OCHRANA OSOBNÍCH ÚDAJŮ
podle Nařízení EPaR (EU) 2016/679

OBSAH:

Datum vydání: 25. 5. 2018

Zpracoval: ing. Jiří Mann, MBA
KOMORA s.r.o.
……

Schválila: PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
……

Záznam o změnách

Datum	Číslo stránky	Charakter změny	Změnu provedl

1 Účel

Směrnice je určena výhradně k popisu procesů při uplatňování systému ochrany osobních údajů v příspěvkové organizaci **Galerie Benedikta Rejta**, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01, ke stanovení odpovědnosti a specifikace rozsahu řízených záznamů.

2 Rozsah platnosti

Vzhledem k charakteru a činnosti příspěvkové organizaci **Galerie Benedikta Rejta**, zřízené podle §27 zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů v platném znění, se postupy popsané v této systémové směrnici týkají všech osobních údajů fyzických osob dotčených zpracováním osobních údajů a to bez ohledu na jejich státní příslušnost nebo bydliště, neboť je zřejmé, že činnosti organizace realizované na jednotném trhu Evropského hospodářského společenství nebo ve třetích zemích, nemohou být z hlediska přístupnosti širokému spektru dotčených osob regulovány či omezeny, mohou však být považovány za činnosti realizované ve veřejném zájmu.

Směrnice je určena pouze pro vnitřní potřebu organizace a je závazná pro všechny její zaměstnance.

Majitelem procesu ochrany osobních údajů je **pověřenec pro ochranu osobních údajů**, zřízený podle čl. 37, odst. 4 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.

3 Zkratky a definice

- EU - Evropská unie
- EP - Evropský parlament
- R (EU) - Rada EU
- GDPR - ochrana osobních údajů
- OÚ - osobní údaj
- ÚOOÚ - Úřad pro ochranu OÚ
- SOOÚ - subjekt ochrany OÚ (fyzická osoba)
- GBR - Galerie Benedikta Rejta
- DPO - externí pověřenec pro ochranu osobních údajů
- ČSÚ - Český statistický úřad
- DPIA - posouzení vlivu na ochranu osobních údajů

- IT - informační technologie
- ŘG - ředitelka GBR
- EG - ekonomka GBR
- SW - software
- HW - hardware
- DRP - Disaster Recovery Plan (plán obnovy provozu IT po výpadku)
- BCM - řízení kontinuity činností organizace
- XML - eXtensible Markup Language (rozšiřitelný značkovací jazyk), jehož znaková sada implicitně využívá Unicode podle ISO 10646

- Obecné nařízení - 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).
- Osobní údaje - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
- Zpracování - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
- Omezení zpracování - označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
- Profilování - jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;
- Pseudonymizace - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

- Evidence - jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;
- Správce - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;
- Zpracovatel - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- Příjemce - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní 4.5.2016 L 119/33 Úřední věstník Evropské unie CS údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;
- Třetí strana - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;
- Souhlas subjektu údajů - jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
- Porušení zabezpečení osobních údajů - porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
- Genetické údaje - osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;
- Biometrické údaje - osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;
- Údaje o zdravotním stavu - osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;
- Hlavní provozovna a) v případě správce s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, ledaže jsou rozhodnutí o účelech a prostředcích zpracování osobních údajů přijímána v jiné provozovně správce v Unii a tato jiná provozovna má pravomoc vymáhat provádění těchto rozhodnutí, přičemž v takovém případě je za hlavní provozovnu považována provozovna, která tato rozhodnutí přijala;

b) v případě zpracovatele s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, nebo pokud zpracovatel nemá v Unii žádnou ústřední správu, pak ta provozovna zpracovatele v Unii, kde probíhají hlavní činnosti zpracování v souvislosti s činnostmi provozovny zpracovatele, v rozsahu, v jakém se na zpracovatele vztahují specifické povinnosti podle tohoto nařízení;

