Univerzita Hradec Králové
Filozofická fakulta

DIPLOMOVÁ PRÁCE

2020 Bc. Barbora Borůvková

Univerzita Hradec Králové
Filozofická fakulta
Katedra pomocných věd historických a archivnictví

Analýza dopadu GDPR na archivnictví

Diplomová práce

Autor: Bc. Barbora Borůvková
Studijní program: Historické vědy
Studijní obor: Archivnictví – Moderní systémy v archivnictví
Vedoucí práce: Ing. Monika Borkovcová, Ph.D.
Oponent práce: Mgr. Radek Pokorný

Hradec Králové, 2020

Univerzita Hradec Králové
Filozofická fakulta

Zadání diplomové práce

Autor:	**Barbora Borůvková**
Studium:	F18NP0003
Studijní program:	N7105 Historické vědy
Studijní obor:	Archivnictví
Název diplomové práce:	**Analýza dopadu GDPR na archivnictví**
Název diplomové práce AJ:	Analysis of the impact of the GDPR to the Archiving

Cíl, metody, literatura, předpoklady:

Diplomová práce se zabývá problematikou postoje archivů k nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně osobních údajů, neboli GDPR. Práce se soustředí na zveřejňování kronik pomocí digitálních oblastních archivů. Teoretická část se věnuje problematice samotného nařízení GDPR, provádí analýzu a syntézu ve vztahu k českému archivnictví. Dále se soustředí na hlavní oblasti činností jednotlivých oblastních archivů v ČR, kterých se GDPR dotýká a tyto jsou následně popsány s případnými hrozbami ve formě postihů za nedodržení nařízení.

Praktická část analyzuje dopad evropského nařízení na on-line zveřejňované kroniky. První část výzkumu bude založena na sběru dat z veřejných zdrojů oblastních archivů a na základě metody indukce dojde k zmapování současného stavu procesu zveřejňování kronik. Na základě výstupů z této analýzy budou v druhé části výzkumu stanoveny hypotézy, jejichž zhodnocení bude provedeno formou dotazování na úrovni státních oblastních archivů. Třetí část výzkumu se bude soustředit na obecnou situaci v rámci EU, kde je pro celé území nařízení účinné a následně dojde metodou komparace ke zhodnocení současného stavu po implementaci GDPR do soustavy archivnictví v ČR a v zahraničí, převážně se jedná o Slovenskou republiku, Rakouskou republiku a Spolkovou republiku Německo.

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

Zákon č. 110/2019 Sb. O zpracování osobních údajů.

Úřad pro ochranu osobních údajů. Úřad. uoou.cz [online]. Dostupné na internetu: https://www.uoou.cz/urad/ds-1059/p1=1059

Obecné nařízení o ochraně osobních údajů [online]. Praha 6. Dostupné z: https://www.gdpr.cz/

NULÍČEK, M., DONÁT, J., NONNEMANN, F. a kol. GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU) - Praktický komentář - 2., aktualizované vydání. Praha: Wolters Kluwer, 2018.

ČERVINKOVÁ, B., TUPEC, R. Některé aspekty ohlašování porušení zabezpečení osobních údajů podle GDPR. EPRAVO.CZ Magazine, 1/2018.

NULÍČEK, M.; KOVAŘÍKOVÁ, K.; TOMÍŠEK, J.; ŠVOLÍK O., GDPR v otázkách a odpovědích. Bulletin Advokacie. 2017, č. 9.

KOHÚTOVÁ Z., Anonymizace, a šifrování osobních údajů jako bezpečnostní opatření dle GDPR. [online]. Dostupné z: https://fly-eye.cz/blog-detail-1.html.

Garantující pracoviště:	Katedra pomocných věd historických a archivnictví, Filozofická fakulta
Vedoucí práce:	Ing. Monika Borkovcová, Ph.D.
Oponent:	Mgr. Radek Pokorný

Datum zadání závěrečné práce: 17.12.2019

PROHLÁŠENÍ

Prohlašuji, že jsem tuto diplomovou práci vypracovala pod vedením vedoucí práce Ing. Moniky Borkovcové, Ph. D. samostatně a uvedla jsem všechny použité prameny a literaturu.

V Hradci Králové dne 31. července 2020

BC. BARBORA BORŮVKOVÁ

PODĚKOVÁNÍ

Mé poděkování patří Ing. Monice Borkovcové, Ph. D. za odborné vedení při psaní diplomové práce, trpělivost a ochotu, kterou mi v průběhu zpracování práce věnovala. Také bych ráda poděkovala Mgr. Janu Jindrovi, za jeho odborné poznatky k tématu GDPR.

ANOTACE

BORŮVKOVÁ, Barbora. *Analýza dopadu GDPR na archivnictví*. Hradec Králové: Filozofická fakulta Univerzity Hradec Králové, 2020, 168 s. Diplomová práce.

Diplomová práce je zaměřena na problematiku GDPR v archivech. V teoretické části je popsáno GDPR ve vztahu k archivnictví, vliv a dopad nařízení. Diplomová práce popisuje dostupné metodické pokyny a legislativu, která s GDPR souvisí. Praktická část analyzuje konkrétní problémy z pohledu archivů prostřednictvím kvalitativního výzkumu. Práce sleduje implementaci GDPR v dalších členských zemích EU a porovnává jej s implementaci v České republice.

KLÍČOVÁ SLOVA

GDPR, Archivnictví, Kroniky, Digitální zdroje, Implementace GDPR, Digitální archivy

ANOTATION

BORŮVKOVÁ, Barbora. *Analysis of the impact of GDPR on the archiving*. Hradec Králové: Philosophical Faculty, University of Hradec Králové, 2020, 168 p. Diploma Degree Thesis.

The aim of the Diploma thesis is focus to the GDPR matters in Czech archives. It deals with the definition of GDPR in relation to archiving and the influence and impact of the regulation. The thesis also focuses on the available methodological guidelines and legislation related to GDPR. The practical part focuses closely on specific problems from the point of view of archives through a questionnaire survey. The work also monitors the implementation of GDPR in other EU member states.

KEY WORDS

GDPR, General Data Protection Regulation, Archiving, Chronicles, Digital sources, Digital archive

SEZNAM ZKRATEK A POJMŮ

AKP	Archivní kulturní památka
CPVP	La Commission de la protection de la vie privé (belgický úřad pro ochranu osobních údajů)
Čl.	Článek
DPO	Pověřenec pro ochranu osobních údajů (také jen Pověřenec)
DSG	Datenschutzgesetz (rakouský zákon o ochraně osobních údajů)
EAG	European Archives Group
eSSL	Elektronický systém spisové služby
EU	Evropská unie
FO	Fyzická osoba
GDPR	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 94/46/ES (Obecné nařízení o ochraně osobních údajů)
Listina	Zákon č. 2/1993 Sb., Listina základních práv a svobod
LZPS	Zákon č. 2/1993 Sb., Listina základních práv a svobod
MV	Ministerstvo vnitra České republiky
MZA	Moravský zemský archiv v Brně
NKP	Národní kulturní památka
Odst.	Odstavec
Písm.	Písmeno
PO	Právnická osoba
SOA	Státní oblastní archiv
ÚOOÚ	Úřad pro ochranu osobních údajů (také jen Úřad)

Adaptační zákon	Zákon č. 110/2019Sb., o zpracování osobních údajů
Anonymizace	Nevratný proces mazání osobních informací bez možnosti informace později dohledat.
Archivní zákon	Zákon č. 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů.
Biometrický údaj FO	Jedinečná informace, která jednoznačně identifikuje
Citlivý údaj	informace o FO, která může být poškozující, či diskriminační (také jako zvláštní kategorie osobních údajů).
Digitální archiv	Vyhledávací aplikace, která umožňuje přístup do databází k vybraných digitalizovaným archiváliím. Tato aplikace je většinou přístupná z webového prohlížeče.
Dozorový úřad	Úřad pro ochranu osobních údajů.
Elektronický dokument	Jedná se o jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka (také jako e-dokument).
Osobní údaj	Jakákoli informace o FO, kterou ji lze přímo či nepřímo identifikovat (také jako údaj).
Pověřenec	Monitoruje soulad zpracování údajů s GDPR.
Privacy by design	Přístup k návrhu a tvorbě systémů, který v sobě obsahuje prvky ochrany soukromí. Přístup se prolíná celým cyklem navrhování systému – například informačního systému nebo návrhu procesního řízení organizace.
Profilování	Automatizované zpracování údajů, na jehož základě dochází k vyhodnocení nebo předvídání různých aspektů.

Pseudonymizace	Vratný proces nahrazení či zakrytí osobních informací, které lze později opět získat.
Správce údajů	Subjekt, který stanovuje účel zpracování údajů.
Subjekt údajů	Žijící osoba, k níž se vztahují osobní údaje.

OBSAH

Úvod

Obecné nařízení o ochraně osobních údajů (*General Data Protection Regulation neboli GDPR*) je legislativa Evropské unie, která výrazně zvyšuje ochranu osobních dat a napomáhá snižovat neoprávněného zacházení s osobními údaji občanů členských zemí EU.

Od 25. května 2018 dopadá vliv GDPR na instituce bankovního, zdravotnického i veřejně-správního charakteru. Všechny instituce jenž zpracovávají osobní údaje se od tohoto data potýkají s nutností upravit způsob, jakým dochází k zpracovávají osobních údajů klientů, zaměstnanců, či dodavatelů.
V opačném případě hrozí těmto institucím vysoké, mnohdy až likvidační pokuty v rámci milionů eur či procent z celkového ročního obratu. Maximální možnou výši sankce by mohla obdržet společnost s pár zaměstnanci či nadnárodní korporace bez rozdílu. Avšak *Dozorové úřady* napříč EU přistupují k udělování spíše nižších sankcí či nápravných opatření a vysoké pokusy bývají spíše pro výjimečné případy.

GDPR má dopad i na archivy v České republice, které evidují badatele a tím dochází ke zpracování jejich osobních údajů. Vliv má GDPR ovšem i na samotné archiválie, ve kterých se nachází osobní údaje stále žijících občanů, například kroniky. To před zavedením GDPR upravovala už i česká legislativa v podobě archivního zákona či zákona o ochraně osobních údajů, který již pozbyl platnost, ovšem nikoli v takové míře.

Současní archiváři, kronikáři, specialisti na digitalizaci a jiní se tak museli vypořádat s dodržováním zásad GDPR. Toto období se výrazně dotklo, jak zaměstnanců archivů, tak i badatelské veřejnosti, historiků, redaktorů a dalších,

kteří v důsledku dodržování GDPR přišli o některé materiály, ze kterých čerpali informace.

Některé archiválie včetně kronik prochází také procesem digitalizace a následně jsou zveřejňovány na portálech digitálních archivů. Digitálním archivem je v práci rozuměno serverové řešení či uložení dat na discích, až po certifikované LTP úložiště[1]. Kroniky obecně patří mezi oblíbené zdroje informací a bývají častým zájmem badatelů k nahlížení. Jejich digitalizování pomohlo uchránit jejich hodnotu, jelikož již nemusí být předkládány v takové míře, jako před digitalizací.

Jelikož je pravděpodobné, že například v kronice z roku 1960 se mohou vyskytovat osobní údaje o stále žijících občanech, je přistupováno k jejich zveřejňování v digitálních archivech různě. Jakákoli archiválie, obsahující osobní údaje nesmí být bez souhlasu dané osoby zveřejněna a předkládána k bádání.

Cílem diplomové práce je nezávisle nastínit problematiku archivů spolu se zveřejňováním archiválií. Práce se zaměřuje a popisuje, jak si archiváři a specialisté na digitalizaci poradili s implementací GDPR. Soustředí se na přínos GDPR a jeho význam pro občana i pro instituce v Evropské unii. Výstupem diplomové práce bude analýza současného stavu digitalizace a zveřejňování archiválií se zaměřením na kroniky ve vztahu k GDPR. Součástí práce je i snaha nastínit problémy, se kterými se archivy v návaznosti na tuto problematiku potýkají.

Diplomová práce se člení na šest kapitol. První kapitola se zaměřuje na znění GDPR zjednodušeným právním výkladem nastiňuje vybrané části znění, které mají určitou souvislost s archivnictvím. Druhá kapitola popisuje dostupné metodiky pro archivnictví v postoji k GDPR a zároveň přehledově popisuje

[1] Certifikované LTP úložiště je dlouhodobě důvěryhodné úložiště digitálních dokumentů, které je ověřeno prostřednictvím auditů a stvrzuje jej certifikace.

srovnání a určení jejich přínosu v praxi. Třetí kapitola se věnuje přímému dopadu GDPR na české archivnictví. Zabývá se i dalšími legislativními úpravami vážící se k ochraně osobních údajů opět v kontextu k archivnictví. Zároveň se podrobněji zaměřuje na kroniky - jejich vedení a následné zpřístupňování badatelům. Čtvrtá kapitola zkoumá dopad GDPR přímo na portály digitálních archivů. Analyzuje, jakým způsobem se jednotlivé státní oblastní archivy vypořádaly s uvedením do stavu splňující kritéria GDPR a sleduje nuance mezi vedením jednotlivých portálů digitálních archivů. Pátá kapitola představuje analýzu implementace GDPR ve vybraných zemích EU a srovnává jejich přístup. Šestá kapitola zahrnuje kvalitativní výzkum na úrovni SOA a nižších archivů. Zkoumá vnímání GDPR u zaměstnanců a jejich zkušenosti s nasazováním nových pravidel.

1 General Data Protection Regulation

V době rozvoje moderních technologií bylo zavedení regulace nakládání s osobními údaji nezbytné. V současnosti, kdy existuje mnoho věrnostních programů a podobných nabídek pro klienty, je celkem jednoduché osobní údaje získat. Právě s rostoucím využíváním vznikla potřeba regulace, což je následek jednoho z hlavních cílů GDPR. Současná doba zvyšuje hodnotu informací a s ní spojeného soukromí, které se stalo další hodnotou na poli internetu. GDPR přináší větší přehled o nakládání s osobními údaji a také jistoty, že se nedostanou do nepověřených rukou.[2]

Nejde jen o to, že by se osobní údaje dostaly do cizích rukou, ale také o variantu, že by se cizí osoba mohla vydávat za osobu, které byly osobní údaje odcizeny a pomoci ní páchat trestnou činnost či by mohla data využít k průmyslové špionáži. Čím více informací se o nějaké osobě ví, tím jednodušší je se za ni vydávat. Další úrovní jsou pak citlivé údaje, které mohou být v neoprávněných rukou i život ohrožující záležitost. Může se jednat o sexuální orientaci, náboženské či filozofické smýšlení.

Na druhé straně existuje svobodný pohyb informací tak, aby mohlo docházet k obchodním styku při mezinárodních či tuzemských on-line transakcích, což se také váže k eIDAS neboli nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu. eIDAS se promítá i do spisových řádů veřejnoprávních původců a s ním souvisejícího zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce[3]. eIDAS by měl být uplatňován v souladu s GDPR.

[2] ÚOOÚ: *Nebojte se GDPR.* UOOU [online]. Praha, ©2013 [cit. 2020-01-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32682

[3] K problematice aktualizace spisových řádů veřejnoprávních původců v roce 2018. In: Národní archiv ČR [online]. Praha, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/spisovy-rad-novelizace.pdf

S ohledem na vzájemné uznání by se měla autentizace pro účely on-line služeb týkat zpracování pouze těch osobních údajů, které jsou přiměřené, podstatné a rozsahem úměrné pro přístup k dané on-line službě.[4]

Evropské nařízení o ochraně osobních údajů platí celoplošně pro celou Evropskou unii, a pokud by ochrana osobních údajů fungovala méně než v zemích mimo EU, mohla by tato skutečnost například bránit mezinárodnímu obchodu, spolupracím a mohla by vést až za hranice špionáže a kriminality.[5]

Evropská unie se snaží reagovat na vývoj technologií, který s sebou nese zpracování a sběr dat či monitorování a profilování chování uživatele na internetu. Stejně jako se kdysi ohrožení počítačovým virem týkalo jen určité skupiny organizací, dnes se proti nim brání každý jedinec. Takto by se mělo přistupovat k ochraně osobních údajů, protože se stoupajícím významem přímo úměrně roste i riziko jejich zneužití.[6]

Kolem GDPR se ve vztahu k archivnictví vytvořilo několik nepravdivých mýtů. Např. že vědci mohou nahlížet do veškerých archiválií, že badatelé mohou publikovat, co chtějí, nebo že archiváři si mohou využít jakýkoli archivní pramen. Už před GDPR tyto mýty vyvracel archivní zákon nebo zákon č. 101/2000 Sb., o ochraně osobních údajů, který zásadně ovlivnil práva a povinnosti těch, jimž osobní údaje patří, i těch, kteří s nimi pracují. Tento zákon aktuálně nahrazuje zákon č. 110/2019 Sb. o zpracování osobních údajů. Dále v pomyslném seznamu legislativy, která se zabývá ochranou uživatele, je zákon o kybernetické bezpečnosti č. 181/2014 Sb.[7]

[4] PIFFL, Robert. Dopady GDPR na informační systémy a evidenci elektronických dokumentů. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.
[5] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
[6] Tamtéž.
[7] ŠIMŮNKOVÁ, Karolína a Jiří ÚLOVEC. *GDPR v archivní praxi: Setkání archivů* [online]. Národní archiv, 2019, 18. 01. 2019 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/2_GDPR_v_archivni_praxi.pdf.

1.1 Cíle a platnost GDPR

Hlavním a obecným cílem GDPR je uzpůsobení právní ochrany osobních údajů současné době a sjednocení jeho výkladu. Dále také ucelení právního systému v zemích Evropské unie a posílení práv osoby, které osobní údaje náleží.[8]
Mimo již zmíněné oblasti je vyvinuta snaha o posílení důvěryhodnosti EU a jejich členských zemí a zemí, které do oblasti GDPR spadají, převáženě z důvodu rozvoje obchodních styků s jinými mimoevropskými zeměmi.[9]

Zpracování osobních údajů by primárně měla být funkce, která bude sloužit lidem. Právo na ochranu osobních údajů musí být dle zákona posuzováno v souvislosti se svou funkcí ve společnosti a musí být v rovnováze s dalšími základními právy. Nařízení o ochraně osobních údajů ctí hodnoty uznávané Listinou základních práv, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost.[10]

Pro účinnost GDPR byla zvolena poměrně dlouhá legisvakanční lhůta, tedy doba mezi okamžikem platností a účinností nařízení. Evropské nařízení o ochraně osobních údajů začalo platit v dubnu 2016, ale jeho účinnost započala až 25. května 2018 a teprve od tohoto data je nařízení vymahatelné. Téměř po roce účinnosti byl v ČR vydán zákon č. 110/2019 Sb. o zpracování osobních údajů, tedy adaptační zákon pro oblast GDPR.

[8] MVČR. *MVČR: Ochrana osobních údajů* [online]. Praha: Ministerstvo vnitra ČR, ©2019 [cit. 2020-01-05]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx.
[9] NAVRÁTIL, Jiří a kolektiv, *c. d.* 2018.
[10] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.

Adaptační zákon umožňuje některé výjimky, a právě kvůli chybějícím úpravám v tomto období bylo nařízení uplatňováno v originálním a nejpřísnějším znění. [11]

Bezpečnostní zóna představuje závislost s kybernetickou bezpečností si GDPR klade za cíl zajistit bezpečnější IT systémy a zvýšení důvěry občanů k jejich využívání s ohledem na změnu přístupu k ochraně osobních údajů. S tím souvisí i nutnost zapracovat na vzdělávání a zvýšení počítačové gramotnosti všech vrstev společnosti.[12]

1.2 Pojem, hodnota a druhy osobních údajů

Podle zákona o ochraně osobních údajů se osobním údajem rozumí prakticky jakákoli informace, která umožní identifikaci fyzické osoby - subjektu údajů. Subjekt údajů může být určitý či neurčitý, dle toho, lze-li subjekt přímo či nepřímo identifikovat na základě čísla, kódu či jiného prvku specifického pro jeho fyzickou, fyziologickou, psychickou, ekonomickou nebo sociální identitu. [13]

Dále také rozlišuje citlivý a anonymní údaj. Citlivým údajem je takový osobní údaj, který má vypovídající hodnotu o národnostním, rasovém nebo etnickém původu. Může vypovídat o politickém postoji subjektu údajů, o členství v odborových organizacích, nebo o náboženském a filozofické přesvědčení. Za citlivý údaj je považován i zdravotní stav, sexuální život, genetické údaje a biometrické údaje. Právě ty mohou přímo identifikovat subjekt údajů. [14]

[11] NAVRÁTIL, Jiří a kolektiv, *c. d*. 2018.
[12] PIFFL, Robert. *Dopady GDPR na informační systémy a evidenci elektronických dokumentů*. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.
[13] KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Praha, 2013. ISBN 978-80-7273-173-2.
[14] Tamtéž.

Jakékoli zpracování a uchovávání citlivých údajů je již z kontextu Evropského nařízení zakázáno. Možnou výjimku umožňuje speciální předpis, který prokazuje ve veřejném zájmu citlivé údaje zpracovávat pro účely pracovního práva a práva v oblasti sociální ochrany – tedy pokud se týkají důchodů, zdravotní bezpečnosti a možnému předejití závažným hrozbám. Zpracování citlivých údajů je přípustné i pro účely archivace, vědeckého a historického výzkumu, pro statistické účely a ochranu právních nároků. Nařízení připouští zpracování údajů orgány veřejné moci za účelem dosažení cílů uznaných náboženských sdružení nebo shromažďování osobních údajů o politickém názoru fyzických osob v souvislosti s volbami. To vše za předpokladu, že jsou dodrženy stanovené záruky. Zpracování tohoto typu údajů podléhá zvýšeným opatřením s hlavním cílem chránit práva a svobody fyzických osob. [15]

Za osobní údaj je také považován podpis či rukopis, jelikož se jedná o osobní značkou každé fyzické osoby. Rukopis může mít vypovídající hodnotu o charakteru člověka a je nezaměnitelný.[16] V rámci grafologie je forenzní expert schopen odhalit informace o osobnosti člověka, například diagnostiku a průběh některých psychických poruch, nebo z psychologického hlediska různé povahové rysy a emoční naladění.[17]

Nosičem osobních údajů může být i multimediální záznam, například fotografie či video. Ten má vypovídající hodnoty o rasovém či etnickém původu a v určitých případech nese i biometrické údaje. V tomto případě je nutnost znát účel a způsob zpracování multimediálního obsahu. Pokud se jedná o shromažďování údajů například za účelem přístupu zaměstnanců do určitých prostor anebo za účelem třídění na základně biometrickými údajů, pak by toto bylo posuzováno jako

[15] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
[16] KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Praha, 2013. ISBN 978-80-7273-173-2.
[17] SVOBODA, Mojmír. *Psychologická diagnostika dospělých*. Praha: Portál, 2005. ISBN 80-7367-050-X.

zpracování citlivých údajů a je očekáván výslovný souhlas zaměstnance nebo příslušné fyzické osoby s tímto zpracováním.[18]

Identifikátor datové schránky je jedinečná a nezaměnitelná informace, díky které se datové schránky odlišují a slouží k jejímu jednoznačnému určení. Pokud je datová schránka zřizována na jméno fyzické osoby, pak lze i identifikátor považovat za osobní údaj. Jedná se o číselný kód, díky kterému lze kontaktovat příslušného vlastníka datové schránky.[19]

Půjdeme-li do hloubky toho, co je bráno jako osobní údaj, je třeba se zaměřit i na biometrické údaje. Identifikátory biometriky se kategorizují na silné (otisk prstu, rohovka), slabé (chůze, hlas) a jemné (pohlaví, věk). V kontextu s digitálními technologiemi je zajímavá především specifická behaviorální biometrika. Ta je specifická hlavně díky tomu, že je nenápadná na sběr dat a může být prováděna bez vědomí subjektu.[20] Behaviorální biometrika může identifikovat osobu na základě analýzy textu s účelem určení autorství, zvláštních znaků vykazovaných osobou při používání počítače, nebo i na základě analýzy schopností, které člověk vykazuje při plnění určitých, zejména kognitivních úloh.[21]

GDPR pojem biometrické údaje zařazuje do zvláštní kategorie osobních údajů, které mohou být zpracovány zvláštními technickými prostředky umožňujícími identifikaci nebo autentizaci osoby. Mohou být poměrně jednoduše odezírány z těla osoby nebo například videa či fotografie. Na tento typ údajů se tedy vztahuje specifický způsob zpracování, ze kterého jsou uděleny i výjimky.

---

[18] KUČEROVÁ, Alena a František NONNEMANN, *c. d.* 2013.
[19] Tamtéž.
[20] Matejka, J., Matochová, S. a Prokeš, J. *Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů*. Acta Informatica Pragensia, 2019, vol. 8, iss. 2, p. 88-111. [cit. 2020-03-02]. DOI: 10.18267/j.aip.126. Dostupné z: https://journals.muni.cz/revue/article/view/8801/pdf.
[21] YAMPOLSKIY, Roman V., GOVINDARAJU, Venu. *Taxonomy of Behavioural Biometrics*. InWNAG, Liang, GENG, Xin (eds.). Behavioral Biometrics for Human Identification: IntelligentApplications. IGI Global, August 2009. doi:10.4018/978-1-60566-725-6. Dostupné z: https://www.igi-global.com/book/behavioral-biometrics-human-identification/99#table-of-contents.

Například autentizace pomocí otisku prstu či skenu tváře pro odemčení mobilního telefonu. Zde dochází k porovnání otisku či skenu s již dříve uloženým údajem a společnost nevytváří databázi z těchto hodnot.
Biometrické údaje jsou tedy úzce spjaty s osobností člověka, a právě individualitu každého jedince chrání Listina základních práv a svobod a občanský zákoník.[22]

1.3 Povinnosti a změny

GDPR navazuje na předešlou právní úpravu, tedy směrnici Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů z roku 1995. Ta cílila na zakotvení jednotné úpravy ochrany osobních údajů na o jejich pohybu na území EU, což umožnilo volnější pohyb osob po zemích Schengenského prostoru. Právě až volný pohyb osobních údajů umožnil snazší pohyb osob po území EU.[23]

Ke změně došlo z důvodu, že předešlá směrnice již přestala odpovídat požadavkům současné doby. Zpracování údajů nebylo před lety tak komplexní, co se týče například profilování, automatizace, zpracování atd. GDPR má přiblížit ochranu osobních údajů současnosti.[24]

Nahlížení do archiválií upravují také §37 a §38 zákona č. 499/2004 Sb., které omezují přístup do archiválií mladších třiceti let nebo vyžadují souhlas s nahlížením do archiválií obsahující osobní údaje žijících osob. Některé archiválie lze předložit i bez souhlasu žijící osoby, jejíž osobní údaje v archiválii figurují, což

[22] Matejka, J., Matochová, S. a Prokeš, J. *Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů*. Acta Informatica Pragensia, 2019, vol. 8, iss. 2, p. 88-111. [cit. 2020-03-02]. DOI: 10.18267/j.aip.126. Dostupné z: https://journals.muni.cz/revue/article/view/8801/pdf.
[23] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
[24] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.

upravuje odst. 11 § 37 archivního zákona.[25] Týká se to například archiválií vzniklé před 1. lednem 1990 z činnosti vojenských soudů a všech bezpečnostních složek minulých režimů, což také upravuje i zákon o Ústavu pro studium totalitních režimů[26].

GDPR stojí na nových principech. Princip odpovědnosti správce závisí na odpovědnosti správce osobních údajů za dodržování zásad korektního zpracování transparentním a zákonným způsobem, shromažďovány pro konkrétní, vyslovené a legitimní účely, osobní údaje musí být přiměřené vůči účelu zpracování, které musí být přesné a aktuální. Správce odpovídá za dodržení článku 5 odst. 1 GDPR a musí být schopen toto dodržení souladu doložit odpovědnost.[27]

Druhý z principů stojí na riziku. Osobní údaje musí být zpracovávány takovým způsobem, který zajistí jejich patřičné zabezpečení a ochrany před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.[28] Správce osobních údajů musí tedy od začátku brát v potaz povahu, rozsah a účel zpracování a dle toho nastavit opatření, aby nedošlo k žádné z výše uvedených možností.
Správce má přístup k údajům založených i na riziku v případě jejich zpracování a porušení zabezpečení. V tomto případě se uplatňuje povinnost ohlašování případu porušení zabezpečení ÚOOÚ.[29]

[25] ŠIMŮNKOVÁ, Karolína a Jiří ÚLOVEC. *GDPR v archivní praxi: Setkání archivů* [online]. Národní archiv, 2019, 18. 01. 2019 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/2_GDPR_v_archivni_praxi.pdf.
[26] ČESKO. § 37 odst. 11 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499#p37-11.
[27] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.
[28] Tamtéž.
[29] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.

1.4 Výhody

Bezesporu největším přínosem GDPR z pohledu možných subjektů zpracování údajů je požadování souhlasu se zpracováním údajů, anonymizace shromážděných údajů k ochraně soukromí, poskytování oznámení o narušení zabezpečení údajů a bezpečné nakládání s přeshraničním přenosem údajů.
GDPR přináší i příležitosti na rozvoj digitálních služeb pro občany a do budoucna by mohl fungovat jako akcelerátor v této oblasti, protože vytváří podmínky pro efektivnější fungování zejména e-governmentu v EU.[30]

Protože v minulosti došlo k mnoha incidentům v oblasti kybernetické bezpečnosti a k narušení dat, GDPR nyní vyžaduje, aby správce údajů oznámil porušení při nakládání s osobními údaji orgánu dohledu bez zbytečného odkladu a, pokud je to proveditelné, nejpozději do 72 hodin poté, co se o skutečnosti dozvěděl. Organizace proto musí zvýšit své úsilí v oblasti kybernetické bezpečnosti, aby chránily subjekty údajů před hrozbami a narušením.
Mimo to, GDPR zvýšilo poptávku po odbornících z oblasti kybernetické bezpečnosti a ochrany osobních údajů. Vlády a technologické společnosti v celé EU musely výrazně investovat do školení a vzdělávacích programů v oblasti kybernetické bezpečnosti, aby vyřešily současný nedostatek znalostí a dovedností nejen pro profesionálů v oblasti kybernetické bezpečnosti, ale úředníků pracujících s osobními údaji. [31]

Podle průzkumu Capgemini Research Institute provedené v březnu až dubnu 2018 jsou spotřebitelé, klienti či zákazníci ochotnější spíše jednat s organizacemi, které dostatečně chrání svá data a polovina respondentů se o své kladné zkušenosti

[30] PIFFL, Robert. Dopady GDPR na informační systémy a evidenci elektronických dokumentů. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19].
Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.
[31] LI, He, Lu YU a Wu HE. *The Impact of GDPR on Global Technology Development.* Journal of Global Information Technology Management [online]. 2019 (22), 1-6 [cit. 2020-02-22].
DOI: 10.1080/1097198X.2019.1569186. Dostupné z:
https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186?scroll=top&needAccess=true

podělila ve svém okolí. To má jasný dopad na zvýšení zájmu o danou organizaci. Mimo kladné dopady na ekonomiku organizace má toto i vliv na zaměstnance, jejich loajalitu vůči organizaci a klima uvnitř pracovního prostředí.[32]

1.5 Právo na výmaz

Další podstatnou výhodou z pohledu občanů je právo na výmaz osobních údajů, tedy občan má nárok žádat po zpracovateli údajů jejich výmaz bez odkladu. Toto může žádat v případě, že jeho údaje byly zpracovány protiprávně, nebyly určené pro daný účel zpracování, byl odvolán souhlas s jejich zpracováním, byly zpracovány přes námitku na jejich zpracování, nebo například rodiče neposkytli souhlas se zpracováním osobních údajů dítěte. Rozšířením práva na výmaz osobních údajů je tak právo být zapomenut. To spočívá v provedení takových operací, které vedou k vymazání veškerých, nejen digitálních stop osobních údajů poskytovaných minulosti. [33]

Toto se však netýká archivnictví, přesněji archivace ve veřejném zájmu podle Článku 17 odst. 3 písm. d).[34] Posouzení tohoto faktu je zajímavé už jen z hlediska uchování digitálních dat. Problém nastává právě u spisové služby, kde i kdyby došlo ke smazání všech dat, bude stále jejich část figurovat z důvodů jiných zákonných povinností v příslušných systémech.

[32] CAPGEMINI RESEARCH INSTITUTE. *Seizing the GDPR Advantage: From mandate to high-value opportunity* [online]. 2018 [cit. 2020-02-22]. Dostupné z: https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf.
[33] GDPR SOLUTIONS*: Jaké plynou z gdpr výhody pro občany*? [online]. Praha, ©2020 [cit. 2020-02-22]. Dostupné z: https://www.gdprsolutions.cz/narizeni-gdpr/vyhody-pro-obcany/.
[34] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 17. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/17.htm.

GDPR nelimituje výmaz zpracování, jako tomu bylo u předchozí směrnice 95/46/ES, která omezovala výmaz pouze na to, co způsobovalo škody či újmu. Strana, jenž osobní údaje zpracovává, může výmaz odmítnout podle článku 17 odst. 3 GDPR například z důvodů[35]:

- na uplatnění práva na svobodu projevu a informace
- splnění zákonné povinnosti či plnění úkolů veřejného zájmu nebo výkonu veřejné moci
- veřejného zájmu v oblasti zdraví v souladu s článkem 9 odst. 2 písm. h) a i) a odst. 3
- pro účely archivní, statistické, vědecké, historické, nebo pro obhajobu právních nároků[36]

Vše výše uvedené částečně eliminuje článek 89 GDPR, jenž upravuje zpracování pro účely archivace, vědeckého či historického výzkumu a statistické účely. Dle článku 17 GDPR Právo na výmaz se toto právo neuplatní, pokud je zpracování nezbytné, a to v souladu s článkem 89 GDPR a protože by „*znemožnilo nebo vážně ohrozilo splnění cílů daného zpracování*“.[37]

Poměrně nový pojem ‚právo na výmaz‘ přinesl potřebu novelizace v podobě zákona č. 111/2019 Sb., GDPR přineslo možnost situace, kdy je třeba provést výběr archiválií před uplynutím skartační lhůty, a to právě z důvodu práva na výmaz, např. na základě rozhodnutí soudu. V takovém případě je nyní možné tento

[35] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.
[36] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 17 Právo na výmaz („právo být zapomenut“). Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.
[37] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě.* Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

dokument vyřadit mimo skartační řízení. Novela se velmi podobně potýká s problémem vyřazení zdravotnické dokumentace.[38]

1.6 Postihy a tresty za porušení GDPR

Pokud se subjekt údajů domnívá, že bylo porušeno jeho právo na ochranu osobních údajů, má stanovené právo podat stížnost u dozorového úřadu. Ten, pokud zjistí pochybení, zajišťuje, aby uložení správní pokuty proběhlo v souladu s článkem 83 GDPR.[39] Udělování sankcí a opatření musí být účinné, přiměřené danému porušení, a hlavně odrazující v dalším případném porušování. Sankce jsou ukládány po přezkoumání daného případu, což nemusí vždy vyústit v likvidační sankci. Správce osobních údajů může být pouze upozorněn, že jistá činnost porušuje Obecné nařízení či může být uděleno napomenutí.[40]

Při porušení se posuzují kritéria, která jsou uvedena v článku 83 odst. 2 GDPR.

Zohledňuje se:

- Povaha závažnost a délka trvání porušení – na těchto kritériích stojí rozhodnutí dozorového úřadu o výši sankce či v případě méně závažného porušení má úřad možnost nahradit pokutu napomenutím.
- K porušení došlo/nedošlo z úmyslu – úmyslná porušení nařízení spíše vedou k uložení finanční pokuty. Za úmysl je považováno nezákonné zpracování údajů bez patřičného souhlasu, pozměnění za účelem klamu, obchodování s údaji. Za nedbalost se považuje selhání lidského faktoru, neprovedení kontroly údajů ve zveřejňovaných informacích, neprovedení včasných aktualizací.

[38] INFORMAČNÍ LIST: *Bulletin pro otázky elektronické spisové služby a dokumentů v digitální podobě*. In: Národní archiv ČR [online]. Praha, 2019, 26. června 2019 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/07/InfoList_201904-oprA.pdf.

[39] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě.* Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

[40] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.

- Kroky podniknuté ke zmírnění škod – jedná se o snahu snížení dopadu svých činů, např.: včasného zabránění pokračování porušování nařízení nebo kontaktování jiných správců osobních údajů, kteří mohli být také zapojeni do možného zpracování, kdy mohli být určité údaje poskytnuty třetím stranám.
- Úroveň odpovědnosti správce s ohledem k technickým a organizačním opatřením.
- Veškerá předchozí porušení nařízení.
- Míra spolupráce s dozorovým úřadem.
- Druhy osobních údajů porušením dotčené.
- Způsob, jakým se úřad dozvěděl o porušení.[41]

Opatření

Dozorový úřad ukládá podle situace jednotlivých případů správní pokutu nebo zavádí opatření podle článku 58 odst. 2 GDPR. Mezi tato opatření patří:

- Upozornění na porušení nařízení;
- Udělení napomenutí;
- Nařízení správci/zpracovateli údajů, aby uvedl své činnosti do souladu s nařízením;
- Nařízení správci/zpracovateli údajů, aby oznámil událost porušení zabezpečení osobních údajů;
- Nařídit omezení či zákaz zpracování;
- Nařídit opravu nebo výmaz osobních údajů;
- Odebrání osvědčení;
- Nařídit přerušení pohybu údajů ve třetí zemi nebo mezinárodní organizaci.[42]

[41] Evropský sbor pro ochranu osobních údajů. *Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679* [online]. Brusel, 2017, [cit. 2020-02-09]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886.

