle čl. 17 nebo čl. 19.[106] Subjekt může vznést námitku proti zpřístupnění nebo uveřejnění údajů, pokud doloží konkrétní důvody, které nasvědčují tomu, že zájem na ochranu jeho práv a svobod převyšuje zájem zveřejnění nebo zpřístupnění údajů.

6.1. Zpracovávání v souvislosti s trestnou činností, zajištění bezpečnosti a veřejného pořádku

Údaje shromažďované za účelem předcházení, vyhledávání nebo odhalování trestné činnosti; stíhání trestných činů; výkonu trestů a ochranných opatření; zajišťování bezpečnosti ČR nebo zajišťování veřejného pořádku a vnitřní bezpečnosti jsou zpracovávané orgánem stanoveným zákonem, pokud jsou nezbytné pro plnění úkolu nebo výkonu veřejné moci spravujícího orgánu.[107] Pro zpracování musí být stanoven jak konkrétní účel zpracování, tak musí být přijata taková opatření, aby byly údaje využity jen k danému účelu (uchování pro další možnou identifikaci). Spravující orgán připojí informaci o postavení subjektu v trestním řízení, pravomocných rozhodnutí orgánů činných v trestním řízení a případně označí nepřesné údaje. Subjekt je nadále oprávněn požadovat informace o spravujícím orgánu; má právo na přístup k údajům, které jsou o něm shromažďovány; právo na opravu, omezení zpracování nebo výmaz. Přístup mu bude odepřen v případě předcházení; vyhledávání nebo odhalování trestné činnosti (viz. začátek podkapitoly); při průběhu řízení přestupku, v případě ochrany utajovaných informací nebo oprávněných zájmů třetí osoby. Spravující orgán může dále opravit, popřípadě doplnit údaje na žádost subjektu. Výmaz údajů se provede v případě porušení zásad zpracování, v případě porušení jiného právního přepisu, nebo pokud je orgán povinen údaje vymazat.

[106] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 7.
[107] Tamtéž, s. 8.

Omezení zpracovávání je použito v případě nutnosti dalšího uchování pro účely dokazování. O provedených stanoviscích je vedena dokumentace.[108] Pro ověření zákonnosti zpracování může subjekt požádat Úřad o ověření. Ten odpoví na podnět subjektu do 4 měsíců. V případě, že kontrolu neprovede, podá odůvodnění svého postupu. Dále může subjekt informovat o možnosti soudní ochrany. Správce nadále zajišťuje technická a organizační opatření, aby bylo zajištěno a doloženo plnění jeho povinností (účinné chránění údajů, omezování nepřiměřeného zpracovávání, poskytování nezbytných záruk, předcházení automatického zveřejňování). Vede písemné přehledy o názvu a kontaktních údajích orgánu a pověřence; kategorii stávajících a budoucích příjemců, subjektů údajů a osobních údajů; informaci o profilování, přenosů do třetích zemí a mezinárodních organizací; právních základů pro operace zpracovávání; lhůty pro výmaz nebo přezkum u osobních údajů a obecný popis jejich zabezpečení.[109] V případě spolupráce více spravujících orgánů, je tato spolupráce zaštítěna smlouvou. Stejně tak je uzavřena smlouva mezi orgánem a pověřeným zpracovatelem, která obsahuje jeho práva a povinnosti, pokud tak nestanový zvláštní právní předpis. Zpracovatel dále vede a uchovává písemné přehledy; je povinen ohlašovat porušení zabezpečení; v případě že chce zpracováváním pověřit dalšího zpracovatele, může tak učinit pouze s povolením od orgánu. Pořizování automatizovaných záznamů prováděné orgánem (operační shromáždění, vložení, pozměnění, kombinování, nahlédnutí, předání, sdělení a výmaz) jsou využívané pouze pro účely trestního řízení; ověření zákonitosti; zajištění neporušenosti zabezpečení; zajištění plnění úkolů orgánu, zpracovatele a osob zajišťujících přístup k informacím. Záznamy jsou shromážděny, tak aby bylo možno určit a ověřit důvod nebo čas těchto operací, totožnost příjemce a osoby provádějící operaci. Při možnosti vzniku neoprávněného zásahu do práv a svobod subjektu je nutné od správního orgánu zajistit alespoň obecný popis připravovaného zpracování údajů a operací, posouzení rizika, plánována opatření a vhodné záruky pro zmenšení rizika.[110] V případě vzniku nové evidence, ze které by mohlo vzniknout riziko neoprávněného zásahu, je orgán povinen obeznámit Úřad, který dále projedná toto zpracování. Zásah do práv a právem chráněných zájmů subjektu lze pouze, pokud to stanový jiný zákon. V případě jakéhokoliv jiného porušení zabezpečení je nutno tuto skutečnost bez prodlení ohlásit Úřadu, který zaujme potřebná stanoviska pro vyřešení vzniklé situace. Stejně tak je obeznámen i subjekt údajů.[111]

[108] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 9.
[109] Tamtéž, s. 10.
[110] Tamtéž, s. 11.
[111] Tamtéž, s. 12.

6.2. Ochrana údajů při zajišťování obranných a bezpečnostních zájmů České republiky

Správce provádí zpracovávání na základě souhlasu se zpracováním, bez souhlasu může zpracovávat údaje, pokud provádí zpracování nezbytné pro dodržení povinnosti správce; pro provedení smlouvy; jedná-li se o oprávněné zveřejněné osobní údaje; v případě ochrany práv a právem chráněných zájmů správce, příjemce či jiné osoby; poskytnutí informací o veřejně činné osobě; pro archivní účely. Přičemž subjekt údajů musí být před zpracováváním obeznámen s účelem procesu zpracování. Nadále platí existence smlouvy mezi správce a zpracovatelem, která musí mít písemnou formu. Při zjištění, že správce porušuje právní předpisy tímto nebo jiným zákonem, je zpracovatel povinný na tuto skutečnost upozornit a ukončit spolupráci. V případě jeho nečinnosti nese stejný díl odpovědnosti.[112] Správce je nadále povinen přijímat nezbytná technologická a organizační opatření spjatá s jemu svěřenými údaji. Zaměstnanci správce nebo zpracovatele jsou vázaní mlčenlivostí o osobních údajích, technologických a organizačních opatření, a to i po uplynutí zadané práce či po skončení zaměstnání. Po pominutí účelu zpracování je proveden výmaz. Subjekt má právo požadovat vysvětlení, opravu, doplnění nebo výmaz údajů, pokud se domnívá, že zpracovávání porušuje jeho soukromý a osobní život nebo jsou nepřesné s účelem jejich zpracování.[113]

6.3. Úřad pro ochranu osobních údajů

Plní funkci ústředního správního úřadu pro oblast ochrany osobních údajů. Do jeho činnosti lze zasahovat pouze na základě zákona, postupuje nezávisle a řídí se pouze právními předpisy a přímo použitelnými předpisy Evropské unie. V čele stojí předseda jmenovaný a odvolávaný prezidentem republiky na návrh Senátu. Funkce předsedy viz *Kapitola zákon o ochraně osobních údajů.* Dále má úřad dva místopředsedy voleny a odvolávány na návrh Úřadu Senátem. Místopředseda je ředitelem sekce, považuje se za člena dozorového orgánu podle čl. 53 nařízení EU 2016/679. Zastupuje předsedu v jeho nepřítomnosti, pořadí zastoupení je určeno podle pořadí zvolení do funkce. Činností úřadu jsou přivádění auditu podle čl. 58 a kontrolního řádu, vyzívá k vyjasnění nebo nápravě, upozorňuje správce nebo zpracovatele, stanovuje kritéria a požadavky podle čl. 41, 42 nebo 43, může nařídit subjektu vydávající osvědčení, aby ho odebral, schvaluje kodexy chování, zveřejňuje standardní smluvní doložky podle čl. 28 nebo 46.[114] Pokud nejde o zpracovávání osobních údajů soudy a státním zastupitelstvím provádí dozor nad dodržováním povinností stanovených zákonem; ověřuje zákonnost zpracování;

[112] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 13.
[113] Tamtéž, s. 14.
[114] Tamtéž, s. 15.