- Zástupce - jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení;
- Podnik - jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost;
  - pro předmětnou směrnici je pojem podnik nahrazován v některých částech pojmem společnost a to dle významu konkrétní kapitoly.
- Skupina podniků - skupina zahrnující řídící podnik a jím řízené podniky; Řídícím podnikem by měl být podnik, jenž může uplatňovat dominantní vliv na jiné podniky například na základě vlastnictví, finanční účasti nebo pravidel, kterými se podnik řídí, či pravomoci prosazovat pravidla týkající se ochrany osobních údajů. Podnik, který vykonává správu zpracování osobních údajů v podnicích k němu přidružených, by měl být společně s těmito podniky považován za skupinu podniků
- Závazná podniková pravidla- koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost;
- Dozorový úřad - nezávislý orgán veřejné moci zřízený členským státem podle článku 51 Obecného nařízení;
- Dotčený dozorový úřad - dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť:
  a) správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu;
  b) subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo
  c) u něj byla podána stížnost;
- Přeshraniční zpracování a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě; nebo

  b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě;

- Relevantní a odůvodněná námitka - námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení tohoto nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie;
- Služba informační společnosti - služba ve smyslu čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535 (1);
- Mezinárodní organizace - organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě.
- Strojově čitelný formát - formát souboru s takovou strukturou, která umožňuje softwarovým aplikacím v něm snadno nalézt, rozpoznat a získat z něj konkrétní údaje, včetně jednotlivých uvedených fakt a jejich vnitřní struktury; Za strojově čitelné údaje se považují údaje zakódované v souborech strukturovaných ve strojově čitelném formátu. Strojově čitelné formáty mohou být otevřené nebo chráněné vlastnickým právem; mohou být formálně normalizované, či nikoli. Dokumenty ve formě souboru, který toto automatické zpracování omezuje, jelikož údaje z nich nelze získat snadno či vůbec, by za dokumenty ve strojově čitelném formátu být považovány neměly.
- ePrivacy - soubor předpisů (EU/2017), deklarující snahu o novelizaci současných směrnic EU, zejména 2009/136/ES (původně 2002/58/ES) s vazbou do českého právního systému, zejména zákon č. 127/2005 Sb., o elektronických komunikacích a zákon č. 480/2004 Sb., o některých službách informační společnosti.
- Business Continuity Management - řízení kontinuity činností organizace je řídící proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností organizace, na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty. BCM ochraňuje zájmy klíčových podílníků, akcionářů a dalších zájmových skupin, dobrou pověst a značku společnosti. Kontinuita činností organizace je chápána jako strategická a taktická způsobilost organizace být připraven a reagovat na incidenty a narušení činností organizace za účelem pokračování na předem stanovené přijatelné úrovni.
- Workflow - předdefinované schéma SW produktu určující vazby při plnění požadavků bez vlivu uživatele. V relevantním případě je jím interní definice zabezpečení OÚ, složená z jednotlivých činností GDPR vč. naprogramovaných vazeb. Celková koncepce SW tak podporuje workflow k dosažení požadovaného výsledku.
- Příspěvková organizace - nezisková právnická osobou veřejného práva zřízená organizační složkou státu nebo územně samosprávným celkem, k plnění úkolů ve veřejném zájmu. Jejich činnosti jsou zpravidla neziskové, ale jejich rozsah, struktura a složitost vyžadují samostatnou právní subjektivitu. O vzniku příspěvkové organizace vydává zřizovatel zřizovací listinu.