[42] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě.* Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

Uplatňování pravidel pro ochranu osobních údajů má svůj podstatný důvod v celkovém systému nařízení o ochraně osobních údajů.

Prosazování správních pokut spolu s dalšími opatřeními stanovenými článkem 58 GDPR tvoří mocnou součást souboru donucovacích prostředků dozorového úřadů.[43]

Vztah přestupků k archivům

Archivy vystupují z pohledu zákona č. 110/2019 Sb. o ochraně osobních údajů jako správci či zpracovatelé osobních údajů. Zákon č. 110/2019 Sb. je adaptačním zákonem k GDPR, který v § 62 spravuje přestupky a sankce pro správci a zpracovatele. Konkrétně se toto týká Čl. 8, 11, 25 až 39, 42 až 49 GDPR. Tyto články zahrnují podmínky souhlasu dítěte, zpracování nevyžadující identifikace, standartní ochranu osobních údajů a další. ÚOOÚ může upustit od uložení správního trestu také tehdy, pokud uloží opatření podle § 54 odst. 1 písm. e) nebo § 60 podle zákona o ochraně osobních údajů. Jedná se o případ, kdy dojde k odebrání osvědčení udělené ÚOOÚ nebo opatření k odstranění nedostatků. V případě veřejný archivů spadající pod orgán veřejné moci dochází dle § 62 odst. 5 zákona o ochraně osobních údajů k upuštění od uložení správního tresu a že to podle výjimky, kterou umožňuje čl. 83 odst. 7 GDPR. Každý členský stát EU si může stanovit pravidla, do jaké míry je bude ukládat správní pokuty orgánům veřejné moci a veřejným subjektům působícím v daném členském státě EU. [44]

[43] Evropský sbor pro ochranu osobních údajů. *Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679* [online]. Brusel, 2017, [cit. 2020-02-09]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886.

[44] Zákon č. 110/2019 Sb. o ochraně osobních údajů. In: Sbírka zákonů České republiky. 2019, částka 47. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=63840.

Sankce

Udělování sankcí musí být účinné, přiměřené danému porušení, a hlavně v první řadě odrazující. Sankce jsou ukládány po přezkoumání daného problému, což nemusí vždy vyústit ve finanční postih. Správce osobních údajů může být pouze upozorněn, že jistá činnost porušuje Obecné nařízení či může být uděleno pouze napomenutí.[45]

Podle okolností uvedených výše či v článku 83 odst. 2, může dozorový úřad uložit správní pokutu. Ty se dělí do dvou kategorií podle toho, které články Obecního nařízení porušily. Níže jsou uvedeny kategorie a příklady porušených článků.

1) Sankce až do výši 10 milionů EUR, nebo v případě podniku 2 % z celkového ročního obratu za předchozí období. Vždy se bere v potaz vyšší z obou částek. Došlo k porušení článků 8, 11, 25 až 39, 42 a 43 GDPR.
   - ⇨ Podmínky souhlasu dítěte v souvislosti s informačními službami společnosti (čl. 8 GDPR)
   - ⇨ Zpracování nevyžadující identifikaci (čl. 11 GDPR)
   - ⇨ Záměrná a standardní ochrana údajů (čl. 25 GDPR)
   - ⇨ Zabezpečení zpracování (čl. 32 GDPR)
   - ⇨ Oznamování porušení zabezpečení osobních údajů (čl. 34 GDPR)

[45] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.

2) Sankce až do výši 20 milionů EUR, nebo v případě podniku 4 % z celkového ročního obratu za předchozí období. Vždy se bere v potaz vyšší z obou částek. Došlo k porušení základních zásad pro zpracování článků 5, 6, 7 a 9 GDPR, práv subjektů údajů články 12 až 22 GDPR, předání osobních údajů třetím zemím/mezinárodní společnosti články 44 až 49 GDPR, povinností plynoucí z kapitoly IX, došlo k nesplnění příkazu či dočasnému/trvalému zákazu zpracování nebo toku údajů nebo nesplnění opatření udělené dozorovým úřadem podle čl. 58 odst. 2 GDPR.
   - ⇨ Zásady zpracování osobních údajů (čl. 5 GDPR)
   - ⇨ Zákonnost zpracování (čl. 6 GDPR)
   - ⇨ Podmínky vyjádření souhlasu (čl. 7 GDPR)
   - ⇨ Zpracování zvláštních kategorií osobních údajů (čl. 9 GDPR)
   - ⇨ Transparentnost informací (čl. 12 GDPR)
   - ⇨ Právo subjektu na přístup k osobním údajům (čl. 15 GDPR)
   - ⇨ Právo na výmaz (čl. 17 GDPR)
   - ⇨ Právo na omezení zpracování (čl. 18 GDPR)
   - ⇨ Právo vznést námitku (čl. 21 GDPR)
   - ⇨ Obecná zásada pro předávání (čl. 44 GDPR)
   - ⇨ Závazná podniková pravidla (čl. 47 GDPR)[46]

V rámci nejkritičtějších případů porušení ochrany osobních údajů, je v GDPR uvedena také možnost trestání i v rámci trestního řízení, což v případě České republiky splňuje §180 trestního zákoníku, odnětí svobody na patřičnou dobu. Nicméně GDPR upozorňuje i na skutečnost, že nesmí docházet ke dvojímu trestání za též provinění.

[46] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 83 Obecné podmínky pro ukládání správních pokut. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

Došlo by tak k porušení zásady *ne bis in idem*, tedy trestat dvakrát v jedné a též záležitosti. Pro příklad ale uložení dvou sankcí není porušením této zásady.[47]

1.7 Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů neboli dozorový úřad je nezávislý orgán veřejné moci, který je pověřen dohledem nad prosazováním GDPR s hlavním záměrem ochraňovat základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů. Dozorový úřad může být jeden nebo více v každém státě Evropské unie.[48]

Od začátku roku 2020 získal dozorový úřad novou odvolací a přezkumnou pravomoc. Nově se bude úřad zabývat i právem na informace. Tato nová kompetence by neměla nahradit soudy, do jejichž kompetence tato agenda spadala dříve, pouze má eliminovat počet soudních řízení v této oblasti. Lze říct, že právo na informace a ochrana osobních údajů jsou dvě strany jedné mince a Česká republika by nebyla tak prvním státem v EU, kde by tyto dvě agendy spravoval jeden úřad. Takto to je nastavené například ve Velké Británii, Maďarsku, Německu nebo Slovinsku.[49]

Mgr. Šimůnková z Národního archivu uvádí, že správce údajů by měl před zpracováním provést posouzení vlivu na ochranu osobních údajů. Mělo by dojít k posouzení konkrétních pravděpodobností a zvážení závažnosti rizika a zohlednit přitom povahu, rozsah, kontext a účely zpracování a zdroje rizika u takových typů

[47] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
[48] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 51 Dozorový úřad. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679
[49] CIBULKA, Jan. *Bez několikaletého čekání na soud. Nově bude právo na informace posuzovat Úřad pro ochranu osobních údajů.* Český rozhlas [online]. Praha, 2019 [cit. 2020-03-02]. Dostupné z: http://irozhl.as/8vd.

operací zpracování. Ty mohou s ohledem na svou povahu, rozsah, kontext a účely představovat vysoké riziko pro práva a svobody subjektů údajů.[50]
Jednou z ústředních vlastností dozorového úřadu je nezávislost v oblasti ochrany osobních údajů, což je podstatné pro efektivní ochranu práva a potřebnou eliminaci vlivů výkonné moci na dozorový úřad.

Nezávislost je třeba držet ve třech rovinách:

1) Funkční nezávislost neboli nezávislost na jiných institucích. Zásahy jiných institucí či úřadů jsou akceptovatelné pouze dle GDPR. Dozorový úřad se řídí pouze právními předpisy a předpisy EU.
2) Materiální nezávislost apeluje na ucházející vybavení úřadu po technické a finanční stránce, dále lidských zdrojů a prostorami. Dle GDPR má dozorový úřad vlastní roční rozpočet. Nezávislost v tomto ohledu by neměla ovlivnit ani kontrola hospodaření úřadu.
3) Personální nezávislost stanovuje, že v úřadu mohou být zaměstnáni pouze ti pracovníci, kteří spadají do kompetence tohoto úřadu a nejsou řízení zvenčí. Poměry těchto pracovníků se řídí služebním a správním zákonem.[51]

[50] ŠIMŮNKOVÁ, Karolína. *GDPR – spisová služba a původci v předarchivní péči Národního archivu* [online]. Národní archiv, 2017, 22.11.2017 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/GDPR.pdf
[51] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě*. Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

2 Archiv jako správce údajů

2.1 Metodické pokyny MVČR

Archivy, stejně tak jako jiné malé podniky či živnostníci mohou využívat tzv. *Desatero zpracování pro správce*, jenž uvádí Úřad pro ochranu osobních údajů i Národní archiv.

1) Zpracování musí být legitimní a být prováděno správcem nebo po dohodě se subjektem zpracování údajů.
2) Podstatou je, aby zpracování bylo podloženo některým ze základních důvodů ke zpracování – jedná se nejčastěji o smluvní plnění, výkon právních povinností, výkon veřejné moci nebo souhlas dotyčné osoby.
3) Vymezit účel, za kterým jsou údaje zpracovávány.
4) Rozsah a doba zpracování musí být přiměřené účelu.
5) Zpracování údajů musí podléhat danému zákonnému podkladu, které nelze nahradit souhlasem se zpracováním údajů.
6) Nutno zabezpečit a ochránit osobní údaje technicky nebo organizačně.
7) Zpracování je prováděno korektně, férově a transparentně vůči subjektu údajů. Informace o zpracování musí být jasné, srozumitelné a v ideálním rozsahu.
8) Nesmí zasahovat do soukromí.
9) Zlikvidovat osobní údaje po naplnění účelu, pro který byly zpracovávány.
10) Poskytovat údaje do zemí mimo EU lze za předpokladu splnění dodatečných pravidel či za okolností jako plnění smlouvy se subjektem údajů.[52]

[52] *Desatero zpracování pro správce - archiv dokumentů*. Úřad pro ochranu osobních údajů [online]. Praha: Úřad pro ochranu osobních údajů, ©2013 [cit. 2020-06-02]. Dostupné z: https://www.uoou.cz/desatero-zpracovani-pro-spravce/ds-4821/archiv=2&p1=3938.

Tyto základní principy GDPR jsou uvedené i Mgr. Karolínou Šimůnkovou z Národního archivu v dokumentu pro spisovou službu a předarchivní péči, který je součástí diplomové práce v příloze č. 5.[53]
Metodický pokyn MVČR z června 2019 upravuje řešení problematiky poskytování osobních údajů ze strany badatelů formou nového badatelského listu. Ten obsahuje poučení pro badatele ve smyslu nakládání s jeho osobními údaji, poskytovanými archivu.[54] Metodický pokyn upravující problematiku poskytování osobních údajů je uveden v příloze č. 1 v celém znění.

Tato problematika je rovněž upravena legislativně, a to novelizací zákona č. 499/2004 o archivnictví a spisové službě. Vyhláška ze dne 19. března 2019 upravila některá znění Badatelského listu týkající se osobních údajů. Například údaj o rodném příjmení badatele se stává nepovinným nebo dnes již neplatný zákon č. 101/2000 Sb., byl nahrazen právními předpisy upravujících zpracování osobních údajů. [55]

Nový badatelský list definuje správce údajů, poskytuje kontaktní údaje pověřence pro ochranu osobních údajů, definuje účel zpracování osobních údajů a dobu jejich uložení, která se řídí skartační lhůtou. Badatel se nemůže dožadovat výmazu, pokud jde o zpracování pro účely archivace. Rovněž obsahuje poučení badatele o rozsahu jeho práv, co se GDPR týče. Badatel svým podpisem stvrdí, že veškeré poučení, bere na vědomí. [56]

[53] ŠIMŮNKOVÁ, Karolína. *GDPR – spisová služba a původci v předarchivní péči* Národního archivu [online]. Národní archiv, 2017, 22.11.2017 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/GDPR_sylabus.pdf
[54] Metodický pokyn č. 3/2018 [online]. Praha: MVČR, 2018, 1. června 2018 [cit. 2020-06-02]. Dostupné z: https://www.mvcr.cz/soubor/metodicky-pokyn-c-3-2018.aspx.
[55] Vyhláška č. 85/2019 Sb., kterou se mění vyhlášky provádějící zákon o archivnictví a spisové službě. 2019. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-85.
[56] Metodický pokyn č. 3/2018: Badatelský list [online]. Praha: MVČR, 2018, 1. června 2018 [cit. 2020-06-02]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-1-badatelskeho-listu.aspx.

2.2 Metodika European Archives Group

Metodika European Archives Group (zkráceně EAG), vznikla nejen pro národní a státní archivy, ale také pro regionální a obecní archivy, muzea, knihovny, nadace a další veřejné a soukromé subjekty, které se zabývají archivací dokumentů. Cílem vytvořeného dokumentu je poskytnout archivářům základní informace a praktické pokyny týkající se konkrétních problémů při uplatňování obecného nařízení o ochraně údajů v odvětví archivnictví.

Dokument neposkytuje pokyny pro zpracování osobních údajů pro archivy jakožto zaměstnavatele, nebo badatelů, dárců, původců atd. Metodika se zaměřuje výhradně na údaje, které se nachází v archivních fondech. Její originální znění se nachází v příloze č. 2 diplomové práce.

GDPR sice platí ve všech členských státech jednotně, nicméně ponechává státům určitý prostor pro zavedení výjimek v konkrétních oblastech. Jedním z nich je i archivace ve veřejném zájmu a historický výzkum. Je již na zákonodárcích, zda tuto možnost využili. Zákonodárci EU uznali archivy jako instituce nezbytné k prosazování základních práv. Ve skutečnosti GDPR uvádí, že „*osobní údaje mohou být uchovávány déle, pokud budou osobní údaje zpracovávány pouze pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu*“[57]. Což podléhá opatření, že zpracování proběhne za předpokladu ochrany práv a svobod.

Mezi lhůtou, kdy dochází k uchování údajů a kdy může dojít k jejich poskytnutí může být značný rozdíl. Tyto lhůty si určují jednotlivé členské státy ve svých předpisech. Například Itálie má lhůtu 40 let na poskytnutí dokumentů, které

[57] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 5. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/5.htm.

obsahují informace odhalující rasový nebo etnický původ jedince, náboženské a politické názory, či členství ve stranách apod. Lhůty týkající se údajů osoby, které prozrazují zdraví a sexuální život, jsou uzavřeny na dobu 70 let a záznamy, které mohou odhalit identitu matky, která chtěla porodit anonymně, jsou uzavřeny na 100 let. České archivnictví zpřístupňuje archiválie až po uplynutí ochranné lhůty třiceti letech a matriční záznamy jsou v archivu přístupné po uplynutí lhůty 110 let. [58]

GDPR nemění zákony o svobodě projevu. Mezi badatele patří také novináři, akademičtí pracovníci a další vědci, jejichž cílem je zveřejnit svá zjištění. GDPR nemění tiskové zákony a další pravidla týkající se svobody projevu. Stanovuje, že: „*Členské státy podle zákona uvedou v soulad právo na ochranu osobních údajů podle tohoto nařízení s právem na svobodu projevu a informací, včetně zpracování pro žurnalistické účely a na akademické, umělecké nebo literární účely*."[59] A pro tyto účely si rovněž členské státy mohou stanovit určité výjimky nebo odchylky od ustanovení GDPR.

Archivy by si měli být vědomi obecných zásad týkající se zpracování osobních údajů stanovených v Čl. 5, které jsou uvedené i v desateru MVČR a jsou zmíněné v předchozí podkapitole. Tyto zásady mají pro archivnictví mnoho důsledků. Se zajištěním zásady důvěrnosti jsou archiváři již z praxe obeznámeni, protože ochrana archivních materiálů před neoprávněným přístupem je běžnou praxí. Některé důsledky principů zmiňovaných v Čl. 5 jsou nicméně méně zřejmé.

[58] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-27].
[59] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 85. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/85.htm.

Zásada průhlednosti znamená, že archivy musí zveřejňovat jasné a uživatelsky přívětivé informace o jejich zpracování a jaký k nim mají subjekty údajů přístup. Další zásada integrity znamená mimo jiné, že nekalé praktiky v oblasti archivace, které vedou ke ztrátě dokumentů obsahujících osobní údaje, jsou nejen porušením profesionálních zásad archivace a archivních zákonů, ale také porušením GDPR.[60]

Ochrana pouze pro živé osoby

GDPR chrání osobní údaje pouze živých osob a již neřeší osobní údaje zesnulých. Mělo by však být bráno v potaz, že by vnitrostátní zákony mohly GDPR doplnil i o ochranu, která se bude částečně vztahovat i na již nežijící osoby. GDPR ve skutečnosti stanovuje, že: „*členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zemřelých osob*“.[61]

Ve většině případů mohou archiváři pouze odhadovat, zda je subjekt údajů stále ještě žijící osoba. Mohou však rozumně předpokládat, že osoby narozené před více než sto lety již nežijí. Například archivář zpracovávající osobní soubory vojáků, kteří bojovali v 1. světové válce, může předpokládat, že již nejsou naživu a že GDPR se tedy na tyto soubory nevztahuje. Toto je jeden z mála případů, který je jasně dán, ale archiváři budou muset případ od případu ověřovat možnost, že archivní fondy, které jsou v jejich péči, obsahují osobní údaje stále žijících jednotlivců.[62]

[60] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-27].

[61] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Recitál 27. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/r27.htm.

[62] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-26].
Dostupné z: https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.

Různá pravidla pro různé archivy

GDPR umožňuje řadu výjimek ve prospěch účelů archivace ve veřejném zájmu, tedy pro orgány či subjekty, které mají "právní povinnost získávat, uchovávat, posuzovat, uspořádat, popisovat, sdělovat, podporovat a šířit záznamy trvalé hodnoty pro obecný veřejný zájem a poskytovat k nim přístup".[63] Každý jednotlivý členský stát si může stanovit, "že osobní údaje mohou být dále zpracovávány pro účely archivace, například s cílem poskytnout konkrétní informace související s politickým chováním za bývalých totalitních režimů, s genocidou, zločiny proti lidskosti, zejména holokaustem, nebo válečnými zločiny"[64].

V praxi to znamená, že hlavně archivy národní a státní archivy, ale i veškeré další archivy, které uchovávají archiválie ve veřejném zájmu mohou zpracovávat údaje a informace pro historický výzkum, který bude mít nějaký kulturní přesah. Při těchto informacích by mohlo vzniknout oddělení, které se bude zabývat získáváním, uchováváním a zpřístupňováním informací například spisovatelů či jiných významných osob. Příklad: pokud by vznikalo muzeum dějin vědy, jedna z jeho činností by zahrnovala získávání a uchovávání osobních dokladů vědců. Právo členských států by mohlo vytvořit institut pro dějiny minulého autoritářského režimu, jehož poslání zahrnuje uchovávání dokumentárního dědictví týkajícího se obětí politické represe. V případě ČR takto funguje Archiv bezpečnostních složek. [65]

[63] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Recitál 158. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/r158.htm.
[64] Tamtéž.
[65] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-27].

Archiv bezpečnostních složek spravuje veškeré písemnosti bezpečnostních složek z dob obou minulých režimů. Jedná se o dokumenty Státní bezpečnosti, Veřejné bezpečnosti, civilní a vojenské rozvědky a další. Ty jsou v souladu se zákonem č. 499/2004 Sb. o archivnictví a spisové službě každému přístupné.[66]

Jelikož ne všechny subjekty uchovávající archiválie, mají zákonnou povinnost je získávat, a proto ne všechny spadají pod definici recitálu č. 158 GDPR. V mnoha případech však takové subjekty mají jasné kulturní poslání a archivují za účelem historického výzkumu. GDPR umožňuje výjimky pro zpracování osobních údajů pro historický výzkum, které jsou stanoveny v celém nařízení a zejména v článku. 89 GDPR.

Archiváři by si měli být také vědomi, že výjimky ve prospěch archivačních účelů ve veřejném zájmu se týkají pouze zpracování osobních údajů zahrnutých do archivních fondů, které uchovávají. Na veškerá další zpracování osobních údajů prováděná archivy se vztahují stejná pravidla, která platí pro jakýkoli jiný veřejný nebo soukromý subjekt. Pro příklad, když archivní služby zpracovávají osobní údaje badatelů nebo studentů, kteří se účastní vzdělávacích aktivit nebo účastníků konferencí atd., nemají žádnou výjimku z pravidel.[67]

Možné odchylky pro historický a vědecký výzkum

Článek 89 GDPR stanovuje, že pokud dochází k technickým a organizačním opatřením, pseudonymizaci a minimalizaci a již nedochází k jasné identifikaci osoby, je zpracování pro tyto účely možné. Právní předpisy EU nebo členského státu mohou stanovit odchylky od práv uvedených v článcích 15, 16, 18 a 21 GDPR. Zásada minimalizace údajů a povinnost přijmout příslušná ochranná opatření za účelem ochrany práv subjektů údajů jsou proto společné jak pro

[66] Ústav pro studium totalitních režimů [online]. Praha, © 2020 [cit. 2020-07-16]. Dostupné z: https://www.ustrcr.cz/o-nas/.
[67] Tamtéž.

„zpracování pro účely archivace ve veřejném zájmu“, tak pro zpracování pro „vědecké nebo historické výzkumné účely nebo statistické účely“. Konkrétní uplatňování těchto principů se však bude v různých oblastech lišit. Archiváři prosazují princip minimalizace dat jinak než vědci a statistici. Zákonná omezení přístupu k archiváliím se v jednotlivých členských zemích může lišit a pro určité druhy osobních údajů může být doba uzavření až 120 let. Rovněž lze v archivech využívat pseudonymizaci, ale ta by měla být plně reverzibilní a měla by být prováděna způsobem, který neohrožuje důkazní hodnotu informací. V případě osobních údajů uchovávaných v archivech by měly být ukládané nezměněné původní archiválie a vytvořit pseudonymizovanou kopii osobních údajů pro přístup k výzkumným pracovníkům, pokud lze tyto účely tímto způsobem splnit.[68]

Informace získané jinak než od subjektu údajů

Poté co archiváři získají, uspořádají, popíšou, uchovají a zpřístupní badatelům archivní fondy je možné, že archivní materiál obsahuje osobní údaje týkající se neurčitého počtu osob. Informovat jednotlivé subjekty údajů o takovém zpracování by bylo nemožné nebo by vyžadovalo nepřiměřené úsilí. Nejlepší možností je v takovém případě zpřístupnit informace o takovém zpracování na webových stránkách archivu, aby se o něm mohla veřejnost dozvědět, jedná se o informační povinnost dle GDPR.

V některých případech by mohlo být vyvinuto cílenější úsilí o informování subjektů údajů. Pokud je například získán archivní fond sdružení, politické strany nebo odborového svazu, který zpracovával osobní údaje pouze svých spolupracovníků, můžou s nimi souhlasit skrze jejich informační kanál.

[68] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-28].

Právo být zapomenut

Podle GDPR právo na zapomnění se vztahuje na skutečné vymazání osobních údajů. Článek 17 GDPR ve skutečnosti poskytuje subjektům údajů právo získat od správce výmaz osobních údajů, které se ho týkají, bez zbytečného odkladu.

Právo být zapomenut zároveň podléhá různým omezením a nevztahuje se na případy, kdy je zpracování nezbytné pro účely archivace ve veřejném zájmu, pokud by vymazání znemožnilo nebo vážně narušilo dosažení cílů zpracování.[69]

Vymazání osobních údajů obsažených v archiváliích by proto archivům znemožnilo plnit poslání, které jim zákon ukládá. Právo na výmaz podle článku 17 GDPR se proto nevztahuje na dokumenty vybrané pro trvalé uchování archivářskými službami, na které se vztahuje definice podle recitálu 158 GDPR.

Nicméně začernění, vymazání nebo jiné způsoby, které brání k vyhledávání jmen v dokumentech, ve skutečnosti neovlivní integritu archivních dokumentů ani neohrozí jejich trvalé uchování. Archivní služby navíc mohou zabránit vyhledávání jmen online dokumentu, zatímco je udržují vyhledatelné pomocí vyhledávacích klíčů odlišných od osobních jmen. Archivy se musí zdržet zveřejňování online dokumentů nebo pomůcek obsahujících osobní údaje, které by mohly ohrozit důstojnost subjektů údajů. Navíc, kdykoli zveřejňují dokumenty nebo pomůcky, které obsahují osobní údaje žijících jednotlivců online, musí podle povahy osobních údajů zvážit, zda by bylo vhodné zveřejnit je v oblasti jejich webů s omezeným přístupem, tedy mimo dosah vyhledávačů.[70]

[69] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 17. Brusel. 2016. Dostupné také z: https://www.privacy-regulation.eu/cs/17.htm.

[70] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-28].

Oznamování oprav nebo výmazu osobních údajů či omezení zpracování

Dle nařízení GDPR správce musí oznámit jakoukoli opravu nebo výmaz osobní údaje nebo omezení o zpracování každému příjemci, ledaže by to bylo nemožné nebo by to vyžadovalo neúměrné úsilí. Vnitrostátní právní předpisy si výjimku z práv na opravu nebo výmaz nebo omezení zpracování mohou do vlastního znění zakomponovat dle svého uvážení. Jedná se pouze o zpracování pro účely archivace ve veřejném zájmu. Je ale málo pravděpodobné, že údaje obsažené v archivních fondech budou předmětem opravy, výmazu či jiného zpracování. [71]

Zpracování zvláštních kategorií osobních údajů

Obecně GDPR zakazuje zpracování údajů, které se týkají rasového či etnického původu, politických názorů či náboženského přesvědčení. I zde jsou povolené odchylky od tohoto ustanovení. Zpracování musí být založeno na právu a musí být přiměřené stanovenému cíli. Musí být respektováno právo na podstatu ochrany údajů a zajistit vhodné opatření na ochranu základních práv a zájmů subjektu údajů.[72]

Ochrana dat

Minimalizace dat je jedním ze základních principů ochrany údajů. Ve skutečnosti Článek 25 GDPR vyžaduje, aby správci prováděli příslušné technické a organizační opatření k zajištění toho, že bude docházet ke zpracování pouze nezbytně nutných údajů. Článek 25 GDPR se vztahuje zejména na vývoj nových informačních systémů. Pro archivy to může znamenat například vytvoření digitálního uložiště, databáze údajů o narození nebo jiných fondech obsahujících osobní informace, informačního systému pro správu služeb badatelny nebo nástrojů pro on-line přístup.

[71] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-29].
[72] Tamtéž

Archivy obchází minimalizaci, když vytvářejí vyhledávací pomůcky. Když uspořádají a popisují archivní fondy, které zahrnují citlivé osobní údaje žijících jednotlivců o zdraví, sexuálním životě, politice názory a jiné, musí být vytvořena vyhledávací pomůcka, která uvádí jména, aby to bylo možné reagovat na možné žádosti o přístup subjektů údajů a dodržovat ostatní údaje práva subjektů. Totéž neplatní pro pomůcky, které jsou online na portálech archivů. Zde musí dojít k pseudonymizaci údajů v pomůcce. Příslušný software v dnešní době umí vytvořit dvě stejné pomůcky, ale jedna je určena pro online vyhledávání, kde jsou jména pseudonymizována. [73]

Bezpečné zpracování

Bezpečnostní princip vyžaduje analýzu rizik a jistá fyzická i technická opatření. Opatření musí zajistit důvěrnost, integritu a dostupnost systémů a služeb a osobních údajů, které jsou v nich zpracovávány. GDPR nedefinuje žádné konkrétní opatření, které by měl správce a zpracovatel provádět. Vyžaduje se pouze „vhodné“ zabezpečení. To by měl zpracovatel a správce posoudit dle řízení rizik.

Za bezpečnost údajů v archivech odpovídají samy archivy. Práce s údaji musí být v souladu s odbornými postupy a chránit integritu a pravost údajů před neoprávněným vstupem, změnami či poničením. Úroveň zabezpečení by měla být přiměřená povaze údajů a škodě, která by mohla vzniknout v důsledku narušení bezpečnosti. Elektronická data by měla být zabezpečena prostředky softwarové ochrany před viry a trojskými koni a autorizovaným přístupem pouze pro oprávněné uživatele. Osobní údaje by měly být přenášeny bezpečně, tedy zašifrovaně pro bezpečný přenos elektronikou cestou. [74]

[73] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-29].
[74] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-29].

Tohoto tématu se rovněž dotýká zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který také upravuje práva, povinnosti, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. [75]

Co by následovalo při porušení bezpečnosti? Porušení by mělo být nahlášeno podle článku 35 GDPR příslušnému dozorovému úřadu a pokud možno do 72 hodin od incidentu. [76]

DPO

Pověřenec po ochranu osobních údajů pomáhá správci se všemi potřebami okolo ochrany údajů. GDPR zavedlo povinnost jmenovat DPO jak pro veřejné orgány, tak pro soukromé subjekty, které provádějí určité druhy zpracovatelské činnosti. To se týká i archivů.

Úředník vykonávající tuto funkci může být zaměstnancem správce nebo externista na základě smlouvy. Podle nařízení může být pověřenec jmenován i pro několik státních orgánů, institucí či firem, které mají podobnou organizační strukturu. [77]

2.3 Národní archiv a GDPR

Národní archiv je instituce, která je pro ostatní archivy určitým vzorem v postupech. NA nemá na svých webových stránkách zveřejněnou přímo metodiku postupu v rámci GDPR, ale vyslovil se k některým situacím. Pro své vlastní potřeby vydává informační dokumenty k určitým tématům souvisejícím s GDPR, které jsou ale volně dohledatelné.

[75] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 29.8.2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181.
[76] EUROPEAN ARCHIVES GROUP, *c. d.* 2018.
[77] EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-29].

K právu být zapomenut se NA staví dle článku 17 GDPR tak, že archiválie uložené v této instituci, jsou z této možnosti vyjmuty a nelze z nich, na základě podnětu subjektu údajů, žádné údaje vyjímat. Trvalé uložení pro archivní účely není v rozporu s GDPR.

Badatel při podávání žádosti poskytuje údaje, které umožní jeho jednoznačnou identifikaci. GDPR neupravuje způsob identifikaci žadatele, proto archiv požaduje standardní informace o badateli. Jedná se o jméno, příjmení, datum narození, adresu místa trvalého pobytu nebo bydliště, případně adresu pro doručování, pokud se liší od adresy trvalého pobytu nebo bydliště.[78]

NA komunikuje na dotazy výhradně datovou schránkou, pokud ji má dotyčná osoba zřízenou nebo prostřednictvím poštovních služeb do vlastních rukou dotyčného.

Národní archiv nezískává osobní údaje, které nebyly získány výhradně od subjektu údajů, pokud se nejedná o přejímání dokumentů vybraných a evidovaných jako archiválie podle zákona č. 499/2004 Sb., o archivnictví a spisové službě. [79]

Národní archiv zveřejnil také dokument, kde jsou uvedené činnosti, při kterých dochází ke zpracování údajů, za jakým účelem, kdo je příjemcem údajů a na jakou dobu jsou údaje uchovány. Celý dokument se nachází v příloze č. 3 diplomové práce.

[78] SBÍRKA INTERNÍCH AKTŮ ŘÍZENÍ ŘEDITELKY NÁRODNÍHO ARCHIVU: *Bulletin pro otázky elektronické spisové služby a dokumentů v digitální podobě.* In: Národní archiv ČR [online]. Praha, 2015, 21. července 2015 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/02/badatelsky-rad-pokyn.pdf.

[79] Národní archiv: *Ochrana osobních údajů/GDPR* [online]. Praha [cit. 2020-07-05]. Dostupné z: https://www.nacr.cz/uredni-deska/ochrana-osobnich-udaju-gdpr.

K zpracování dochází u těchto činností:

- Při poskytování informací podle zákona 106/1996 Sb., o svobodném přístupu k informacím, konkrétně § 14 odst. 2. Účel zpracování podléhá článku 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plněn právních povinností. Údaje získané za tímto účelem jsou poskytovány jen při odvolání odvolacím orgánům – MVČR a soudy. Dle skartačního znaku V10 budou informace po 10 letech ve skartačním řízení posouzeny, zda budou uloženy dále v archivu či doje k jejich zničení (skartaci).

- Při využití wifikonektivity v areálu instituce. Účel zpracování podléhá článku 6 odst. 1 písm. b) GDPR – zpracování nezbytné pro účely splněn smlouvy. Data o připojených zařízeních nejsou zpracovávána ani NA ani jinými osobami. Po uplynutí doby životnosti připojení IP adresy dochází k okamžitému mazání informací.

- Při výkonu spisové služby v eSSL. Účel zpracování podléhá článku 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plněn právních povinností. Stojí na právním základu zákona č. 499/2004 Sb., o archivnictví a spisové službě, konkrétně § 3 odst. 1 a §63-70, dále na vyhlášce č. 259/2012 Sb., o podrobnostech výkonu spisové služby. Získané údaje nejsou poskytovány mimo NA. Centrální podací protokoly (registraturní pomůcky) se stanou archiváliemi po 1 roce a evidenční pomůcky specializovaných spisoven po 5 letech. Podací protokoly jednotlivých oddělení, pomocné knihy (doručovací knihy a zápisníky) a ostatní evidenční pomůcky podlehnou skartaci po 5 letech.

- Při výběru archiválií. Účel zpracování podléhá článku 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plněn právních povinností. Zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě, konkrétně §7-12 a §15, Vyhlášky č. 645/2004 Sb., kterou se provádějí některá

ustanovení zákona o archivnictví a spisové službě a o změně a 259/2012 Sb., o podrobnostech výkonu spisové služby.
Nedochází k předávání dalším osobám, pouze v případě odvolání a kontrolní činnosti MVČR. Protokoly o výběru archiválií se po 10 letech stávají archiválií.

- Při vědeckých činnostech a projektech. Účel zpracování podléhá článku 6 odst. 1 písm. a), b), c) GDPR – zpracování nezbytné pro plnění právní povinnosti, pro splnění smlouvy, případně je udělen souhlas. Zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě, konkrétně § 46 a 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací § 32. Konkrétním příjemcem údajů může být poskytovatel grantu pro výzkum a vývoj – TAČR, GAČR, MVČR a další subjekty. Dokumentace pro dotace na větu a výzkum pro domácí poskytovatele se stává archiválií po jednom roce. Dokumentace ze spoluúčasti na mezinárodních projektech a grantech, grantové projekty, hlášení z výzkumů a vědy a národní digitální výzkum se stávají archiválií po pěti letech. Vědecké úkoly a projekty, které nebyly podpořené dotací budou po pěti letech posouzeny ve skartačním řízení.

- Při smluvních vztazích. Účel zpracování podléhá článku 6 odst. 1 písm. b), c) GDPR – zpracování nezbytné pro plnění právní povinnosti a naplnění smlouvy; ochrana majetku, závazky vyplývající ze smluvního vztahu. Zpracování stojí na následujících zákonech: č. 89/2012 Sb., občanský zákoník, č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), č. 262/2006 Sb., zákoník práce a č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Příjemce údajů je jedna ze

smluvních stran. Může dojít k předložení smluv ke kontrole příslušným orgánům (NKÚ nebo jiný). Smlouvy jsou v registru smluv zveřejňovány anonymizované. Po třech letech dojde k archivaci smluv a dohod o vzájemné výpůjčce archiválií a o výměně publikací. Po pěti letech dojde k archivaci smluv a dohod: o vědecké a odborné spolupráci, o vydání díla, o technické podpoře, o dílo, o zřízení bankovního účtu, o převodu majetku, o zajištění provozu, depozitních smluv, autorských smluv, kupních a darovacích smluv archiválií. Po pěti letech půjdou do skartačního řízení smlouvy a dohody o stravování, mandátní smlouvy, inominátní smlouvy.

- Při vytváření personální agendy. Účel zpracování podléhá článku 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti, vedení informací o zaměstnancích k plnění povinností zaměstnavatele dle zákoníku práce a služebního zákona. Právní základ zpracování stojí na výčtu mnoha zákonů, například se jedná o zákon č. 262/2006 Sb., zákoník práce, zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci a další. Příjemci osobních údajů jsou Ekonomický informační systém (EKIS) a Informační systém o státní službě (ISoSS). Do skartačního řízení po 50 letech půjdou osobní spisy zaměstnanců. Do skartace po roce konkurzy, výběrová řízení a inzeráty. Po třech letech informace o nepřijatých uchazečích. Po pěti letech zápisy o ztrátě služebních průkazů a informace personálních referentů. Po deseti letech kompletní evidence služebních průkazů.