přijímá podněty a stížnosti na porušení povinností; projednává přestupky a ukládá pokuty; poskytuje konzultaci; informuje veřejnost o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováváním; informuje správce a zpracovatele o jejich povinnostech v oblasti ochrany osobních údajů; vykonává další působnost stanovenou zákonem; zpracovává a zpřístupňuje výroční zprávy; zajišťuje plnění požadavků vyplývajících z mezinárodních smluv; poskytuje Parlamentu vyjádření k návrhu právních předpisů; podílí se na činnosti Evropského Sboru pro ochranu osobních údajů; spolupracuje a poskytuje pomoc obdobným orgánů, orgánům EU a orgánům mezinárodních organizací působící ve stejné oblasti. Úřad může využívat informace z registru obyvatel; informačního systému evidence obyvatel; informačního systému cizinců v takovém rozsahu, aby byl splněn jemu zadaný úkol.[115] Dále je oprávněn seznamovat se s informacemi nezbytnými pro plnění konkrétního úkolu, výjimku tvoří informace chráněné mlčenlivostí, pokud zvláštní předpis nestanový jinak. Zaměstnanci úřadu jsou rovněž vázáni mlčenlivostí i po skončení stanoveného úkolu či zaměstnaní.[116] Při porušení povinností stanovené zákonem uloží Úřad opatření k odstranění zjištěných nedostatků a stanoví lhůtu pro jejich odstranění. Rovněž se zabývá stanovením přestupků fyzických, právnických a podnikajících osob; projednává přestupky; udílí a vybírá pokuty.[117]

Paragrafem 67 se zrušil dosavadní zákon č. 101/2000, o ochraně osobních údajů zákon č. 177/2001, nařízení vlády č. 277/2011 a další části vybraných zákonů.[118] Zákon nabyl účinnosti 24. 4. 2019.

[115] ÚZ 1319 Zpracování osobních údajů, GDPR: Sagit, 2019, s. 16.
[116] Tamtéž, s. 17.
[117] Tamtéž, s. 18.
[118] Tamtéž, s. 20.

7. Elektronický systém spisové služby a GDPR

Podle zákona č. 499/2004 Sb., o archivnivctví a spisové službě je spisová služba vykonávaná písemnou nebo elektronickou formou.[119] S nárůstem informací a množství dokumentů je kladen stále větší důraz na vedení spisové služby v elektronické podobě, ať již z důvodu snadnějšího přístupu či menší produkce papírových dokumentů. Samotný zákon upravuje povinnost jednotlivým původcům vést spisovou službu v listinné podobě, v elektronické, někteří původci si mohou zvolit mezi těmito možnostmi.[120] Požadavky na vedení elektronické spisové služby jsou uvedeny v Národním standardu pro elektronické systémy spisové služby, který vydává a aktualizuje Ministerstvo vnitra,[121] dokument je volně dostupný na stránkách ministerstva vnitra. Současná verze NSESSS vychází z evropské specifikace MoReq2, zároveň je již čtvrtá platná verze tohoto předpisu.[122] Mezi další prováděcí předpisy upravující spisovou službu patří zákon č. 297/2016 Sb., o službách vytvářející důvěru pro elektronické transakce, dříve zmíněný zákon č. 106/1999 Sb., nařízení eIDAS a GDPR.[123] Pro vedení dokumentace v elektronické podobě lze používat ESSL nebo ISSD, požadavky upravuje Národní standard.[124]

ESSL (ERMS) tedy elektronický systém zajišťující elektronické vedení spisové služby je upraven zákonem č. 499/2004 Sb., vyhláškou č. 259/2012 a Národním standardem. Pro usnadnění zde můžeme využít základní evidenční pomůcku ESSL.

Po zavedení GDPR by měly být všechny systémy ISSD upraveny tak, aby splňovaly požadavky zmíněného nařízení. Hlavním cílem je ochrana údajů i před zneužitím ze strany zaměstnanců institucí využívajících tyto informační systémy. Smlouvy zaměstnanců tedy mohou přesně vymezovat jejich oprávnění nebo jsou upraveny vnitřní normy a omezují se formy řetězcového a fulltextového vyhledávání, dále lze využívat pseudonymizaci a anonymizaci subjektů. V případě, že subjekt údajů vznese požadavek na výmaz, zohledňujeme, zda je dokument zpracováván v systému ISSD nebo v dalších evidencích. Pokud ano jeho odstranění je možno provést až po uplynutí skartační lhůty, kde nebyl dokument vybrán jako archiválie. Při tvorbě samotného systému je velmi žádané navrhnutí ochrany soukromí, již v počátku samotného vytváření IT programu.[125]

[119] KUNT, M.; LECHNER, T. *Spisová služba*: Leges, 2017, s. 23.
[120] Tamtéž, s. 42.
[121] Tamtéž, s. 47.
[122] Tamtéž, s. 48.
[123] Tamtéž, s. 53.
[124] Národní standard, VMV část 57/2017 (část II), s. 1.
[125] LANGEROVÁ, J. *Změny kvůli GDPR se nevyhnou ani spisové službě* [online].

8. GDPR a firmy v praxi

V této části budou představeny dvě navzájem nezávislé firmy, pracující s citlivými osobními údaji. Jednotlivé otázky, které byly firmám položeny, se týkaly základních znalostí a informací o GDPR, přípravě na přijetí opatření v rámci toho nařízení a celkovému dodržování stanovených postupů. Další pak byly kladeny podle jejich zaměření. S ohledem na povahu získaných informací budou obě firmy anonymizovány, tak aby nedošlo k poškození jejich práv, práv zaměstnanců a klientů.

První oslovená firma XY a.s., se zabývá finančním poradenstvím a službami.[126] Jedná se o mezinárodní firmu, která v České republice působí více než 16 let. Zaměstnanci jsou převážně nezávislí poradci se statusem osoba samostatně výdělečné činná. Klienti jsou při uzavírání smluv vždy obeznámeni s nařízením GDPR a, dávají písemný, popřípadě elektronický souhlas se zpracováním osobních údajů. Uzavřené smlouvy jsou ukládány do spisovny podle stanovených kategorií a podkategorií (např. pojištění osoby, majetku …). Do spisovny mají přístup všichni zaměstnanci pobočky. Zástupce firmy se před zavedením nařízení GDPR potýkal s otázkou nedostatečného prostoru pro archivaci dokumentů v jedné z poboček. Jedna z možností, jak tento problém řešit bylo, cituji: „*Zrušíme dámské toalety a prostory využijeme jako sklad, abychom měli ty papíry kam dávat, protože už vážně nevím“*. Pobočka posléze vyčlenila dostatečné prostory v suterénu.

Druhá firma YZ a.s., se zabývá poskytováním služeb městské veřejné dopravy a opravami dopravní infrastruktury. Jde o českou firmu založenou v roce 1991. Zde se zaměříme na proces uzavírání smluv s klienty a se samotnými zaměstnanci, sponzory, a otázku propagace. Za klienty v tomto případě považujeme cestující využívající městskou hromadnou dopravu, kteří uzavírají smlouvu s přepravcem při zakoupení platné jízdenky či kupónu. V případě zakoupení běžné jízdenky souhlasí s dodržováním pravidel předpravy.[127] Pokud si kupují měsíční jízdné, činní tak prostřednictvím formuláře (v listinné nebo elektronické podobě), kde jsou obsaženy jejich osobní údaje, který rovněž musí obsahovat jejich souhlas se zpracováváním osobních údajů.

U sponzorů se setkáváme s darovací smlouvou, která zpravidla neobsahuje citlivé osobní údaje převážně jméno a adresu dárce, zástupce firmy, jméno obdarovaného (název

[126] Mezi nabízené služby kromě finančního poradenství patří zprostředkovávání pojistných smluv, hypoteční úvěry, úvěry ze stavebního spoření, investiční zhodnocení volného kapitálu, investiční fondy, spořící účty, termínované vklady, možnost sjednání penzijního pojištění a připojištění apod.
[127] § 18a zákona č. 111/1994 Sb., o silniční dopravě.

firmy), adresa a IČO. Při reklamní propagaci jsou zde využívány plochy dopravních prostředků a billboardů na zastávkách. Stejně jako v případě uzavírání darovacích smluv se ani zde nesetkáváme s citlivými osobními údaji. Na rozdíl od předchozí smlouvy se zde setkáváme s oboustrannou mlčenlivostí o velikosti peněžního (hmotného) daru.