- Veřejný zájem - odpovídá přibližně termínům společenský zájem, celospolečenský zájem, popř. obecný zájem, který v identickém kontextu používá Evropský soud pro lidská práva a v jehož duchu mohou být omezeny dílčí zájmy. Veřejný zájem se používá především v konkrétních případech, ve kterých dochází k rozporu mezi právy jednotlivce a zájmem společnosti.
- Zpravodajská licence - ustanovení § 89, zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, upravující přiměřené používání, tj. pořizování a zveřejňování podobizny, fotografie, zvukového nebo audiovizuálního záznamu z veřejné akce, bez souhlasu SOOÚ, pokud to není v rozporu s jeho oprávněnými zájmy.
- Metadata - digitální údaje, určené pro jednoznačnou katalogizaci a identifikaci, zejména při pořizování fotografií, zvukových nebo audiovizuálních záznamů. Metadata ve formátu Exif nebo protokolu IPTC obsahují informace o vzniku souboru - datum a čas pořízení, použitou ohniskovou vzdálenost, použití blesku, typ a výrobce fotoaparátu, aktuální software, čas expozice, digitální zoom, kompresi, údaje o poloze místa fotografování (GPS, GIS) apod. Metadata zvukových souborů (např. pro MP3 v ID3 tagu) obsahují informace o názvu záznamu, použitém kodeku, datovém toku apod.

4 Vývojový diagram procesu a koncepční dokumenty

Vývojový diagram procesu je uveden v **příloze č. 1**.

Směrnice č. 1 GDPR je koncipována tak, aby její obsah odpovídal struktuře Obecného nařízení a byla tak srozumitelná pro všechny pracovníky GBR. Vztah mezi jednotlivými články v Obecném nařízení a kapitolami ve směrnici je popsán v **příloze č. 2** – „**Korelační tabulka**“.

DPO zpracoval dokument „**Politika ochrany osobních údajů**“ – **příloha č. 3**, který schválila ŘG a jenž tvoří základní koncepční materiál ochrany OÚ podle Obecného nařízení. Dokument je určen k veřejné deklaraci koncepce ochrany OÚ a jako takový je v tištěné formě vyvěšený v sídle GBR. Současně je dokument v elektronické podobě vystavený prostřednictvím webových stránek GBR na http://www.gbr.cz.

DPO každoročně rozpracuje dokument „Politika…“ do konkrétních a měřitelných cílů na období 1 roku, které povedenou k dosažení úplné shody činností GBR s požadavky Obecného nařízení, ostatních legislativních předpisů, metodických pokynů a technických norem, relevantních pro oblast ochrany OÚ. Dokument „Cíle ochrany osobních údajů na rok …“ jsou interním dokumentem GBR, určeným pro vnitřní potřebu zřizovatele, vedení i zaměstnanců GBR.

5 Popis procesu a odpovědnost

S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody SOOÚ zavedla GBR v roli správce, dále popsaná, vhodná a přiměřená technická i organizační opatření tak, aby zajistila a doložila, že zpracování OÚ je prováděno v souladu s Obecným nařízením.

5.1 Identifikace SOOÚ a zásady zpracování OÚ

Vzhledem k charakteru a činnosti GBR odpovídá DPO za zajištění volného pohybu OÚ. Žádná z činností zpracování nesmí z důvodů souvisejících s ochranou SOOÚ a v souvislosti se zpracováním OÚ jejich pohyb omezit ani zakázat a to i pro případy zpracování specifikované v **kap. 5.4.2** – „**Výjimky pro zpracování zvláštních OÚ**".

Identifikaci SOOÚ zajišťuje majitel příslušného procesu zpracování OÚ, specifikovaný v **příloze č. 4** – „**Seznam majitelů dílčích procesů zpracování**".
SOOÚ musí být prokazatelně zainteresován na řídících a administračních procesech a vyplývající kategorie OÚ musí být majitelem příslušného procesu nahlášeny DPO tak, aby výčet OÚ uvedený v **příloze č. 5** – „**Analytická tabulka OÚ**", byl úplný.

V součinnosti s majiteli dílčích procesů zpracování OÚ, vypracuje DPO slovní popis identifikovaných OÚ tak, aby bylo zcela zřejmé, jak jsou OÚ v GBR vnímány. Popis OÚ tvoří nedílnou součást **přílohy č. 5**.

Za úplnost záznamů, jejich zákonnost, korektnost a transparentnost odpovídá DPO.

Za stanovení doby nezbytné k uložení resp. zpracovávání OÚ odpovídá majitel dílčího procesu zpracování.