- Při nahlížení do archiválií. Účel zpracování podléhá čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; nahlížení do archiválií badatelem dle zákona č. 499/2004 Sb. Právní základ zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě a vyhlášce č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. Příjemci údajů

mohou být: zaměstnanci organizačních složek státu, ozbrojených sil, bezpečnostních sborů, zpravodajských služeb České republiky a územních samosprávných celků. V archivu zůstane evidence badatelů a badatelských návštěv, badatelské lisy a kniha výpůjček. Do skartace půjdou korespondence se zahraničními i tuzemskými badateli a institucemi.

- Při knihovnické činnosti. Účel zpracování podléhá čl. 6 odst. 1 písm. a), b), c) GDPR – zpracování na základě souhlasu, nezbytné pro splnění smlouvy, nezbytné pro plnění právní povinnosti. Právní základ zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě, zákonu č. 257/2001 Sb., knihovní zákon, vyhlášce č. 88/2002 Sb., prováděcí vyhláška ke knihovnímu zákonu, zákonu č. 89/2012 Sb., občanský zákoník (smlouva o výpůjčce). Údaje čtenářů nejsou poskytovány mimo Národní archiv. Z pozice administrátora RIV NA předává údaje o autorech vědeckých výsledků poskytovatelům dotace. Do souboru Národních autorit jsou poskytovány údaje na základě souhlasu subjektu údajů. Po ukončení souhlasu s vedením osobních údajů čtenářem a po zhodnocení, zda nemá čtenář vůči knihovně nesplněné závazky, jsou všechny dokumenty s osobními údaji navrženy po uplynutí skartační lhůty do skartačního řízení, zároveň je ukončena registrace čtenáře v elektronickém systému (údaje jsou vymazány).

- Při evidenci původců. Účel zpracování podléhá 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti a evidence původců je vedená archivem dle zákona č. 499/2004 Sb. a vyhlášky č. 645/2004 Sb., které jsou zároveň i právním základem pro zpracování. Přístup k údajům má MVČR a vlastník archiválie. V archivu zůstávají spisy o archivním souboru a dokumentace o původci, evidence AKP a NKP, kontroly fyzického stavu AKP a NKP uložených v NA, knihy kontrol, kniha přírůstku a úbytku, spis o vnější změně po provedení skartačního řízení.

- Při evidenci archiválií. Účel zpracování podléhá čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti a evidence původců je vedená archivem dle zákona č. 499/2004 Sb. a vyhlášky č. 645/2004 Sb., které jsou zároveň i právním základem pro zpracování. Přístup k údajům má MVČR a vlastník archiválie. V archivu zůstávají spisy o archivním souboru, spisy o vnitřní změně, evidence AKP A NKP, knihy kontrol, kontroly fyzického stavu AKP a NKP. Do skartačního řízení půjdou po pěti letech návrhy na prohlášení za AKP nebo NKP a UNESCO.

- Při vlastnictví archiválií. Účel zpracování podléhá čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti. Právní základ zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě a vyhlášce č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. Příjemcem je pouze MVČR. V archivu zůstanou knihy kontrol, kontroly fyzického stavu AKP a NKP uložených mimo archivy a kulturně vědecké instituce.

- Při užívání eLearningového vzdělávacího systému MOODLE. Účel zpracování podléhá čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti. Právní základ zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě. Údaje nejsou poskytovány třetím stranám, pouze subjektu údajů a jsou vedeny pouze po dobu účasti na vzdělávání.

- Při správě archivního portálu. Účel zpracování podléhá článku 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti. Právní základ zpracování stojí na zákonu č. 499/2004 Sb., o archivnictví a spisové službě. Údaje nejsou poskytovány třetím stranám, pouze

příslušnému veřejnému archivu. Údaje jsou vedeny trvale dle článku 17 písm. 3 písm. d) GDPR.[80]

Jak uvádí Mgr. Šimůnková, povinnost řádného vyřazování dokumentů ve skartačním nebo mimo skartační řízení, která je adresována původcům dle § 3 zákona č. 499/2004 Sb., není GDPR dotčena. Jak NA, tak i ostatní archivy dle zákona č. 499/2004 Sb. je oprávněn ukládat trvale archiválie, včetně archiválií obsahujících osobní údaje žijících osob, což vyplývá z článku 17 a článku 89 GDPR.[81]

2.4 Souhrn

Závěrem této kapitoly vyplývá, že ani MVČR nebo NA nezhotovily tak obsáhlou metodiku výhradně pro postup ochrany osobních údajů v archivnictví. NA alespoň zhotovil praktiky přehled činností, při kterých dochází ke zpracování osobních údajů, na jakém právním základu stojí a jak dlouho zůstávají informace o údajích v instituci, případně, co se s nimi poté děje a samozřejmě, kdo je příjemcem těchto informací.

Metodiku EAG, která je celá sepsaná by stačilo pouze přeložit a uvést do kontextu s českým zněním GDPR. Pokud lze dokument NA o GDPR považovat za metodiku, lze zde vidět snahu o přehlednost a jednoduchou informovanost, což by bylo naprosto dostačující. Nicméně se zmiňovaný dokument týká skutečně hlavně NA a nelze ji takto vztáhnout na ostatní archivy bez úprav.

[80] Národní archiv: *Ochrana osobních údajů/GDPR* [online]. Praha [cit. 2020-07-05]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2020/04/GDPR_priloha.pdf.
[81] ŠIMŮNKOVÁ, *Karolína. GDPR – spisová služba a původci v předarchivní péči Národního archivu* [online]. Národní archiv, 2017, 22.11.2017 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/GDPR_sylabus.pdf.

Na stránkách MVČR se v metodikách těžko orientuje. Část metodických pokynů odkud některé archivy také čerpaly, která je obsažená v metodice pro obce, by se se daly obecně též vztáhnout i na archivy. Navíc metodický pokyn upravuje problematiku GDPR pouze badatelským listem, ale už se dále nezabývá dalšími oblastmi, kam GDPR zasahuje.

Všechny uvedené metodické pokyny a dokumenty jsou obsažené v příloze této diplomové práce.

3 Jak GDPR ovlivnilo české archivnictví

GDPR se archivnictví dotýká hlavně článkem 89 Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Nařízení ve svém znění počítá s možnostmi odchýlení se od jeho znění, jenž zmiňuje odst. 52 v úvodním znění.[82]

Největší vliv má GDPR na předkládání archiválií badatelům. Správně by archivy měli postupovat tak, že zjistí přítomnost údajů žijících občanů v daném materiálu a ten podstoupí pseudonymizací. Archivy postupují tak, že vytvoří kopii dokumentu a v ní začerní osobní údaje manuálně. Další možností je předkládat digitalizovaný dokument, který byl upraviten do takového stavu, jenž může být badateli předložen. S tím úzce souvisí prodloužení čekací lhůty na vydání archiválie, kterou pak badatel dostane v upravené formě. Některé archivy také pořizují více kopií a ty následně ukládají. Což nese další komplikace, kdy už v současnosti mají archivy nedostatek místa pro uložení standartních archiválií, natož uchovávat kopie.[83]

Pokud by archivy řešily anonymizaci osobních údajů pouze v digitální rovině, bylo by to jisté řešení, nicméně archivy se mnohdy potýkají i s nedostačující kapacitou digitálního uložiště dat. Archivy na okresní a nižší úrovni mají mnohdy problém jak se zastaralým hardware, tak software či nemají dostupné zařízení v badatelně, kde by mohly být archiválie předloženy.

[82] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: (52) Úvodní znění. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.

[83] ČTVRTNÍK, Mikuláš. Právo být (ne)zapomenut: inflace soukromí, vy(zne)užívání dat a prekérní situace archivů v mladém 21. století – podněty к diskusi. Archivní časopis. Praha. Ministerstvo vnitra České republiky – Sekce archivní správy, 1951-, 2018(68). ISSN 0004-0393.

Pokud by se archiváři skutečně pokusili o pseudonymizaci veškerých archiválií, nezbyl by jim čas na vyřizování dalších činností spojených s jejich prací. Archiváři ve Státním oblastním archivu v Praze se pokusili spočítat, jaký čas by v průměru zabralo jednomu člověku takto zpracovat jeden karton archiválií a dostali se k číslu 17,9 hodiny/1 karton. Časovou náročnost testovali na dvou kartonech – jeden obsahoval fond Krajský výbor KSČ a druhý fond Mimořádný lidový soud Praha. Nutno podotknout, že v tomto čase není obsaženo dotazování v Informačním systému evidence obyvatel, zda jsou občané stále ještě na živu. [84]

Minimalizace údajů žijících občanů je tedy mnohdy za hranicemi možností archivářů. Článek 89 odst. 1 GDPR říká, že: „*opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely*.“[85] Časem by toto mohlo znamenat, že se badatelé k archiváliím nedostanou vůbec, protože archiváři budou zahlceni činností pseudonymizace natolik, že jednotlivé archivy nebudou předkládat takovéto archiválie vůbec.

V rámci GDPR jsou zpřísněny požadavky na souhlas (např. čl. 4 odst. 11; čl. 6 odst. 1 písm. a); čl. 7). Specifický souhlas „*pro jeden nebo více konkrétních účelů*“ (čl. 6 odst. 1 písm. a), by mohl představovat výzvu pro výzkum, protože „*často není možné plně určit účel zpracování osobních údajů pro vědecký výzkum. v době sběru údajů*“. Bod 33 úvodního ustanovení uvádí možnost subjektům údajů „*udělit souhlas některým oblastem vědeckého výzkumu, pokud jsou v souladu s uznávanými etickými normami pro vědecký výzkum. Subjekty údajů by měly mít možnost udělit souhlas pouze určitým oblastem výzkumu nebo částem výzkumných projektů v rozsahu povoleném zamýšleným účelem*.“[86]

[84] ČTVRTNÍK, Mikuláš. Právo být (ne)zapomenut: inflace soukromí, vy(zne)užívání dat a prekérní situace archivů v mladém 21. století – podněty к diskusi. Archivní časopis. Praha. Ministerstvo vnitra České republiky – Sekce archivní správy, 1951-, 2018(68). ISSN 0004-0393.

[85] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě*. Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

[86] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.

Alternativním důvodem pro zpracování je legitimní zájem správce (čl. 6 odst. 1 písm. f)). Správce může zpracovávat osobní údaje „*za účelem svých oprávněných zájmů, s výjimkou případů, kdy jsou tyto zájmy potlačeny zájmy nebo základními právy a svobodami subjektu údajů*“. Výzkum sice není v textu výslovně uveden jako legitimní zájem, ale již podle směrnice 95/46 pracovní skupina zřízená podle článku 29 GDPR představila výzkum (včetně marketingového výzkumu) jako kontext, ve kterém může vyvstat otázka oprávněného zájmu. Platné použití tohoto důvodu bylo omezeno na konkrétní okolnosti, kdy správce zavádí vhodná ochranná opatření.[87]

GDPR se dotýká i spisové služby hlavně v její elektronické podobě. 4. 7. 2017 byl zveřejněn nový standard pro eSSL, který přinesl jeho zjednodušení, upřesňuje fázi „vzniku“ dokumentu a pojem rozpracovaný dokument neboli koncept. Dále také porovnává rozhraní mezi systémy eSSL a ostatními informačními systémy, a to hlavně u on-line a off-line propojení. Změna standardu dala vzniknout novému datovému modelu metadat dokumentů spisové služby. Nicméně je nutné podoktnout, že řada organizací státní správy stále nemá dlouhodobě IT systémy v souladu s národním standardem pro spisové služby.
S rozvojem elektronických služeb se změní životní cyklus dokumentů a dojde k nárustu e-dokumentů. [88]

Rozvoj v oblasti e-dokumentů legislativně souvisí jak s eIDAS, tak s GDPR. Přibude množství zpracování osobních údajů a s tím souvisí i hrozby v podobě zneužití e-dokumentu, osobních údajů nebo identity. Na tuto oblast je třeba se více zaměřit metodicky a je potřeba, aby to mělo dopad i na oblast vzdělání. Je třeba, aby došlo k většímu využití privacy by design, tedy založit přístup na předem

[87] BERTELS, Natalie. *Scientific research under the GDPR: what will change*? [online]. 2016 [cit. 2020-03-20]. Dostupné z: https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/.
[88] PIFFL, Robert. Dopady GDPR na informační systémy a evidenci elektronických dokumentů. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.

definovaném riziku, anonymizaci, šifrováním a dalšími metodami vedoucí k ochraně dat.[89]

GDPR má rovněž dopad na oblast IT. Architektura IT řešení by měla kromě architektonických postupů a shodou s NAP obsahovat s ohledem na GDPR zejména pak principy Privacy by design, který se ochranou zabývá už od návrhu. Jedná se o prevenci, protože je to trvalý dlouhodobý proces, nikoli jednorázová pomoc. Je zde snaha o minimální množství dat, plnou funkčnost, bezpečnost a transparentnost celého systému.

Aby došlo k souladu s cíli GDPR, je nutné zrevidovat veškeré smlouvy se zpracovateli dat, a to jak těch zákaznických (případně badatelských), tak zaměstnaneckých. Pokud se jedná o smlouvy dodavatele IT systémů, je zde nutnost uvést i povinnost odpovědnosti za případnou škodu a musí být stanoveny dostatečné záruky na zavedení vhodných podmínek. Například při nároku na výmaz dat by nemělo dojít k obnově dat nebo IT systém by měl být takový, aby se při nutnosti přenosu dat nemusela data ona přenášet ručně.[90]

[89] PIFFL, Robert. Dopady GDPR na informační systémy a evidenci elektronických dokumentů. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.
[90] Tamtéž.

3.1 Další právní nástroje ochrany osobních údajů v archivnictví

GDPR je jedno z nejsledovanějších a nejvýraznějších legislativních opatření v celé EU, ale ochrana osobních údajů měla své místo i na poli české legislativy už před příchodem samotného nařízení. V českém prostředí toto (do příchodu GDPR) zastřešoval zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl k 24. 4. 2019 zrušen a nahrazen novým takzvaným adaptačním zákonem. V této kapitole budou nastíněny české legislativní opatření a způsob, jaký mají dopad na vztah ochrany osobních údajů k archivnictví.

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

Adaptační zákon nabyl právní účinnosti ve stejný den, kdy došlo ke zrušení předešlého zákona č. 101/2000 Sb., tedy 24. 4. 2019. Jeho hlavní rámec je Evropské nařízení o ochraně osobních údajů. Asi nejzásadnější změnu, kterou adaptační zákon přinesl, se týká nulových sankcí za porušení GDPR pro orgány veřejné moci a veřejné subjekty. To nemění nic na tom, že dozorový úřad může nařídit nápravná opatření například i provedení náprav, což může mít daleko větší finanční a časový dopad pro danou instituci než jednorázová pokuta.[91] Tato problematika je též popsána v kapitole *1.6 Postihy a tresty za porušení GDPR*.

Další podstatnou změnou je § 8, který se týká informační povinnosti. Ten říká, že správce může tuto povinnost naplnit i tím, že potřebné informace zveřejnění dálkovým přístupem. Tato změna je užitečná z praktického důvodu, protože veřejná dostupnost stručných, srozumitelných a transparentních informací o zpracování je dostatečnou zárukou informovanosti subjektu údajů. K informační povinnosti se váže i § 9, který se týká oznamovací povinnosti ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování.[92]

[91] ŠKORNIČKOVÁ, Eva. *Adaptační legislativa byla schválena* [online]. Praha, 2019, 5. 5. 2019 [cit. 2020-07-22]. Dostupné z: https://www.gdpr.cz/blog/adaptacni-legislativa-byla-schvalena/.
[92] MUNIS.CZ. *Zákon o zpracování osobních údajů a spisová služba* [online]. Praha, © 2020 [cit. 2020-07-22]. Dostupné z: https://www.munis.cz/art/654.

Jako další specifikum rozšiřuje problematiku pověřence na ochranu osobních údajů. V § 14 jmenuje další orgány s povinností jmenovat DPO. Jedná se o orgány, zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu. Jedná se zejména o Českou národní banku, Nejvyšší kontrolní úřad, dále i exekutory, notáře, veřejného ochránce práv a další. [93]

Zákon č. 110/2019 Sb., je doprovázen dalším zákonem č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. Tento předpis měl dopad na 39 dalších zákonů včetně většiny hlavních procesních předpisů jako je trestní řád, občanský soudní řád, soudní správní řád a daňový řád.[94]

Zákon č. 499/2004 Sb., o archivnictví a spisové službě

Ochrany údajů se dotýká i archivní zákon. Zde se nástroje ochrany osobních údajů nachází v § 37, který jasně uvádí, že archiválie jsou přístupné pouze starší třiceti let. Do archiválií obsahující osobní údaje lze nahlížet pouze se svolením osoby, ke které se údaje vztahují. Tázaná osoba má třicet dní na podání námitky proti nahlížení, a pokud takto neučiní, míní se tím její souhlas. Žádost je doručována veřejnou vyhláškou vyvěšenou na úřední desce daného archivu. Nezřizuje-li archiv úřední desku, bude vyhláška vyvěšena na úřední desce SOA, v jehož obvodu má archiv sídlo. [95]

Už před příchodem GDPR archivy zpracovávaly osobní údaje badatelů, a to prostřednictvím badatelského listu, který jsou badatelé povinni vyplnit před nahlížením do archiválií. Je to primárně z důvodu ochrany archiválií.

[93] ČESKO. § 14 zákona č. 110/2019 Sb., o zpracování osobních údajů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 22. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110#p14.
[94] MUNIS.CZ. *c. d* .© 2020.
[95] ČESKO. § 37 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 22. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499#p37.

V oblasti spisové služby se o největší změnu jedná v zavedení povinného vedení jmenného rejstříku pro všechny určené původce, kteří musí, nebo si dobrovolně vybrali vedení spisové služby v elektronické podobě eSSL.
Jmenný rejstřík musí obsahovat následující údaje:

- Jméno a příjmení (v případě FO i PO)
- Dodatek odlišující osobu podnikatele nebo druh podnikání (pokud jde o PO)
- Název obchodní firmy (pokud jde o podnikající FO)
- identifikační číslo osobo (pokud je)
- identifikátor datové schránky
- bezvýznamový identifikátor pro potřeby výkonu spisové služby, pokud byl určeným původcem přidělen. [96]

Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů

Ve své podstatě se vyhláška zaměřuje na evidenci Národního archivního dědictví. Problematika se snaží zohlednit i kauzu, která se týkala archivního zákona v ohledu na zpřístupňování a zveřejňování archiválií bezpečnostních složek totalitních režimů. § 37 odst. 11 byl řešen u ústavního soudu kvůli posouzení ústavnosti, zda nahlížení do archiválií obsahující osobní údaje může být vyjmuto z ochrany osobních údajů tímto ustanovením. Vyhláška v reakci na tuto kauzu uvádí, že zpřístupňování archiválií složek minulých totalitních režimů je v pořádku, ale jejich zveřejňování musí respektovat ochranu osobních údajů a osobnostní práva.[97] Tato záležitost byla do patřičné míry probírána i na konferenci Osobní údaje v archivnictví, kterou pořádala České archivní společnosti v Plzni.

[96] MUNIS.CZ. *c. d* .© 2020.
[97] ČESKÁ ARCHIVNÍ SPOLEČNOST: *GDPR a obecné trendy a překážky v akvizici a zpřístupňování archiválií s osobními údaji.* In: Osobní údaje v archivnictví [online]. Plzeň, 23. 4. 2019 [cit. 23. 7. 2020]. Dostupné z: https://www.youtube.com/watch?v=BPAarJgAN-4.

Vyhláška stanovuje v § 12a odst. 1 písm. i), že už v základní identifikaci archiválie musí být údaj o tom, že se v archiválii nachází osobní údaje nebo tajemství obchodního či bankovního typu. Na tyto archiválie se vztahuje zvláštní režim ochrany.[98]

3.2 Kroniky v současnosti

Slovo kronika pochází z latiny *chronica, chronico*, podle původně řeckého *chronos*, znamenající čas a chronika ve významu věci časové. V raném středověku se lze setkat s označením *acta (series, sum) temporum*. Tento termín byl hojně používán, a kromě kroniky označoval jiné narativní texty. Ve středověku docházelo k žánrovému prolínání kronik s historií a anály. Tato nesourodost pak vyústila v řadu kronik pod názvem historie či anály, resp. letopisy.[99]

Kroniky jsou jedním z nejdůležitějších narativních historiografických pramenů. Legislativně jsou upravovány zákonem č. 132/2006 Sb., o kronikách obcí. Do kronik obce se zaznamenávají zprávy o důležitých událostech obce, které nesou informace a poučení pro budoucí generace.

Kroniky musí nést určité prvky:

- Papír musí splňovat normu ČSN ISO 9706 vyhlášky č. 646/2004 Sb., § 5,
- Jedna kronika má obvykle 400 listů.
- Rozměry 30 x 38 cm.
- Celokožená nebo polokožená vazba s nápisem Kronika na předních deskách
- Uložená v pouzdře chránícím před prachem, znečištěním a otěrem.
- Psána výhradně dokumentárním inkoustem.

[98] ČESKO. § 12a odst. 1 písm. i) vyhlášky č. 645/2004 Sb., vyhláška, kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 23. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-645#p12a-1-i.
[99] Slovník literární teorie. Edited by Štěpán Vlašín. Praha: Československý spisovatel, 1984. 465 s.

- Musí nést určité grafické prvky – názvy hlavních kapitol přes celou šířku stránky, hesla pro rychlou orientaci na levém / pravém okraji, číslování stran, zvýrazněná podstatná hesla v textu.
- Nelze používat techniky, které poškozují papír jako vlepování fotografií či jiných dokumentů.
- Musí obsahovat rejstřík. [100]

Podle zákona o kronikách obcí může být kronika psána ručně s číslováním nebo elektronicky a následně tisknuta. Její součástí jsou i přílohy, které obsahují fotografie a další doplňující záznamy. Pro elektronickou kroniku a její přílohy mohou být použity tři datové formáty podle norem ISO 19005-1 a ISO/IEC 15948. PDF/A-1a je určen pro textové, obrazové a kombinované dokumenty. PNG a TIFF pro obrazové dokumenty.

Vytištěná kronika musí nést stejné prvky, pouze se liší v těchto bodech:

- Standartní formát listů A4 nebo A3.
- Tisk musí mít kvalitu nejméně 150 DPI (bodů na jeden palec).
- Nesmí se ukládat do umělých obalů a vazeb.[101]

Zákon nedefinuje přesnou strukturu obecních kronik, ale rozvoj publicistiky v této oblasti je velmi nápomocen pro začínající kronikáře. Literatura a dostupné zdroje se shodují na těchto kapitolách:

1) Titulní list – název obce, časové vymezení, úřední razítko a podpis starosty
2) Úvod – usnesení o vedení kroniky a kolik svazků předchází, kde se nachází a jaký časový úsek pojímají
3) Stručný životopis kronikáře

[100] DUŠEK, Radim. Vedení kronik: Obecní kronika. Východočeské archivy [online]. [cit. 2020-07-23]. Dostupné z: https://vychodoceskearchivy.cz/ustinadorlici/vedeni-kronik/.
[101] HROMÁDKA, Tomáš. *Kroniky obcí* [online]. Praha, 2014, 62 [cit. 2020-07-25]. ISBN 978-80-7068-280-7. Dostupné z: https://invenio.nusl.cz/record/358316/files/nusl-358316_1.pdf.

4) Popis obce – poloha, popis vzhledu, historie, znak, prapor, obyvatelstvo, veřejná správa, hospodářství obce, školství, kultura a zdravotní zařízení obce
5) Roční zápisy – počasí, obyvatelstvo, rozpočet, stavby, kultura, školství, zdravotní zařízení a další obecní záležitosti a informace, dle toho, co kronikář uzná za podstatné.[102]

Obec je povinna zabezpečit kroniku proti ztrátě a odcizení. Současně i určuje její obsah a četnost zápisu. Zápis do kroniky musí být vykonán alespoň jedenkrát ročně. Do kroniky může nahlédnout každý na obecním úřadě pod dohledem kronikáře. Každý občan starší 18 let může navrhnout změnu, úpravu nebo doplnění kroniky.[103]

Text kroniky obce nepodléhá autorskému zákonu č. 121/2000 Sb., ale řídí se podle něj nakládání s autorskými díly, které byly použity např. k jako ilustrativní nebo vloženy jako příloha. [104]

[102] HROMÁDKA, Tomáš. *Kroniky obcí* [online]. Praha, 2014, 62 [cit. 2020-07-25]. ISBN 978-80-7068-280-7. Dostupné z: https://invenio.nusl.cz/record/358316/files/nusl-358316_1.pdf.

[103] ČESKO. Zákon č. 132/2006 Sb., o kronikách obcí. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 23. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-132#p1.

[104] Metodický pokyn č. 1/2020 k archivnímu zpracování fondů typu „Archiv města" [online]. Praha: MVČR, 2020 [cit. 23. 7. 2020]. Dostupné také z: https://www.mvcr.cz/soubor/metodicky-pokyn-c-1-2020-k-archivnimu-zpracovani-fondu-typu-archiv-mesta.aspx.

3.3 Vedení kronik v souladu s GDPR a jejich ukládání v archivu

Pokud se něco bude po implementaci nařízení muset změnit, tak je to způsob vedení kroniky, které je v České republice povinné dle zákona 132/2006, o kronikách obcí. GDPR vedení kronik přímo nezmiňuje v žádném ze svých článků, ale i u nich musí dojít ke splnění zásad GDPR.

Článek 85 GDPR *Zpracování a svoboda projevu informací* přímo zmiňuje pouze novinářské, umělecké, akademické a literární účely. Členské státy si dle znění článku 85 GDPR uvedou „*nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu*.“A také si stanoví odchylky a výjimky. Při vážení práva na svobodu projevu a práva na ochranu osobních údajů se bere v potaz veřejný zájem.[105] Vyvstává tak otázka, co vše může a nemůže být v kronice uvedeno.

V souladu s GDPR a zákonem č. 110/2019 Sb,. zápis v kronice nesmí zasahovat do soukromého života uváděných osob. Kronika nesmí obsahovat soupis místních občanů, který nese některý z atributů jako jméno, příjmení, adresa a datum narození. Totéž platí pro soupisy narozených, úmrtí, sňatky a dále vlastníků nemovitostí s uvedeným číslem popisným dané nemovitosti. Kronika obsahující soupisy výše uvedené musí též obsahovat souhlas těchto osob se zpracováním v kronice. Souhlas musí být udělen i ke zpřístupnění, zveřejnění, pořízení výpisů a kopií. Kronika může být totiž zveřejněna i na webu příslušené obce. [106]

[105] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 85 Zpracování a svoboda projevu informací. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.

[106] HROMÁDKA, Tomáš. *Kroniky obcí* [online]. Praha, 2014, 62 [cit. 2020-07-25]. ISBN 978-80-7068-280-7. Dostupné z: https://invenio.nusl.cz/record/358316/files/nusl-358316_1.pdf.

Na druhou stranu, kronika může obsahovat soupis narozených dětí v témž roce, ovšem bez konkrétní adresy a datum může být uvedeno pouze se souhlasem zákonných zástupců. Rovněž může obsahovat soupis občanů, zastupitelů obce a členů rady, výborů a komisí opět se souhlasem subjektu údajů.[107] Jelikož se GDPR nevztahuje na osobní údaje zemřelých, lze zveřejnit i úmrtí. [108]

Článek 89 GDPR se zaměřuje výhradně na zpracování pro archivní, vědecké, statistické a historické účely. Zpracování pro tyto účely podléhají zárukám práv a svobod subjektu údajů a také musí dojít k technickým a organizačním opatřením, které vedou k minimalizaci údajů. Zde se zákon dále vyjadřuje o podmínce pseudonymizace a současně o splnění daných účelů. Což pro kronikáře také není řešení. Rovněž je v nařízení stanoveno, že si členský stát stanoví odchylky.[109]
S jistotou lze říct, že se kronikářství dotýká obou těchto článků, ale plně se nezačleňuje ani do jednoho z nich. Kroniky jsou výsledkem jak získávání informací o životě občanů, tak o jejich statistickém zpracování pro budoucí účely.

Uložení kroniky do archivu

Jelikož jsou kroniky považovány za dokumenty, které budou podle obsahu vždy předkládány k výběru za archiválie, zařazují se do I. kategorie výběru ve skartačním řízení. Ten je prováděn příslušným státním archivem. Kroniky mají stanovený skartační znak „A“ a skartační lhůtu 10 let od uzavření svazku, tedy po této době se kronika stane archiválií. [110]

[107] Tamtéž.
[108] ÚOOÚ. *Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů*. In: Ministerstvo vnitra České republiky [online]. Praha, ©2019 [cit. 2020-07-26]. Dostupné z: http://www.mvcr.cz/gdpr/soubor/gdpr-sesit-pdf.aspx
[109] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 89 Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.
[110] HROMÁDKA, Tomáš. *c. d. 2014*.

Kroniky jsou předávány do archivů po vzájemné dohodě. V praxi se nachází i oponenti této skutečnosti, že kronika je ukládána v archivu. Archivy se tak snaží vyjít vstříc i těmto oponentům a nabízí pořízení duplikátu v případě ručně psané kroniky, která by obci zůstala. Výhodou je vedení v elektronické podobě, kdy obec má kroniku stále k dispozici v její digitální podobě. [111]

Pro to, aby byly kroniky řádně chráněny i v archivu, probíhá jejich digitalizace. Výhodou tohoto procesu je v první řadě vyhnutí se fyzickému namáhání knihy a v neposlední řadě možnost zpřístupnění digitální kroniky pro vzdálený přístup. Před tím, než se digitalizáty dostanou na portál digitálního archivu, prochází kontrolou, která zahrnuje například číslováním listů a každý snímek je popsán metadaty ve formátu XML. Některé archivy přidávají na snímky i své vodoznaky. Digitální kroniky jsou umisťovány na externí datové uložiště – servery.[112]

3.4 Problematika zpřístupnění kronik na webu

Svaz měst a obcí se věnoval nejen zpřístupňování obecních kronik na webu dané obce, která kroniku provozuje. Zaměřil se na zveřejňování článků s uvedením jmen občanů v místním tisku či zveřejňování fotografií v lokálních médiích na základě výjimky z GDPR novinářské licence dle §84 a Občanského zákoníku. Se stanovisky ÚOOÚ seznamují v oficiálních dopisech, které jsou zveřejněné na jejich webových stránkách.[113]

Podle Úřadu podmínky pro zpřístupňování kroniky stanoví zákon o kronikách obcí v § 4 jako nahlížení: "*Do kroniky může každý nahlédnout ve vymezené době na obecním úřadě; pokud je nahlížení umožněno do kroniky ručně psané nebo do*

[111] DUŠEK, Radim. Vedení kronik: Obecní kronika. Východočeské archivy [online]. [cit. 2020-07-23]. Dostupné z: https://vychodoceskearchivy.cz/ustinadorlici/vedeni-kronik/.
[112] Pokyn ředitele SOA v Zámrsku ze dne 25. srpna 2010 č. 1/2010, Digitalizace archiválií, archivních pomůcek a vybraných dokumentů. [cit. 2020-07-23].
[113] Svaz měst a obcí České Republiky [online]. Praha, ©2019 [cit. 2019-11-12]. Dostupné z: https://www.smocr.cz/cs/cinnost/gdpr/a/vedeni-obecnich-kronik-v-souladu-s-pravidly-gdpr.

kroniky v podobě tištěné vázané papírové knihy s číslovanými listy, děje se tak pod dohledem kronikáře. V případě zveřejňování obecních kronik na internetu to znamená, že nemohou být, bez souhlasu žijících občanů, který by ovšem bylo obtížné získat, zveřejňovány výše uvedené soupisy místních občanů, jestliže je starší kroniky obsahují. Neznamená to však, že by musela být anonymizována všechna jména osob zapsaná do kroniky, jestliže jsou přiměřeně použita jako jména účastníků pamětihodných událostí obce či města a netýkají se soukromého života těchto (žijících) osob".[114]

To by v praxi znamenalo, že pokud již byla kronika převezena do archivu, muselo by dojít ke kontrole údajů archivářem či kronikářem, který by ještě musel být i při nahlížení přítomen. Po kontrole by museli být kontaktováni žijící občané a ti by museli vydat souhlas s nahlédnutím.
Zde článek 89 odst. 2 GDPR hovoří, že: „*členský stát EU může stanovit odchylku od práv, aby neznemožnila či neohrozila splnění účelů, které jsou nezbytné*." Ale není už specifikováno, jaký účel lze považovat za nezbytný.[115]

Zákon o kronikách obcí umožňuje vedení kroniky i v elektronické podobě, ale už nijak neformuluje její možnost zveřejňování na webových stránkách obce. Ministerstvo vnitra sestavilo doplňující informace z často kladených dotazů. Jeden z nich se týkal právě zveřejňování kronik na webu. „*Jestliže za aktéry důležitých a pamětihodných událostí považujeme především lidi, neobejde se kronika bez informací o lidech, kteří v kronikářově době žijí a konkrétně jednají. Je ovšem nutné mít na paměti, že kronika má sloužit pro informaci a poučení budoucím generacím, jde tedy o historický pramen, nikoli o „společenskou kroniku. Pokud jde o zveřejnění kroniky na internetových stránkách obce, je nutné zdůraznit, že*

[114] HEJLÍK, Ladislav. Stanovisko Úřadu pro ochranu osobních údajů. Praha, 2018. Dostupné také z: http://www.smocr.cz/getFile.aspx?itemID=967832.
[115] PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě*. Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

zákon obci zveřejňování kroniky na internetu neukládá. Na zpracování osobních údajů v kronice jejich zveřejněním na internetu tedy nelze použít důvod plnění právní povinnosti podle čl. 6 odst. 1 písm. c) obecného nařízení. Zveřejnění by bylo možné považovat za zpracování prováděné ve veřejném zájmu nebo pro účely oprávněných zájmů obce (prezentace obce navenek), zásada přiměřenosti zde však bude velet k anonymizování osobních údajů.
V případě zveřejňování obecních kronik na internetu v zásadě nemusejí být anonymizována toliko jména osob, která jsou přiměřeně použita jako jména účastníků pamětihodných událostí obce a netýkají se soukromého života těchto osob. "[116]

Z tohoto citovaného úryvku by eventuelně mohlo vyplynout, že kronikář může používat osobní údaje pro účely kroniky, ty by se pak ale neměly nikde objevit, dokud nebudou považovány za historický pramen. Rovněž také úryvek neodpovídá na položený dotaz ohledně zveřejňování na webu. Zveřejňování je ale možné, pokud je provedeno ve veřejném zájmu či ve prospěch zájmů obce ovšem s anonymizovanými údaji.

To, že ÚOOÚ zmiňuje skutečnost, že se kroniky na webových stránkách vůbec objevit nemusí neřeší obecnou problematiku online zveřejňování. Kroniky nemusí být zveřejňovány přímo obcemi, ale SOA, protože ty je hojně v digitalizaci upřednostňují z důvodů jejich historické významnosti. V rámci badatelské činnosti jsou kroniky nejčastěji předkládanými archiváliemi, a prostřednictvím digitalizace dochází k předcházení jejich možnému poškození stejně jako u jiných hojně využívaných archiválií badateli.
Některá opatření, které archivy pro dodržení GDPR uskutečnily, znepokojily nejednoho badatele či historika. Kroniky totiž sloužily jako podstatné materiály

[116] Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů. In: Ministerstvo vnitra České republiky [online]. Praha, ©2019 [cit. 2019-11-10]. Dostupné z: http://www.mvcr.cz/gdpr/soubor/gdpr-sesit-pdf.aspx

pro výzkum či pro psaní odborných či publicistických článků a zrušení jejich zveřejnění v digitálních archivech tuto činnost značně zkomplikovalo. Podle právníků jsou však tato opatření naprosto úměrná vzniklé právní situaci. Pokud se tedy archiv snaží dohledat informace, zda osoba uvedená v kronice stále žije, je pravděpodobné, že se určitá část kronik navrátí na portály digitálních archivů.[117]

Otázkou zůstává, jak dlouho tato činnost potrvá a zda není vhodné uvažovat o jiném řešení. Případně vytvoření takového opatření/doporučení již při tvorbě samotné kroniky a zakomponování do legislativy vztahující se ke kronikám. Cílem by tak bylo, že by již archivy následně nemusely řešit, zda mohou kroniku zveřejnit, případně složitě zjišťovat jaké subjekty musí vyzvat k udělení souhlasu, aby kronika mohla být zveřejněna v rámci digitálního archivu či jinak zpřístupněna badateli.