Pracovní smlouvy jsou se zaměstnanci sjednávány podle zákoníku práce č. 262/2006 Sb. V případě těchto smluv se již setkáváme s citlivými osobními údaji zaměstnanců, popřípadě ve složkách pracovníků se můžeme setkat s údaji jejich rodinných příslušníků (manžel, manželka, děti) pro potřebu daňového přiznání. Správou těchto dokumentů jsou pověřeni personalisté, kteří jsou po dobu pracovního poměru i po jeho skončení vázáni mlčenlivostí. Tato skutečnost je popsána v zákoníku práce §303 odst. 2 písm. b).[128] Smlouvy standardně obsahují osobní údaje zaměstnance (jméno, příjmení, adresu, datum narození, rodné číslo) údaje o zaměstnavateli, formu pracovního poměru, informaci o zkušební době, mzdové podmínky, pracovní povinnosti, odpovědnost za škodu, pracovní dobu a další práva a povinnosti, které vyplývají z pracovní pozice. Při kopírovaní občanského průkazu je nutný souhlas jeho držitele podle platného nařízení GDPR.[129] Kartička pojištěnce zpravidla nebývá kopírována, postačí poznamenání nezbytných údajů.[130] Uchází-li se o místo cizinec je zde nezbytné vyplnění žádosti o zaměstnaneckou kartu, setkáváme se zde také s uzavřením smlouvy o budoucí pracovní smlouvě. Zde se kopírují cestovní doklady uchazečů/zaměstnanců, které jsou uchovávány po dobu 3 let.[131] V případě řidičů městské hromadné dopravy se do spisů přidává kopie řidičského průkazu. Kopírování těchto průkazů je činěno pouze v případě profesionálních řidičů z povolání.[132] Součástí všech zmíněných smluv je doložka o zpracovávání osobních údajů po dobu pracovního poměru zaměstnance. Po skončení pracovního poměru již nejsou složky zaměstnanců dostupné pro personální činnost a jsou přesunuty do spisovny podniku, pokud zde přetrvává důvod jejich úschovy.[133] V případě pracovníků zajišťujících komunikaci s klienty, sponzory apod., jsou po skončení jejich pracovního poměru, ponechány aktivní, po dobu 6 měsíců, jejich emailové adresy. Je tak činěno pro usnadnění přechodu informací, které byly zprostředkovávány pracovníkem zastupujícím firmu a třetí osobou. Po uplynutí nezbytně nutné doby uchovávání[134] jsou dokumenty bývalých zaměstnanců skartovány. K těmto složkám

[128] JUDR. ŽŮŘEK, J. *GDPR v personalistice*. 1. vydání: ANAG, 2019, EDICE Právo, s. 139.
[129] Tamtéž, s. 124.
[130] Tamtéž, s. 126.
[131] Tamtéž, s. 128.
[132] Tamtéž, s. 125.
[133] Tamtéž, s. 102.
[134] Tamtéž, s. 129.

má přístup pouze jedna zmocněná osoba, veškeré dotazy ohledně bývalých zaměstnanců a přístupu k jejich složkám může zpřístupnit pouze ona. Podle zjištěných informací je standardní postup kontaktování zmocněnce s prosbou o vyhledání dané složky, popřípadě informace, ten má určitý čas na zjištění a předání nezbytněn nutné informace, tak aby nebyla porušena práva subjektu informací. Odpověď pracovníka však často bývá: „*Lituji, ale požadovanou informaci se mi nepodařilo dohledat"*. Můžeme zde mluvit o menší neochotě ze strany pracovníka. V případě složek stávajících zaměstnanců, se kterými pracují personalisté, se takovéto problémy zpravidla nevyskytují. Osobní spisy zaměstnanců by měly obsahovat pouze takové písemnosti, které jsou nutné pro výkon pracovně právního vztahu.[135] Můžeme zde například nalézt osobní dotazník, mzdový výměr, dohodu o odpovědnosti za způsobenou škodu, doklady o absolvování povinných školení apod. V případě záznamů o rodinných příslušnících pro úlevy na daních (zvýhodnění na vyživované dítě), zpravidla postačí nahlédnutí mzdového úředníka na rodný list dítě. Není zde nutnost pořizování kopie.[136] Všechna zmíněna pravidla jsou firmou v rámci spisu dodržovány.

Byl zde vyzdvihnut přečin jedné ze mzdových účetní firmy, která při auditu poskytla kontrolorovi k nahlédnutí informace o čisté a hrubé mzdě, a veškeré úlevy na daních, které si mohou zaměstnanci firmy odečíst z daní. Tím však neoprávněně zpřístupnila údaje, které není nezbytně nutné při kontrole předkládat. Při auditu se zpravidla zpřístupňují osobní údaje (jméno, příjmení zaměstnance) a průměrná hrubá mzda za minulý uzavřený kvartál. Průměrná čistá mzda se za kvartál může zpřístupnit např., pokud by zde bylo podezření na diskriminování žen v jejich finančním ohodnocení apod. Stejné pravidlo platí při požadavku kontroly na zpřístupnění celého spisu zaměstnance, může tak být učiněno jen v nezbytně nutné situaci, pokud to vyžaduje povaha kontroly.[137] Zde šlo o politování hodné pochybení pracovnice, věc byla dále řešena nadřízenými.

[135] JUDR. ŽŮŘEK, J. *GDPR v personalistice*. 1. vydání: ANAG, 2019, EDICE Právo, s. 132.
[136] Tamtéž, s. 113.
[137] Tamtéž, s. 136.

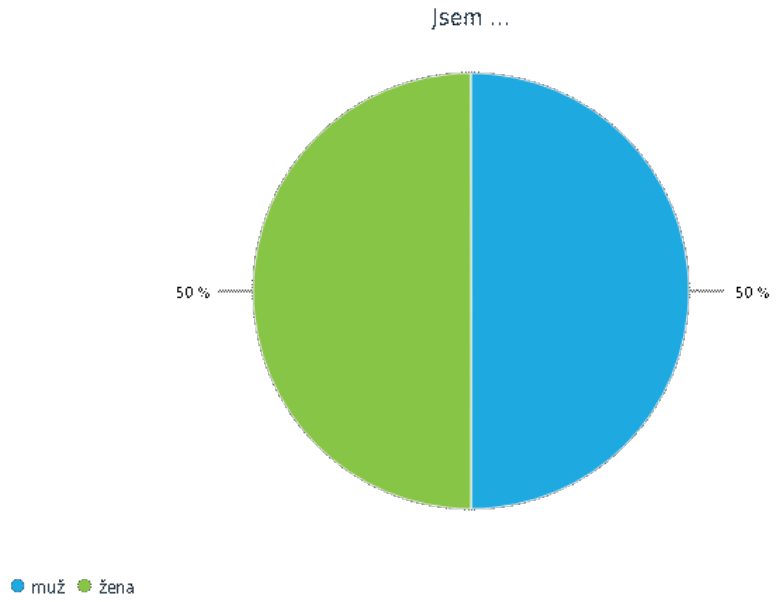
Ze získaných informací může vyvodit, že obě firmy pracují v souladu s platným nařízením GDPR. V první firmě se převážně setkáváme s uzavíráním pojistných smluv v druhé pak nejčastěji s pracovními smlouvami, při jejichž uzavírání je nezbytný souhlas osoby se zpracováváním osobních údajů. Obě firmy zajišťují svým pracovníků náležitě vybavené kanceláře pro usnadnění práce se spisy. U firmy XY a.s. nebylo zjištěno žádné protiprávní jednání ve smyslu porušení tohoto nařízení, můžeme však vytknout manipulaci a pozdější uchovávání dokumentů, kterým by měla být kladena vyšší pozornost a ochrana. Naopak firma YZ a.s. vyčleňuje ochraně dokumentů s citlivými osobními údaji dostatečnou pozornost, setkáváme se zde však s neuvědomělým personálem, který se svým jednáním může dopustit protiprávní činnosti a porušení nařízení ve smyslu ochrany práv fyzické osoby. I přes tato zjištění můžeme zaujmout stanovisko, že obě firmy vynakládají maximální úsilí pro dodržování zmíněného nařízení a zabránění možného zneužití svěřených údajů.