Pro každý případ jiného zpracování OÚ, než pro které byly původně určeny, provádí DPO posouzení slučitelnosti.

V případě kladného výsledku posouzení zaznamená DPO nové zpracování do **přílohy č. 5** – „**Analytická tabulka OÚ**" tak, aby neustále tvořila přesný záznam o průběhu zpracování OÚ v GBR.

V případě negativního výsledku posouzení slučitelnosti zpracování OÚ zajistí DPO v součinnosti s majitelem dílčího procesu zpracování OÚ okamžité ukončení navazujícího zpracování OÚ a odstranění případných záznamů zpracování, které by mohly poškodit práva či svobody dotčených SOOÚ. Současně s okamžitým ukončením navazujících zpracování OÚ provede DPO neprodleně prověření ostatních zákonných důvodů zpracování OÚ, které by ukončené zpracování umožnily.

Výjimkami z této povinnosti DPO jsou zpracování OÚ pro statistická šetření vyhlašovaná nebo periodicky požadovaná ČSÚ, případně zpracování OÚ pro účely historického výzkumu prováděného ve veřejném zájmu nebo pro potřeby, na nichž je GBR přímo zainteresována, např. vědeckovýzkumnou činnost, související s výstavní, restaurátorskou či akviziční činností nebo k předkládání návrhů akviziční komisi pro zařazení do sbírkového fondu galerie.

DPO ve spolupráci s majitelem dílčího procesu zpracování stanoví před prvním zpracováním nezbytné metody pro ověřování relevantnosti a přesnosti OÚ, včetně konkrétních lhůt aktualizace pro každý OÚ. Veškeré lhůty budou stanoveny s ohledem na význam konkrétního OÚ a možnou míru ohrožení práv SOOÚ.

V případě zjištění nepřesnosti konkrétního OÚ zpracuje majitel dílčího procesu zpracování záznam, ve kterém specifikuje identifikovanou nepřesnost a zajistí spolu s DPO neprodlenou opravu OÚ. Vzor záznamu je uveden v **příloze č. 6** – „**Protokol aktualizace OÚ**".

5.2 Zákonnost zpracování OÚ

Za zákonnost zpracování odpovídá ŘG a tuto odpovědnost nemůže přenést na zaměstnance GBR nebo na jakýkoliv externí subjekt. Pro zajištění shody ochrany OÚ s požadavky Obecného nařízení vydává ŘG tuto systémovou směrnici „**Ochrana osobních údajů podle nařízení EPaR (EU) 2016/679**“, stanovující odpovědnost za monitorování souladu činností v oblasti ochrany OÚ a jmenuje DPO.

Jmenovací dekret DPO tvoří nedílnou součást komplexní dokumentace GDPR a jeho kopie je uložena v osobní složce DPO. Vzor jmenovacího dekretu tvoří **přílohu č. 7** – „**Jmenovací dekret DPO**“.

Zákonné důvody pro zpracování OÚ nelze kombinovat, ani zaměňovat. Za správnost vymezení zákonnosti zpracování OÚ odpovídá DPO.

5.2.1 Vymezení zákonnosti zpracování

Zpracování OÚ je zákonné, pouze pokud je splněna nejméně jedna z dále uvedených podmínek. Za vymezení zákonnosti zpracování odpovídá DPO, která jej specifikuje záznamem do **přílohy č. 5** – „**Analytická tabulka OÚ**“.

Podmínky zákonnosti zpracování:

a) SOOÚ udělil **souhlas** se zpracováním svých OÚ pro jeden či více konkrétních účelů;
b) zpracování je nezbytné **pro splnění smlouvy**, jejíž smluvní stranou je SOOÚ, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto SOOÚ;
c) zpracování je nezbytné **pro splnění právní povinnosti**, která se na správce vztahuje;
d) zpracování je nezbytné **pro ochranu životně důležitých zájmů** SOOÚ nebo jiné fyzické osoby;
e) zpracování je nezbytné **pro splnění úkolu prováděného ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je pověřen správce;
f) zpracování je nezbytné **pro účely oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody SOOÚ vyžadující ochranu OÚ, zejména pokud je SOOÚ dítě.