3.5 Problematika archivních materiálů v postoji k GDPR

Archivy mají kilometry materiálů v podobě matrik, kronik a dalších typů archiválií, ve kterých stále mohou figurovat žijící osoby. Pamětní zápisy vedou města již po mnoho století. V roce 1920 byla uložena samosprávným obcím povinnost vést obecní knihu, později úlohu kronik v České republice stanovil zákon o kronikách z roku 2006, podle kterého je povinna vést kroniku každá obec. Zákon sice neukládá četnost zápisů, nicméně obce nemohou přestat s vedením kronik.

Obecně společnost vnímá, že archiválie jsou podstatným zdrojem informací, které jsou využity pro různé účely. GDPR pohlíží na zpracování osobních údajů z jiného úhlu pohledu v případě novinářské a publikační činnosti a pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro

[117] KRUPKA, Jaroslav. *Zmatky kolem GDPR: archívy skrývají kroniky, májové slavnosti doplňují výzvy*. Dotyk.cz [online]. 2018, č. 149 (29.05.2018) [cit. 2020-01-16]. Dostupné z: https://www.dotyk.cz/publicistika/zmatky-kolem-gdpr-archivy-skryvaji-kroniky-majove-slavnosti-doplnuji-vyzvy-20180529.html.

statistické účely. V roce 2019 byly přijaty výjimky pro média, které se týkají minimalizování informování, což v praxi znamená, že publicista se například na demonstraci nemusí žádat každého o souhlas se zveřejněním fotografie či nemusí žádat osobu o publikování jeho postojů a názorů. [118]

Bylo by zajímavé sledovat praxi, pokud by byla přijata podobná výjimka pro badatele, který se zabývá historickým výzkumem. Zde vyvstává otázka, jak definovat vědce, protože to GDPR přesněji nedefinuje. Týkalo by se to například publicisty populárně historického časopisu?

Článek 89 odst. 1 se zaměřuje na záruky a odchylky týkající se zpracování právě pro výše zmíněné oblasti. "*Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely*." [119]

Za plnění těchto záruk lze považovat tzv. standardizované formuláře, které jsou umístěné na webových stránkách SOA. Ty obecně informují veřejnost, že dle archivního zákona osobní údaje nezískávají od třetích stran.

Dále, že neposkytují archiválie s osobními údaji, pokud nebyly získány od subjektu údajů a nacházejí se v archiváliích v souladu s GDPR. V příloze č. 6 diplomové práce se nachází formulář ze SOA v Třeboni.

Tytéž informace se nachází v příloze badatelského listu NA, který je pro srovnání rovněž uveden v příloze č. 7.

[118] Podle novely už novináři nemusí každého demonstranta žádat o souhlas. IDnes.cz [online]. Praha: ČTK, iDNES.cz, 2019, 2019 [cit. 2020-03-19]. Dostupné z: https://www.idnes.cz/zpravy/mediahub/gdpr-evropska-unie-novinar-vedec.A190425_101540_mediahub_jpl

[119] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Článek 89 Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

Jedním z technických faktorů, které musí být brány též v potaz je indexace vyhledávači, pokud má digitalizovaný dokument OCR. Jedná se o metodu optického rozpoznávání textu, ale je proveditelná převážně na tištěné dokumenty. Pro ručně psané dokumenty není tato technologie stále přívětivá. Metoda OCR je aplikována například na některé staré tisky na portále digitální knihovny Kramerius verze 5. Příkladem použití metody OCR je obrázek 1, který zobrazuje výběr textu z Brněnských noviny z roku 1919. Obrázek 2 již ukazuje výsledek vybraného textu.

Vyhláška.

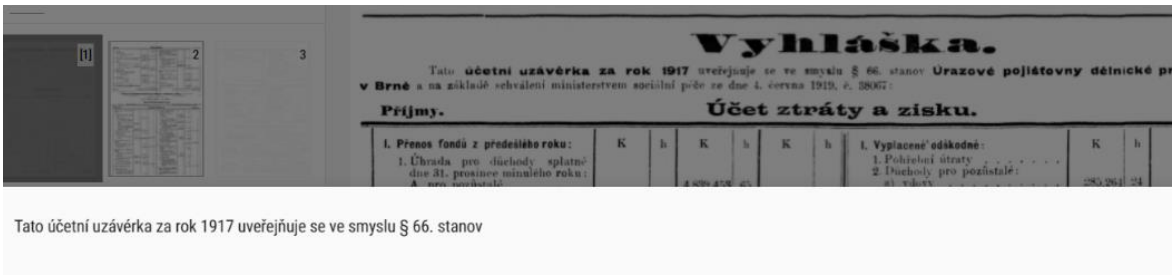
Tato **účetní uzávěrka za rok 1917** uveřejňuje se ve smyslu § 66. stanov **Úrazové pojišťovny dělnické pro Moravu a Slezsko v Brně** a na základě schválení ministerstvem sociální péče ze dne 4. června 1919, č. 38067:

Příjmy. **Účet ztráty a zisku.** **Vydání.**

I. Přenos fondů z předešlého roku:	K	h	K	h	K	h
1. Úhrada pro důchody splatné dne 31. prosince minulého roku:						
A. pro pozůstalé			4,839.453	65		
B. pro výdělku neschopné, kteří dne 31. prosince účetního roku:						
a) ještě léčení jsou	1,078.209	50				
b) již v léčení nejsou a od jeho ukončení důchodů požívají:						
α) méně než 2 roky	5,600.813	92				
β) 2 roky a déle	25,964.726	08	32,643.749	50		

I. Vyplacené odškodné:	K	h	K	h	K	h
1. Pohřební útraty			7.198	—		
2. Důchody pro pozůstalé:						
a) vdovy	285.264	24				
b) děti	227.234	31				
c) ascendenty	29.289	90	541.788	45		
3. Důchody k výdělku neschopné:						
a) po dobu léčení	315.467	99				
b) po uplynutém léčení	2,766.672	25	3,082.140	24		
4. Odbytné:						
a) vdovám, které se opět provdaly (§ 7 úr. zák.)			11.864	91		

Obrázek 1 *Brněnské noviny 1919 – výběr textu*
Zdroj: kramerius5.nkp.cz



Vyhláška.

Tato účetní uzávěrka za rok 1917 uveřejňuje se ve smyslu § 66. stanov

Obrázek 2 Brněnské noviny 1919 – OCR
Zdroj: kramerius5.nkp.cz

Tato ukázka jasně dokazuje, že pokud by archiválie, jenž obsahuje stále osobní údaje žijící osoby, prošla OCR snímáním a následným zveřejněním na digitálním portálu SOA, byť nedopatřením, bylo by možné tento údaj vyhledat prostřednictvím webových vyhledávačů.

4 Dopad GDPR na digitální archivy SOA v ČR

Předchozí kapitola se zabývala dopadem implementace na archivnictví a problematikou digitalizace nejen kronik. Následující kapitola shrne dopad GDPR na digitální portály archivů, kde jsou uveřejněné digitalizáty archiválií, a hlavně se zaměří na digitalizované kroniky ve Státních oblastních archivech (SOA).

Digitální archivy SOA zpřístupňují vybrané archivní fondy a sbírky prostřednictvím webových aplikací. Tyto aplikace umožňují badatelům komfortní vyhledávání digitalizovaných archiválií uložených ve Státních oblastních archivech Zámrsku, Plzni, Třeboni, Praze, Litoměřicích, Moravském zemském archivu v Brně a Zemském archivu v Opavě. Ty mají působnost vymezenou v oblasti dvou až třech krajů na území ČR.

Následující podkapitoly se zaměří na aktuální stav přístupu digitálních portálů všech SOA k digitalizace se zájmem o zpřístupnění kronik. Jedno šetření již proběhlo začátkem roku 2020, které zachytilo některé nedostatky. Další průzkum poukázal na to, do jaké míry archivy postoupily k digitalizaci v souladu s GDPR. Data pro šetření byla čerpána pouze z dostupných webových zdrojů digitálních portálů a webových stránek daných SOA.

4.1 Oblastní archiv Zámrsk

Oblastní archiv v Zámrsku měl na svých webových stránkách umístěny digitalizované obecní kroniky s obsahem pokrývajícím období mladší 105 let. Badatel si mohl celou digitální kroniku stáhnout do vlastního počítače a poté v ní bádat. Vzhledem k platné legislativě na ochranu osobních údajů a rozhodnutí ředitele SOA v Zámrsku, byly veškeré soubory s digitálními kronikami staženy z webových stránek. Archiv se snaží tyto materiály zpracovat do takové podoby,

aby mohly být znovu poskytnuty badatelské veřejnosti prostřednictvím vzdáleného přístupu. Kroniky v nezměněné podobě jsou stále k dispozici městům, které kroniky sepsaly a pro badatele v upravené verzi přímo na badatelně. Jelikož se soubory s kronikami SOA Zámrsku zobrazovaly jako jeden celek, bylo jednoduší je jako celek stáhnout do svého lokálního uložiště.[120]

Tento stav zůstává nadále aktuální. Archiváři oblastního archivu nadále pracují na kontrole digitalizátů na přítomnost osobních údajů žijících osob, po kontrole a případné nutné anonymizaci údajů budou kroniky opět zveřejněny.

4.2 Oblastní archiv v Plzni

Každá oblast má digitalizáty zpracované a zveřejněné trochu jinak, obnova kronik tak probíhá v jiných časových intervalech. Oblastní archiv v Plzni spolu s Bavorským archivem spravuje portál Porta fontium. K problematice GDPR se přímo nevyjadřují, ale je patrné, že digitalizáty, které mohli údaje o žijících občanech obsahovat, byly staženy. Na digitálním portálu zůstaly pouze ty archiválie, které nejsou v rozporu s GDPR. Digitalizované archiválie jsou publikovány na digitální archiv po jednotlivých knihách, nikoli jako celek v případě kronik. Tento způsob usnadnil archivářům SOA v Plzni práci s kontrolou a stažením nevyhovujících kronik a na druhou stranu, vyhovující archiválie byly ponechány badatelům online.

[120] Statní okresní archiv Hradec Králové [online]. Hradec Králové [cit. 2019-11-09]. Dostupné z: https://vychodoceskearchivy.cz/hradeckralove/4270-2/kroniky/.

4.3 Oblastní archiv v Třeboni

Digitální archiv Oblastního archivu v Třeboni v únoru 2020 stále obsahoval materiál, kde se mohly vyskytovat údaje o stále žijících občanech. To bylo zjištěno při hledání v jedné z kronik. Nelze však s přesností říct, zda aktuálně neprobíhala kontrola, či tato kronika nebyla přehlédnuta v množství digitalizovaných archiválií.

Po 5 měsících byla ta samá kronika znovu prohlédnuta na DigiArchivu a byl znatelný zásah anonymizace. Tento proces probíhá ponecháním digitalizovaného archivního materiálu, ale pouze strany, kde se nachází osobní údaje nejsou přístupné. Za přínosné lze považovat i informaci o roce, kdy bude snímek odkryt. Interval zde byl zvolen přibližně 100let.

4.4 Oblastní archiv v Praze

V důsledku ochrany osobních údajů byl systematicky změněn plán digitalizace SOA Prahy už od zavedení samotné platnosti GDPR. E-badatelna se tak přizpůsobila situaci již od začátku, kdy vešlo nařízení do povědomí. Za zlomový je považován rok 1945, kdy kroniky z období po tomto roce jsou zveřejňovány pouze vybrané s ohledem GDPR. Badatel tedy může dohledat archiválie z různých let i po této době, ale v žádné se osobní údaje nenachází

SOA se zabývá vědeckým projektem Analýza zpracování osobních údajů v archiváliích a v rámci spolupráce s Univerzitou Karlovou připravovali workshop *Právní aspekty ochrany osobních údajů v kontextu jejich uchovávání a zpřístupňování,* která se kvůli koronavirové situaci nekonala. [121]

[121] SOA PRAHA. *Plán práce 2020* [online]. Praha: Státní oblastní archiv v Praze, 2020, 30. ledna 2020 [cit. 2020-07-26]. Dostupné z: http://www.soapraha.cz/Files/plán%20soap2020.pdf.

4.5 Oblastní archiv v Litoměřicích

Digitální archiv Oblastního archivu Litoměřice postupně stahuje, kontroluje a znovu obnovuje digitalizované kroniky a další archiválie, mezi které patří například listy ze sčítání lidu v roce 1921, evidence obyvatel z roku 1918 a další archivní materiály. Jistou výhodou může být uveřejněný seznam všech kronik, takže badatelé mají šanci zjistit, co se v archivu nachází a případně se o danou kroniku zajímat. Z uveřejněných kronik je jen velmi malé množství těch, které se datují ve 20. století.[122]

4.6 Moravský zemský archiv v Brně

Moravský zemský archiv v Brně na svém portálu Acta Publica zveřejňuje hlavně matriky a kroniky, které si zpřístupňovaly donedávna oblastní archivy, které pod něj spadají na vlastních platformách. Ty většinou ponechaly kroniky zpřístupněné do roku 1945 a stažené kroniky jsou pak k předložení v příslušené badatelně.[123]

MZA se k problematice Evropského nařízení postavil obdobně jako Oblastní archiv v Plzni. Na portále Acta Publica, budou dle rozhodnutí Zemského archivu nadále zveřejňovány archiválie s datací narozených ve lhůtě 110 let od posledního zápisu v příslušné matriční knize, matriky oddaných ve lhůtě 90 let a matriky zemřelých ve lhůtě 75 let od posledního zápisu. MZA na svém digitálním portále kroniky sice neuveřejňuje, ale na webových stránkách ani neinformuje o jejich možném poskytování k nahlížení.[124]

Mimo to má MZA na webových stránkách zveřejněnou metodiku, jak zacházet s osobními údaji v archiváliích. V dokumentu *Ochrana osobních údajů a spisová*

[122] Státní oblastní archiv v Litoměřicích [online]. Litoměřice [cit. 2020-02-07]. Dostupné z: http://vademecum.soalitomerice.cz/vademecum/archiv.jsp.
[123] Moravský zemský archiv v Brně [online]. Brno [cit. 2020-02-07]. Dostupné z: http://www.mza.cz/a8web/a8Apps1/soka/sokauh/A8SL4DD2Bad3SOKAUH.htm.
[124] Acta Publica [online]. Brno: Moravský zemský archiv v Brně, ©2010 [cit. 2019-11-09]. Dostupné z: http://actapublica.eu/aktuality/.

služba veřejnoprávních původců zmiňuje mimo jiné, že: „*Elektronické systémy spisové služby, stejně jako další samostatné elektronické evidence dokumentů a informační systémy (databáze a jakékoliv soubory informací obsahující osobní údaje žijících osob), musí být upraveny tak, aby po provedené úpravě zajišťovaly nejen omezený přístup k dokumentům a k osobním údajům, ale i možnost výmazu údajů a dokumentů po provedeném výběru archiválií*.“[125]

4.7 Zemský archiv v Opavě

Zemský archiv v Opavě se k situaci rovněž na svých webových stránkách nevyjádřil, ale digitální archiv je pravidelně a často aktualizován, tudíž lze pouze odhadovat, že zde probíhá anonymizace osobních údajů. Při procházení digitalizátů kronik nebyly nalezeny žádné informace, které by osobní údaje obsahovaly.

[125] *Ochrana osobních údajů a spisová služba veřejnoprávních původců* [online]. Brno: MZA Brno, 2018 [cit. 2020-03-20]. Dostupné z: http://www.mza.cz/informace-metodicke-materialy.

5 Implementace GDPR v zahraniční

Předchozí kapitoly se zabývaly postojem Česka ke GDPR. Tato kapitola se pokusí nastínit situaci v několika členských zemích EU a jejich vypořádání se se zavedením GDPR.

5.1 Slovenská republika

Úřad pro ochranu osobních údajů Slovenské republiky uveřejnil vlastní verzi Evropského nařízení o ochraně osobních údajů a směrnice č. 680/2016 a velmi přehledně jej srovnal se zákonem č. 122/2013 o ochrane osobných údajov.

Slovenská republika jako jediný členský stát EU přijala kompletní znění zákona v plném rozsahu. Slovenská vláda předložila parlamentu návrh zákona provádějící GDPR a související směrnici již 20. září 2017. V prosinci téhož roku prezident Andrej Kiska zákon podepsal a tímto dnem začala běžet legisvakanční doba. Během této doby se mohla široká veřejnost se zněním Evropského nařízení seznámit a začít se připravovat na dobu, kdy začne platit.
GDPR na Slovensku nabyl účinnosti 25. května 2018 tímto dnem byl zrušen zákon č. 122/2013 Z. z. o ochrane osobných údajov.[126]

Podle dostupných informací na webu Úřadu na ochranu osobních údajů Slovenské republiky je metodika doplňována postupně. Dle dokumentu MVČR o implementaci na Slovensku, je Česká republika, co se vytváření vlastní metodiky publikovaná více a častěji. První metodika se týká úřadu města a obce a byla publikována 25. dubna 2018. Další metodiky byly přidány až o měsíc později.[127]

[126] *Implementace GDPR na Slovensku: Zákon ano, metodika zatím nikoli* [online]. Praha: MVČR, 2018, 21. ledna 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/implementace-gdpr-na-slovensku.aspx.
[127] Úřad na ochranu osobních údajů Slovenské republiky: *Metodiky a FAQ* [online]. Bratislava: Úrad na ochranu osobných údajov Slovenskej republiky, 2020 [cit. 2020-06-11]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/main-content/metodiky-uradu?page=2.

Metodiky týkající se archivnictví jsou stále podle již zrušeného zákona č. 122/2013 Z. z. o ochrane osobných údajov.[128]

5.2 Rakouská republika

Datenschutzgesetz neboli DSG byl původní rakouský zákon z roku 2000, který je od července 2017 nahrazen rakouským zákonem o ochraně osobních údajů nesoucí stejný název. Legislativní úprava z 25. května 2018 přináší jisté změny a úpravy oproti starému DSG. Tyto změny se zahrnují:

- Přenesení ochrany osobních údajů jak u FO, tak i PO (GDPR se týká pouze FO, ochrana PO je přenesena z DSG);
- Zpracování týkající se trestních činů může být zpracováno na nezbytné účely oprávněných zájmů správce či třetí stranou;
- Snížení věku souhlasu se zpracováním u dětí na 14 let z 16 let;
- Zavedení zvláštních podmínek u sankcí pro PO;
- U veřejných subjektů a orgánů veřejné moci jsou do jisté míry odpuštěné sankce za porušení pravidel v souvislosti s ochranou údajů;
- Došlo k zachování registru zpracování údajů pouze pro archivní účely do konce roku 2019.

V důsledku zavádění GDPR do praxe přinesla Hospodářská komora Rakouska praktické návody a materiály. Jednalo se o přípravu na GDPR, analýzu aktuálního stavu a potřebné úpravy a plán opatření. Došlo ke stanovení priorit cílů a časového harmonogramu na celou realizace implementace GDPR včetně rozpočtového výhledu.

[128] Úřad na ochranu osobních údajů Slovenské republiky: *Archívna informácia – Metodické usmernenia* [online]. Bratislava: Úrad na ochranu osobných údajov Slovenskej republiky, 2020 [cit. 2020-06-11]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/archivna-informacia-metodicke-usmernenia.

Rovněž byla v červnu 2017 vydána příručka, která měla za cíl seznámit širší veřejnost s GDPR, upozornit nejen na změny, které přinese a popsat novou terminologii.[129]
Hospodářská komora Rakouska vydala základní návod nebo vzor podle čl. 30 GDPR Záznamy o činnostech zpracování, kde správce odpovídá za záznamy a to, že obsahují všechny potřebné údaje. Uvádí základní obsah záznamu při zpracování osobních údajů rozdělených do kategorií. Další podobný vzor byl vytvořen i pro zpracovatele, který vede záznamy o zmíněných kategoriích.

Rakousko také v únoru 2018 převzalo předsednictví pracovní skupiny WP29 po Francii. Tato významná funkce spočívala v zajišťování jednotlivých uplatňování nařízení za účelem monitorovat uplatňování a vydávat pokyny, doporučení a postupy, a to i pro některé oblasti a instituty nařízení.

GDPR mělo samozřejmě dopad i na rakouské archivnictví. Rakouské úřady a organizace mají ze zákona povinnost jmenovat pověřence pro ochranu údajů. Řada větších archivů v Rakousku taktéž jmenovala svého DPO.
GDPR stanovuje základní pravidla pro zpracování osobních údajů pro účely archivace ve veřejném zájmu a Rakousko přijalo své výjimky pro archivy. Archivy mohou zpracovávat omezené osobní údaje určité kategorie a jsou osvobozeny od povinnosti informovat každou osobu o jejich zpracování. Právo „být zapomenut“ se nevztahuje na archivní materiál. Vyžaduje však větší důraz na provádějící spisy, že archivní záznamy mají vyšší priority než povinnost výmazu. Archivnictví je rovněž považováno za výzkum a je specificky odděleno od historického výzkumu a statistických účelů.

Novela zákona o federálním archivu stanovuje, že federální archivy jsou podle GDPR zodpovědné za bezpečné uchovávání údajů, ale Rakouský státní archiv je

[129] *Implementace GDPR v Rakousku: Zákon mezi prvními* [online]. Praha: MVČR, 2018, 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/gdpr-v-rakousku-pdf.aspx.

odpovědný i za zpracování osobních údajů po jejich přenosu do jeho kompetence. Zpracování dat musí být vedeno v Obecném adresáři zpracování. Zde je vedeno i zpracování Rakouským státním archivem. Toto komplexní zpracování má 8 bodů zpracování: registrace a indexace, registrace původců archiválií, záznamy badatelů, správa metadat, sběr biografií politiků, databáze adres, videozáznamy z veřejné sféry a záznamy zaměstnanců. [130]

5.3 Spolková republika Německo

Německý parlament schválil jakožto první členský stát EU nový zákon o ochraně osobních údajů neboli *EU-Datenschutzgrundverordnung* (EU-DSGVO). GDPR nabízela jednotlivým zemím možnost upravit přibližně 50 článků národním zákonem a některé články tak uvést podrobněji. Německo přijalo přísnější podmínky povinnosti jmenovat DPO. Pověřence pro ochranu osobních údajů tak musí jmenovat každá společnost která má více než 10 zaměstnanců. Dále jej musí jmenovat všichni správci, kteří jsou povinni vést posouzení vlivu na ochranu údajů či komerčně zpracovávají osobní údaje pro účely jejich převodu, průzkumu trhu nebo výzkumu veřejného mínění.[131]

Německo dále využilo možnost zpřísnit některé další požadavky GDPR. Německá legislativa zavedla například rozšiřující okruh správců jmenovaných DPO a zpřísňuje nakládání s údaji zaměstnanců.[132]

[130] SCHÖGGL-ERNST, Elisabeth. Die Auswirkungen der Datenschutzgrundverordnung auf Archive in Österreich. Atlanti [online]. Gratz, 2018, 28. 2. 2018, 2018(2), 123-130 [cit. 2020-07-26]. DOI: https://doi.org/10.33700/2670-451X.28.2.123-130(2018). Dostupné z: http://journal.almamater.si/index.php/Atlanti/article/view/305/281

[131] ČESKÁ ASOCIACE OCHRANY OSOBNÍCH ÚDAJŮ. GDPR pro malé a střední podniky: Nový německý zákon o ochraně osobních údajů [online]. Praha, ©2020 [cit. 2020-06-11]. Dostupné z: http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/.

[132] EPravo: *GDPR* [online]. Praha, 2017, 16. 8. 2017 [cit. 2020-06-11]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-106244.html.

V důsledku uvedení EU-DSGVO v platnost muselo také dojít k anulování některých národních předpisů, které byly s Evropským nařízením neslučitelné.
EU-DSGVO nově také upravuje trestně právní delikt. To se týká vědomého převodu či zpřístupnění velkého množství osobních údajů. V tomto případě může být udělen trest odnětí svobody až ve výši 3 let.[133]
V mezích vědeckého, historického či statistického zájmu lze zpracovat osobní údaje i bez souhlasu subjektu údajů. Nicméně zpracovatel může být vyzván k prokázání zájmu o zpracování, které musí převyšovat zájme subjektu údajů. Nicméně je zde stále třeba dbát na anonymizaci. [134]

5.4 Belgické království

Belgický *La Commission de la protection de la vie privé* (CPVP) neboli místní ekvivalent českého Úřadu pro ochranu osobních údajů projevil ze všech dalších orgánů asi největší očekávání na příchod GDPR. Dokonce na svých webových stránkách spustil odpočet s přesností na sekundy. Belgie, podobně jako další země, se zabývala blížícími se změnami od doby, kdy GDPR přišlo v platnost. CPVP vydalo metodickou příručku, kde se mohla široká veřejnost dočíst, jak se na GDPR připravit ve 13 etapách. Ty sice nebyly v přesné časové posloupnosti, nicméně s podobným řešením přišla například i Francie a Velká Británie.

Velkou pozornost zaměřil CPVP na roli pověřence, dopad vlivu na soukromí, etický kodex a registr údajů. Registr údajů má umožnit správci údajů nebo zpracovateli každého zpracování údajů a uspořádání procesů, ke kterým dochází. Ten musí být vyhotoven srozumitelně a elektronicky. Základem registru jsou otázky: kdo, co, jak, proč, do kdy, kde. CPVP doporučuje vést dokumentaci i za předpokladu, že se jedná o velkou organizaci čítající přes 250 zaměstnanců, na

[133] GDPR pro malé a střední podniky: *Nový německý zákon o ochraně osobních údajů* [online]. Praha, ©2020 [cit. 2020-06-11]. Dostupné z: http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/.
[134] The GDPR in Germany: *Data Processing for Research & Statistical Purposes* [online]. Berlín, ©2020, 16. 8. 2017 [cit. 2020-06-11]. Dostupné z: https://allcloud.io/blog/gdpr-in-germany-are-you-covered/.

které se vztahuje výjimka této povinnosti. Vzor registru je pro širokou veřejnost k dostání na webových stránkách úřadu CPVP.

V souvislosti s příchodem GDPR se úřad CPVP začal věnovat edukaci o ochraně údajů u dětí a vytvořil i materiály pro rodiče a pedagogy. Věnuje se problematice soukromého života na sociálních sítích, soukromého života na vzdělávací instituci, fotografiím a videím, mobilním zařízením, sextingu a dalším. Rovněž úřad připravil i didaktické podklady pro pedagogy do výuky. [135]

V květnu 2018 GDPR nahradilo belgický zákon o ochraně soukromí z roku 1992. Ten zpřísnil pravidla upravující dohled nad zpracováním. Umožněna je ale odchylka pro účely archivace ve veřejném zájmu. Belgické archivnictví se muselo tomuto novému nařízení též přizpůsobit. S cílem poskytnout pomoc archivářům a badatelům v této oblasti při uplatňování GDPR byla vydána stručná příručka o všech aspektech této nové legislativy, která se dotýká též archivů. [136]

5.5 Spojené království Velké Británie a Severního Irska

Velká Británie přišla s velmi ambiciózním způsobem implementace GDPR do jejich struktury. Dle oficiálního vyjádření vlády se Velká Británie hodlá stát nejbezpečnější online místo v kyberprostoru a rozvinout tak více online podnikání. V britském prostředí je tak kybernetická bezpečnost velmi úzce spjata s ochranou osobních údajů a implementace GDPR má sloužit k tomuto posílení. Hlavně se jedná o posílení důvěry nejen ve využití nových technologií u občanů, a to i v souvislosti s ochranou osobních údajů.
Stejně jako Francie či Belgie, tak i britská verze ÚOOÚ vydala přípravnou metodiku ve dvanácti krocích, která je totožná s belgickou či francouzskou.

[135] GDPR V Belgii: *Čerstvý vánek, nikoliv ničivý uragán* [online]. Praha, 2018, 23. ledna 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/implmentace-gdpr-belgie.aspx.
[136] STATE ARCHIVES OF BELGIUM. *Personal Data and Archives* [online]. Brusel: State Archives of Belgium, 2020 [cit. 2020-07-26]. Dostupné z: http://arch.arch.be/index.php?l=en&m=practical-information&r=data-protection&sr=personal-data-and-archives.

Začátkem srpna 2017 britská vláda prezentovala záměr posílit zákon o ochraně údajů takovým způsobem, aby měli občané větší kontrolu nad svými údaji hlavně v době digitálních technologií. Tento záměr figuruje pod názvem Data protection bill, něco ve smyslu Účet na ochranu údajů. Součástí toho byla výzva k připomínkám ohledně samotnému GDPR. Elektronicky mohla FO či PO vyjádřit připomínky pomocí formuláře dostupného na stránkách Data protection bill. Po analýze připomínek vznikl dokument obsahující informace, například, že se digitální ekonomika ocitá v z centru britských zájmů. Po vyhodnocení výzkumu byla vypracována kvantifikace výhod GDPR v souvislosti s analýzou připomínek.

Stránky britského ekvivalentu ÚOOÚ obsahují velmi přehledné informace ohledně implementace GDPR. Nachází se zde různé definice, právní zásady, osobní práva, formuláře, analýzy dopadů atd. Rovněž se zde nachází aktuality k různým metodikám. Zajímavostí je, že ve Velké Británii je zpracování osobních údajů pro nově registrované správce zpoplatněné. Poplatek se odvíjí od počtu zaměstnanců a ročního obratu. Menší podniky do 10 zaměstnanců platí průměrně £40 a podniky do 250 zaměstnanců průměrně £60.[137]

Národní archiv VB na svých webových stránkách shrnul pokyny k právním předpisům o ochraně osobních údajů. Tyto pokyny se zabývají výhradně oblastí vztahu archivnictví a GDPR.
GDPR bere v potaz veřejný zájem a povoluje tak trvalé uchování osobních údajů pro dlouhodobý prospěch společnosti v archivech. K tomu se váže pojem archivace ve veřejném zájmu, který se vztahuje na archivaci veřejnými, soukromými nebo dobrovolnými subjekty.
Zpracování údajů pro účely archivace musí být odlišeno od zpracování, které podporuje každodenní podnikání, protože na tyto případy se výjimka nevztahuje.

[137] Implementace GDPR ve Velké Británii: *Ambice nejbezpečnějšího kyberprostoru* [online]. Praha, 2018, červen 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/implementace-gdpr-ve-velke-britanii-pdf.aspx.

Jedná se z pravidla o údaje shromážděné pro marketingové účely. Zpracování musí být rovněž transparentní. Musí dojít ke splnění záruk, aby bylo možné využít výjimku, která minimalizuje jakýkoli nepříznivý dopad na živé osoby. Zpřístupnění doposud archivovaných osobních údajů bude obecně umožněno, jakmile budou dotyčné osoby po smrti. Přístup k osobním údajům živých osob je možné za předpokladu, že byl dán písemný souhlas.[138]

5.6 Srovnání

Pro lepší přehlednost souhrnu implementace GDPR v zahraničí byla vytvořena tabulka č. 1.

	Informace/metodika před implementací	Zvláštní pozornost věnovaná DPO	Přísnější opatření v rámci GDPR	Zaměření na edukaci	Přijetí v plném znění bez zásahů	Sankce	
						Peněžité	Odnětí svobody
Česká republika				✓		✓	✓
Slovenská republika					✓	✓	
Rakouská republika	✓			✓		✓	
Německá spolk. rep.		✓	✓			✓	✓
Belgické království	✓	✓	✓			✓	
Spojené království	✓			✓		✓	

Tabulka 1 Implementace GDPR ve vybraných zemích EU

Srovnání toho, jak si s implementací poradily okolní země EU s Českou republikou by mohlo poukázat na skutečnost, že naše implementace není zdaleka taková, komplikovaně ji média popisovala. Nedošlo ke vzniku úvodní metodika jako například v Rakousku, Belgii, Velké Británii či Francii, ale četnost tvorby aktuálních metodik převyšuje minimálně Slovensko. Naše postihy jsou stále „pouze“ finanční a nikoli po vzoru Německa i odnětí svobody.

[138] THE NATIONAL ARCHIVES. *Archives and data protection law in the UK – an overview* [online]. Londýn: The National Archives, 2020 [cit. 2020-07-26]. Dostupné z: https://www.nationalarchives.gov.uk/archives-sector/legislation/archives-data-protection-law-uk/overview/.

6 Vnímání GDPR v Oblastních archivech v ČR

Dle nejednoho názoru je celá koncepce implementace do archivnictví poněkud komplikovaná. Celý koncept GDPR vychází z potřeby ochránit subjekt údajů před zneužitím jeho údajů primárně ze strany třetích organizací, které by na tom mohli profitovat. Jelikož GDPR dopadá jak na komerční, tak i na státní instituce, toto nařízení se tak nevyhýbá ani stání správě, resp. archivnictví v ČR.

V archivu badatel při vstupu do badatelny vyplňuje badatelský list, který obsahuje jeho osobní údaje. Ty jsou ale zpracovávány primárně za účelem ochrany archiválií a slouží tedy pouze pro vnitřní potřebu archivu. Archivy tedy nejsou v postoji, kdy by mohli data dále využít. Nicméně archivní materiály obsahují informace, kde se mohou rovněž nacházet osobní údaje.

Na tomto základě proběhlo v březnu dotazníkové šetření, kde bylo zjišťováno vnímání implementace GDPR do archivnictví přímo ze strany archivů a jejich zaměstnanců. V dotazníkovém šetření mohl respondent uvést i vlastní problémy s implementací. Nejčastěji byly uváděny: povinnosti pro původce související s GDPR, časová náročnost kontroly předkládaných archiválií a nejednotné postupy.

Pro zjištění této problematiky byl použit dotazník rozeslaný prostřednictvím emailů. Dotazník obsahoval převážně otázky otevřeného a specifikovaného charakteru, aby bylo dosáhnuto co nejkonkrétnějších odpovědí. Dotazník obsahoval v menšině i ordinální otázky. Poslední otázky dotazníku se týkaly částečné identity respondenta. Pro toto šetření bylo žádoucí znát konkrétní archiv, pozici respondenta a pohlaví. Cílem dotazníku bylo získat vzorek, který by mohl přiblížit aktuální problém českého archivnictví. Jak již bylo zmíněno, GDPR necílí v první řadě na státní instituce, ale ani ty se nařízení nevyhnou.

Jelikož v praktické části práce byl zjišťován aktuální stav prostřednictví dotazníkového šetření, jehož výsledky jsou následně popsány. Součástí práce je i příloha č. 4, kterou tvoří původní dotazník šetření.

6.1 Otázky kladené pro šetření

Stěžejní otázky výzkumu, byly:

- Kde archivy spatřují největší problém v implementaci GDPR?
- Jaký mají archivy postoj ke GDPR?
- Jak jsou pracovníci archivu spokojeni s podporou MVČR?
- Kdo a jak postupoval v případě digitalizovaných kronik, aby bylo dodrženo GDPR?
- Pokud by byla možnost úpravy znění GDPR v ohledu na archivy, kde by zaměstnanci archivů uvítali změny?
- Kdo jsou respondenti tohoto statistického šetření a jaké pozice zastávají?

6.1.1 Problémy implementace GDPR do archivnictví

Hlavní předdefinované problémy v této části byly: časová náročnost kontroly vstupních archiválií, legislativní opatření, složitost vnitřních procesů a technologie. Respondent mohl uvést i vlastní zkušenosti s implementací.

Problémy implementace GDPR

Sum

Státní oblastní archiv	Technologie	Legislativa	Proškolování zaměstnanců	Kontrola archiválií	Vnitřní procesy	Jiné
MZA Brno	1	4	1	6	0	1
SOA Litoměřice	0	5	0	6	4	1
SOA Plzeň	1	1	2	4	1	0
SOA Praha	1	2	0	4	1	0
SOA Třeboň	0	2	1	1	0	0
SOA Zámrsk	1	0	0	1	0	0
ZA Opava	0	10	2	9	3	0
Neuvedeno	1	1	1	3	1	1
Total	5	25	7	34	10	3

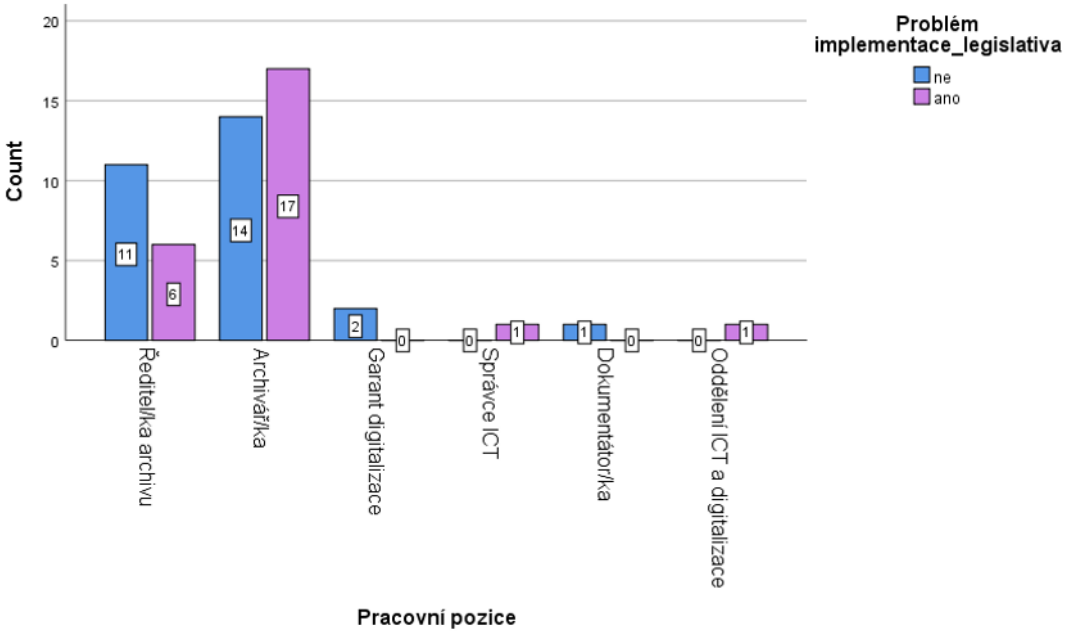
Tabulka 2 Problémy implementace GDPR do jednotlivých SOA
Zdroj: vlastní dotazníkové šetření

Nejčastěji se objevovaly odpovědi typu: povinnosti pro původce související s GDPR, časová náročnost kontroly předkládaných archiválií a nejednotné postupy. Jeden z respondentů přímo uvedl, že problém spatřuje také v tom, že „*původní smysl GDPR byl zcela jiný a s archivy nemá příliš co společného.*“.