9. Veřejný průzkum a povědomí občanů

Následující kapitola je věnovaná výsledkům veřejného průzkumu občanů hlavního města Prahy. Do výzkumu se aktivně zapojilo 50 mužů a 50 žen. Z celkového počtu 122 navštívených bylo 22 odpovědí nedokončených, žádná z odeslaných odpovědí nebyla vyřazena. Odkaz na dotazník byl sdílen prostřednictvím sociálních sítí. Cílem tohoto dotazníku je provést rozbor a hodnocení přístupu respondentů k poskytování osobních údajů a důvěry v zavedené právní nařízení na jejich ochranu.

Otázka č. 1: Jsme muž x žena

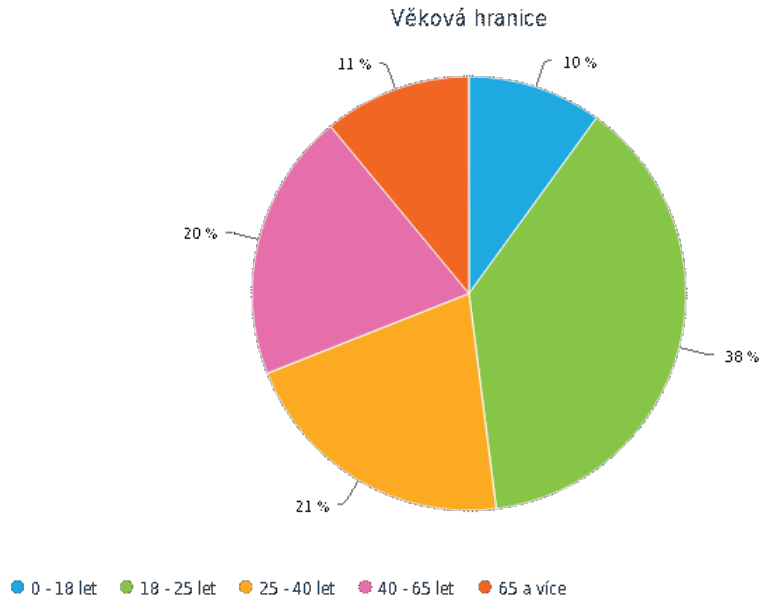
Jak již bylo v úvodním odstavci kapitoly zmíněno, studie se zúčastnilo 122 osob, z toho dotazník dokončilo 100 oslovených.



Graf č. 1: Pohlaví respondentů

Otázka č. 2: Věk respondentů

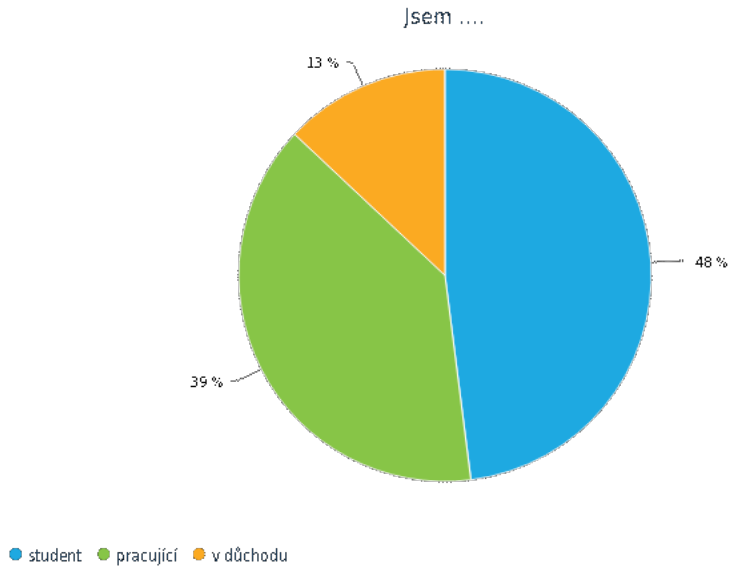
Z celkového počtu oslovených bylo 10 odpovědí v kategorii 0 – 18 let, 38 v kategorii 18 – 25 let, 21 v kategorii 25 – 40 let, 20 v kategorii 40 – 65 let a v kategorii 65 let a více 11 responzí.



Graf č. 2: Věková hranice

Otázka č. 3: Socioekonomický status

Respondentů se statusem studenta bylo 48, dále pak 39 pracujících a 13 důchodců.



Graf č. 3: Socioekonomický status

Otázka č. 4: Jak často poskytujete osobní údaje?

Tato otázka, stejně jako otázky č. 6, č. 8 a č. 9, byla postavena na škále od 1 do 5, přičemž číslo 1 mělo nejmenší hodnotu, číslo 5 pak nejvyšší.

Dotazovaní měli na škále zaznamenat četnost poskytování svých osobních údajů v rámci každodenních činností či společenského života. Celkový průměr odpovědí se pohybuje na hodnotě 3,1. Nejméně odpovědí se vyskytlo u čísla 1 (tedy vůbec neposkytuji) 3 %, dále pak 9 % u čísla 5 (možnosti neustále). Nejvíce odpovědí zaznamenal o číslo 3 (občas) s 38 %, po ní číslo 2 (výjimečně) s 26 % a číslo 4 (často) s 24 %. Můžeme tedy konstatovat, že většina z nás se setkává v rámci našich běžných činností s potřebou poskytnout nějaký osobní údaj pro případné kontaktování ze strany druhé osoby, a tím nemusí být nutně adresa bydliště, rodné číslo či jiný citlivý údaj, který by nás blíže identifikoval. V rámci komunikace s okolním světem je dnes naprosto nezbytné vlastnit emailovou adresu nebo alespoň telefonní číslo. U starší generace je pochopitelná větší míra nedůvěry v moderní komunikační systémy a sdílení svých osobních dat, které mohou být zneužity. I přes tento fakt ovlivňující následující graf ani mladší generace nemám příliš velký zájem na poskytování kontaktních údajů. Responze u čísel 4 a 5 můžeme tedy připisovat lidem, jejichž pracovní status poskytování takovýchto kontaktů nějak vyžaduje (např. personalisté, podnikatelé, úřednici apod.)

3 %	26 %	38 %	24 %	9 %

Graf č. 4: Poskytování osobních údajů

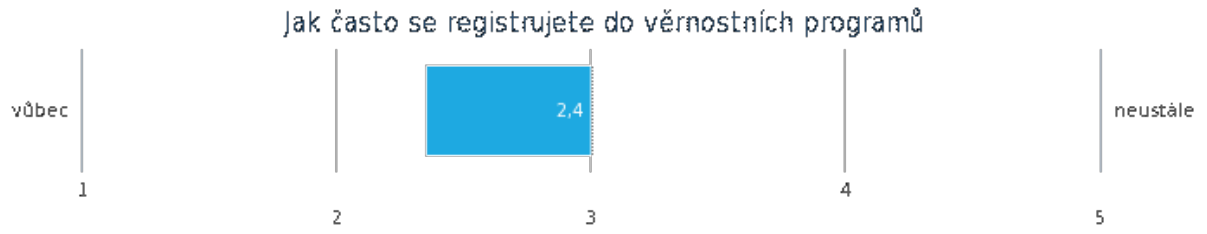
Otázka č. 5: Čtete podrobně podmínky zpracování osobních údajů?

Je alarmující, že 50 % dotázaných nečte podmínky zpracovávání. Mohou tak například odsouhlasit nechtěné monitorování či dálkový přístup k soukromým datům, které proběhne bez povšimnutí. I přes omezení a zabezpečení dat či aplikací se můžeme setkat se zneužitím dat soukromé povahy. Například pokud si stáhneme do mobilního telefonu aplikace pro přehrávání zvukových záznamů, je od nás vyžadován přístup k mikrofonu a reproduktoru, což je zcela oprávněné v souladu s požadovanou funkcí aplikace. Pokud však tato aplikace vyžaduje přístupy k dalším aplikacím v telefonu (např. seznamu telefonních kontaktů, galerie, fotoaparátu …) měli bychom zpozornit, může se jednat o skrytou hrozbu pro naše zařízení i údaje. Z celkového počtu jen 30 % dotázaných důkladně čte podmínky, ale pouze občas. Můžeme tedy říct, že míra četnosti podrobného čtení je odvozena o jakési relevantní nutnosti souhlasu respondenta, pro získání přístupu k dalším produktům a funkcím (aplikace, smlouvy, věrnostní programy …). Většina z nás tak často dává souhlas, aniž by si přečetla plné znění stanovených podmínek.