Na základě analýzy zpracování OÚ v GBR je do systému zpracování OÚ zařazen i zákonný důvod dle kap. 5.2.1, písm. (e), neboť správce je oprávněn provádět zpracování OÚ ve veřejném zájmu, či jako subjekt pověřený výkonem veřejné moci.

5.3 Souhlas se zpracováním OÚ

Vzhledem k charakteru zpracování OÚ a jejich citlivosti je kladen zvláštní důraz na úplnou shodu požadavků v oblasti rozsahu a obsahu souhlasu se zpracováním OÚ od všech SOOÚ.

DPO odpovídá v každém okamžiku zpracování OÚ za schopnost správce doložit, že SOOÚ udělil souhlas se zpracováním svých OÚ pro předmětnou agendu zpracování.

DPO vypracoval návrh souhlasu se zpracováním OÚ, který schválila ŘG a který je nedílnou součástí systému ochrany OÚ v GBR. V zájmu maximální transparentnosti je souhlas se zpracováním OÚ koncipován jako zcela samostatný dokument, jehož součástí není prohlašování jiných skutečností.

Pokud tvoří souhlas SOOÚ právní základ pro zpracování OÚ, odpovídá DPO za evidenci formálně i věcně správného, písemného nebo jinak prokazatelného souhlasu SOOÚ.

Z běžné činnosti GBR je zřejmé, že může docházet i ke zpracování některých kategorií OÚ, které by standardně podléhaly souhlasu od SOOÚ, avšak v konkrétních případech bude zpracování OÚ založeno na jiných zásadách, logicky slučitelných a konzistentních s požadavky GDPR, zejména na základě zpravodajské licenci viz. **kap. 3** – „**Zkratky a definice**".

O konkrétních podmínkách **zpracování specifických kategorií OÚ**, běžně podléhajících souhlasu SOOÚ rozhoduje DPO, který musí být schopen v jakémkoliv okamžiku zpracování prokázat, že aplikované řešení neohrožuje práva, ani svobody SOOÚ a poskytuje jim ve vztahu k obecně informačnímu (zpravodajskému) charakteru daného zpracování dostatečné záruky.

Specifickými kategoriemi se pro potřeby GBR rozumí výhradně podobizna, fotografie, zvukový záznam nebo kombinovaný, audiovizuální záznam. Tyto kategorie OÚ mohou být v odůvodněných případech doplněny souvisejícími metadaty viz. **kap. 3** – „**Zkratky a definice**".

Postup bez získaného souhlasu se zpracováním OÚ uplatní správce vždy, bude-li se prokazatelně jednat o **veřejnou akci**, u níž mohou SOOÚ legitimně očekávat, že budou specifické kategorie jejich OÚ zpracovávány. Postup je však neuplatnitelný, pokud budou SOOÚ osoby mladší 15 let, neboť lze účelně předpokládat, že jejich schopnost rozpoznat a pochopit veškeré důsledky vlastní účasti je nižší, než u osob nepodléhajících tzv. rodičovskému souhlasu. Na základě provedené analýzy OÚ je však v souladu s **kap. 5.3.2** zpracování obdobného typu vyloučeno, resp. omezeno výhradně na legislativně určené povinnosti správce.

Zpracování OÚ v rámci **uzavřené akce s omezeným přístupem veřejnosti**, pro předem částečně definovanou skupinu SOOÚ (např. vernisáž, pro pozvané i nepozvané hosty), kde SOOÚ nemohou oprávněně očekávat, že budou ve své účasti, konání, úkonech, chování, vyjadřování ad. dokumentováni, nelze podložit zpravodajskou licencí, bez související informace. Pro obdobný typ akce zajistí DPO vhodnými prostředky prokazatelné informování všech přítomných SOOÚ (na pozvánkách, textově, prostřednictvím piktogramů apod.) a umožní jim vznést odůvodněnou námitku proti zpracování. Pro SOOÚ, které vznesly námitku proti zpracování specifických kategorií OÚ musí DPO zajistit prokazatelné odstranění OÚ, které by mohly představovat riziko pro práva a svobody těchto SOOÚ.