Z tabulky č. 2 lze vyčíst, že za největší problém je považována kontrola archiválií před zveřejněním v digitálním archivu nebo před poskytnutím badateli k nahlédnutí. V poznámkách od respondentů bylo mnohdy uváděno, že se tento problém netýká pouze vstupních archiválií, ale archiválií komplexně. Kontrolou musí procházet také archiválie, které se předkládají badatelům do badatelny, zdali dokument neobsahuje osobní údaje nebo zda má badatel souhlas od příslušené osoby k předložení dokumenty údaje obsahující. Kontrola je nutná i v případě převodu analogových archiválií do digitální podoby které jsou zveřejněny prostřednictvím webových portálů jednotlivých SOA.
Další v pořadí byl hojně zmiňován problém ohledně legislativy. O legislativách příslušných k tomuto tématu pojednává kapitola *2 Archiv jako správce údajů*.

Naopak nejmenší problémem ze strany archivů jsou považovány technologie a proškolování zaměstnanců. Informace mohou archiváři získávat prostřednictvím konferencí pořádaných například Českou archivní společností. Archivy na základě poznatků z těchto speciálních konferencí mohou vypracovávat vlastní pokyny a postupy pro nakládání s archivním materiálem, který obsahuje osobní údaje.

S legislativou souvisí i otázka, jak jsou respondenti spokojeni s podporou MVČR. K této variantě se přiklonilo nejvíce respondentů spadající pod Zemský archiv Opava. Pokud se na tuto část zaměřím podrobněji, zjistím že nejvíce se pro tuto odpověď přiklonilo archivářů (17) a dále ředitelé a ředitelky archivů (6), jak ukazuje Graf 1.



Graf 1Problémy implementace z pohledu pracovních pozic v archivech
Zdroj: vlastní dotazníkové šetření

6.1.2 Postoj zaměstnanců archivů ke GDPR

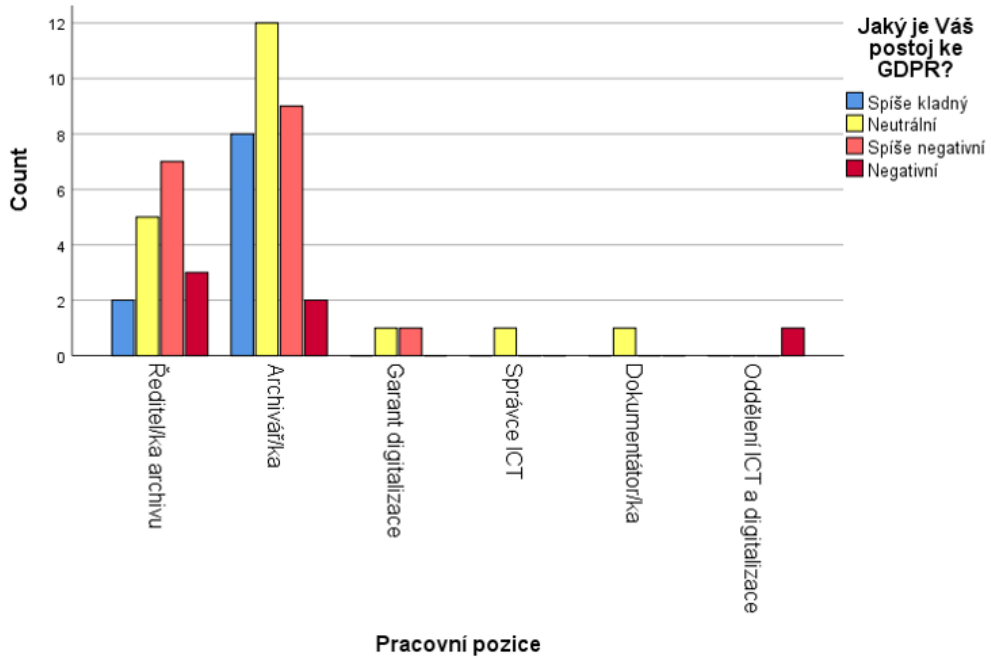
Dalším bodem tohoto šetření bylo zjištění spokojenosti či nespokojenosti s obecným zavedením GDPR s konkrétními profesemi a respondenty. Z tabulky 3 vyplývá, že obecně převládá neutrální až negativní postoj k GDPR. Tyto postoje zastávají většinově ženy. Žádný z respondentů nemá vysloveně kladný postoj vůči GDPR.

		Jaký je Váš postoj ke GDPR?				
		Kladný Count	Spíše kladný Count	Neutrální Count	Spíše negativní Count	Negativní Count
Pohlaví	1 muž	0	5	8	4	2
	2 žena	0	5	11	10	4
	3 nechci uvést	0	0	1	3	0

Tabulka 3 Postoj respondentů k GDPR
Zdroj: vlastní dotazníkové šetření

Obecně lze tvrdit, že neutrální a spíše negativní postoj k GDPR mají hlavně archiváři a archivářky. Spíše negativní a negativní postoj zastávají ředitelé, částečně i archiváři a pracovníci oddělení ICT a digitalizace. Toto jsou profese,

které se setkávají s GDPR v rámci svého povolání nejčastěji, ať se to již týká předkládání archiválií badatelům na badatelně nebo se zabývají kontrolou či anonymizováním digitalizátů s osobními údaji, které jsou nahrané na digitálních



portálech. Celkové srovnání se nachází v grafu 2.

Graf 2 Postoj zaměstnanců k GDPR
Zdroj: vlastní dotazníkové šetření

Zajímavý je i pohled na situaci, jak jednotliví zaměstnanci vidí důležitost problémů ve spojitosti s GDPR. V tabulce 4 lze sledovat, že nejpočetnější skupina respondentů, tedy archiváři, nejčastěji volili jako zásadní problémy legislativní opatření a časovou náročnost kontroly archiválií, podobně jako ředitelé archivů, kteří zároveň vidí problém také ve složitosti vnitřních procesů.

Naopak jako nejmenší komplikace jsou z pohledu všech různých postů spatřovány technologické potíže a proškolování zaměstnanců.

6.1.3 Metodika a podpora ze strany MVČR

Dle odpovědí respondentů, zda v archivech používají či nepoužívají metodiku pro správný postup při řešení případů vztahující se k GDPR, odpovědělo 51 %, že v daném archivu metodiku nepoužívají. Další nejvíce zastoupená možnost byla vnitřní směrnice/předpis, což lze spolu se služebním předpisem považovat za

Tabulka 4 Četnost komplikací na různých pracovních pozicích
Zdroj: vlastní dotazníkové šetření

		1 MZA Brno	2 SOA Litoměřice	3 SOA Plzeň	4 SOA Praha	5 SOA Třeboň	6 SOA Zámrsk	7 ZA Opava	8 Neuvedeno	Total
Typ metodiky	0 Nemají metodiku	2	3	5	3	1	0	9	3	26
	1 Vnitřní předpis/směrnice	1	6	1	0	0	0	1	1	10
	2 Vlastní vytvořená metodika	1	0	0	0	0	0	0	1	2
	3 Metodika MV	0	0	0	1	0	0	2	0	3
	4 Služební předpis ředitele archivu	1	1	0	0	1	1	3	0	7
	5 Metodika NA	2	0	0	0	0	0	0	0	2
	6 Převzatá metodika	0	0	0	2	0	0	0	1	3
Total		7	10	6	6	2	1	15	6	53

vlastní metodiku k problematice GDPR. Pouze dva archivy využívají metodiku Národního archivu.

Tabulka 5 Metodiky využívané v SOA
Zdroj: vlastní dotazníkové šetření

Není překvapující, že žádný z respondentů není plně spokojen s podporou Ministerstva vnitra ČR. Jak již bylo uvedeno v kapitole *2 Archiv jako správce*

		Archivář/ka	Garant/ka digitalizace	Ředitel/ka	Dokumentátor/ka	Správce ICT	Total
V čem archivy spatřují největší komplikace při implementaci GDPR?	V technologiích	2	1	2	0	0	5
	V legislativních opatřeních	17	3	5	0	0	25
	V proškolování	4	3	2	1	0	10
	V časové náročnosti kontroly vstupních archiválií	23	2	8	0	1	34
	Ve složitosti vnitřních procesů archivů	5	1	5	0	1	12
	V povinnosti pro průvodce související s GDPR	1	0	0	0	0	1
	V tom, že původní smysl GDPR byl zcela jiný a s archivy nemá příliš společného	1	0	0	0	0	1

údajů, metodika MVČR je velmi stručná a nezahrnuje praktické příklady jako například metodika EAG. Vyslovená nespokojenost a částečná spokojenost

s podporou MVČR jsou dvě nejméně časté odpovědi. Respondenti z SOA

Count

		Absolvují zaměstnanci v rámci archivu školení ke GDPR?					
		Ano, pravidelně	Ano, ale zřídka	Pouze jednou	Ne, informace se dozvídám průběžně	Ne	Total
Jste spokojen s podporou Ministerstva vnitra při řešení a následné implementaci GDPR?	Spíše ano	1	3	2	3	0	9
	nemám výhrady	4	3	5	3	0	15
	spíše ne	0	9	9	3	2	23
	Ne	2	2	1	1	0	6
Total		7	17	17	10	2	53

Litoměřice a ZA Opava jsou spíše spokojeni s podporou Ministerstva vnitra ČR. 14 respondentů nemá k této problematice výhrady. Nejčastěji jsou respondenti spíše nespokojeni s touto situací (26), a to převážně z SOA Litoměřic, ZA Opavy, SOA Plzně a SOA Prahy

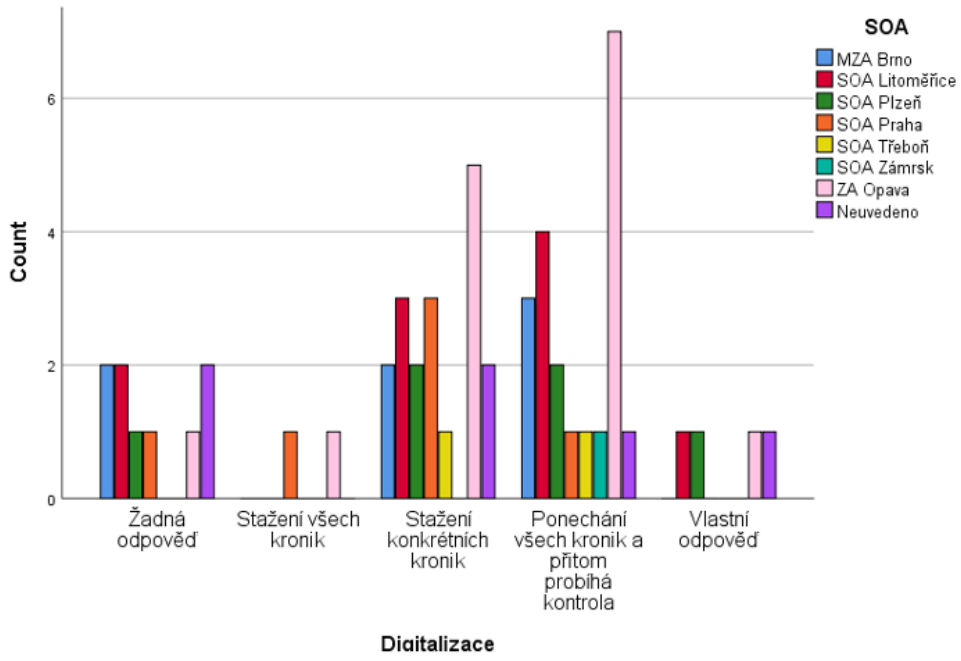
Další z kladených otázek směřovala ke spokojenosti respondentů s podporou ze strany MVČR, kteří již absolvovali školení/konference či workshopy k GDPR. Z tabulky 6 je zřejmé, že respondenti, kteří školení absolvovali pravidelně či zřídka jsou spíše nespokojeni či nemají k tomuto výhrady. Spokojenost s podporou ministerstva je podle 23 respondentů spíše negativní a podle 15 respondentů bez

Tabulka 6 Spokojenost respondentů
Zdroj: vlastní dotazníkové šetření

výhrad. Úplná nespokojenost byla pouze u šesti respondentů a úplná spokojenost pouze u devíti respondentů z 53. Školení v rámci GDPR bylo pravidelně pouze u sedmi respondentů, sedmnáct respondentů uvedlo, že bylo provedeno, ale zřídka, anebo pouze jednou. Jen dva respondenti uvedli že neměli žádné proškolení. Deset respondentů uvedlo, že se informace dozvídají průběžně a neproběhlo u nich žádné školení.

6.1.4 Digitalizace pod nátlakem GDPR

Jedním z hlavních bodů celého šetření bylo zjistit, jaké kroky museli archivy učinit pro dodržení GDPR při digitalizaci, zveřejňování obsahu na digitální archivy a co museli udělat pro to, aby bylo Evropské nařízení dodrženo vzhledem ke stávajícímu stavu na digitálních archivech.

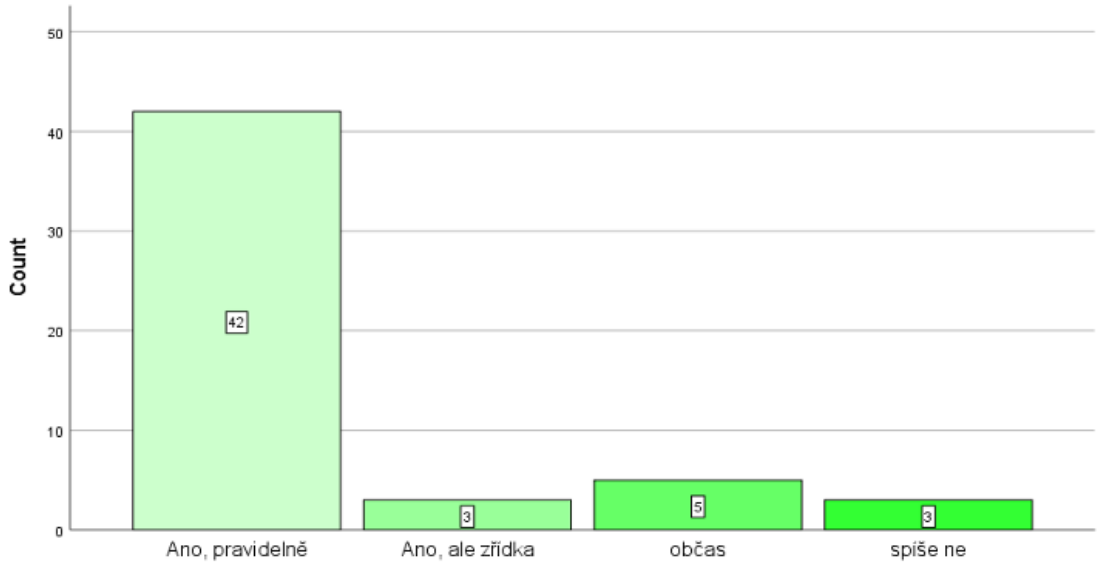


Graf 2 Digitalizace kronik
Zdroj: vlastní dotazníkové šetření

Osobní preferencí bylo sledovat tento stav primárně u kronik, jelikož se jedná v mnoha případech o nejčastější badatelský materiál. Výsledky z grafu 4 vykazují poměrně extrémní možné varianty, tedy buďto úplné ponechání (a kontrola přitom) nebo částečné stažení. Tento stav byl patrní již při kontrole digitálních archivů, které jsou popsané v kapitole 4. Z této činnosti lze stanovit, že do sekce „Stažení všech kronik“ se řadí také SOA Zámrsk, ze kterého bohužel nemám velký vzorek.

Do výzkumu též přispěli respondenti vlastními odpověďmi. Některý SOA bude teprve kroniky zveřejňovat a chystá se postupovat obdobně, jak tomu je zvykem u matrik, tedy cirka po 100 letech od posledního zápisu. Celkem velký vzorek archivů (9) se shodlo na skutečnosti, že kroniky ani publikovat nebudou.

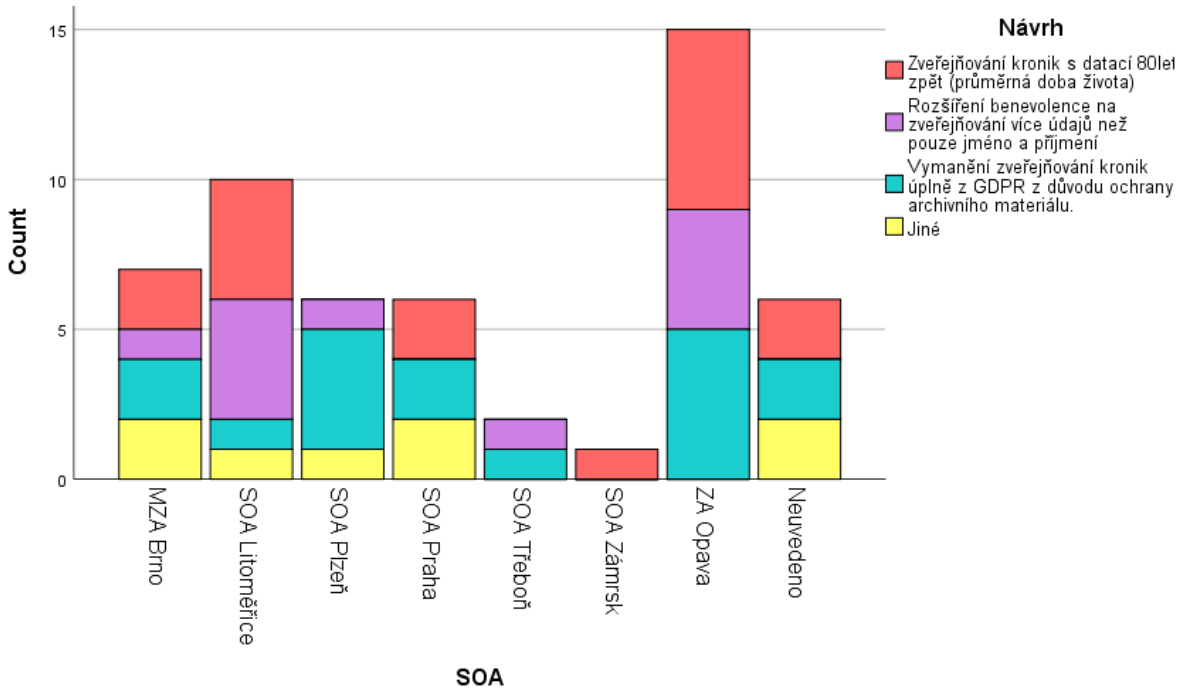
V důsledku tohoto zjištění byl vytvořen graf 5, který zobrazuje skutečnost, jak často jsou kroniky žádány v archivech k předložení badatelům. Z grafu jasně vychází, že kroniky jsou badateli žádány pravidelně, jak odpovědělo 42 respondentů. Nelze tedy stažení veškerých kronik z webů považovat za korektní postup, jelikož se tímto zavírají cesty drobným badatelům, zájemcům o genealogickou informaci nebo historikům. Mnohdy se požadovaný archivní materiál nachází ve vzdáleném archivu, a právě digitální archivy byly velmi oblíbené napříč badateli právě díky dostupnosti.



Graf 3 *Četnost vyžádání kronik na badatelnu*
Zdroj: vlastní dotazníkové šetření

6.1.5 Návrh na úpravu znění podle respondentů

Zajímavý byl názor respondentů na situaci, kdyby se mělo znění GDPR upravit. V několika případech se v šetření objevil názor, že obecně historické prameny by měly být vymaněny z GDPR a odpovědnost by měla být přenesena na badatele. Další z respondentů byli s nařízením jako takovým docela spokojeni, pouze jim vadí jeho komplikované znění a uvítali by specifičtější znění některých článků. Nejčastěji se respondenti přikláněli k variantě, aby kroniky byly vymaněny z GDPR úplně, případně aby mohlo probíhat jejich zveřejňování po uplynutí stanovené doby nehledě na to, jaký obsah nesou.



Graf 4 *Návrhy změn GDPR*
Zdroj: vlastní dotazníkové šetření

Mezi odpovědi kategorie Jiné se objevovaly také názory, že vyjmut by měl být veškerý archivní materiál a řídit by se měl příslušnou legislativou dané země (u nás tedy zákonem č. 499/2004 Sb. o archivnictví a spisové službě).

Závěr dotazníkového šetření se zaměřil na trochu hlubší poznání toho, kdo jsou respondenti tohoto šetření v rámci zachování anonymity. Tabulka 7 sleduje frekvenci respondentů v přesně daném archivu. Tato konkrétní data nebyla v šetření tak často využívána, jelikož většinou hlavní zájem spočíval na zjišťování různé problematiky za oblast Státního oblastního archivu nebo přímo za funkci respondenta.

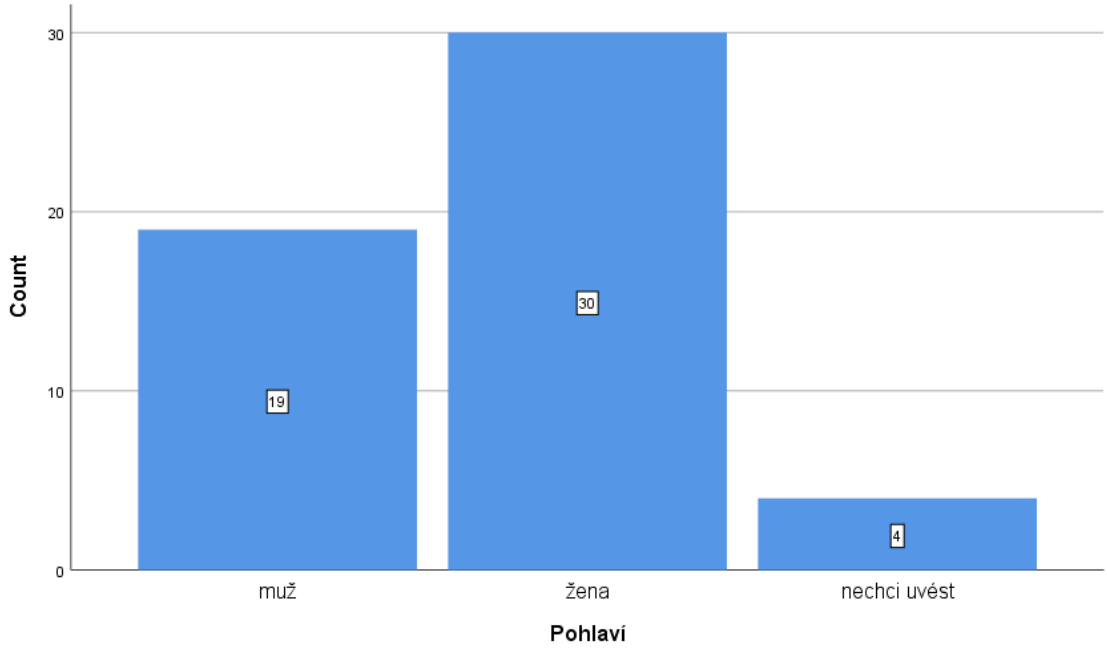
Počet odpovědí z archivů

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	MZA Brno	3	5,7	5,7	5,7
	SOA Litoměřice	1	1,9	1,9	7,5
	SOA Plzeň	1	1,9	1,9	9,4
	SOA Praha	3	5,7	5,7	15,1
	SOA Třeboň	2	3,8	3,8	18,9
	SOA Zámrsk	1	1,9	1,9	20,8
	ZA Opava	7	13,2	13,2	34,0
	Nechci uvést	6	11,3	11,3	45,3
	SOkA Kladno	1	1,9	1,9	47,2
	SOkA Děčín	1	1,9	1,9	49,1
	SOkA Plzeň	1	1,9	1,9	50,9
	SOkA Rokycany	1	1,9	1,9	52,8
	SOkA Opava	5	9,4	9,4	62,3
	SOKA Příbram	1	1,9	1,9	64,2
	SOkA Beroun	1	1,9	1,9	66,0
	SOKa Domažlice	1	1,9	1,9	67,9
	SOkA Pelhřimov	1	1,9	1,9	69,8
	SOkA Olomouc	1	1,9	1,9	71,7
	SOkA Liberec	2	3,8	3,8	75,5
	SOkA Kutná Hora	2	3,8	3,8	79,2
	SOkA Šumperk	1	1,9	1,9	81,1
	SOkA Tachov	1	1,9	1,9	83,0
	SOkA Litoměřice se sídlem v Lovosicích	2	3,8	3,8	86,8
	SOkA Most	1	1,9	1,9	88,7
	SOkA Jablonec	1	1,9	1,9	90,6
	SOkA Kadaň	1	1,9	1,9	92,5
	SOkA Cheb	1	1,9	1,9	94,3
	SOkA Česká Lípa	1	1,9	1,9	96,2
	SOkA Břeclav	1	1,9	1,9	98,1
	SOkA Přerov	1	1,9	1,9	100,0
	Total	53	100,0	100,0	

Tabulka 7 Archivy
Zdroj: vlastní dotazníkové šetření

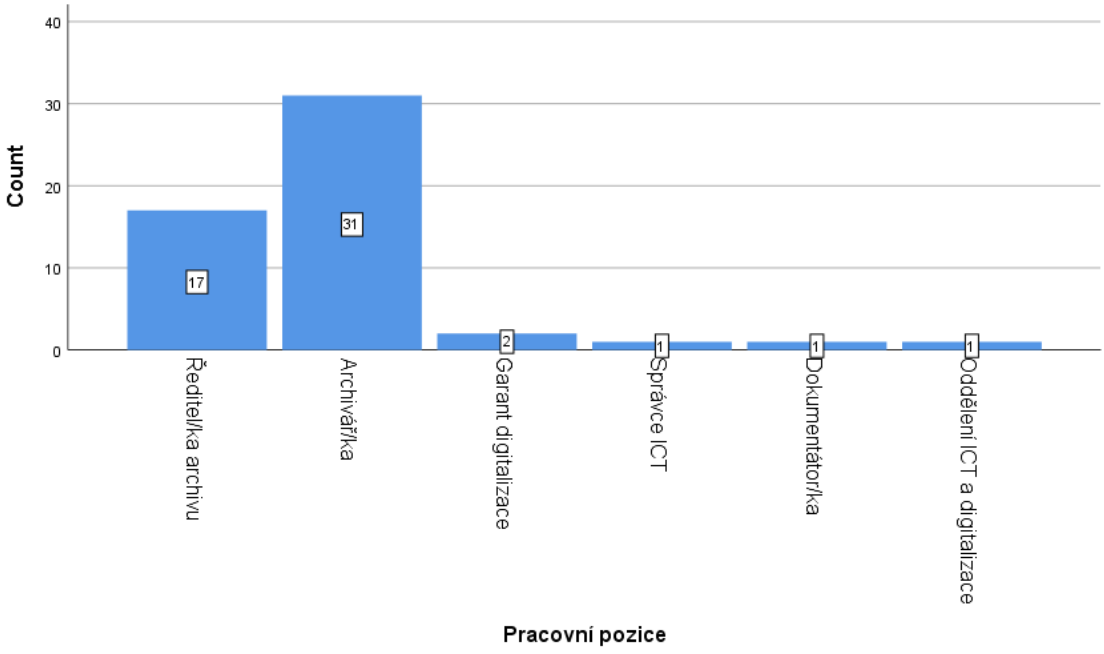
Lze tedy sledovat například to, že nejvíce reakcí na zaslané dotazníky přišlo zpět ze Zemského archivu v Opavě (13,2 %), dále ze Státního oblastního archivu v Opavě (9,4 %) a rovnocenně ze Státního oblastního archivu v Praze a Moravského zemského archivu v Brně (5,7 %). Lze také sledovat, že poměrně velké procento respondentů odmítlo uvést místo svého působení (11,3 %).

V následujícím grafu 7 lze vysledovat, že více než polovinu respondentů tvoří ženy (30) a muži zastupují vzorek 19 respondentů. Respondenti, kteří nechtěli uvést, zvolili tuto variantu 4x.



Graf 5 Pohlaví respondentů
Zdroj: vlastní dotazníkové šetření

Závěrečný graf 8 se zabývá četností profesí v rámci archivu. Nejmenší vzorek tvoří zaměstnanci na pozici ICT a digitalizace, dokumentátoři a správci IT, což je škoda, protože právě tito pracovníci se dostávají velmi často k problematice GDPR a digitalizace archivních materiálů a jejich názor na celou situaci by byl jistě velmi přínosný. Největší počet respondentů tvoří archiváři/archivářky (31) a vedení jednotlivých archivů (17).



Graf 6 *Pracovní pozice respondentů*
Zdroj: vlastní dotazníkové šetření

Je zajímavé sledovat názory na vybranou problematiku u lidí z řídících funkcí v archivu. Jelikož v šetření nebyli zapojeni respondenti na profesní oblasti právník, knihovník nebo výzkumný a vývojový pracovník, tak i zde je postrádán významný názor.

6.2 Souhrn

Dotazníkového šetření bylo aplikováno na všechny zaměstnance na pracovních pozicích: ředitel, archivář, knihovník, garant digitalizace, výzkumný/vývojový pracovník, správce ICT, restaurátor, technický pracovník, dokumentátor a další pozice, které mohl respondent uvést.

Šetření probíhalo 03. 03. 2020 - 23. 03. 2020 a bylo rozesláno mezi zaměstnance MZA Brno, ZA Opava, SOA Litoměřice, SOA Plzeň, SOA Praha, SOA Třeboň a SOA Zámrsk. Návratnost dotazníků činila 53 vyplněných dotazníků. Všichni zaměstnanci byli kontaktováni na pracovní email a rovněž bylo požádáno

o součinnost se všemi řediteli SOA. Dotazník obsahoval převážně otázky otevřeného a specifikovaného charakteru, aby bylo dosáhnuto co nejkonkrétnějších odpovědí. Dotazník obsahoval v menšině i ordinální otázky. Poslední otázky dotazníku se týkaly částečné identity respondenta. Pro toto šetření bylo žádoucí znát konkrétní archiv, pozici respondenta a pohlaví.

Cílem dotazníku bylo získat vzorek, který by mohl přiblížit aktuální problém českého archivnictví. Jak již bylo zmíněno, GDPR necílí v první řadě na státní instituce, ale ani ty se mu nevyhnou.
Pro tuto analýzu byl využit program IBM SPSS, kde byl zpracován vzorek 53 dotazníků. Návratnost byla 42,2 %.

Většina respondentů není toho názoru, že GDPR přineslo pouze to dobré. Na jedné straně je sice podstatná ochrana dat, nicméně na té druhé, stojí velký nárust práce pro nejen české archiváře.

Kroniky patří všeobecně k nejcennějším badatelským zdrojům informací pro historiky, demografy, statistiky a v neposlední řadě také genealogy či jen nadšené badatele. Digitální archivy ušetřili mnohým z vyjmenovaných čas a mohli tak bádat z pohodlí domova, pokud byla kronika, či jiný archivní materiál, zpřístupněna. Jak vyplývá z šetření, část kronik z digitálních archivů zmizela úplně. Včetně té, která tam mohla zůstat.

Dle osobního názoru bylo GDPR potřebné a je prospěšné, ale ne v této konkrétní sféře. Článek 89 GDPR by měl projít alespoň částečnou úpravou, a to nejen z pohledu zveřejnění kronik, ale z pohledu historických pramenů obecně. Archivy krom své klasické činnosti nyní musí plnit i funkci správce údajů. Jsou to instituce, které schraňují archivní materiál, díky kterým si běžní lidé mohli až do nedávna dohledávat svůj původ či se dozvídat zajímavosti o svých předcích.

V únoru po průzkumu stavu dodržování GDPR v rámci digitálních portálů jsem doufala, že vše bude co nejdříve uvedeno přesně do takového stavu, jaký by měl být dle GDPR a žádný archiv nebude muset čelit postihům a sankcím, které za nedodržení hrozí. Při druhém procházení digitálních archivů mnoho portálů prošlo značnou změnou a archivy začaly publikovat výsledky digitalizace, které jsou již v souladu s platným nařízením EU.

7 Závěr

Tématem, kterým se zabývala tato diplomová práce, bylo *„Analýza dopadu GDPR na archivnictví“.*

Cílem diplomové práce bylo přiblížit problematiku českého archivnictví v kontextu se zveřejňováním archiválií na portálech digitálních archivů v době po implementaci GDPR. Diplomová práce se důkladněji zaměřila na zpřístupňování kronik, které jsou z badatelského pohledu velmi zajímavým zdrojem informací. Došlo k potvrzení této teze i kvalitativním výzkumem.

Úvodní kapitola nastínila, jaký přínos má GDPR pro občana a jaký pro instituce v EU. Byly vymezeny rozdíly mezi osobními údaji, citlivými údaji a biometrickými údaji, jelikož jejich případné zveřejnění by mohlo mít následky pro osobu k niž by se údaje vztahovaly.

Následující kapitola se blíže zaměřila na činnost archivů jakožto správce údajů a jaké metodické pokyny mají k dispozici. Došlo k porovnání tří selektovaných metodik – metodického pokynu 3/2018 Ministerstva vnitra, metodického pokynu zpracovaného European Archives Group, jenž působí pod Evropskou komisí a souborem dokumentace vydané Národním archivem. Z pohledu množství informací je nejobsáhlejší metodika EAG a pokud dojde ke srovnání s metodikou MVČR, je tento rozdíl patrný. Rozdílné množství informací se odráží na přínosu metodiky MVČR pro archivy. Přesto přináší novou formu badatelského listu, která přesně uvádí, jakým způsobem je s osobními údaji badatelů nakládáno. Národní archiv se zasadil o přesnou informovanost a uvádí přesný výčet situací, kdy dochází ke zpracování osobních údajů badatelů i jak dlouho informace o badateli v archivu zůstanou. Přínosnost metodik potvrzuje rovněž i kvalitativní výzkum.

Třetí kapitola pojednávala o vlivu GDPR na české archivnictví. Zde byl kladen důraz na kroniky – došlo k popisu jejich struktury i způsobu, jakým s nimi je nakládáno před tím, než se ocitnou v archivech. Tato kapitola popisuje, jakým způsobem jsou kroniky vedeny i ukládány. Přitom naráží na problémy vznikající u činnosti zpřístupňování na portálech digitálních archivů. Zaměřuje se také na českou legislativní úpravu, která GDPR doprovází.

Čtvrtá kapitola započala výzkum srovnáním procesů, jenž musely být v digitálních archivem provedeny, aby byly dodrženy zásady GDPR a došlo tak k naprosté ochraně osobních údajů. Jelikož kontrola dosavadních digitálních archiválií na portálech je považována za jednu z největších komplikací, bylo zajímavé pozorovat, k jakým změnám se SOA uchylovaly. Nejracionálnějším přístupem bylo znepřístupnění digitálních archiválií mladších 100let. Tyto digitální archiválie byly podrobeny kontrole a v případě, že splňovaly zásady GDPR, mohly být znovu uvedeny jako přístupné na digitálním archivu – takto postupoval například SOA Třeboň. Striktněji se ke kontrole postavil SOA Litoměřice, který ze svého digitálního archivu odebral většinu archiválií z 20. století. Tato analýza poukázala na fakt, že absence sjednocujících postupů v případě anonymizace osobních údajů digitálních archiválií postihuje nejen zaměstnance archivu, kteří musí kontroly vykonávat, ale i badatele, kteří se nemusí dostat ani k těm digitálním archiváliím, ve kterých se zrovna žádné osobní údaje nenachází.