Graf č. 5: Čtení podmínek zpracovávání

Otázka č. 6: Jak často se registrujete do věrnostních programů?

Stále více se setkáváme s nabídkami různých marketingových společností o možnosti vstupu do věrnostních programů, které nabízejí. S tímto je spjato poskytování naši údajů (nejčastěji jméno, příjmení, datum narození, adresa bydliště, telefonní a emailový kontakt). Většina z nás je členem nějakého klubu či programu, který mu přináší jisté slevové výhody. S těmito výhodami jsou však spjaté i nevyžádané emaily a přehlcené poštovní schránky různými časopisy nebo slevovými kupóny pro další nákup. Z výsledků grafu (jehož hodnota se pohybuje na čísle 2,4) může soudit, že míra potřeby občanů pro vstupování do takovýchto programů není příliš velká. Nejvyšší zaznamenané hodnota je 43 % u čísla 2 (výjimečně), dále 29 % u č. 3 (občas) a 17 % u č. 1 (tedy vůbec). S nadměrným vstupování do programů se setkáme jen výjimečně, potvrzují to hodnoty u č. 4 kdy hodnoty dosahují 10 % a č. 5 kde se setkáme pouze s 1 %.



17 %	43 %	29 %	10 %	1 %

Graf č. 6: Věrnostní programy

Otázka č. 7: V rámci poskytování osobních údajů souhlasíte s cíleným marketingem

Se vstupem do věrnostních programů dále souvisí cílený marketing, který je odvozen o seznamu zboží a služeb, které si klient u dané společnosti zakoupí. Někteří to mohou vnímat jako pozitivum, které je zvýhodní při nákupu jejich oblíbených produktů. Naopak další zde mohou vidět nevyžádané emaily a zbytečné vytištěné papíry. Pouze 16 % dotázaných souhlasí s cíleným marketingem, 38 % dává občasný souhlas, 46 % pak na otázku odpovědělo ne. Při předávání našich údajů elektronickou formou je nutný souhlas se zpracováním, souhlas s cíleným marketingem je převážně volitelná funkce. Ze sebraných dat můžeme usoudit, že většina poskytovatelů bude při souhlasu váhat a pravděpodobně možnost této služby nevyužije.

Graf č. 7: Cílený marketing

Otázka č. 8: Jste často kontaktování prostřednictvím emailu nevyžádanými reklamami?

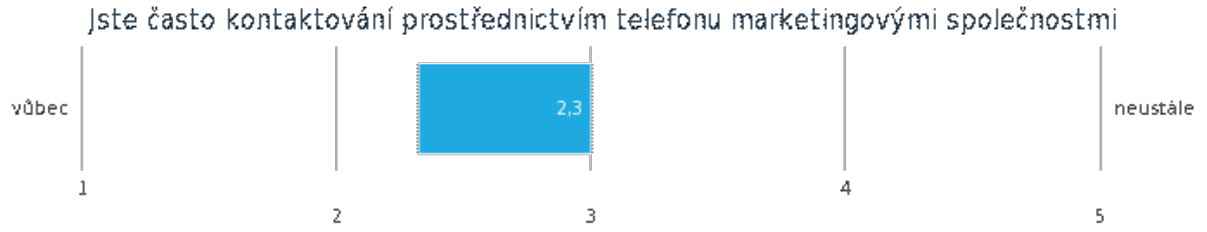
Spamové reklamy související s nabídkami zboží či slevami jsou v dnešní době velmi časté. V případě zadaní našich údajů při online nákupech souhlasíme se zpracováváním našich údajů, spolu s tím je volitelná položka doručování novinek, elektronických časopisů apod. Ne vždy však tyto emaily souvisí s nabídkami firem, se kterými jsme uzavřeli nějakou smlouvu nebo se registrovali do jejich programu. Velmi často se můžeme setkat s automatickým generování emailových adres prostřednictvím různých serverů, které takto odesílají nevyžádanou poštu. 18 % dotázaných na tuto otázku zareagovalo odpovědí vůbec, při bližším rozboru nešlo pouze od zástupce starších generací, ale i o mladší ročníky. To samé tvrzení platí i u č. 2 (výjimečně) zastoupené 20 %. Zde můžeme vzít v potaz, že většina lidí nevnímá spamovou poštu, pokud jim nepřijde přímo do kolonky doručené. V případě neustálého kontaktování pak bylo zaznamenáno pouze 9 odpovědí, tento fakt můžeme přisoudit cíleném marketingu. Z celkového počtu responzí můžeme stanovit, že většina je tímto způsobem kontaktována často (č. 3) nebo také občas (č. 4). Průměrná hodnota grafu byla stanovena na 2,9.

18 %	20 %	25 %	28 %	9 %

Graf č. 8: Kontaktování prostřednictvím emailové adresy

Otázka č. 9: Jak často jste kontaktováni prostřednictvím telefonu marketingovými společnostmi?

Kontaktování prostřednictvím telefonního čísla je jeden z nejčastěji využívaných způsobů pro získání informací nebo jejich předání. Tento způsob často využívají velké korporace (např. mobilní operátoři, firmy dodávající elektřinu …), menší firmy nabízející svoje služby, ale také marketingoví podvodníci. Většina z nás nezvedne příchozí hovor od neznámého čísla, pokud si ho neprověří nebo neočekává předem domluvený hovor. Snad každý z nás se někdy setkal s nevyžádaným hovorem ze strany firem ať už po předání těchto údajů námi samotnými nebo za přítomnosti tzv. loterie čísel. Z nasbíraných dat bylo velmi překvapující, že míra způsobu tohoto kontaktování nedosáhla tak vysoké hodnoty, jakou měl původní předpoklad při sestavování dotazníků. Průměrná hodnota dosáhla čísla 2,3 což je vzhledem k počtu oslovených respondentů velmi malá hodnota. Nejvyšší zastoupení zaznamenalo č. 2 (výjimečně) s 34 %, poté č. 3 (občas) s 28 % a č. 1 (vůbec) s 25 %. Naopak nejmenší možno vůbec (č. 5) s pouhými 3 %. Výsledek grafu můžeme přičítat upřednostňování elektronických či písemných komunikací společností se zákazníky či potencionálními klienty.

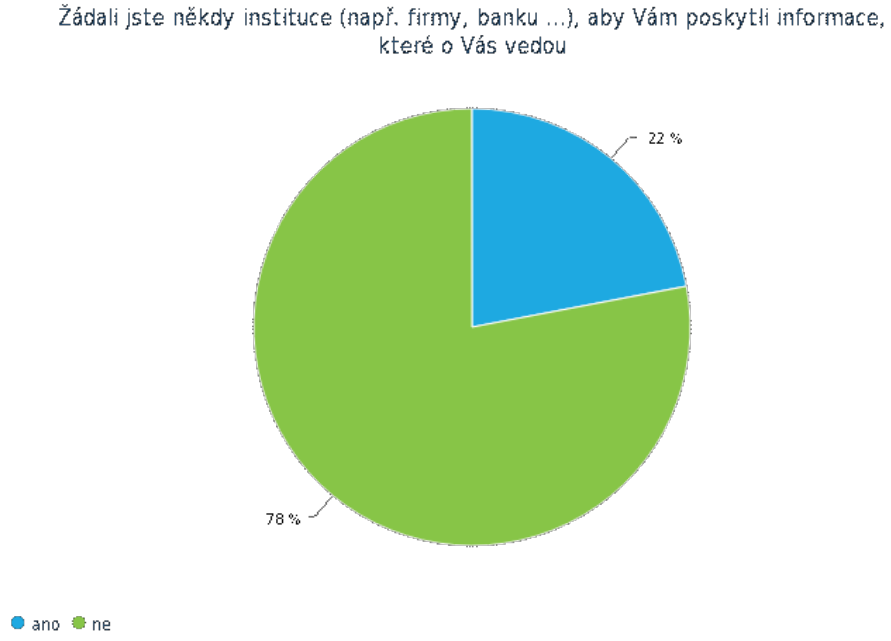


25 %	34 %	28 %	10 %	3 %

Graf č. 9: Kontaktování prostřednictvím telefonního čísla

Otázka č. 10: Žádali jste někdy instituce, aby Vám poskytly informace, které o Vás vedou?

Možnost přístupu k našim datům je velice důležitá z hlediska důvěry a ochrany, v případě podezření na zneužití je tak snadné ověření našich domněnek. Právo na přístup k osobním údajům (podle § 28 zákona č. 110/2019 Sb.) využilo pouze 22 dotázaných. Z výsledku může usoudit, že zbylá většina neměla potřebu o tento typ informací žádat ať už z důvodu důvěry ve zpracovavatele nebo z nevědomosti existence tohoto práva.



Graf č. 10: Žádost o poskytnutí informací o vedení osobních údajů

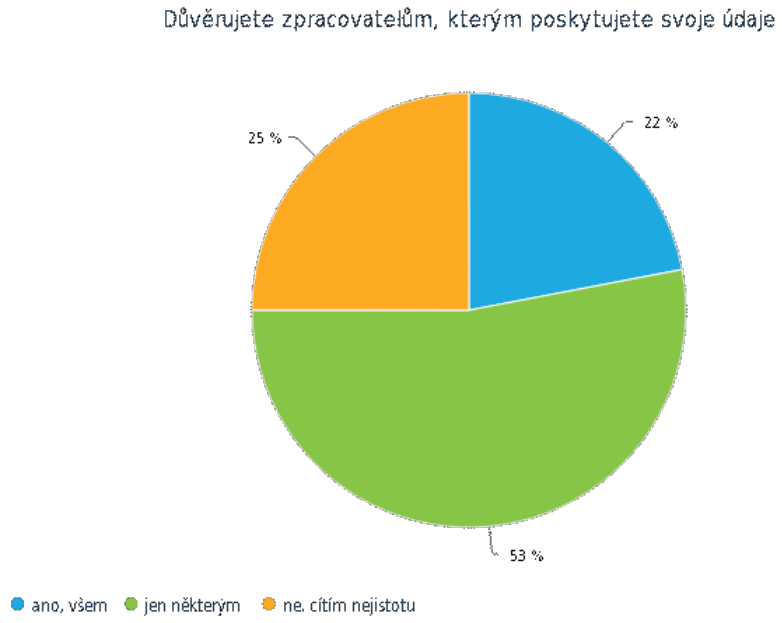
Otázka č. 11: Žádali jste někdy o výmaz informací, které o Vás byly nashromážděny?

Každý subjekt poskytující údaje má nárok na opravu, omezení zpracovávání nebo výmaz údajů o něm vedených podle § 29 zákona č. 110/2019 Sb. a čl. 17 nařízení EU 2016/679. Možnost výmazu informací v minulosti využilo pouze 19 dotázaných. V rámci studie by rovněž bylo zajímavé připojit podotázku, zda byla žádost kladně vyřízena. Náležitost na vyřízení jsou zmíněny v předchozích kapitolách viz *Nařízení evropského parlamentu a rady EU a Zákon o zpracování osobních údajů*.

Graf č. 11: Žádost o výmaz informací

Otázka č. 12: Důvěřujete zpracovatelům, kterým poskytujete svoje údaje?

Jedna z důležitých věcí při poskytování informací soukromé povahy je důvěra v druhou osobu. Na otázku důvěryhodnosti zpracovatelů vyslovila nadpoloviční většina důvěru jen v některé. Pouhých 22 % dotázaných jednoznačně odpověděla ano, 25 % pak ne s pocitem nejistoty. Výsledek průzkumu můžeme přičítat obavě ze zneužití poskytnutých údajů druhé straně, která je bez našeho souhlasu může za určitých okolností nebo také protiprávně předat dál. Je pozoruhodné, že většina respondentů dává svůj souhlas i přes pochybnosti ve zpracovatele. Můžeme říct, že dotazovaní převážně upřednostní nutnost poskytnutí souhlasu se zpracováváním před 100% jistotou.



Graf č. 12: Důvěra ve zpracovatele

Otázka č. 13: Stali jste se někdy obětí zneužití Vašich citlivých údajů?

S množstvím poskytovaných dat se také můžeme setkat s možností zneužití našich údajů. V rámci dotazníku jsme se setkali s 6 takovýmito zkušenostmi.

Graf č. 13: Oběti zneužití údajů

Otázka č. 14: V případě že ano, krátce popište danou situaci

První případ se týkal odcizení instagramového profilu, tedy i identity dotazovaného. Ve druhém případě se jednalo o zneužití emailové adresy a následného rozesílání pošty jménem původního vlastníka. V dalších dvou případech jsme se setkali se zneužitím telefonního čísla respondentů, u prvního byl vytvořen inzerát na prodej bytu (zde dotazovaný zmínil, že číslo bylo nejspíše náhodně sestaveno), ve druhém pak šlo o nabídku práce na pozici vrátného. Také jsme se setkali s porušením listovního tajemství a předáváním dokumentů obsahující citlivé údaje třetí osobě, která nebyla, jakkoliv spřízněna s poškozeným. Ten uvedl, že jeho soukromá pošta byla neoprávněně i po opakovaných stížnostech předávána dál. S velmi závažným trestným činem jsme byli obeznámeni v posledním případě, kde byl dotázanému odcizen občanský průkaz, na který byla vystavena půjčka. Všechny tyto případy jsou příklady hrubého zneužití údajů citlivé povahy, které by měly být bez prodlení nahlášeny a řešeny příslušnými orgány.

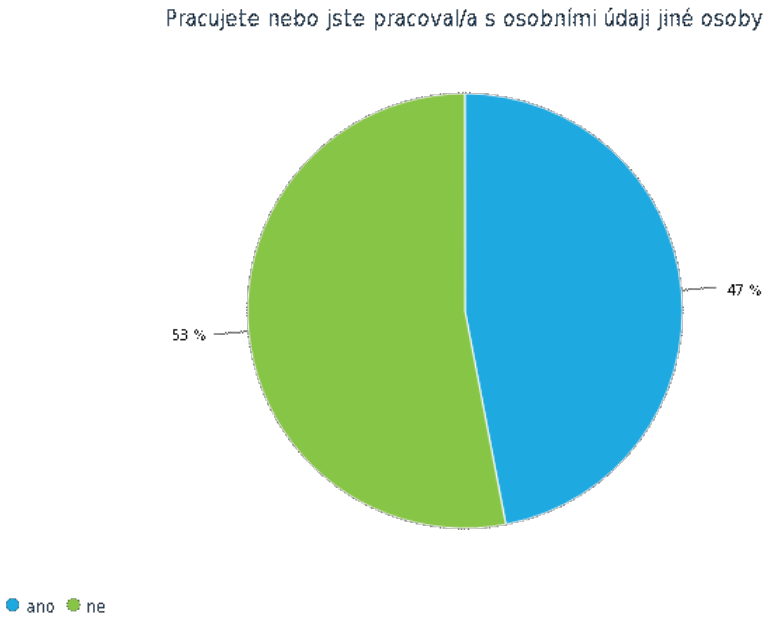
Otázka č. 15: Podal/a jste někdy výslovný nesouhlas se zpracováváním Vašich údajů?

Možnost výslovného nesouhlasu využilo pouze 27 respondentů.

Graf č. 14: Nesouhlas se zpracováváním

Otázka č. 16: Pracujete nebo jste pracoval/a s osobními údaji jiné osoby?