Pátá kapitola se zabývala implementací GDPR v Evropě, konkrétně u Slovenska, Rakouska, Německa, Belgie a Spojeného království Velké Británie a Severního Irska. Navzdory tomu, že implementace GDPR v českém prostředí byla médii popisována jako komplikovaná, výsledky srovnání poukazují na skutečnost, že se jedná o jednu z verzí GDPR, kterou lze považovat za zdařile uplatněnou. V porovnání se Slovenskem disponuje Česko kvantitativně větším počtem metodických pokynů. Avšak na počátku nevznikla přípravná metodika jako tomu bylo v Belgii či Velké Británii. Naše postihy jsou stále „pouze“ finanční a nikoli

po vzoru Německa i odnětí svobody, pokud se jedná o fyzické osoby. Rovněž se tato kapitola pokusila zhodnotit i dopad na zahraniční archivnictví, nicméně pro Německo a Slovensko nebyly dohledány relevantní a vhodné prameny. Lze se domnívat, že implementace GDPR do archivnictví bude podobná jako v ČR. Německo projevilo větší vůli předložit dokumenty s osobními údaji v mezích vědeckého, historického a statistického výzkumu. Zpracovatel může být vyzván k prokázání zájmu o zpracování, které musí převyšovat zájem subjektu údajů. Slovensko přijalo GDPR v jeho plném znění. Pokud by došlo k dalšímu výzkumu v oblasti implementace GPDR v zahraničí naskytuje se možnost oslovit konkrétní archivy (ekvivalenty Národního archivu ČR), zda by mohly poskytnout patřičné prameny k této problematice.

Výzkum pokračuje v šesté kapitole. Ta se zabývala kvalitativním šetřením na pozicích Státních oblastních archivů a nižších. Zaměstnanci na různých pracovních pozicích v SOA hodnotili stav implementace GDPR a jeho přijetí v českém archivnictví. I tato část výzkumu potvrzuje tezi z kapitoly 2. Respondenti se shodli, že podpora MVČR není vyhovující. Většina respondentů se uchýlila k vytvoření vlastních vnitřních předpisů na základě české legislativy – konkrétně archivního zákona 499/2004 Sb., a zákona o zpracování osobních údajů 110/2019 Sb. Za hlavní problém splnění podmínek GDPR je z pohledu respondentů považována náročnost kontroly archiválií a s tím spojené vnitřní procesy. V tomto ohledu se jedná o časovou náročnost při anonymizaci archiválie, jenž obsahuje osobní údaje. Pro badatele to znamená delší prodlevu od podání žádosti o předložení archiválie k jejímu fyzickému vydání. Šetření nepotvrdilo ani hypotézu, zda jsou ti respondenti, kteří absolvují školení spokojeni s podporou MVČR. Zajímavé byly reakce respondentů na otázku, jakou změnu by v legislativně udělali, pokud by mohli. Nejvíce by ocenili zavedení jednotné lhůty, kdy mohou být kroniky zveřejňovány (nabízí se zde 80 let, což je průměrná délka dožití v ČR podle Českého statistického úřadu).

Archivy se snažily reagovat na GDPR co nejaktuálněji. Mnohdy jejich kroky vedly sice k naplnění cílů GDPR, ale to odnesli opět badatelé Rychlé jednání znamenalo stáhnout veškerý zdigitalizovaný materiál a provést kontrolu. Některé SOA znepřístupnily pouze vymezené časové období – většinou to byla doba 100let od posledního zápisu. Jiné je z portálů digitálních archivů odebrali úplně.

Diplomová práce splňuje cíle vymezené v úvodu a některé části ještě rozšiřuje. Téma GDPR v archivnictví se neustále vyvíjí a je zde prostor na další pokračování výzkumu (například kapitolu *6 Vnímání GDPR v Oblastních archivech v ČR*). Více než půl roční mapování digitálních archivů stále neposkytlo všechna data. Bylo by zajímavé zkoumat skrze dotazníkové šetření i názory, jaké mají na problematiku GDPR specialisté zabývající se digitalizací ve zkoumaných oblastech. I když vzhledem k nečekané koronavirové krizi, po jejíž dobu probíhalo dotazníkové šetření, bylo sesbírání mnohem méně odpovědí, než by tomu bylo v běžném stavu. Lze se domnívat, že vzorek byl i tak dostačující a pomohl získat odpovědi na vybrané otázky z tohoto výzkumu.

8 Seznam použitých pramenů a literatury

8.1 Literatura

ČTVRTNÍK, Mikuláš. Právo být (ne)zapomenut: inflace soukromí, vy(zne)užívání dat a prekérní situace archivů v mladém 21. století – podněty κ diskusi. Archivní časopis. Praha. Ministerstvo vnitra České republiky – Sekce archivní správy, 1951-, 2018(68). ISSN 0004-0393.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volnem pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Brusel. 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.

NEZMAR, Luděk. GDPR: *Praktický průvodce implementací*. Praha: GRADA, 2017. ISBN 978-80-271-0668-4.

PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a kolektiv. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě.* Praha 2: Leges, 2018. ISBN 978-80-7502-288-2.

Pokyn ředitele SOA v Zámrsku ze dne 25. srpna 2010 č. 1/2010, Digitalizace archiválií, archivních pomůcek a vybraných dokumentů.

Zákon č. 110/2019 Sb. o ochraně osobních údajů. In: Sbírka zákonů České republiky. 2019, částka 47. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=63840.

8.2 Elektronické zdroje

MZA BRNO. *Acta Publica* [online]. Brno: Moravský zemský archiv v Brně, ©2010 [cit. 2019-11-09]. Dostupné z: http://actapublica.eu/aktuality/.

BERTELS, Natalie. *Scientific research under the GDPR: what will change?* [online]. 2016. Dostupné z: https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/.

CAPGEMINI RESEARCH INSTITUTE. *Seizing the GDPR Advantage: From mandate to high-value opportunity* [online]. 2018 [cit. 2020-02-22]. Dostupné z: https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf.

CIBULKA, Jan. *Bez několikaletého čekání na soud. Nově bude právo na informace posuzovat Úřad pro ochranu osobních údajů*. Český rozhlas [online]. Praha, 2019 [cit. 2020-03-02]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/informace-uoou-soud-zakon-rychlost_1912250600_cib.

ČESKÁ ARCHIVNÍ SPOLEČNOST: *GDPR a obecné trendy a překážky v akvizici a zpřístupňování archiválií s osobními údaji*. In: Osobní údaje v archivnictví [online]. Plzeň, 23. 4. 2019 [cit. 23. 7. 2020]. Dostupné z: https://www.youtube.com/watch?v=BPAarJgAN-4.

ČESKO. § 12a odst. 1 písm. i) vyhlášky č. 645/2004 Sb., vyhláška, kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 23. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-645#p12a-1-i.

ČESKO. § 14 zákona č. 110/2019 Sb., o zpracování osobních údajů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 22. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110#p14.

ČESKO. § 37 odst. 11 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499#p37-11.

ČESKO. Zákon č. 132/2006 Sb., o kronikách obcí. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 23. 7. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-132#p1.

ČESKÁ ASOCIACE OCHRANY OSOBNÍCH ÚDAJŮ. *GDPR pro malé a střední podniky: Nový německý zákon o ochraně osobních údajů* [online]. Praha, ©2020 [cit. 2020-06-11]. Dostupné z: http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/.

ČTK, iDNES.cz *Podle novely už novináři nemusí každého demonstranta žádat o souhlas. IDnes.cz* [online]. Praha: ČTK, iDNES.cz, 2019, 2019 [cit. 2020-03-19]. Dostupné z: https://www.idnes.cz/zpravy/mediahub/gdpr-evropska-unie-novinar-vedec.A190425_101540_mediahub_jpl.

DUŠEK, Radim. *Vedení kronik: Obecní kronika*. Východočeské archivy [online]. [cit. 2020-07-23]. Dostupné z: https://vychodoceskearchivy.cz/ustinadorlici/vedeni-kronik/.

EPravo: *GDPR* [online]. Praha, 2017, 16. 8. 2017 [cit. 2020-06-11]. Dostupné z: https://www.epravo.cz/top/clanky/gdpr-106244.html.

EUROPEAN ARCHIVES GROUP. *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* [online]. Brusel, 2018, Říjen 2018.[cit. 2020-06-26]. Dostupné z: https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.

EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679* [online]. Brusel, 2017, [cit. 2020-02-09]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886.

GDPR SOLUTIONS: *Jaké plynou z gdpr výhody pro občany?* [online]. Praha, ©2020 [cit. 2020-02-22]. Dostupné z: https://www.gdprsolutions.cz/narizeni-gdpr/vyhody-pro-obcany/.

GDPR.cz: *Obecné nařízení o ochraně osobních údajů prakticky* [online]. Praha [cit. 2019-11-07]. Dostupné z: https://www.gdpr.cz/.

GIL, Eran. The GDPR in Germany: Data Processing for Research & Statistical Purposes [online]. Berlín, ©2020, 16. 8. 2017 [cit. 2020-06-11]. Dostupné z: https://allcloud.io/blog/gdpr-in-germany-are-you-covered/.

HEJLÍK, Ladislav. *Stanovisko Úřadu pro ochranu osobních údajů*. Praha, 2018. Dostupné také z: http://www.smocr.cz/getFile.aspx?itemID=967832.

HROMÁDKA, Tomáš. *Kroniky obcí* [online]. Praha, 2014, 62 [cit. 2020-07-25]. ISBN 978-80-7068-280-7. Dostupné z: https://invenio.nusl.cz/record/358316/files/nusl-358316_1.pdf.

INFORMAČNÍ LIST: *Bulletin pro otázky elektronické spisové služby a dokumentů v digitální podobě*. In: Národní archiv ČR [online]. Praha, 2019, 26. června 2019 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/07/InfoList_201904-oprA.pdf.

LI, He, Lu YU a Wu HE. *The Impact of GDPR on Global Technology Development*. Journal of Global Information Technology Management [online]. 2019 (22), 1-6 [cit. 2020-02-22]. DOI: 10.1080/1097198X.2019.1569186. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186?scroll=top&needAccess=true.

MATEJKA, J., Matochová, S. a Prokeš, J. *Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů*. Acta Informatica Pragensia, 2019, vol. 8, iss. 2, p. 88-111. [cit. 2020-03-02]. DOI: 10.18267/j.aip.126. Dostupné z: https://journals.muni.cz/revue/article/view/8801/pdf.

MUNIS.CZ. *Zákon o zpracování osobních údajů a spisová služba* [online]. Praha, © 2020 [cit. 2020-07-22]. Dostupné z: https://www.munis.cz/art/654.

MVČR. MVČR: *Ochrana osobních údajů* [online]. Praha: Ministerstvo vnitra ČR, ©2019 [cit. 2020-01-05]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx.

MVČR. *Implementace GDPR na Slovensku* [online]. Praha: MVČR, 2018, 21. ledna 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/implementace-gdpr-na-slovensku.aspx.

MVČR. *Implementace GDPR v Rakousku: Zákon mezi prvními* [online]. Praha: MVČR, 2018, 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/gdpr-v-rakousku-pdf.aspx.

MVČR. Implementace GDPR ve Velké Británii: *Ambice nejbezpečnějšího kyberprostoru* [online]. Praha, 2018, červen 2018 [cit. 2020-06-11]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/implementace-gdpr-ve-velke-britanii-pdf.aspx.

MVČR. *Metodický pokyn č. 1/2020 k archivnímu zpracování fondů typu „Archiv města"* [online]. Praha: MVČR, 2020 [cit. 23. 7. 2020]. Dostupné také z: https://www.mvcr.cz/soubor/metodicky-pokyn-c-1-2020-k-archivnimu-zpracovani-fondu-typu-archiv-mesta.aspx.

MVČR. *Metodický pokyn č. 3/2018* [online]. Praha: MVČR, 2018, 1. června 2018 [cit. 2020-06-02]. Dostupné z: https://www.mvcr.cz/soubor/metodicky-pokyn-c-3-2018.aspx.

MVČR. *Metodický pokyn č. 3/2018: Badatelský list* [online]. 1. června 2018 [cit. 2020-06-02]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-1-badatelskeho-listu.aspx.

MZA Brno. *Moravský zemský archiv v Brně* [online]. Brno [cit. 2020-02-07]. Dostupné z: http://www.mza.cz/a8web/a8Apps1/soka/sokauh/A8SL4DD2Bad3SOKAUH.html.

MZA Brno. *Ochrana osobních údajů a spisová služba veřejnoprávních původců* [online]. Brno: MZA Brno, 2018 [cit. 2020-03-20]. Dostupné z: http://www.mza.cz/informace-metodicke-materialy.

NÁRODNÍ ARCHIV. *Ochrana osobních údajů/GDPR* [online]. Praha [cit. 2020-07-05]. Dostupné z: https://www.nacr.cz/uredni-deska/ochrana-osobnich-udaju-gdpr.

NÁRODNÍ ARCHIV. *K problematice aktualizace spisových řádů veřejnoprávních původců v roce 2018*. In: Národní archiv ČR [online]. Praha, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/spisovy-rad-novelizace.pdf.

NÁRODNÍ ARCHIV. *Ochrana osobních údajů/GDPR* [online]. Praha [cit. 2020-07-05]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2020/04/GDPR_priloha.pdf.

NÁRODNÍ ARCHIV. *Sbírka interních aktů řízení ředitelky Národního archivu: Bulletin pro otázky elektronické spisové služby a dokumentů v digitální podobě*. In: Národní archiv ČR [online]. Praha, 2015, 21. července 2015 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/02/badatelsky-rad-pokyn.pdf.

PIFFL, Robert. *Dopady GDPR na informační systémy a evidenci elektronických dokumentů*. In: Národní archiv ČR [online]. Praha: MVČR, 2018 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/1_GDPR_archivy_01_18.pdf.

POKORNÝ, Jakub. *Nová překážka při tvorbě rodokmenu: GDPR. Archivy stahují data z internetu*. In: iDnes.cz - Zpravodajství [online]. 2018, č. 238 (26.08.2018) [cit. 2020-01-16], Dostupné z: https://www.idnes.cz/zpravy/domaci/gdpr-rodokmen-archivy.A180817_095322_domaci_jumi.

SCHÖGGL-ERNST, Elisabeth. *Die Auswirkungen der Datenschutzgrundverordnung auf Archive in Österreich. Atlanti* [online]. Gratz, 2018, 28. 2. 2018, 2018(2), 123-130 [cit. 2020-07-26]. DOI: https://doi.org/10.33700/2670-451X.28.2.123-130(2018). Dostupné z: http://journal.almamater.si/index.php/Atlanti/article/view/305/281.

SOA PRAHA. *Plán práce 2020* [online]. Praha: Státní oblastní archiv v Praze, 2020, 30. ledna 2020 [cit. 2020-07-26]. Dostupné z: http://www.soapraha.cz/Files/plán%20soap2020.pdf.

STATE ARCHIVES OF BELGIUM. *Personal Data and Archives* [online]. Brusel: State Archives of Belgium, 2020 [cit. 2020-07-26]. Dostupné z: http://arch.arch.be/index.php?l=en&m=practical-information&r=data-protection&sr=personal-data-and-archives.

Statní okresní archiv Hradec Králové [online]. Hradec Králové [cit. 2019-11-09]. Dostupné z: https://vychodoceskearchivy.cz/hradeckralove/4270-2/kroniky/.

Svaz měst a obcí České Republiky [online]. Praha, ©2019 [cit. 2019-11-12]. Dostupné z: http://www.smocr.cz/cz/oblasti-cinnosti/gdpr/vedeni-obecnich-kronik-v-souladu-s-pravidly-gdpr.aspx.

ŠIMŮNKOVÁ, Karolína a Jiří ÚLOVEC. *GDPR v archivní praxi: Setkání archivů* [online]. Národní archiv, 2019, 18.01.2019 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/2_GDPR_v_archivni_praxi.pdf.

ŠIMŮNKOVÁ, Karolína. *GDPR – spisová služba a původci v předarchivní péči Národního archivu* [online]. Národní archiv, 2017, 22.11.2017 [cit. 2020-07-19]. Dostupné z: https://www.nacr.cz/wp-content/uploads/2019/01/GDPR_sylabus.pdf.

ŠKORNIČKOVÁ, Eva. *Adaptační legislativa byla schválena* [online]. Praha, 2019, 5. 5. 2019 [cit. 2020-07-22]. Dostupné z: https://www.gdpr.cz/blog/adaptacni-legislativa-byla-schvalena/.

THE NATIONAL ARCHIVES. *Archives and data protection law in the UK – an overview* [online]. Londýn: The National Archives, 2020 [cit. 2020-07-26]. Dostupné z: https://www.nationalarchives.gov.uk/archives-sector/legislation/archives-data-protection-law-uk/overview/.

ÚOOÚ. *Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů*. In: Ministerstvo vnitra České republiky [online]. Praha, ©2019 [cit. 2019-11-10]. Dostupné z: http://www.mvcr.cz/gdpr/soubor/gdpr-sesit-pdf.aspx.

ÚOOÚ: *Nebojte se GDPR*. UOOU [online]. Praha, ©2013 [cit. 2020-01-28]. Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32682.

ÚOOÚ. *Desatero zpracování pro správce – archiv dokumentů.* Úřad pro ochranu osobních údajů [online]. Praha: Úřad pro ochranu osobních údajů, ©2013 [cit. 2020-06-02]. Dostupné z: https://www.uoou.cz/desatero-zpracovani-pro-spravce/ds-4821/archiv=2&p1=3938.

Úřad na ochranu osobních údajů Slovenské republiky: *Archívna informácia – Metodické usmernenia* [online]. Bratislava: Úrad na ochranu osobných údajov Slovenskej republiky, 2020 [cit. 2020-06-11]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/archivna-informacia-metodicke-usmernenia.

Úřad na ochranu osobních údajů Slovenské republiky: *Metodiky a FAQ* [online]. Bratislava: Úrad na ochranu osobných údajov Slovenskej republiky, 2020 [cit. 2020-06-11]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/main-content/metodiky-uradu?page=2.

Ústav pro studium totalitních režimů [online]. Praha, © 2020 [cit. 2020-07-16]. Dostupné z: https://www.ustrcr.cz/o-nas/.

Vyhláška č. 85/2019 Sb., kterou se mění vyhlášky provádějící zákon o archivnictví a spisové službě. 2019. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-85.

YAMPOLSKIY, Roman V., GOVINDARAJU, Venu. *Taxonomy of Behavioural Biometrics.* InWNAG, Liang, GENG, Xin (eds.). *Behavioral Biometrics for Human Identification: IntelligentApplications*. IGI Global, August 2009. doi:10.4018/978-1-60566-725-6. Dostupné z: https://www.igiglobal.com/book/behavioral-biometrics-human-identification/99#table-of-contents-

9 Seznam tabulek a obrázků

10 Seznam příloh

Příloha č. 1 - Metodický pokyn č. 3/2018

Příloha č. 2 - Metodika European Archives Group

Příloha č. 3 - Zpracování osobních údajů v NA – tabulka

Příloha č. 4 - Dotazníkový formulář využitý v kvalitativním výzkumu

Příloha č. 5 - Spisová služba a původci v předarchivní péči Národního archivu

Příloha č. 6 - Příklad standardizovaného formuláře u SOA Třeboň

Příloha č. 7 - Příloha badatelského listu NA

Příloha č. 1 –Metodický pokyn č. 3/2018

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX03ZEZSC
prvotní identifikátor

odbor archivní správy a spisové služby
Nad Štolou 3
170 34 Praha 7

Č. j.: MV- 62832-1/AS-2018

Praha 1. června 2018

Metodický pokyn č. 3/2018

upravující problematiku poskytování osobních údajů badatelů archivům cestou badatelských listů v souladu s nařízením Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR")

Tento metodický pokyn upravuje řešení uvedené problematiky formou nové přílohy badatelského listu „Příloha č. 1", která obsahuje poučení pro badatele ve smyslu nakládání s jeho osobními údaji, poskytovanými správci osobních údajů (archivu). Poučení definuje správce údajů, poskytuje kontaktní údaje pověřence pro ochranu osobních údajů, definuje účel zpracování osobních údajů a dobu jejich uložení. Rovněž obsahuje poučení badatele (subjekt údajů) o rozsahu jeho práv v intencích GDPR.

Na základě tohoto metodického pokynu se zavádí „Příloha č. 1". Formulář přílohy k doplnění údajů konkrétním archivem je jeho přílohou, resp. jeho nedílnou součástí. Svým podpisem badatel stvrdí, že uvedené poučení vzal na vědomí.

Metodický pokyn nabývá účinnosti dnem 1. června 2018.

PhDr. Jiří Úlovec
ředitel

Příloha č. 2 –Metodika European Archives Group

EUROPEAN ARCHIVES GROUP

GUIDANCE
ON DATA PROTECTION FOR ARCHIVE SERVICES

EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector

These guidelines are intended to help archive services in Europe apply the General Data Protection Regulation. They are a work in progress, subject to improvement and enrichment, thanks to your experience and comments. These guidelines may also be amended on the basis of future jurisprudence and of opinions and guidelines issued by the European Data Protection Board.

The European Archives Group warmly welcomes your comments. Comments can be sent to the following e-mail address: SG-EAG-GUIDELINES@ec.europa.eu.

LEGAL DISCLAIMER

This document is not intended to provide, and does not constitute or comprise, legal advice on any particular matter and is provided for general information purposes only. You should not act or refrain from acting on the basis of any material contained therein, without seeking appropriate legal or other professional advice.

Title: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector
Author: © European Archives Group
Date: October 2018

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS USED IN THESE GUIDELINES

DIRECTIVE 95/46/EC: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

DPA: Data Protection Authority

DPO: Data Protection Officer

EAG: European Archives Group

EDPB: European Data Protection Board

GDPR: General Data protection Regulation, i.e. the *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

I. INTRODUCTION

1. **Audience:** these guidelines are addressed to public and private institutions that hold archives, i.e. records that have been selected for permanent preservation. They are not only addressed to National Archives or to State Archives but also to Regional and Municipal Archives, museums, libraries, foundations and other public and private entities that preserve archives.

2. **Goal:** these guidelines are intended to provide basic information and practical guidance to archivists regarding the specific challenges for the application of the General Data Protection Regulation (GDPR) in the archival sector.

3. **Scope.** Just like any other public and private entity, archive services process personal data regarding their own personnel. These Guidelines do not provide guidance for processing of personal data by an archive service in its role as an employer. Nor do these Guidelines provide guidance for the processing of personal data of users, of donors, of contractors, and so on and so forth. National Data Protection Authorities and national governments, the European Commission, the European Data Protection Board and other actors are already providing guidance on such matters (see the Appendix: *Where to look for further guidance*). These Guidelines focus exclusively on the processing of personal data contained in archival fonds.

4. The **GDPR: the same rules across the EU (but with exemptions for the archives sector).** An EU regulation is a binding legislative act which must be applied in its entirety across the Union. The EU decided to adopt a regulation – instead of another directive – to replace the previous data protection legislation (EU Directive 95/46/EC[1]) in order to have more uniform norms across all Member States. However, the GDPR leaves some room for Member States to introduce exemptions in specific areas. One of them is for "archiving purposes in the public interest"; another one is for historical research. Archivists have to see if their national lawmakers have made use of the opportunity that the GDPR provides to issue such exemptions.

5. **Data minimisation vs permanent preservation**. A key principle of the GDPR is data minimisation. It is actually not new: Directive 95/46/EC was already predicated on this principle. Personal data should be collected and processed only if it is really necessary to do so and should be "kept in a form which permits identification of data subjects" (i.e. the person to whom the data relate) only as long as it is necessary in order to achieve the purpose for which the personal data was collected (art. 5(1) points (b) and (e)). If no exceptions to this principle were allowed, in the future we would no longer have archives containing personal data. But EU lawmakers did introduce some exemptions to this rule. They acknowledged that archives are necessary to enforce fundamental rights. In fact, the GDPR states that "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes". However, this is subject to the condition that appropriate measures are

[1] *Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

taken "in order to safeguard the rights and freedoms of the data subject" (art. 5(1) point (e)).

6. **Processing personal data only when it is really necessary to do so is nothing new for archivists**. One of the key archival functions is the selection of documents for permanent preservation. Only a very small percentage of the documents created or received by the State and other public administrations, or by private entities in the course of their activity, ends up in archival institutions. Archivists select for permanent preservation only documents that are necessary to enforce citizens' rights and for historical research. Archival institutions should publish the general criteria that they apply for the selection of documents for permanent preservation and should be able to explain why they decided to retain specific archival fonds containing personal data.

7. **Storing personal data is not the same as providing access**: In all EU Member States national legislation sets rules regarding access to documents kept in public archives. The closure period for documents containing personal data changes from one country to the next and according to the nature of the personal data. In Italy, personal data that reveal racial or ethnic origin, religious and political opinions, membership of parties, trade unions, are closed for 40 years, while those disclosing health and sex life are closed for 70 years; and records that can reveal the identity of a mother who wanted to give birth anonymously are closed for 100 years. The closure period can be even longer; for example, in Romania, medical records and civil status registers are closed for 100 years after their creation, while documents regarding the private life of an individual are closed for 40 years after the data subject's death. Citizens can trust archive services: they will not disclose their personal data unduly.

8. **The GDPR does not change the closing period of documents containing personal information**. The Regulation includes provisions regarding the right of data subjects to access the data that concern them. It does not include rules regarding access to archives by the general public. The closing periods of documents containing personal data will remain the same.

9. **The GDPR does not modify freedom of information laws**. The Charter of Fundamental Rights of the European Union[2] considers both the protection of personal data and freedom of expression and information (which includes freedom to receive and impart information) as fundamental rights. The GDPR does not modify freedom of information laws. It states that "Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject." (recital 154).

10. **The GDPR does not modify freedom of expression laws.** Users of archives include, among others, journalists, academics and other researchers from all walks of life who will, in many cases, publish their findings. The GDPR does not change press laws and other rules concerning freedom of expression. It states that: "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary

[2] 2000/C364/01

expression" (art. 85). Member States may provide certain exemptions or derogations to provisions of the GDPR for this purpose (art. 85).

11. **These guidelines are not a code of conduct**. The GDPR encourages "the drawing up of codes of conduct intended to contribute to the proper application" of the Regulation (art. 40.1). It furthermore provides that "Associations and other bodies representing categories of controllers or processors may prepare codes of conduct." (art. 40(2)) and dictates a specific procedure for the approval of codes of conduct by the national Data Protection Authority (if the code has only a national scope) or by the European Data Protection Board and by the EU Commission (if the code will apply in different EU Member States).

    The present Guidelines were drafted by the European Archives Group (EAG), a European Commission expert group composed of representatives from National Archives and Directorates-General of Archives of EU Member States. The Guidelines did not go through the approval procedure provided by art. 40 of the GDPR for codes of conduct. They should be considered a policy document.

II. GENERAL PRINCIPLES

1. GENERAL PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (ART. 5)

Archivists should be aware of some general principles regarding the processing of personal data laid out in art. 5 of the GDPR, which states:

> 1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
>
> 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

These principles have many practical consequences for archive services and should therefore always be kept in mind. Archivists are familiar with ensuring the principle of 'confidentiality' as it is standard practice in archive services to protect confidential information from unauthorised access. Some of the implications of such principles are nevertheless less obvious. For example:

- the principle of 'transparency' means – among other things – that archive services have to publish clear, user-friendly information on their mission, and in particular why and how they process personal data, and how data subjects can access them.
- the principle of 'integrity' means – among other things – that archival malpractice that leads to the loss of documents containing personal data constitutes not only a

violation of archival professional principles and archival laws, but also a violation of the GDPR.

2. LAWFULNESS OF PROCESSING (ART. 6)

Under the GDPR the processing of personal data is legitimate only if at least one of the specific circumstances listed in art. 6 applies, including: "the data subject has given consent to the processing of his or her personal data"; "processing is necessary for the performance of a contract to which the data subject is party"; the "processing is necessary for compliance with a legal obligation to which the controller is subject", etc. Of special interest to archivists is the condition laid out at (1) point (e)), that processing of personal data is legitimate if it "is necessary for the performance of a task carried out in the public interest".

The GDPR leaves it to EU law or national law to determine which kind of activities are considered as being "in the public interest". National law can include provisions that define the processing of archives by a given institution, or the processing of certain categories of archives to be "a task carried out in the public interest".

3. THE GDPR PROTECTS ONLY PERSONAL DATA OF LIVING PERSONS (BUT NATIONAL LAW CAN PROTECT ALSO THE DATA OF DECEASED PERSONS)

The GDPR protects personal data of living persons. It does not apply to the personal data of deceased persons. However, archivists should consider that national laws may do so. The GDPR in fact stipulates that "Member States may provide for rules regarding the processing of personal data of deceased persons" (recital 27).

How can archivists know whether a data subject is deceased? In most cases they cannot. However, they can reasonably assume that persons born more than one hundred years ago are no longer alive. For example an archivist processing personal files of soldiers who fought in Word War I can assume that they are no longer alive and that the GDPR does not therefore apply to those files. Many other cases will, however, not be so clear cut. Archivists will have to make case-by-case assessments of the possibility that archival fonds under their care contain personal data of living individuals.

III. WHAT IS "ARCHIVING PURPOSES IN THE PUBLIC INTEREST"?

4. DIFFERENT RULES FOR DIFFERENT ARCHIVES ("ARCHIVING PURPOSES IN THE PUBLIC INTEREST" UNDER RECITAL 158)

The GDPR allows for a number of exemptions in favour of "archiving purposes in the public interest". Recital 158 explains the meaning of this expression.

> "Public authorities or public or private bodies that *hold records of public interest* should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest." (emphasis added)

Which archive services fall under this definition? As one can see, it is not the nature of archives, but the mission of the institution that holds them that determines whether the exemption can be applied. It is safe to say that National Archives and other historical Archives run by the State or by other public bodies, carry out "archiving purposes in the public interest" according to the GDPR definition, as do the Historical Archives of the European Union.

In accordance with Member State law, other institutions preserving archives can also fall under this definition. For example, national law might dictate that a specific body has the mission of acquiring, preserving and making available to researchers the personal papers of writers; or it could create a museum on the history of science that includes among its tasks the acquisition and preservation of the personal papers of scientists. Member State law might create an institute for the history of a past authoritarian regime, whose mission includes the preservation of documentary heritage concerning the victims of political repression.

It is important to consider that when the GDPR refers to "national law" it does not mean only pieces of law approved by national parliaments. Recital 41 in fact stipulates that "Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament". The legal instrument that can assign to an entity the legal obligation to acquire, preserve, arrange and communicate archives can change from one country to another, in accordance with different constitutional systems. For example, it could be a national law, a regional law, a ministerial decree, and so on and so forth. At any rate, archivists should consider that an archive service or another cultural institution which has the statutory mission of acquiring, preserving and providing access to archives for general public interest, would fall under the definition of recital 158.

Not all the entities that preserve archives have a legal obligation to acquire them and thus not all of them fall under the definition of recital 158. In many cases, however, such entities have a clear cultural mission and preserve archives for the purpose of historical research. The GDPR allows for exemptions for processing of personal data for historical research, which are laid out throughout the Regulation and in particular in article. 89.

Finally, archivists should be aware that exemptions in favour of "archiving purposes in the public interest" concern only the processing of personal data included in the archival fonds that archive services keep. All of the other personal data processing carried out by archive services fall under the same rules that apply to any other public or private entity. In other words, when archive services process the personal data of users, or of students who participate in educational activities, or of participants to conferences and so on, they do not enjoy of any exemption to the rules.

5. SAFEGUARDS AND DEROGATIONS RELATING TO PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES (ART. 89)

Throughout the GDPR one can find many references to archives and historical research. Several articles that set out duties or prohibitions for the controller, in fact allow for exemptions when the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes.

Moreover, the GDPR includes an article specifically dedicated to "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" (art. 89). The first paragraph of this article lays down rules that are common for both processing of personal data "for archiving purposes in the public interest" and for processing for "scientific or historical research purposes or statistical purposes".

> 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Article 89 further states that

> 2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 (…)
>
> 3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 (…)

In both cases, the above mentioned derogations are possible

> (…) subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

The principle of data minimisation and the obligation of taking appropriate safeguards in order to protect data subjects' rights are therefore common to both "processing for archiving purposes in the public interest" and processing for "scientific or historical research purposes or statistical purposes". But the concrete application of these principles will be different in the different areas.

When doing medical research it is important to preserve the correlation of different medical data regarding a given patient but the identity of the patient is irrelevant. In this case, pseudonymisation of medical records would be an appropriate measure. However, an archive service that holds records in the public interest has to preserve the integrity of medical records selected for permanent preservation in the interest of the data subjects. For example, in recent times some countries were able to pay compensation to persons who had been subjected to compulsory sterilisation decades ago because the integrity of the medical records was guaranteed. European history provides for many other instances in which the integral preservation of documents containing personal data has been instrumental in restoring the rights of data subjects.

Enforcing the right to the truth and the right to remedy and reparation for victims of gross violations of human rights requires the integral preservation of archives

Victims of Fascist and Nazi persecutions or of the Nazi use of slave labour could be identified and indemnified because archives containing personal data had been preserved. The integral preservation of archives has been equally instrumental in returning confiscated properties after the fall of Communism. The GDPR encourages the integral preservation of archives documenting human rights violations. Recital 158 in fact states:

> "Member States should also be authorized to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes."

When they take decision about retention or disposal of records containing personal data, archivists should remember that personal data protection needs to be balanced against the right to justice, the right to the truth and the right to remedy and reparation for victims of gross violations of human rights.

Acknowledging that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes requires different kinds of measures in order to enforce the principle of data minimisation, the GDPR does not always require pseudonymisation but only when "those purposes can be fulfilled in that manner".

Archivists enforce the principle of data minimisation differently than scientists and statisticians. Firstly, they select records that contain personal data for permanent preservation only when it is really necessary to do so pursuant to the mission that the law assigns to their archive service. They furthermore enforce laws concerning access to archives, excluding access to documents that contain personal data for as long as their

national law requires. Statutory restrictions on access to archives differ from one country to another and for certain kinds of personal data the closure period can be as long as 120 years.

When documents that contain personal data become accessible, but there is still a chance that the data subject is alive, archivists abstain from any processing that could result in harm to the dignity of the data subject. They always keep art. 1 of the Charter of Fundamental Rights of the European Union in mind: "Human dignity is inviolable. It must be respected and protected." A concrete enactment of this principle is to abstain from publishing online archival documents or finding aids whose diffusion could harm the dignity of data subjects.

Archive services might also make use of pseudonymisation, but if practiced by archive services, pseudonymisation should be fully reversible and should be done in a way that does not endanger the evidential value of records. In case of personal data preserved for archiving purposes in the public interest, archive services should store unaltered original data in a protected storage facility and make a pseudonymised copy of personal data for access by researchers, if such purposes can be fulfilled in that manner.

Does the GDPR allow for the preservation of business archives containing personal data?

Some private companies preserve century-old archives including personal data, which are troves of information for historians. Will historians of the future be able to access similar archival sources? In other words, is the preservation of business archives containing personal data possible under the GDPR? There is no a simple answer to such a question.

Records created by private bodies can be processed for archiving purposes in the public interest just like those created by public bodies. Such processing, however, qualifies as "archiving purposes in the public interest" only if it is performed by a public or private body that has "a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest." (recital 158) What "legal obligation" means, differs in civil law countries and in common law countries.

Bodies that have a historical research mission, but do not have a legal obligation to acquire and process archives, can process business archives containing personal data for historical research purposes. Both the principle of "purpose limitation" and that of "storage limitation" (art. 5(1), points b) and e)) allow in fact for derogations not only for archiving purposes in the public interest, but also for historical research purposes. Such derogations are subject to implementation of appropriate measures in order to safeguard the rights and freedoms of the data subject. The interpretation of such provisions will become progressively clearer, as long as DPAs and the EDPB issue decisions and guidelines.

IV. DATA SUBJECTS' RIGHTS

6. THE HEART OF THE MATTER: GRANTING INDIVIDUALS CONTROL OVER THEIR PERSONAL DATA

One of the main goals of the GDPR is to grant individuals control over their personal data. For this reason, it provides them with a comprehensive set of rights regarding their own personal data (the right to know which data are processed and why, the right to access, to erase and to transfer them, etc.), which allow only limited exemptions. Archiving purposes in the public interest is a ground for derogation from most of data subjects' rights. In two cases – the right to information (art. 14) and the "right to be forgotten" (art 17) – the GDPR directly introduces derogations for archiving purposes in the public interest. In other cases, it allows member States to do so. As already mentioned, in fact, art. 89 allows member states to provide derogations from the rights referred to in articles 15, 16, 18, 19, 20 and 21. This means that archivists in different EU countries might have to obey to different laws, regarding some data subjects' rights.

In all such cases, exemptions are not absolute, but subject to the safeguards provided by art. 89(1), i.e. technical and organizational measures aimed at enforcing the principle of data minimisation, and the protection of the data subject's rights and freedoms. Moreover, archive services should allow data subjects to have the widest possible control over their data. This principle has special relevance when archive services preserve the personal papers of living individuals, who donated, sold or deposited them in archive services; or when archive services preserve oral interviews collected during oral history projects. Archive services, however, cannot accommodate data subjects' requests, if that would imply violating the archive services' statutory mission of preserving the integrity of archives and of arranging, describing and making them available to the public.

7. INFORMATION TO BE PROVIDED WHERE PERSONAL DATA HAVE NOT BEEN OBTAINED FROM THE DATA SUBJECT (ART. 14)

The GDPR states that the controller has to provide data subjects with certain information regarding the processing that he or she carries out. This is applicable even if the controller did not obtain the personal data directly from the data subject, as set out in article 14. This is generally the situation of archive services which process documents containing personal information that they did not collect, but were collected by the entity that created the archive.

However, the GDPR allows for some exemptions, and one concerns archives. Article 14 states in fact that the obligation to provide information to data subjects where personal data were not obtained from the data subject does not apply when it would be "impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes". In such cases, art. 14 explicitly encourages controllers to make the information about the processing publicly available.

When archive services acquire, arrange, describe, preserve and make available to researchers archival fonds containing personal data regarding an indefinite number of

persons, to the extent that informing data subjects about such processing would be "impossible or would involve a disproportionate effort", the best line of action seems to make information about such processing available on the web site of the archival service, so that the general public can learn about it.

In some cases, a more focused effort to inform data subjects might be undertaken. For example, if an archive service acquires the archive of an association, a political party or a trade union, that processed personal data only of its associates, it might agree with them to use their information channels (newsletters, websites, mailing lists, etc.) in order to inform their associates about the processing that the archive service will perform.

Art. 14 includes a detailed list of the pieces of information that controllers should provide to data subjects when personal data have not been obtained from them. In a nutshell, archive services should explain in terms easily understandable by someone who knows nothing about archives, what kind of data processing they perform and why, and what is the legal basis for that. Moreover, they should inform data subjects how they can access their data and also explain that archival fonds are accessible to users, subject to the statutory limitations on access to records containing personal information. Finally, if data subjects contact archive services to ask for information about the kind of processing they perform, archivists should be prepared to provide data subjects with all possible information about that.

8. RIGHT OF ACCESS BY THE DATA SUBJECT (ART. 15)

As a rule, data subjects have a right to obtain confirmation from the controller whether or not personal data concerning him or her are being processed. Moreover, data subjects also have the right to know the purposes of the processing, the categories of personal data concerned and other information regarding the processing of their personal data.

Archive services process large amounts of personal data that have been collected by other entities. When these entities transfer their records to an archive service, they should transfer finding aids as well to allow archive services to know, among other things, which personal data the transferred records contain. It nevertheless frequently happens that archive services receive transfers without detailed finding aids but with only a generic transmission list. As a consequence, archivists cannot know which personal data are included in the transferred records. Moreover, archive services often receive archives that have lost their original order and require a careful work of arrangement to restore it.

These conditions create objective difficulties in enforcing some of the rights of data subjects' provided by the GDPR. The GDPR acknowledges this and, as already mentioned, article 89 provides that Union law or member states law may introduce derogations from the rights of data subjects.

Archivists should therefore verify if national law introduced derogations from the data subjects' right of access provided by article 15 of the GDPR. Such derogations protect archivists from liability if they are unable to fully comply to requests from data subjects for information about the processing of their personal data by an archive service. However, these derogations do not exempt archivists from doing their best to comply with such requests from data subjects.

If a data subject approaches an Archive service in order to access his/her personal data, archivists should provide all possible assistance by explaining how to do research in the archives, indicating the archival fonds most likely to contain personal data and by explaining how to consult finding aids and submit requests to consult files. If the data subject has specific difficulties in doing research due to old age, level of literacy or a physical impediment, archive services will provide special assistance, to the extent of the possible, taking into account constraints such as the number of staff.

9. RIGHT TO RECTIFICATION (ART. 16)

Art. 16 of the GDPR stipulates that data subjects have the right to have their personal data rectified if they are inaccurate and completed if they are incomplete. The controller has to comply with data subject's requests "without undue delay".

Archive services must guarantee the integrity of archives in order to retain the evidential value of documents. This is necessary to protect the rights of data subjects. For example, police files of repressive regimes typically include derogatory information about political opponents. Maintaining the integrity of such files is necessary to allow data subjects to request indemnification for the discrimination they suffered at the hands of the repressive regime.

The GDPR allows to reconcile the responsibility of archive services to maintain the integrity of documents, and the right of data subjects to have incomplete personal data completed. Rectification can be achieved by "providing a supplementary statement". Moreover, as already mentioned, article 89 provides that Union or Member State law may introduce derogations from the rights of data subjects' provided by article 16.

Archive services shall facilitate the exercise of a data subject's right to have their data updated, rectified or supplemented by "providing a supplementary statement" and ensure that the data are kept in a way allowing the original source material to remain separate and distinct from any such supplementary information.

10. RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN') (ART. 17)

The "right to be forgotten" within the EU was first stated in the 2014 landmark decision by the Court of Justice of the European Union in the Google Spain case. The Court ordered Google Spain to remove two reports on insolvencies from search results regarding a Spanish citizen, Mario Costeja González. The reports had been legitimately published by a newspaper in 1998 and continued to appear prominently when searching Costeja's name. The Court's decision left intact both the analogue and digital archives of the newspaper. It applies only to the result when searching Costeja's name with Google (the reports remain retrievable when using other search terms). Following the Court decision, persons can request that personal data relating to them (if they are inadequate, irrelevant or no longer relevant) are delinked from search engines so that such data will no longer appear if one searches their name.

The decision by the EU Court of Justice in the Google Spain case was grounded on Directive 95/46/EC which did not explicitly include a "right to be forgotten". By contrast,

the GDPR uses this expression in the title of article 17 "Right to erasure ('right to be forgotten')".

Under the GDPR, the right to be forgotten does not refer to delinking but to the actual erasure of the personal data. Article 17 grants in fact data subject the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

This right can apply where "the personal data are no longer necessary in relation to the purposes for which they were collected" or where "the data subject withdraws consent" on their processing, as well in some other circumstances. At the same time the right to be forgotten is subject to different restrictions, and it shall not apply if processing is necessary for archiving purposes in the public interest, if erasure "is likely to render impossible or seriously impair the achievement of the objectives of that processing" (art. 17(3)).

Recital 158 explains that public authorities and other bodies that hold records in the public interest are services that have "the legal obligation" to process archives selected for permanent preservation. The erasure of personal data included in archive documents would thus make it impossible for these services to carry out the mission that the law assigns to them. The right of erasure in article 17 of the GDPR therefore does not apply to documents selected for permanent preservation by archive services that fall under the definition of recital 158.

At the same time, archivists should remember that the right to be forgotten as stated by the EU Court of Justice (i.e. not erasure, but delisting of personal data) can be enforced by archive services without prejudice to their mission. Delinking or delisting, or in other ways preventing the use of search engines to search for names in documents does not in fact affect the integrity of archive documents nor does it endanger their permanent preservation. Moreover, archive services can prevent name search of an online document, while keeping it retrievable by using search keys different from personal names.

In the first place, archive services must abstain from posting online archival documents or finding aids that contain personal data which could jeopardize the dignity of data subjects. Moreover, whenever they post archival documents or finding aids that contain personal data of living individuals online, they have to consider – according to the nature of the personal data – whether it would be appropriate to post them in a restricted-access area of their websites which is out of the reach of search engines. On a case-by-case basis, archivists will assess how to best balance their legal obligation to "describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest" (recital 158) with the principle of data minimisation (art. 5), which requires them to limit the processing of personal data to what is necessary.

11. RIGHT TO RESTRICTION OF PROCESSING (ART. 18) AND RIGHT TO OBJECT (ART. 21)

The GDPR grants data subjects both the right to obtain from the controller restriction of processing and the right to object to processing of personal data concerning him or her. What are the differences between such rights and what are their practical implications relevant for archive services?

Such rights share the same ultimate goal of granting individuals control over the processing of their personal data, but apply in different circumstances, and have different

consequences. What most matter to archivists, national law can introduce derogations from both such rights, in case of processing of personal data for archiving purposes in the public interest (art. 89(3)).

Under specific circumstances listed in art. 18(1), data subjects have the right to obtain the *restriction* of processing of their personal data. Of key relevance for archive services is that the restriction of processing does not prevent the storage of personal data (art. 18(2)). The preservation of archival documents, thus, cannot be the hampered by restriction.

Moreover, data subjects have the right to *object* to the processing of personal data concerning themselves, even if the processing "is necessary for the performance of a task carried out in the public interest". In that case, "the controller shall no longer process the personal data" (art. 21(1)). However, the controller can continue processing personal data, if he can demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject" (art. 21(1)). This provision might apply to the processing of archives in the public interest, but archivists should not take it for granted. It is advisable for them to keep informed on how Courts interpret this provision.

In the first place, archivists should verify if their national lawmakers made use of the possibility to introduce derogations from the rights to restriction of processing (art. 18) and to object (art. 21) and, in this case, if national law indicated which are the appropriate safeguards to the rights and freedoms of data subjects that archive services should take. If national law does not suggest the appropriate safeguards, archive services will consider, on a case-by-case basis, how to best enforce the principles relating to processing of personal data listed in art. 5 of the Regulation.

Finally, archivists should consider that

> Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. (art. 21(6))

This provision might be relevant for archivists who work in museums or other cultural institutes or organizations that preserve archives for reasons of public interest, but do not carry out "archiving purposes in the public interest" according to the definition of recital 158.

12. NOTIFICATION OBLIGATION REGARDING RECTIFICATION OR ERASURE OF PERSONAL DATA OR RESTRICTION OF PROCESSING (ART. 19)

The GDPR dictates that "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out (…) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort." (art. 19). As already mentioned, national law can introduce derogations from the rights of rectification or erasure or restriction of processing, in case of processing of personal data for archival purposes in the public interest. It is therefore unlikely that personal data included in archival fonds preserved by archive services will be the object of rectification or erasure or restriction of processing.

Moreover, national law can introduce a derogation from the obligation of notification as well, if personal data are processed for archival purposes in the public interest (art. 89(3)). Finally, archivists should consider that a data controller should comply with the obligation dictated by art. 19, "unless this proves impossible or involves disproportionate effort" and this might be very much the case for archive services.

13. RIGHT TO DATA PORTABILITY (ART. 20)

The GDPR grants data subjects "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" (art. 20(1)). Moreover, "the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible." (art. 20(2)) Archive services do not receive the personal data included in the archival fonds they hold directly from the data subject, except in the case of personal papers. Most of the archival fonds processed today by archive services are in analogue format, so transmitting the personal data they include to the data subjects in a "machine-readable format" would, by and large, not be "technically feasible".

Finally, archivists should be aware that national law can introduce derogations from the right of data portability if personal data are processed for archival purposes in the public interest (art. 89(3)).

V. PROCESSING CATEGORIES OF DATA THAT REQUIRE SPECIAL SAFEGUARDS

14. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The GDPR provides special protection to certain categories of personal data, the processing of which could create significant risks to the fundamental rights and freedoms of data subjects. It forbids the

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 9(1))

However, the GDPR allows for some derogations from this provision. The prohibition to processing of such sensitive data does not apply in cases where "processing is necessary for archiving purposes in the public interest" and for historical research. Such processing must be based on law and must be "proportionate to the aim pursued". Moreover, it must "respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." (art. 9(2) point (j))

For the most part, the provisions of article 9 are not new. Directive 95/46/EC already prohibited the processing of special categories of personal data, with some exemptions. The GDPR enlarged the categories of personal data deserving special protection, by adding "genetic data, biometric data for the purpose of uniquely identifying a natural person" to the list appearing in art. 9.

In accordance with national law in EU Member States, documents that contain special categories of personal data are excluded from access for extended periods, ranging from a few decades to a century or more. Archivists therefore already have a long and successful experience in applying laws that restrict access to special categories of personal data.

15. PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES (ART. 10)

The GDPR sets very strict rules regarding the processing of personal data relating to criminal convictions and offences and does not allow for any exemptions. Processing of such a kind of personal data can "be carried out only under the control of official authority or when the processing is authorised by Union or Member State law". The law must provide for "appropriate safeguards for the rights and freedoms of data subjects" (art. 10).

In EU Member States, national laws dictate that after a certain number of years – generally 20 or 30 years – court decisions, court files and prison records selected for permanent preservation are transferred to the National Archives or to other archival institutions. These archive services therefore process large amounts of data relating to

criminal convictions: they select them, transfer them to their repositories, arrange and describe them and make them available to researchers. This kind of processing is fully compliant with the GDPR because it is dictated by law and carried out by official authorities with appropriate safeguards for the rights and freedoms of data subjects. For example, if national law restricts access to court files for a given number of years, archivists carefully enforce such restrictions. If they publish on line freely-accessible documents relating to criminal convictions, and there is a chance that the data subjects are still alive, archive services can take measures such as posting such documents on a restricted-access area of their websites, or redacting names, pursuant the paramount principle of respecting and protecting the dignity of individuals.

If a public or private body (e.g. a university, foundation or civil society organisation) holds legal archives or copies of court files and court decisions or otherwise collects, preserves and makes available to researchers documents containing personal data relating to criminal convictions and offences (for example: an academic centre specialized in the study of terrorism or a community archive set up by anti-mafia activists), it should contact its national DPA to seek instructions about the appropriate safeguards for the rights and freedoms of the data subjects concerned.

VI. DATA SECURITY

16. DATA PROTECTION BY DESIGN AND BY DEFAULT (ARTICLE 25): WHAT DOES IT MEAN IN THE ARCHIVES?

Article 25 dictates that when they are planning the means for processing personal data, controllers have to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles". This is what the GDPR refers to as "data protection *by design*".

One of the fundamental data-protection principles is data minimisation. In fact, Article 25 further requires that controllers "implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed." (emphasis added)

Article 25 will apply particularly to the development of new information systems. In the archives, this may involve, for example:

- Creating a digital repository;
- Creating a data bank concerning birth records or other fonds containing personal information
- Creating an information system to manage the reading-room services
- Creating tools for on-line access

Archive services have to keep article 25 in mind when they plan the different kind of activities that typically archive services perform, i.e appraisal, arrangement and description, providing access to archives and communicating them.

Appraisal: Archive services adopt an appraisal policy that limits the permanent preservation of records containing personal data to what is really necessary, according to their mission. They put into practice Article 25 by carefully drafting retention plans that define which kind of files containing personal data have to be selected for permanent preservation. For archive services, retention plans are tools to demonstrate compliance with Article 25.

Arrangement and description: Archive services enforce the principle of personal data minimisation when they create finding aids. When they arrange and describe an archival fonds that includes personal data of living individuals concerning health, sex life, political opinions and other special categories of data, or data relating to criminal convictions, archive services must create a finding aid that shows real names, in order to be able to respond to possible requests of access by data subjects, and comply with other data subjects' rights. At the same time, for online research (in case their national law allows access to such records) archive services might create a version of the finding aid in which real names are replaced by pseudonyms, if their mission to provide access to archives can be fulfilled in this manner. Software for archival description that allows the creation of two different versions of a finding aid (one with real names and one with pseudonyms) is a tool for compliance with art. 25.

Providing access to archives: Archive services are obliged to ensure that access to records is managed appropriately and that correct organisational and technical safeguards are in place. Archive services have a long history of managing and facilitating access to records

and archives, through organisational controls such as the application for a reader's ticket, checking that the requested files are cleared for public inspection and limiting the number of files presented in the reading room.

In the electronic environment, the issues of access will be compounded due to the scale, variety and complexity of electronic records. In many cases large data cannot be manually checked and verified prior to access so safeguards and controls will have to be increasingly automated.

Supervising activities and collaboration with creators of archives. Within the EU, the nature of the relations between the entities that create the archives and archive services change from one country to the other, and according to public sector and private sector. In some cases State Archives have supervising or monitoring or counselling authority, in others they do not.

Relevant to archive services is the design of new systems by public bodies whose records may be transferred to the archive services in the future. The challenge may be with regard to the design of new information systems that endeavour to comply with GDPR, where the archiving in the public interest is not included in the initial planning stage. It is important, therefore, that archive services are involved in system design and planning, to ensure that at the appropriate time the records are able to be exported from the system or replicated for ingest and transfer to an archive service. Ideally, the information system should automatically take into account the final destination of the documents.

17. SECURITY OF PERSONAL DATA (ARTICLE 32-34)

SECURITY OF PROCESSING

A key principle of the GPDR is that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Article 32). This is the 'security principle'.

Doing this requires the controller and the processor to consider risk analysis, organisational policies, and physical and technical measures. They also have to take into account additional requirements about the security of the processing.

The controller and the processor can consider the state of the art and costs of implementation when deciding what measures to take, but these measures must be appropriate both to the circumstances and the risk posed by the processing.

The measures must ensure the 'confidentiality, integrity and availability' of the systems and services and the personal data that are processed within them. The measures must also enable the controller and the processor to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

The controller and the processor also need to ensure that they have appropriate processes in place to test the effectiveness of their measures, and undertake any required improvements.

RISK MANAGEMENT TECHNIQUES

The GDPR does not define the security measures that the controller and the processor should have in place. It requires them to have a level of security that is ‘appropriate’ to the risks presented by their processing. Before deciding what measures are appropriate, they need to assess their information risk through a formal risk management methodology.

PERSONAL DATA BREACHES

The GPDR creates a system of notification of personal data breaches (article 33). This notion of breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data" (Article 4(12)). This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller shall notify the personal data breach to the supervisory authority competent as soon as possible and, if possible, not later than 72 hours.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)).

The content of the notification is provided by the Article 33(3) of the GPDR.

SECURING THE PROCESSING OF PERSONAL DATA IN THE ARCHIVES AND SECURING FROM UNAUTHORISED ACCESS THE PERSONAL DATA HELD IN THE ARCHIVES

Archivists are responsible for the security of personal data in their care and, in accordance with existing professional practices, safeguard their integrity and authenticity and protect them from unauthorised access, alteration, loss, damage or destruction.

Records should be stored securely so that confidentiality is maintained at all times. Access should be provided only to those who have a need to know that can be satisfied within the law. Archival arrangements and provenance should not be compromised through the separation of personal and non-personal records.

The level of security should be appropriate and proportionate to the nature of the data and the harm that could arise from a breach in security. It must reflect professional standards and the utilisation of risk management techniques to assess the nature, level and impact of risks and the appropriate measures to be taken to protect the data.

Practical security measures to be considered include installing physical security devices such as intruder alarms, restricting access to secure areas, keeping a record of visitors and supervising their activities as far as possible. Electronic data should be secured, e.g. by means of software protection against viruses and Trojans, and password-controlled access for authorised users only. Personal data should be transmitted securely: encryption tools should be used for secure transmission of electronic personal data.

While archive services exist to preserve and provide access to documents, they must not disclose documents containing personal data unless they can reconcile the requirements of research, whether historical or for evidence, with the rights and fundamental freedoms of data subjects.

WHAT ARCHIVISTS MIGHT DO/SHOULD DO IN CASE OF A DATA BREACH?

In the event of a serious breach arising from the processing – be it storage, access, communication… – of documents, archive services must consider whether the breach is likely to cause significant damage to the interests of living data subjects. If so, notification of the breach should be considered under the terms of article 34(3) point (c) of the Regulation, and given to the supervisory authority.

Art. 34(1) states "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay". However, in case this would involve 'disproportionate effort' – which of course could be so when a breach with regard to a large archival series containing thousands of personal data would occur – art. 34(1) point (c) offers the alternative of "a public communication or similar measure whereby the data subjects are informed in an equally effective manner". This could be, for example, a notice on the website or a communication via a mailing list.

Security breaches should be recorded and investigated and staff should be encouraged to report and respond to security incidents.

18. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION (ARTICLES 35-36)

The GDPR requires controllers to carry out a data protection impact assessment (DPIA) prior to the processing, when the processing "is likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). "DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate" compliance with the Regulation[3].

WHAT IS A DATA PROTECTION IMPACT ASSESSMENT (DPIA)?

The aim of a DPIA is to identify and to assess the risk that could arise for the individual (as citizen, client, patient, etc.) from a new type of processing. The Article 29 Working Party defined DPIA as: "a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."[4]

WHEN IS (OR IS NOT) A DATA PROTECTION IMPACT ASSESSMENT REQUIRED?

When new technologies for processing personal data or a new kind of processing operation is introduced, as a first step a risk assessment has to be carried out. If the nature of the data or the way of processing is likely to create a high risk for data subjects, a DPIA is required.

A DPIA is not necessary when the processing is *not* likely to create risks for data subjects, and when it is similar to previous processing activities for which a DPIA has already been

[3] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, wp248 rev.01, 13 Oct. 2017.

[4] Ibidem.

carried out. The GDPR makes clear, in fact, that "A single assessment may address a set of similar processing operations that present similar high risks." (Article 35(1))

The Data Protection Authorities are expected to publish a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and also of those which are not.

WHAT DOES "HIGH RISK" MEAN?

The GDPR does not define exactly what kind of processing could entail a high risk. It provides however a few examples, including one that might very well concern archive services, namely the processing on a large scale of personal data relating to criminal convictions or of sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation) (Article 35(3) point (b)). Moreover, when assessing whether the processing could result in a high risk for the rights and freedoms of data subjects, archive services should consider whether the personal data refer to vulnerable data subjects, such as for example mentally ill persons (recital 75).

WHEN DO ARCHIVE SERVICES HAVE TO CARRY OUT DPIAS?

Where archive services decide to digitise material or create digital finding aids to personal data, for use on site or online, a DPIA may be necessary. This will certainly be the case if they are going to process archival fonds containing sensitive personal data, such as medical files, criminal courts' case files, or the personal files of prisons' inmates.

The DPIA will ensure that the archive service has considered the data protection and privacy aspects of the proposed project or work and can satisfy or demonstrate to a Data Protection Authority that such concerns were addressed or factored into the design or implementation.

WHAT HAS TO BE DONE?

In the course of the data protection impact assessment, the planned processing operation and the legitimate interest of the operation has to be described in a systematic way. As a next step the proportionality and the necessity of the envisaged operation has to be evaluated. Then the risks for the rights and freedoms of the data subject have to be assessed followed by a detailed plan of the measures that will be taken to manage the risks. When the processing operation is running it has to be monitored on a regular basis and the DPIA has to be adapted when changes occur.

Some Data Protection Authorities published tools to help controllers to carry out a DPIA. See for example the free software produced by the French DPA: https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact.

WHEN DOES THE SUPERVISORY AUTHORITY HAVE TO BE INFORMED?

The supervisory authority (i.e. the Data Protection Authority) has to be consulted if the data protection impact assessment indicates that processing "would present a high risk in the absence of measures taken by the controller to mitigate the risk" (art.36). If the supervisory authority considers that the planned processing does not conform with the

Regulation or the envisaged measures to mitigate the risk are not sufficient, it has to provide written advice to the controller.

VII. MEASURES FOR TRANSPARENCY AND PROMOTING COMPLIANCE

19. RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30)

Article 30(1) states: 'Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.'

The record of processing activities – also often referred to as '(data) processing register' – is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data – both key components of the principle of accountability contained in the GDPR.

This record must be in writing (including in electronic form), clear and intelligible. Since 'processing activities' within the context of the GDPR concern operations performed on personal data relating to an identified or identifiable natural person, only activities regarding personal data are concerned.

The obligation to keep a record of processing activities does not apply to organisations endowed with less than 250 employees unless they find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or if they are processing personal data on a non-occasional basis, or if they tend to be processing special categories of data under Article 9(1) (i.e. data concerning health, sex life, ethnic origins, political opinions and other kinds of sensitive information) or data relating to criminal convictions under Article 10.
If one of these circumstances applies – which in fact is the case for most, not to say all archival institutions – an organisation is obliged to maintain the record of processing activities.

Organisations and their representatives must provide this record to the Data Protection Authority (DPA) upon request.

WHICH INFORMATION SHOULD THE RECORD OF PROCESSING ACTIVITIES HOLD:

The record must contain specific information about every processing activity carried out:

- the **name and contact data** of:
    - the archive service, or its representative;
    - if necessary other organisations with whom the archive service established in common the purposes and means of the processing;
    - the Data Protection Officer (DPO) if the archive service has appointed one;

- The **purposes** for which the archive service processes personal information.

  Similarly to 'Historical research' which already has been recognised as a 'purpose' in the past, 'archiving (purposes) in the public interest' should be

sufficient as a goal. It is not clear whether or not the addition 'of public interest' must be added to motivate the information.

- A description of the **categories of persons** of which the archive service processes data.

  For example: students, conscripts, defendants, patients…

- A description of the **categories of personal data**. Also identify so-called 'sensitive' data such as information about health and judicial information.

  For example: professional activities, financial transactions, judicial information about criminal convictions and sentences, data from which political opinions can be derived, …

- The **date on which the data must be deleted** (if known).

  Attention: From the point of view of archive services, it is of particular importance to point out to archives' creators that 'retention period' must not be confused with 'disposal' of information, and that they should act in conformity with the Law on Archives and as stipulated in the archival disposal schedules. Data archived in the public interest must indeed never be destroyed.

- The **categories of recipients** to whom the archive service provides personal data.

  Please note that we are speaking of "recipient categories": that is to say, for example 'universities and research institutions', 'individual researchers'…

- Does the archive service share data with a **foreign country or an international organisation outside the EU**? Then it must indicate this in the record.

- The general description of the **technical and organisational measures** taken in order to secure the personal data the archive service is processing: description of the technology, applications, and software used for data processing, that is to say which type of 'data protection by design or by default' has been used.

Organisations should consider this record as an internal tool to help implement the GDPR. The record can contain any additional information that is considered of importance by the data protection officer (DPO) in function of the activities carried out, for example indication of legal basis for data processing or an overview of all breaches regarding personal data.

PROCESSING BY SUBCONTRACTORS

Please note: If an archive service mandates other parties to process personal data on its behalf, a 'data processing agreement' with these organisations must be signed. By concluding such an agreement, the archive service ensures that the third party does not use or process the personal data for its own individual goals.

Only processing agents who can fully guarantee that they abide by legal requirements should be appointed. Archive services deciding to outsource processing activities to third party providers remain fully responsible for abiding by the stipulations of the GDPR.

SOME MODELS OF RECORD OF PROCESSING ACTIVITIES ARE AVAILABLE ONLINE, FOR INSTANCE:

The model offered by the Belgian DPA, which is available in French and Dutch: https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

The French DPA published two model registers, one more complex and one more simple: https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

The European Data Protection Supervisor (i.e. the EU's independent Data Protection Authority) published a "Register template" https://edps.europa.eu/data-protection/our-work/publications/other-documents/register-template-0_en

Member states might create a record of processing activities application, whose use is mandatory for public services. Belgium is a case in point.

20. DATA PROTECTION OFFICER (ARTICLE 37): DO ARCHIVES NEED TO APPOINT ONE?

The Data Protection Officer (DPO) assists the controller or the processor in all issues relating to the protection of personal data. Its main tasks are:

- to inform and advise the controller and the employees who carry out processing of their obligations under the GDPR and national data protection norms;
- to monitor compliance with the GDPR
- to provide advice as regards the data protection impact assessment (DPIA)
- to cooperate with the supervisory authority;

The GDPR introduced an obligation to appoint a DPO for public authorities and for private entities that carry out certain types of processing activities. All public authorities must have a DPO but this does not mean that each archive service in the public sector needs to appoint one. In many cases their parent institution might appoint a DPO whose responsibilities extend to the archive service. For example, a municipality might have a DPO responsible for monitoring compliance with the GDPR and counselling all the offices of the municipality, including the Municipal Archives.

Private sector entities must appoint a DPO if:

- Their core activity requires regular and systematic monitoring of data subjects on a large scale.
- Their core activity consists in the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal data relating to criminal convictions and offences.

It is very unlikely that foundations, museums, libraries, cultural associations, and other private sector bodies that hold archives carry out "regular and systematic monitoring of data subjects on a large scale". By contrast, it is entirely possible that their core activity consists in the processing of sensitive personal data.

There are, in fact, foundations, community archives and other private-sector bodies specialized in processing the archives produced by NGOs and human rights organisations in the course of their activities, which might include, for example, personal data revealing the racial or ethnic origin of persons victim of acts of intolerance. As already mentioned, there are academic centres specialised in the study of terrorism or community archives set up by anti-mafia activists that process personal data relating to criminal convictions and offences. There might be community archives that hold archives produced by feminist organisations that assisted women victims of violence and which include all sorts of highly sensitive personal data.

In all cases of this sort, private bodies processing archives should appoint a DPO. "The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract." (Article 37.6) Small entities might share the same DPO with other similar entities. It is very advisable for small bodies processing archives for "archiving purposes in the public interest" or for research purposes, to share the same DPO with other similar bodies so that the DPO can develop an expertise in the particular kind of personal-data processing that they carry out.

ANNEXES

GLOSSARY

Archive: The GDPR does not define the term "archive". Throughout these guidelines, "archive" is used to refer to the whole of the documents created and received by a person, family, or organisation, public or private, in the conduct of their affairs, and selected for permanent preservation. In some European languages, the same term is used to refer both to current records, and to records selected for permanent preservation. In this text, the term archive is used only to refer to records selected for permanent preservation.

Article 29 Working Party: Working group created in accordance with art. 29 of EU Directive 95/46. The working group was composed of representatives of the Data Protection Authorities in the Member States, the European Data Protection Supervisor and a representative of the EU Commission. The working group ceased to exist on May 25, 2018 when it was replaced by the European Data Protection Board (EDPB).

Controller: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (GDPR, art. 4)

Data subject: the person whose personal data are processed.

Data Protection Authority (DPA): see Supervisory Authority

Data Protection Officer (DPO): The DPO assists the controller or the processor in all issues relating to the protection of personal data. The GDPR introduced an obligation to appoint a DPO for public authorities and for private entities that carry out certain types of processing activities.

European Data Protection Board (EDPB): the GDPR replaced the Article 29 Working Party with the EDPB. Unlike its predecessor, the EDPB has the status of an EU body with legal personality and is provided with an independent secretariat. It has extensive powers to determine disputes between national supervisory authorities and to give advice and guidance on key concepts of the GDPR. It is composed of the DPAs of the Member States and the European Data Protection Supervisor. The Commission has the right to participate in its meetings.

European Data Protection Supervisor (EDPS): The EDPS is an independent EU body responsible for monitoring the application of data protection rules within European Institutions and for investigating complaints.

Personal data: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly

or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR, art. 4)

Archivists should keep in mind that the GDPR protects only the personal data of living persons. However, national law may also provide for the protection of personal data of deceased persons.

Processing: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (GDPR, art. 4)

Archivists should take into account that activities such as selecting documents containing personal data for permanent preservation, transferring them to an archive institution, arranging them, describing them, and making them available to users are all activities that are considered "processing of personal data" under the GDPR.

Personal data breach: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR, art. 4).

This definition is of paramount relevance for archivists. It implies that if personal data have been selected for permanent preservation and enter into the custody of an archive institution, archivists must protect their integrity. Among the principles relating to processing of personal data, the Regulation incudes in fact "integrity and confidentiality" (art. 5). Accidental loss or alteration of such records would violate not only archival ethics but also the GDPR. The same is true if archivists allow unauthorised disclosure of, or access to personal data.

Processor: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, art. 4).

Pseudonymisation: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." (GDPR, art. 4).

It is important to note that the GDPR suggests the possibility of pseudonymisation of personal data preserved for archiving purposes in the public interest or for historical research purposes and does not mention "anonymisation". Unlike anonymisation, pseudonymisation preserves the correlation of different data relating to a person as well as the relation between different data records. Pseudonymised personal data maintain their nature of personal data, and are therefore subject to the provisions of the Regulation.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data

concerning health or data concerning a natural person's sex life or sexual orientation; genetic data, and biometric data where processed to uniquely identify an individual (GDPR, art. 9). Such kinds of data are often referred to as “sensitive personal data”.

Supervisory Authority: Art. 51 of the GDPR stipulates that Each Member State shall provide for one or more independent public authorities, which will be responsible for monitoring the application of the Regulation. Such authorities have different names in different countries (for example, in Finland “Office of the Data Protection Ombudsman”, in France “Commission Nationale de l'Informatique et des Libertés”, in Ireland “Data Protection Commissioner”, in Italy “Garante per la protezione dei dati personali”), and are commonly known as “Data Protection Authorities” (DPAs).

WHERE TO LOOK FOR FURTHER GUIDANCE

- The European Commission has a section on its website "Data protection. Rules for the protection of personal data inside and outside the EU" https://ec.europa.eu/info/law/law-topic/data-protection_en where it has published some FAQs on the GDPR, e.g. What is personal data? What constitutes data processing? What are Data Protection Authorities (DPAs)?, etc.). The information is intended for readers who have no prior knowledge on the GDPR. Currently, it is only available in English.

- *Handbook on European data protection law*, 2018 edition – http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
  The handbook has been prepared by the EU Agency for Fundamental Rights (FRA), with the Council of Europe (together with the Registry of the European Court of Human Rights) and the European Data Protection Supervisor. It outlines both the European Union (EU) and the Council of Europe (CoE) data protection law and includes selected case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

- The European Data Protection Board (EDPB) is going to publish guidelines, recommendations and best practises. It will thus be useful to keep an eye on its website https://edpb.europa.eu/edpb_en, which is in all of the EU languages (although, for the moment, several documents are available only in English). On its first day of existence, the EDPB endorsed the guidelines produced by its predecessor, the Article 29 Working Party.

- The Article 29 Working Party (which ceased to exist on May 25, 2018) published nine guidelines and other documents on the implementation of the GDPR, aimed at contributing to a uniform interpretation and implementation by the different DPAs and governments throughout the EU. The European Data Protection Board (EDPB) endorsed all of such documents and made them available on its website https://edpb.europa.eu/edpb_en

  – *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01), 13-02-2018

  – *Guidelines on Consent under Regulation 2016/679* (wp259), 24-01-2018, [adopted, but still to be finalized]

  – *Guidelines on Data Protection Impact Assessment (DPIA) on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01) 13-10-2017

  – *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01), 30-10-2017

  – *Guidelines on Personal data breach notification under Regulation 2016/679* (wp250rev.01), 13-02-2018

- *Guidelines on the application and setting of administrative fines* (wp253). Now including available language versions, 13-02-2018

- *Guidelines on the Lead Supervisory Authority* (wp244rev.01), 31-10-2017

- *Guidelines on the right to "data portability"* (wp242rev.01), 27-10-2017

- *Guidelines on Transparency under Regulation 2016/679* (wp260), 24-01-2018 [adopted, but still to be finalized]

- *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.

- The Data Protection Authorities of EU Member States publish information material such as pamphlets, info sheets, infographics, translations of Article 29 Working Party Guidelines, to explain their new rights to citizens, and to help public administrations and small and medium-sized enterprises to comply with the GDPR. Check the website of your DPA! Its coordinates can be found on https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

- The European Data Protection Supervisor (EDPS) has a *Glossary* (in English, French and German) with over 70 entries on its website: https://edps.europa.eu/data-protection/data-protection/glossary_en. It has moreover published a free-access Reference Library (https://edps.europa.eu/data-protection/data-protection/reference-library_en) and other informative materials, mostly intended to guide EU institutions in the implementation of the GDPR, but which can be helpful for national public and private bodies as well.