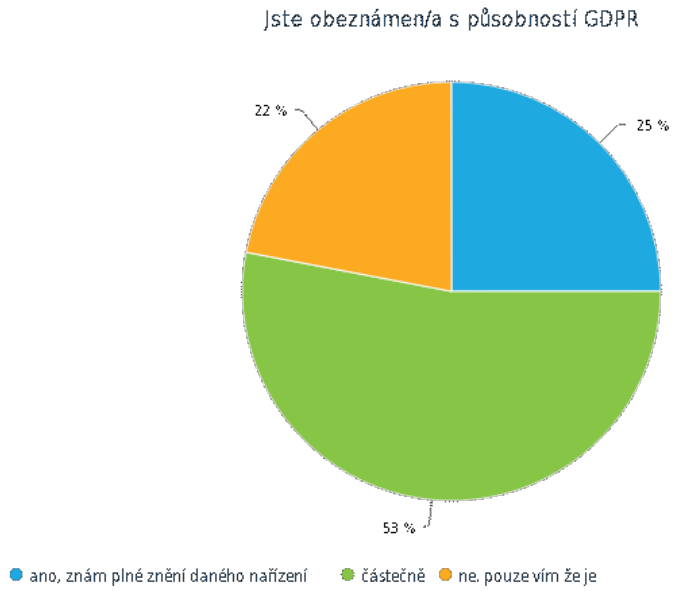
Temné polovina dotázaných (v zastoupení 47 %) odpověděla ano.



Graf č. 15: Práce s osobními údaji druhé osoby

Otázka č. 17: Jste obeznámen/a s působností GDPR?

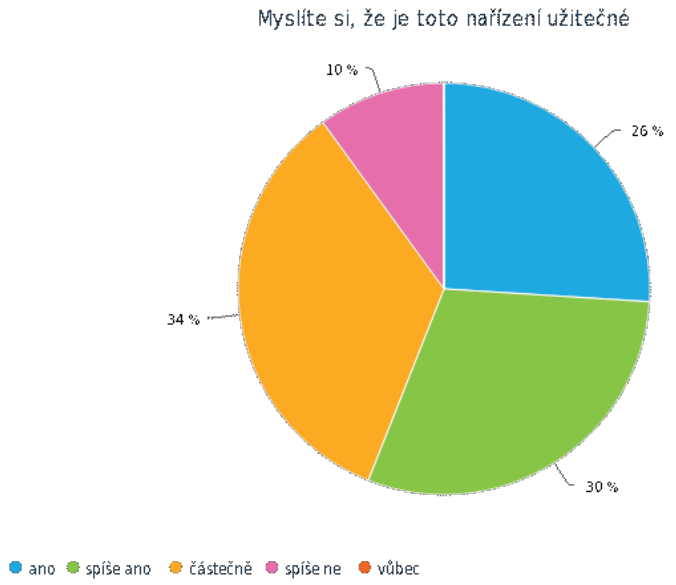
53 respondentů je seznámena s nařízením jen částečně, 25 pak zná plné znění a 22 uvedlo, že pouze ví o existenci nařízení a jeho působností.



Graf č. 16: Znalost působnosti GDPR

Otázka č. 18: Myslíte si, že je toto nařízení užitečné?

Nařízení považuje za užitečné 26 respondentů, 30 se vyslovilo pro odpověď spíše ano, nevíce odpovědí bylo zaznamenáno u odpovědi částečně 34 %, 10 pak u varianty spíše ne.



Graf č. 17: Míra užitečnosti tohoto nařízení

Z výzkumu vyplývá, že většina občanů považuje GDPR spíše za nařízení, které by mělo zaštiťovat určitou ochranu jejich soukromých údajů, nevkládají však do něj přehnanou důvěru. I přes působnost tohoto nařízení a navazujícího zákona č. 110/2019 Sb. se stále setkáváme s úniky citlivých dat, které jsou většinou spojeny s trestným činem nebo pokusem o něj ze strany třetí osoby. Není tudíž překvapující, že se většina lidí potýká s jakýmsi pocitem nedůvěry při poskytování svých údajů. Dále se setkáváme se značnou mírou lhostejnosti při poskytování souhlasu. Nemůžeme považovat za moudré dávat náš souhlas, pokud neznáme plné znění podmínek, které schvalujeme spolu s dalšími oprávněními. Základním doporučením pro běžné občany zůstává větší opatrnost při čtení obchodních podmínek a podmínek zpracovávání. Možnosti zneužití údajů se nikdy nemůžeme stoprocentně vyhnout, může tedy alespoň předejít chybám z naší strany.

10. Závěr

Ať už si chceme nebo nechceme tuto skutečnost připustit, nařízení GDPR do značné míry ovlivňuje naše životy a jeho nepochopení se může pro mnohé stát velkým problémem. V moderním světě plném digitálních zařízení, navzájem propojených internetovou sítí se lidé snadněji dozvídají požadované informace. Každý má právo na svobodný přístup k informacím, ale před jejich zveřejněním musíme zvážit, zda tím nějak neporušíme práva třetí osoby. Může zde dojít ke snadnému zneužití dat a informací. Většina z nás je vlastníkem účtů na sociálních sítích, kde do značné míry zpřístupňuje své osobní údaje okolnímu světu. Provozovatelé těchto sítí musí vynakládat dostatečné úsilí k zabezpečení svých stránek a zajistit uživatelům maximální ochranu údajů, které jim byly svěřeny. Kybernetická bezpečnost je s nárůstem útoků hackerů více než nutná a neměla by být opomíjena v žádném sektoru. Toto vše podléhá zákonným normám jednotlivých států včetně samotného nařízení GDPR. V České republice byl po přijetí nařízení zrušen dosavadní zákon o ochraně osobních údajů a dále vytvořen zákon nový o zpracovávání osobních údajů, který upravuje nařízení pro potřeby a zabezpečení našeho státu. Subjekt údajů, který vyjadřuje souhlas se zpracováváním tedy očekává, že jeho osobní údaje budou dostatečně zabezpečeny a zpracovávány pouze pro účely ke kterému byl souhlas udělen.

V předchozích kapitolách jsme se věnovali samotnému dopadu GDPR na firmy a jednotlivé občany. Ze zjištěných informací lze stanovit, že většina obyvatel dává svůj souhlas se zpracováváním bez podrobného přečtení podmínek zpracovávání, což je možné vyhodnotit jako neuvážený a zbrklý krok. Pokud podepisujeme nějakou smlouvu či smluvní podmínky neměli bychom nic ponechávat náhodě. Souhlas je možné kdykoliv odvolat, musíme si ale uvědomit, že v mezidobí od udělení souhlasu po jeho odvolání jsou naše data legálně zpracovávána. Dále jsme se setkali s celkem běžným postupem kanceláří jednotlivých firem, kde sice jsou pracovníci obeznámeni s platností nařízení GDPR, avšak někteří nejsou dostatečně obeznámeni s celkovou působností nařízení. Jak jsme se mohli přesvědčit, velmi snadno může vlivem nepochopení dojít k neúmyslnému zveřejnění citlivých informací subjektu. Takovýmto situacím lze předejít opakujícím se školením zaměstnanců, pracujících s údaji subjektů. Při svěřování informací a dokumentů do rukou třetích osob, v tomto případě zaměstnancům jednotlivých firem, je dobré předem vymezit jejich oprávnění při práci s dokumenty. Periodické kontroly a dostatečné uvědomění zaměstnanců by tak mohlo zcela odstranit dosavadní přístup některých pracovníků.

V současné době se však potýkáme se značným nedostatkem školitelů a specializovaných firem, které nabízejí odborné vzdělávání v daném oboru. I tento problém můžeme chápat jako značnou brzdu při snaze o přiblížení jednotlivých vládních nařízení našim občanům. V České republice je též velmi malé množství odborné literatury, která je značně potřebná a pro mnohé pracovníky v oboru administrativy či personalistiky zcela nepostradatelná. Nemůžeme tedy zcela vinit jednotlivé pracovníky, pokud zde není dostatečné množství lidí, kteří by je řádně zaškolili, systematicky kontrolovali nebo poskytovali poradenství. Většina populace ani není řádně obeznámena s existencí takovýchto školitelů (firem), i toto by mohlo být tématem dalšího průzkumu. V těchto případech by bylo vhodné zřídit více specializovaných firem, které by proškolovali zaměstnance jednotlivých sektorů pro tuto problematiku nebo alespoň prozatím vydat více publikací, které by se věnovaly této problematice a svými metodickými postupy řádně popisovaly, jak mají zaměstnanci v jednotlivých situacích postupovat. Do budoucna bychom se takto mohli vyhnout zbytečným chybám, které často mívají fatální následky.