- The National Archives of the UK, in conjunction with government archiving policy leads and the Archives and Records Association, has prepared a *Guide to archiving personal data*, and made it is freely available on its website. It can be a useful reading also for archivists from other member states, providing that they keep in mind that this *Guide* is specific to the British legal system.
  http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/

Příloha č. 3 – Zpracování osobních údajů v NA – tabulka

Činnost zpracování osobních údajů	Účel zpracování	Právní základ zpracování	Příjemce	Doba uložení osobních údajů podle spisového a skartačního řádu NA vydaného jako Pokyn ředitelky archivu č. 17/2019
Poskytování informací podle zákona č. 106/1999 Sb.	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, § 14 odst. 2	Údaje jsou poskytovány mimo archiv jen při odvolání odvolacím orgánům (Ministerstvo vnitra, případně soudy).	Stížnosti, žádosti a podněty občanů V 10
Wifikonektivita	Čl. 6 odst. 1 písm. b) GDPR – zpracování nezbytné pro účely splnění smlouvy	Smluvní vztah	Data o připojených zařízeních nejsou poskytována třetím osobám ani zpracovávána Národním archivem.	Údaje jsou smazány okamžitě po uplynutí doby životnosti přidělení IP adresy (TTL) (Lease Time 30 minut).
Výkon spisové služby v eSSL	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., § 3 odst. 1; § 63–70 Vyhláška č. 259/2012 Sb.	Údaje nejsou poskytovány mimo archiv.	Registraturní pomůcky (podací protokoly) – centrální (po uzavření) A 1; Registraturní pomůcky (podací protokoly) – jednotlivých oddělení (po uzavření) S 5; Pomocné knihy (doručovací knihy, zápisníky) (po uzavření) S 5; Evidenční pomůcky specializovaných spisoven (po uzavření) A 5; Evidenční pomůcky ostatní (po uzavření) S 5
Výběr archiválií	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., § 7; § 8; § 9 odst. 1; § 10 odst. 1, 2, 3; § 15 odst. 4; § 46 odst.1 písm. b), c) d), e), f), odst. 2 písm. b) Vyhláška č. 645/2004 Sb. Vyhláška č. 259/2012 Sb.	Vlastní spisy o výběru a přejímce nejsou předávány třetím osobám, mohou být předkládány při odvolání a kontrolní činnosti nadřízenému orgánu, kterým je Ministerstvo vnitra.	Protokoly o výběru archiválií A10
Věda a výzkum/projekty	Čl. 6 odst. 1 písm. a), b), c) GDPR – zpracování nezbytné pro plnění právní povinnosti, pro splnění smlouvy, případně je udělen souhlas	Zákon č. 499/2004 Sb., § 46 odst. 2 písm. g), h) Zákon č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací, § 32 odst. 5	Poskytovatel grantu (GAČR, TAČR, MV a další subjekty)	Dotace na vědu a výzkum – domácí poskytovatelé (po skončení projektu) A 1; Spoluúčast na mezinárodních projektech, grantech – podklady, zprávy, zápisy z jednání A 5; Grantové projekty (žádosti, podklady, rozhodnutí) A 5; Hlášení výsledku vědy a výzkumu, průběžné zprávy A 5; Národní digitální archiv (výzkum) A 5; Vědeckovýzkumné úkoly a projekty nepodpořené dotací V 5

Smluvní vztahy	Čl. 6 odst. 1 písm. b) a c) GDPR – zpracování nezbytné pro plnění právní povinnosti a naplnění smlouvy; ochrana majetku, závazky vyplývající ze smluvního vztahu	Zákon č. 89/2012 Sb., občanský zákoník Zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) Zákon č. 262/2006 Sb., zákoník práce Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv)	Údaji disponují smluvní strany. Smlouvy mohou být předkládány kontrolním orgánům při kontrolní činnosti (NKÚ, Ministerstvo vnitra), případně soudům. Všechny soukromoprávní smlouvy, jakož i smlouvy o poskytnutí dotace nebo návratné finanční výpomoci, jejichž stranou je Česká republika, se povinně uveřejňují v registru smluv, jestliže výše hodnoty jejich předmětu je vyšší než 50 000 Kč bez daně z přidané hodnoty. Smlouvy se v registru zveřejňují anonymizované.	Smlouvy, dohody – o vědecké a odborné spolupráci A 5; Smlouvy, dohody – o zápůjčce a výpůjčce archiválií včetně pojišťovacích smluv V 3; Smlouvy, dohody – o výměně publikací V 3; Smlouvy, dohody – o vydání díla A 5; Smlouvy, dohody – autorské A 5; Smlouvy, dohody – darovací (darování archiválií) a kupní (archiválie) A 5; Smlouvy, dohody – depozitní (úschova archiválií) A 5; Smlouvy, dohody – o dílo V 5; Smlouvy, dohody – rámcové o poskytování služeb V 5; Smlouvy, dohody – o technické podpoře V 5; Smlouvy, dohody – kupní (netýká se archiválií) V 5; Smlouvy, dohody – zřízení bankovních účtů A 5; Smlouvy, dohody – komisionářské V 5; Smlouvy, dohody – nájemní S 5; Smlouvy, dohody – licenční a podlicenční na užívání software S 5; Smlouvy, dohody – o poskytnutí dotace na vědu a výzkum (dle poskytovatelů chronologicky) V 1; Smlouvy, dohody – darovací (netýká se archiválií) V 5; Smlouvy, dohody – smlouvy/zápisy o převodu movitého majetku V 5; Smlouvy, dohody – smlouvy/zápisy o převodu nemovitého majetku A 5; Smlouvy, dohody – o zajištění provozu V 5; Smlouvy, dohody – o závodním stravování S 5; Smlouvy, dohody – mandátní S 5; Smlouvy, dohody – innominátní S 5
Personální agenda	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; vedení informací o zaměstnancích k plnění povinností zaměstnavatele dle zákoníku práce a služebního zákona	Zákon č. 234/2014 Sb., § 153, § 154, § 89, § 94–96 Zákon č. 262/2006 Sb., § 312–315 Zákon č. 435/2004 Sb. Zákon č. 500/2004 Sb. Zákon č. 251/2005 Sb. Zákon č. 89/2012 Sb. Zákon č. 309/2006 Sb. (BOZP) Zákon č. 373/2011 Sb. Vyhláška č. 79/2013 Sb. Nařízení vlády č. 590/2006 Sb. Nařízení vlády č. 304/2014 Sb. Nařízení vlády č. 341/2017 Sb. Zákon č. 121/2000 Sb. (autorské smlouvy) Zákony č. 586/1992 Sb., 198/2009 Sb., 567/2006 Sb., 595/2006 Sb., 222/2010 Sb., vyhláška č. 180/2015 Sb.	EKIS (spravuje MV ČR) – zaměstnanci podle zákoníku práce a služebního zákona ISOSS (spravuje MV ČR) – zaměstnanci podle služebního zákona	Osobní spisy zaměstnanců – služební poměr V 50 (pracovní poměr V 3 po skončení pracovního poměru nebo po pravomocném skončení pracovněprávního sporu); Konkurzy, výběrová řízení (kromě vedoucích funkcí), inzeráty S 1; Nepřijatí uchazeči o zaměstnání S 3; Evidence služebních průkazů – kniha s čísly průkazu po skončení platnosti, vzory služebních průkazů S 10; Zápisy o ztrátě služebního průkazu S 5; Informace personálního referenta S 5

Nahlížení do archiválií	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; nahlížení do archiválií badatelem dle zákona č. 499/2004 Sb.	Zákon č. 499/2004 Sb., § 34 odst. 1, 3, 4, 5, 6; § 35; § 37 odst. 2–13; § 38 odst. 1 písm. c), d), e), odst. 2, odst. 5; § 38a Vyhláška č. 645/2004 Sb., Příloha č. 3	Údaje související se získáním souhlasu k nahlížení do archiválií – osobní údaje žadatele o nahlížení v rozsahu jméno/jména, příjmení, datum a místo narození, státní občanství, adresa místa pobytu fyzické osoby na území ČR, bydliště v cizině, adresa, na kterou mají být doručovány písemnosti – se poskytují subjektu údajů, do jehož osobních údajů má být nahlíženo (dle ust. § 37 odst. 2 a 3 zákona č. 499/2004 Sb.) Zaměstnanci organizačních složek státu, ozbrojených sil, bezpečnostních sborů, zpravodajských služeb České republiky, územních samosprávných celků, jakož i osoby, které jsou podle zvláštních právních předpisů oprávněny nahlížet do dokumentů, jsou oprávněny nahlížet v archivech do archiválií, jejichž původcem je stát nebo územní samosprávný celek dle ustanovení § 38 odst. 5 zákona č. 499/2004 Sb.	Evidence badatelů a badatelských návštěv (včetně knih badatelů) A 5; Badatelské listy A 5; Korespondence se zahraničními a tuzemskými badateli a institucemi, včetně povolování studia V 5; Kniha zápůjček/výpůjček archiválií A 5 (po uzavření); Zápůjčky archiválií S 5 (po vrácení)
Mzdová agenda	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; mzdové účetnictví – splnění povinností v oblasti odvodů na důchodové, sociální, zdravotní pojištění zaměstnanců	Zákon č. 262/2006 Sb., zákoník práce Zákon č. 234/2014 Sb., o státní službě Zákon č. 563/1991 Sb., o účetnictví Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení Zákon č. 586/1992 Sb. (daň z příjmů) Zákon č. 155/1995 Sb. (důchodové pojištění) Zákon č. 187/2006 Sb. (nemocenské pojištění) Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění Zákon č. 592/1992 Sb., o pojistném na zdravotní pojištění Zákon č. 435/2004 Sb. (o zaměstnanosti) Nařízení vlády č. 595/2006 Sb., o nezabavitelných částkách Zákon č. 89/2012 Sb., občanský zákoník Nařízení vlády č. 590/2006, okruh a rozsah jiných důležitých překážek v práci Prováděcí předpisy k výše uvedeným zákonům	Česká správa sociálního zabezpečení Finanční úřad Ministerstvo vnitra (EKIS, ISOSS, atd.) Zdravotní pojišťovny	Sumární měsíční přehledy docházky S 10; Individuální měsíční přehledy docházky S 1; Dovolenky, čerpání, plány S 2; Pracovní neschopnost S 10; Ošetřování člena rodiny S 10; Mateřská dovolená S 10; Evidence fondu pracovní doby S 5; Evidenční listy zaměstnanců (evidence nemocí, dovolených) S 5; Přehledy o stavu pracovníků a čerpání mzdových prostředků S 5; Výkazy počtu pracovníků a čerpání mezd (měsíční) S 5; Pomocné doklady ke sledování čerpání mezd S 5; Podklady pro výpočet pohyblivé složky mezd (odměny) S 3; Dohody o pracích konaných mimo pracovní poměr S 5; Autorské honoráře S 5; Mzdové listy V 50; Výplatní listiny S 10; Prohlášení k dani ze mzdy ze závislé činnosti zaměstnanců S 5; Prohlášení poplatníka o dani z příjmu a související doklady S 10; Doklady o provádění srážek ze mzdy S 5; Doklady o půjčkách a spoření po skončení platnosti S 5; Příspěvek na důchodové připojištění po skončení platnosti S 60; Evidenční listy důchodového zabezpečení (po roce, kterého se týkají) S 80; Statistiky EKIS S 5

Kontrolní činnost	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; kontrola na úseku archivnictví a spisové služby dle zákona č. 499/2004 Sb. a vyhlášek č. 259/2012 Sb. a 645/2004 Sb.	Zákon č. 499/2004 Sb., § 46 odst. 1 písm. a); § 71 odst. 1 písm. b); § 72 Vyhláška č. 645/2004 Sb. Vyhláška č. 259/2012 Sb. Zákon č. 255/2012 Sb., § 8 písm. a), d); § 10 odst. 1 písm. a) a odst. 2	Údaje nejsou poskytovány mimo archiv s výjimkou postupu ve správním řízení odvolacím orgánům včetně orgánů soudních.	Kontrolní činnost a odborný dohled u jiných archivů – všeobecně A 5; Kontrolní činnost a odborný dohled u jiných archivů A 5; Státní kontrola původců (protokoly, korespondence aj.) A 10
Knihovna	Čl. 6 odst. 1 písm. a), b), c) GDPR – zpracování na základě souhlasu, nezbytné pro splnění smlouvy, nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., o archivnictví a spisové službě, § 46 odst. 2 písm. i) Zákon č. 257/2001 Sb., knihovní zákon, § 18 Vyhláška č. 88/2002 Sb., prováděcí vyhláška ke knihovnímu zákonu, § 7 Zákon č. 89/2012 Sb., občanský zákoník (smlouva o výpůjčce)	Údaje čtenářů nejsou poskytovány mimo Národní archiv. Z pozice administrátora RIV NA předává údaje o autorech vědeckých výsledků poskytovatelům dotace. Do souboru Národních autorit jsou poskytovány údaje na základě souhlasu subjektu údajů.	Po ukončení souhlasu s vedením osobních údajů čtenářem a po zhodnocení, zda nemá čtenář vůči knihovně nesplněné závazky (spouštěcí událost), jsou všechny dokumenty s osobními údaji navrženy po uplynutí skartační lhůty do skartačního řízení, zároveň je ukončena registrace čtenáře v elektronickém systému (údaje jsou vymazány). Evidence čtenářů – mimo průvodní korespondenci (po skončení platnosti) S 1 (od poslední návštěvy nebo žádosti o výmaz); Výpůjční agenda knihovny – mimo průvodní korespondenci (po skončení platnosti) S 2; Povolování studia specifických dokumentů z fondu knihovny V 2; Náhrady škody (za ztracené publikace knihovny) V 10; Autoři, smluvní partner a zaměstnanec knihovny – data se uchovávají trvale
Evidence původců	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; evidence původců vedená archivem dle zákona č. 499/2004 Sb. a vyhlášky č. 645/2004 Sb.	Zákon č. 499/2004 Sb., § 16, § 17, § 44 odst. 1 písm. k) Vyhláška č. 645/2004 Sb., § 12b	Ministerstvo vnitra (dle § 16 odst. 6 zákona č. 499/2004 Sb.) (PEvA) Držitel-vlastník archiválie (archivních souborů)	Spisy o archivním souboru a dokumentace o původci A 10; Evidence AKP a NKP A 5; Kontroly fyzického stavu AKP a NKP uložených v NA, knihy kontrol, včetně opatření a jejich plnění A 5; Kontroly fyzického stavu AKP a NKP uložených mimo archivy a kulturně vědecké instituce A 5; Kniha přírůstku a úbytku (po uzavření) A 3; Spis o vnější změně A 10 po provedení skartačního řízení
Evidence archiválií	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; evidence původců vedená archivem dle zákona č. 499/2004 Sb. a vyhlášky č. 645/2004 Sb.	Zákon č. 499/2004 Sb., § 15 odst. 1; § 16 odst. 3, 4, 5; § 18a odst. 1; § 27 odst. 1, 2; § 30 odst. 3, 4; § 46 odst. 1 písm. k, l Vyhláška č. 645/2004 Sb., § 4 odst. 1 písm. h); § 6 odst. 3 písm. r), u), y), z), aa), bb); § 7 odst. 2 písm. c), m)	Ministerstvo vnitra (dle § 16 odst. 6 zákona č. 499/2004 Sb.) Držitel-vlastník archiválií (archivních souborů)	Spisy o archivním souboru A 1; Přírůstky/úbytky V 5; Spis o vnější změně (řadí se podle čísel přírůstků/úbytků A 10; AKP a NKP – evidence A 5; Návrhy na prohlášení archiválií za AKP/NKP V 5; Kontroly fyzického stavu AKP a NKP uložených v NA A 5; Knihy kontrol, včetně opatření a jejich plnění A 5; Kontroly fyzického stavu AKP a NKP uložených mimo archivy a kulturně vědecké instituce A 5; Návrhy na prohlášení památky UNESCO V 5

Ekonomicko-provozní agendy	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; ekonomickoprovozní agendy – splnění povinností dle zákona č. 563/1991 Sb. a dalších	Zákon č. 563/1991 Sb., § 31 odst. 2 Zákon č. 134/2016 Sb. (o zadávání veřejných zakázek) Nařízení Ministerstva vnitra č. 45/2016, o zadávání veřejných zakázek Pokyn MF ČR č. R1-2010, čl. 12 k upřesnění postupu Ministerstva financí, správců programů a účastníků programu při přípravě, realizaci, financování a vyhodnocování programu nebo akce a k provozování informačního systému programového financování Zákon č. 340/2015 Sb., o registru smluv Zákon č. 320/2001 Sb., o finanční kontrole Zákon č. 218/2000 Sb., o rozpočtových pravidlech Zákon č. 219/2000 Sb., o majetku České republiky Vyhláška č. 383/2009 Sb., o účetních záznamech v tištěné podobě Vyhláška č. 410/2009 Sb., prováděcí vyhláška k účetnictví	Smluvní strany Ministerstvo vnitra, Ministerstvo financí, Nejvyšší kontrolní úřad	Účetní doklady (faktury přijaté, cestovní příkazy) S 10; Pokladní doklady (příjmové, výdajové) S 10; Faktury vydané S 10; Bankovní výpisy S 10; Veřejné zakázky S 10; Veřejné zakázky z dotačních programů A10; Investiční záměry V 10; Dokumentace k přípravě a realizaci nákupů S 10; Doklady o úplatném pořízení majetku V 10; Protokoly o zařazení/vyřazení majetku z užívání A 10; Výpůjčky/zápůjčky majetku S 5; Požadavky na opravy S 5; Doklady ke skladovému hospodářství S 5
Bezpečnost a ochrana zdraví při práci a PO	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti; bezpečnost a ochrana zdraví při práci – splnění povinností dle zákona č. 320/2001 Sb. a dalších	Zákon č. 309/2006 Sb., § 5 Zákon č. 262/2006 Sb., § 101–108 Zákon č. 234/2014 Sb., § 124 Zákon č. 133 /1985 Sb., § 16	Státní úřad inspekce práce / oblastní inspektoráty práce Krajské hygienické stanice Generální ředitelství hasičského záchranného sboru / hasičské záchranné sbory krajů	Zprávy o školení bezpečnosti práce S 5; Zprávy, protokoly a šetření pracovních úrazů a jejich příčin A 5
Interní audit	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 320/2001 Sb. Vyhláška č. 416/2004 Sb.	Údaje nejsou poskytovány s výjimkou kontrolních orgánů (MV ČR) mimo archiv	Zprávy z interních auditů, vysvětlivky a stanoviska, nápravná opatření V 10; Plány a vyhodnocení interních auditu V 10
Agenda prošetřovatele podle zákona o státní službě	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti – prošetřovatel podle služebního zákona	Nařízení vlády č. 145/2015 Sb. Zákon č. 234/2014 Sb., o státní službě, § 205 písm. d)	Orgány činné v trestním řízení nebo nadřízené orgány správní	Stížnosti zaměstnanců V 5; Hlášení prošetřovatele ke korupční činnosti A 5

Správní řízení a přestupkové řízení	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 500/2004 Sb., správní řád Zákon č. 499/2004 Sb., o archivnictví a spisové službě Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich	Účastník řízení nebo jeho zástupce Osoba, která prokázala právní zájem nahlížet do spisu Ministerstvo vnitra jako nadřízený správní orgán Soudy při soudním přezkumu	Správní řízení/řízení o přestupcích, opravné prostředky V 5
Vlastníci archiválií	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., § 24 odst., 1, 2, 4; § 25 odst. 2; § 31 odst. 1, 3; § 32 odst. 1, 2, 3, 4 Vyhláška č. 645/2004 Sb., § 12b	Ministerstvo vnitra	Knihy kontrol, včetně opatření a jejich plnění A 5; Kontroly fyzického stavu AKP a NKP uložených mimo archivy a kulturně vědecké instituce A 5
eLearningový vzdělávací systém Moodle	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., o archivnictví a spisové službě, § 46 odst. 3 písm. c)	Nejsou poskytovány třetím stranám, pouze subjektu údajů.	Údaje vedeny po dobu účasti účastníka na vzdělávání.
Archivní portál	Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti	Zákon č. 499/2004 Sb., o archivnictví a spisové službě, § 46 odst. 3 písm. b); § 18b	Nejsou poskytovány třetím stranám, pouze subjektu údajů a příslušnému veřejnému archivu.	Údaje jsou vedeny trvale. Srv. čl. 17 odst. 3 písm. d) GDPR

Příloha č. 4 –Dotazníkový formulář využitý v kvalitativním výzkumu

Problematika archivů a GDPR

Vážený pane, vážená paní,
jsem studentkou Univerzity Hradec Králové oboru Moderní systémy v archivnictví a ráda bych Vás požádala o vyplnění dotazníku na téma "Problematika archivů a GDPR". Dotazník je zcela anonymní, nezabere více jak 10 minut. Vyplněním dotazníku mi pomůžete v průzkumu, jak české archivnictví reaguje na Evropské nařízení o ochraně osobních údajů (GDPR). Cílem dotazníku je získat přehled o tom, v jakém stavu je proces digitalizování a zpřístupnění kronik v oblastních archivech po implementaci GDPR. Rozhodně nemám za cíl poukazovat na případné odchylky od jeho znění. Práce čistě zkoumá, jak se s nařízením české archivnictví vypořádalo. Výsledky budou využity ke zpracování diplomové práce Analýza dopadu GDPR na archivnictví pod Katedrou pomocných věd historických a archivnictví na Filozofické fakultě UHK.
Velmi děkuji za Váš čas.

1. Zaznamenal/a jste implementaci GDPR do vašeho archivu?
a. Určitě ano
b. Spíše ano
c. Nevím, o co se jedná
d. Spíše ne
e. Ne

2. V čem spatřujete největší problémy implementace GDPR do archivů? (vyberte více odpovědí)
a. v technologiích
b. v legislativních opatřeních
c. v proškolování
d. v časové náročnosti kontroly vstupních archiválií
e. ve složitosti vnitřních procesů archivů
f. Jiné, uveďte, jaké:_____

3. Jste spokojen s podporou Ministerstva vnitra při řešení a následné implementaci GDPR?
a. Určitě ano
b. Spíše ano
c. Nemám výhrady
d. Spíše ne
e. Ne

4. Absolvují zaměstnanci v rámci archivu školení ke GDPR?
a. Ano, pravidelně
b. Ano, ale zřídka
c. Pouze jednou
d. Ne, informace se dozvídám průběžně
e. Ne

4.1. Pokud ano, jsou tato školení přínosná a dostatečná?
a. Určitě ano
b. Spíše ano
c. Nemám výhrady
d. Spíše ne
e. Ne
5. Používáte v rámci archivu nějakou metodiku? Pokud ano, jakou.
a. Ano
b. Ne

5.1 Pokud ano, napište jakou.

6. Jaký je Váš názor na vyjádření Ministerstva vnitra ČR, že kroniky nemusí být zveřejněné na webu archivu? (Vyjádření a zdroj níže)
a. Plně souhlasím
b. Spíše souhlasím
c. Nemám výhrady
d. Spíše nesouhlasím
e. Plně nesouhlasím

7. Jak postupuje v dnešní době Váš archiv v rámci zveřejňování kronik na webu?
a. Stažení veškerých kronik z webu
b. Stažení kronik, kde se mohli objevit stále žijící občané a jejich kontrola
c. Ponechání všech kronik na webu a při tom probíhá kontrola
d. Jiné, uveďte jaké:_____

8. Jak bude Váš archiv postupovat nadále v rámci zveřejňování kronik na webu?
a. Po úplné kontrole se stáhnou kroniky se stále žijícími občany
b. Kroniky zůstanou stažené, zákon neuvádí povinnost jejich zveřejňování
c. Veškeré kroniky zůstanou na webu
d. Jiné, uveďte jaké:_____

9. Jsou kroniky často žádány k bádání ze stran badatelů ve Vašem archivu?
a. Ano, pravidelně
b. Ano, ale zřídka
c. Občas
d. Spíš ne
e. Vůbec ne

10. Pokud by bylo možné navrhnout úpravu znění článku 89 (znění uvedeno níže), co by podle Vás bylo přijatelné a přípustné? (Uveďte více možností)
a. Zveřejňování kronik s datací 80let zpět (průměrná doba života)
b. Rozšíření benevolence na zveřejňování více údajů než pouze jméno a příjmení
c. Vymanění zveřejňování kronik úplně z GDPR z důvodu ochrany archivního materiálu
d. Jiné, uveďte jaké:_____

11. Jaký je Váš postoj ke GDPR?
a. Kladný
b. Spíše kladný
c. Neutrální
d. Spíše negativní
e. Negativní

11.1 Pokud jste odpověděl/a Spíše negativní či Negativní, proč?
a. Velké postihy a sankce při nedodržení bez ohledu na instituci
b. Velké komplikace v průběhu běžné pracovní činnosti
c. Potřeba investic do vybavení/zabezpečení
d. Nárůst pracovních povinností spojených s GDPR
e. Jiné, uveďte jaké:_____

12. Co musel Váš archiv provést za změny v důsledku s GDPR?
a. Vytvoření nové pracovní pozice
b. Investice do vybavení/zařízení
c. Změny v systému, které archiválie se mohou předkládat badatelům
d. Jiné, uveďte jaké:_____

13. Za jaký Archiv dotazník vyplňujete?

14. Pod jaký SOA Váš archiv spadá?

15. Jaká je Vaše profesní pozice ve Vašem archivu?
a. Ředitel/ka archivu
b. Archivář/ka
c. Knihovník/Knihovnice
d. Garant digitalizace
e. Výzkumný a vývojový pracovník/pracovnice
f. Správce ICT
g. Restaurátor/ka
h. Technický pracovník/pracovnice
i. Dokumentátor/ka
j. Jiné, uveďte jaké:_____

16. Jsem:
a. Žena
b. Muž
c. Nechci uvádět

Vyjádření MV k dotazu na publikování kronik na internetu:
Pokud jde o zveřejnění kroniky na internetových stránkách obce, je nutné zdůraz- nit, že zákon obci zveřejňování kroniky na internetu neukládá. Na zpracování osob- ních údajů v kronice jejich zveřejněním na internetu tedy nelze použít důvod plně- ní právní povinnosti podle čl. 6 odst. 1 písm. c) obecného nařízení. Zveřejnění by bylo možné považovat za zpracování prováděné ve veřejném zájmu nebo pro účely oprávněných zájmů obce (prezentace obce navenek), zásada přiměřenosti zde však bude velet k anonymizování osobních údajů. V případě zveřejňování obecních kro- nik na internetu v zásadě nemusejí být anonymizována toliko jména osob, která jsou přiměřeně použita jako jména účastníků pamětihodných událostí obce a netý- kají se soukromého života těchto osob.
Zdroj: https://www.mvcr.cz/gdpr/soubor/gdpr-sesit-pdf.aspx (str. *9* – 1*0)*

Článek 89 "Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely"
1. *Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podléhá v souladu s tímto nařízením vhodným zárukám práv a svobod subjektu údajů. Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely. Pokud mohou být sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.*
2. *Jsou-li osobní údaje zpracovány pro účely vědeckého či historického výzkumu nebo pro statistické účely, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v článcích 15, 16, 18 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.*
3. *Jsou-li osobní údaje zpracovány pro účely archivace ve veřejném zájmu, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v článcích 15, 16, 18, 19, 20 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.*
4. *Pokud typ zpracování uvedený v odstavcích 2 a 3 slouží zároveň k jinému účelu, povolené odchylky se vztahují pouze na zpracování pro účely uvedené ve zmíněných odstavcích.*
Zdroj: https://www.privacy-regulation.eu/cs/89.htm

Příloha č. 5 –Spisová služba a původci v předarchivní péči Národního archivu

GDPR – spisová služba a původci v předarchivní péči Národního archivu
Národní archiv (Mgr. Karolína Šimůnková)
22. 11. 2017

Nařízení Evropského parlamentu a Rady 2016/679 **o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) nabývá účinnost 25. května 2018**
http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1510084697564&uri=CELEX:32016R0679

- Nařízení – právně závazné v celém rozsahu EU a přímo použitelné
- **Nevztahuje se na údaje zesnulých osob**
- sankce za porušení povinností při ochraně osobních údajů **zatím** národní úpravou v případě orgánů veřejné moci v České republice navrhována na 10.000.000 Kč.

Národní archiv důrazně upozorňuje, že povinnost řádného vyřazování dokumentů ve skartačním nebo mimo skartační řízení, která je adresována původcům dle ust. § 3 zákona č. 499/2004 Sb., **není tímto evropským Nařízením dotčena. Národní archiv** stejně jako ostatní archivy dle zákona č. 499/2004 Sb. **je oprávněn ukládat** trvale **archiválie**, včetně archiválií **obsahujících osobní údaje žijících osob**, což vyplývá mj. z čl. 17 a čl. 89 GDPR.

Co bych měl udělat:

- Analýza činností souvisejících s informacemi (zejména pak s osobními údaji) – přehled agend a systémů (vedení seznamu o činnostech zpracování) – případně vytěžit a aktualizovat obdobnou analýzu provedenou v instituci z důvodu kyberbezpečnosti
- Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.)
- Stanovení postupů a politiky ochrany - analýza přístupových oprávnění, bezpečnosti uložení – dokumentů, spisů, systémů, informací.
- Proškolování zaměstnanců - správná správa hesel, řádné návyky zaměstnanců, nastavení odpovědnosti, procesy při ukončení pracovního/služebního poměru, pracovní náplně odpovídající práci s osobními údaji atp.
- **Revize spisového a skartačního řádu (doplnit všechny evidence vedené v instituci) včetně spisového a skartačního plánu (provést revizi skartačních lhůt z hlediska zákonného zmocnění a provozní potřebnosti)**
- Revize eSSSl a dalších samostatných evidencí s osobními údaji a přijetí opatření – různé cesty - logování nahlížení, přesné stanovení pole „věc" v agendách s osobními či citlivými údaji příprava procesů včetně šablon odpovědí a nastavení lhůt na podání, která přijdou podle GDPR (čl. 12 – 22 GDPR)
- Správa dat a jejich záloh
- Stanovení postupů pro detekování bezpečnostních incidentů a řešení porušení zabezpečení

K tomu doporučujeme:

- **Ustanovení pracovního týmu/skupiny** pro provedení analýz a návrhů řešení implementace GDPR do provozu úřadu (včetně spisové služby a dalších informačních systémů), který provede výše uvedené analýzy včetně analýzy rozporů, konfliktních, rizikových míst, předloží návrhy řešení rozporů a návrhy postupů pro nově vzniklé agendy (čl. 13 – 21) a postupy pro kontrolu a ohlašovací povinnost v případě incidentu

- proškolit zaměstnance na téma GDPR a s ním související činnosti a nové agendy – rozhodně nestačí proškolit jen personalisty!
- zavést výstupy z analýz do praxe

Základní principy GDPR:

- zákonnost, korektnost, transparentnost, účel, minimalizace, přesnost, integrita, důvěrnost, omezení uložení
- konkrétní **účely**, pro které jsou osobní údaje zpracovávány, mají být **jednoznačné a legitimní** a aby byly **stanoveny v okamžiku shromažďování osobních údajů**
- osobní údaje mají **být přiměřené, relevantní a omezené** na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány
- **přesné** a v případě potřeby aktualizované;
- osobní údaje by měly být **zpracovány pouze tehdy, nemůže-li být účelu** zpracování **přiměřeně dosaženo jinými prostředky.**
- osobní údaje **zpracovávány na základě souhlasu subjektu údajů nebo s ohledem na nějaký jiný legitimní základ** stanovený právními předpisy
- je nezbytné zejména zajistit, aby byla **doba, po kterou jsou osobní údaje uchovávány, omezena na nezbytné minimum**.
- správce by měl **stanovit lhůty pro výmaz** nebo **pravidelný přezkum**. Měla by být přijata veškerá vhodná opatření, aby nepřesné osobní údaje byly opraveny nebo vymazány.
- osobní údaje by měly být **zpracovávány způsobem**, který zaručí náležitou **bezpečnost a důvěrnost** těchto údajů, mimo jiné za účelem **zabránění neoprávněnému přístupu** k osobním údajům (ISO 27001)
- správce nebo zpracovatel musí **posoudit rizika** spojená se zpracováním a **přijmout opatření** ke zmírnění těchto rizik, například **šifrování**

Pověřenec pro ochranu osobních údajů

Po 25. 5. 2018 nejpozději uvede veřejnoprávní původce kontaktní údaje na tzv. „pověřence na ochranu osobních údajů"

K činnosti a ustanovení pověřence pro ochranu osobních údajů odkazujeme na materiál:

- „Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017" http://www.mvcr.cz/odk2/
- „Pověřenci ochrany osobních údajů ve služebních úřadech – metodické doporučení" http://www.mvcr.cz/sluzba/clanek/ministerstvo-vnitra-zverejnuje-metodicke-doporuceni-k-problematice-poverencu-pro-ochranu-osobnich-udaju.aspx
- „Pokyn týkající se pověřenců pro ochranu osobních údajů" z 13. 12. 2016 z činnosti pracovní skupiny WP 29 publikovaný mj. na webových stránkách Úřadu pro ochranu osobních údajů https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750

Další výklady – web Úřadu pro ochranu osobních údajů:

- **Odkazy na** https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750

Příloha č. 6 – Příklad standardizovaného formuláře u SOA Třeboň

ČESKÁ REPUBLIKA

STÁTNÍ OBLASTNÍ ARCHIV V TŘEBONI

Husova 143, 379 01 Třeboň

Informace poskytované v případě, že osobní údaje nejsou získány od subjektu údajů

podle čl. 14 nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR")

Státní oblastní archiv v Třeboni s výjimkou přejímání dokumentů vybraných a evidovaných jako archiválie postupuje podle zákona č. 499/2004 Sb., o archivnictví a spisové službě, nezískává osobní údaje od třetích stran (osobní údaje, které nebyly získány od subjektu údajů přímo správcem). Archiv neposkytuje informace subjektu údajů podle čl. 14 GDPR o osobních údajích subjektu údajů ve správě archivu, pokud nebyly získány od subjektu údajů a nacházejí se v archiváliích v souladu s čl. 14 odst. 5 písm. b) GDPR. Archivní soubory požívají výjimky z práva na výmaz dle čl. 17 odst. 3 písm. d) a další odchylky a záruku při zpracování osobních údajů dle čl. 89 GDPR.

Příloha č. 7 –Příloha badatelského listu NA

PŘÍLOHA Č.1 Badatelského listu č.

Informace pro badatele:
Informace poskytované subjektu údajů podle čl. 13 nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR"):

Správcem osobních údajů podle GDPR je ARCHIV, IČO: Poštovní adresa: E-mailová adresa: ID datové schránky: **Kontaktní údaje pověřence pro ochranu osobních údajů** – … • **Účel** zpracování osobních údajů: nahlížení do archiválií badatelem dle zákona č. 499/2004 Sb. • **Právní základ** pro zpracování: čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti: zákon č. 499/2004 Sb. § 34 odst. 1, 3, 4, 5, 6, § 35, § 37 odst. 2 až 13, § 38 odst. 1) písm. c), d), e), odst. 2, odst. 5, § 38a; vyhláška č. 645/2004 Sb. příloha č. 3 • **Doba, po kterou budou osobní údaje uloženy:** Platí skartační lhůty uvedené ve spisovém a skartačním plánu ARCHIVU, který je součástí spisového a skartačního řádu ARCHIVU vydaného jako č. • **Práva subjektu údajů**: Subjekt údajů má podle čl. 15 GDPR právo na přístup k osobním údajům, které se ho týkají, podle čl. 16 GDPR právo požadovat po správci opravu nepřesných osobních údajů, které se ho týkají, podle čl. 17 GDPR právo na výmaz osobních údajů, které se ho týkají. Právo na výmaz nelze uplatnit, pokud jde o zpracování pro účely archivace ve veřejném zájmu, výmaz osobních údajů se dle čl. 17 odst. 3 písm. d) GDPR proto v archivních souborech uložených v ARCHIVU neprovádí. Subjekt údajů má právo na to, aby správce omezil zpracování osobních údajů subjektu údajů v případech vyjmenovaných v čl. 18 GDPR. Subjekt údajů má právo požadovat, aby ho správce informoval o příjemcích osobních údajů podle čl. 19 GDPR. Správce neprovádí zpracování osobních údajů automatizovaně, právo na přenositelnost údajů podle čl. 20 GDPR se proto neuplatní. **Podle čl. 21 GDPR má subjekt údajů právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, jde-li o zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci podle čl. 6 odst. 1 písm. e) GDPR.** Pokud je zpracování osobních údajů subjektu údajů založeno na souhlasu subjektu údajů se zpracováním jeho osobních údajů, má subjekt údajů právo souhlas kdykoliv odvolat. Odvoláním není dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním. **Subjekt údajů má právo podat stížnost u dozorového úřadu**, kterým je Úřad pro ochranu osobních údajů. Poštovní adresa: ÚOOÚ, Pplk. Sochora 27, 170 00 Praha 7, E-mailová adresa: posta@uoou.cz, ID datové schránky: qkbaa2n • Při zpracování osobních údajů správcem nedochází k automatizovanému rozhodování ani k profilování • **Příjemci**, příp. kategorie příjemců: osobní údaje badatele dle § 37 odst. 3 a § 35 a), b), c) zákona č. 499/2004 Sb. *(v rozsahu jméno, příjmení, datum a místo narození, státní občanství, adresa místa pobytu na území ČR, případně bydliště v cizině, adresy, na kterou mají být doručovány písemnosti podle zvláštního právního předpisu)*, se poskytují v souvislosti se získáním souhlasu k nahlížení do archiválií, které obsahují osobní údaje žijících osob, subjektu údajů, do jehož osobních údajů má být nahlíženo (dle ust. § 37 odst. 2 a 3 zákona č. 499/2004 Sb.); organizační složky státu, ozbrojené síly, bezpečnostní sbory, zpravodajské služby ČR, územní samosprávné celky, jakož i osoby, které jsou podle zvláštních právních předpisů oprávněny nahlížet do dokumentů, jsou oprávněny nahlížet v archivech do archiválií, jejichž původcem je stát nebo územní samosprávný celek dle ustanovení § 38 odst. 5 zákona č. 499/2004 Sb. • Správce nepředává ani nemá v úmyslu předat osobní údaje do třetí země nebo mezinárodní organizaci • Poskytnutí osobních údajů badatelem je zákonným požadavkem; v případě neposkytnutí těchto údajů nebude badateli umožněno nahlížení do archiválií. Tato Příloha č. 1 je nedílnou součástí badatelského listu.

Prohlášení badatele:
Svým níže uvedeným podpisem stvrzuji, že jsem se seznámil s obsahem informace a beru ji na vědomí.

V	dne	Podpis badatele

Elektronický podpis - 1.6.2018
Certifikát autora podpisu :
Jméno : PhDr. Alt Ulrych
Vydal : PostSignum Qualified C...
Platnost do : 9.11.2018