Vláda se dále snaží urychlit přechod v administrativní oblasti zajištěním elektronických portálů, kde si občané mohou podat žádost elektronicky. Tento způsob se však netěší velkému úspěchu, čelí totiž jisté nedůvěře lidí, kteří stále dávají přednost papírové formě dokumentu. I přes dané jistoty, které stát zařizuje, někteří lidé se stále potýkají s nejistotou ohledně svěřování svých údajů elektronickou formu, v níž vidí snadnější možnost zneužití. V tomto případě můžeme doufat v postupné zavádění jednotlivých vládních opatření, které usnadní podání a vyřizování různých žádostí v elektronické formě. Naše společnost by měla vkládat do systému více důvěry, bez níž není možné se posunout kupředu.

11. Zdroje:

11.1. Seznam použité literatury:

JUDR. ŽŮŘEK, Jiří. *GDPR v personalistice*. 1. vydání: ANAG, 2019, EDICE Právo. ISBN 978-80-7554-210-6.

KUNT, Miroslav; LECHNER, Tomáš. *Spisová služba*: Leges, 2017, 2. aktualizované vydání. ISBN 978-80-7502-233-2.

NULÍČEK, Michal; DONÁT, Josef; NONNEMANN, František; LICHNOVSKÝ, Bohuslav; TOMÍŠEK, Jan. *GDPR / Obecné nařízení o ochraně osobních údajů*: Wolters Kluwer, 2017, ISBN 978-80-7552-765-3.

ÚZ 1319, *Zpracování osobních údajů, GDPR*: Sagit, 2019, ISBN 978-80-7488-353-8.

11.2. Legislativní prameny:

Národní standard pro elektronické systémy spisové služby, VMV část 57/2017 (část II). Dostupné na https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx (zpřístupněno 14. 06. 2020)

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Dostupné na

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02014R0910-20140917&from=EN (zpřístupněno 18. 7. 2020)

Sdělení č. 115/2001 Sb. m. s., Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108. Dostupné na https://www.zakonyprolidi.cz/ms/2001-115 (zpřístupněno 21. 3. 2020)

Smlouva o Evropské Unii (Konsolidované znění), Úřední věstní Evropské Unie C 326/30 Dostupné na https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0008.02/DOC_1&format=PDF (zpřístupněno 16. 4. 2020)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Dostupné na https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148 (zpřístupněno 25. 3. 2020)

Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě (v úplném znění č. 192/2009 Sb.).

Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2015/04/16/22-44-50/vyhlaska_645-2004-sb_uplne-zneni_192-2009-sb.pdf (zpřístupněno 18. 7. 2020)

Vyhláška č. 496/2004 Sb., o elektronických podatelnách Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2015/09/15/15-01-19/2004-496.pdf (zpřístupněno 18. 7. 2020)

Vyhláška č. 259/2012 Sb.**,** o podrobnostech výkonu spisové služby**.** Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2015/09/14/14-38-11/2012-259.pdf (zpřístupněno 18. 7. 2020)

Vyhláška č. 85/2019 Sb., kterou se mění vyhlášky a provádějící zákon o archivnictví a spisové službě.

Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2020/02/05/14-54-01/85-2019.pdf (zpřístupněno 18. 7. 2020)

Zákon č. 111/1994 Sb., o silniční dopravě. Dostupné na https://www.zakonyprolidi.cz/cs/1994-111 (zpřístupněno 12. 6. 2020)

Zákon č. 106/1999 Sb. o svobodném přístupu k informací. In: Sbírka zákonů. Dostupné na https://www.zakonyprolidi.cz/cs/1999-106#f1946266 (zpřístupněno 24. 3. 2020)

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých nařízení. In: Sbírka zákonů. Dostupné na https://www.zakonyprolidi.cz/cs/2000-101 (zpřístupněno 22. 3. 2020)

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

Dostupné na https://www.zakonyprolidi.cz/cs/2004-480 (zpřístupněno 23. 3. 2020)

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákon, ve znění pozdějších předpisů.

Dostupné na https://www.zakonyprolidi.cz/cs/2004-499 (zpřístupněno 18. 7. 2020)

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2015/09/15/14-53-36/2008-300.pdf (zpřístupněno 18. 7. 2020)

Zákon č. 56/2014 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Dostupné na https://www.zakonyprolidi.cz/cs/2014-56 (zpřístupněno 18. 7. 2020)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů.

Dostupné na https://www.zakonyprolidi.cz/cs/2014-181 (zpřístupněno 27. 3. 2020)

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2017/11/12/19-05-25/sb0115-2016-297-2016.pdf (zpřístupněno 18. 7. 2020)

Zákon č. 298/2016 Sb., o změně zákonů v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce.

Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2017/11/12/19-05-51/sb0115-2016-298-2016.pdf (zpřístupněno 18. 7. 2020)

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Dostupné na https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2020/02/05/15-01-38/111-2019.pdf (zpřístupněno 18. 7. 2020)

11.3. Internetové zdroje:

LANGEROVÁ, Jana. *Změny kvůli GDPR se nevyhnou ani spisové službě* [online]. [cit. 17.6.2020]. Dostupné na: https://www.podnikatel.cz/clanky/zmeny-kvuli-gdpr-se-nevyhnou-ani-spisove-sluzbe/ (zpřístupněno 17. 6. 2020)

11.4. Seznam grafů

12. Seznam zkratek

CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

EDPB (European Data Protection Board) – Sbor Evropské unie

eIDAS – Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním

ESSL – elektronický systém spisové služby

ERMS – Electronic Dokument and Record Management

GDPR – General Data Protection Regulation

ISSD – informační systém spravující dokumenty

MoReq2 – Model Requirements for the management of electronic records

NSESSS – Národní standard pro elektronické systémy spisové služby

13. Přílohy

13.1. Příloha č. 1: Dotazník

GDPR

Dobrý den,

věnujte prosím několik minut svého času vyplnění následujícího dotazníku na téma ochrana osobních údajů a GDPR.

1. Jsem ...

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ muž
- ◯ žena

2. Věková hranice

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ 0 - 18 let
- ◯ 18 - 25 let
- ◯ 25 - 40 let
- ◯ 40 - 65 let
- ◯ 65 a více

3. Jsem ....

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ student
- ◯ pracující
- ◯ v důchodu

Jak často poskytujete osobní údaje (telefon, emailová adresa ...)

Nápověda k otázce: *1 nejméně, 5 nejvíce*

	1	2	3	4	5	
vůbec	◯	◯	◯	◯	◯	neustále

5. Čtete podrobně podmínky zpracování osobních údajů

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne
- ○ občas

Jak často se registrujete do věrnostních programů

Nápověda k otázce: *1 nejméně, 5 nejvíce*

	1	2	3	4	5	
vůbec	○	○	○	○	○	neustále

7. V rámci poskytování osobních údajů souhlasíte s cíleným marketingem

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne
- ○ občas

Jste často kontaktování prostřednictvím emailu nevyžádanými reklamami

Nápověda k otázce: *1 nejméně, 5 nejvíce*

	1	2	3	4	5	
vůbec	○	○	○	○	○	neustále

Jste často kontaktování prostřednictvím telefonu marketingovými společnostmi

Nápověda k otázce: *1 nejméně, 5 nejvíce*

	1	2	3	4	5	
vůbec	○	○	○	○	○	neustále

10. Žádali jste někdy instituce (např. firmy, banku ...), aby Vám poskytli informace, které o Vás vedou

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne

11. Žádali jste někdy o výmaz informací, které o Vás byly nashromážděny

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne

12. Důvěrujete zpracovatelům, kterým poskytujete svoje údaje

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano, všem
- ○ jen některým
- ○ ne, cítím nejistotu

13. Stali jste se někdy obětí zneužití Vašich citlivých údajů

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne

14. V případě že ano, krátce popište danou situaci

15. Podal/a jste někdy výslovný nesouhlas se zpracováváním Vašich údajů.

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne

16. Pracujete nebo jste pracoval/a s osobními údaji jiné osoby

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ ne

17. Jste obeznámen/a s působností GDPR

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano, znám plné znění daného nařízení
- ○ částečně
- ○ ne, pouze vím že je

18. Myslíte si, že je toto nařízení užitečné

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ano
- ○ spíše ano
- ○ částečně
- ○ spíše ne
- ○ vůbec