Při pořádání **neveřejné akce**, jejíž účastníci nejsou osobami veřejného zájmu a mohou oprávněně předpokládat, že žádné specifické kategorie OÚ nebudou předmětem zpracování, by jakýkoliv postup správce založený na jiném zákonném důvodu, než souhlasu SOOÚ byl v rozporu s relevantními legislativními předpisy dle **kap. 6** – „**Související dokumentace**" a správce není oprávněn jej připustit. Výhradně pro výše definovanou specifickou kategorii OÚ je možné považovat za souhlas aktivní přístup SOOÚ např. pózování pro fotografování, videozáznam apod.

5.3.1 Podmínky souhlasu se zpracováním OÚ

Veškeré souhlasy jsou v GBR strukturovány jako samostatné dokumenty, založené na jednoduchosti, srozumitelnosti, pochopitelnosti, dostupnosti, transparentnosti a dalších potřebných zásadách, které SOOÚ zcela umožní pochopit veškeré aspekty vyjádření souhlasu a možných následků tohoto závazného úkonu.

Souhlas nesmí být učiněn v nouzi nebo v tísni, ale musí být svobodným projevem vůle SOOÚ. Z výše uvedených důvodů zajistí DPO u každého souhlasu splnění 4 zásad, nezbytných k prokázání legitimity zpracování OÚ podle kap. 5.2.1, písm. a). Veškeré souhlasy SOOÚ se zpracováním vlastních OÚ jsou v GBR:

- svobodné – představují svobodnou vůli SOOÚ souhlas udělit a je zřejmé, že mezi SOOÚ a GBR neexistuje zjevná nerovnováha v jejich postavení,
- konkrétní – obsahují přesnou specifikaci účelu zpracování OÚ, které SOOÚ poslouží ke zvážení míry rizika, které svým souhlasem podstoupí,
- informované – jsou založeny na transparentním poskytnutí potřebných informací, zejména o rozsahu a účelu zpracování, době zpracování a uložení OÚ, předávání OÚ zpracovatelům a příjemcům i všech dalších rozhodných parametrech zpracování, které by mohly sehrát roli při rozhodnutí SOOÚ, zda souhlas poskytnout či nikoliv,
- jednoznačné - nesmí vyvolat pochybnosti nebo umožnit nejednoznačný výklad zpracování OÚ, z něhož by SOOÚ mohl nabýt dojmu, že bude docházet k jiným operacím s OÚ nebo k méně závažnému zpracování OÚ a to zejména pokud se jedná o OÚ zvláštního charakteru.

V podmínkách GBR a s ohledem na konkrétní typ zpracování nemusí být zásada konkrétnosti vždy explicitně zahrnuta v souhlasu SOOÚ a to zejména když je zcela zřejmé, k jakému účelu je souhlas vyžadován/ poskytován.

V mimořádném případě může být v GBR souhlas SOOÚ součástí jiného dokumentu (např. smluvních nebo obchodních podmínek apod.). V uvedeném případě je nezbytné, aby navrhovatel tohoto řešení (majitel dílčího procesu zpracování) uvedl nezbytné důvody takového řešení v záznamu „Interní sdělení“ a předložil jej před prvním zpracováním DPO k posouzení a schválení.

Vzor záznamu je uveden v **příloze č. 8** – „**Interní sdělení**“.

Současně, při stanovení formálního i věcného obsahu souhlasu, musí DPO stanovit i adekvátní možnost jeho odvolání a zajistit seznámení SOOÚ s postupem. Odvolání souhlasu musí být stejně snadné/ složité, jako jeho udělení.

Zájmem GBR je to, aby udělení souhlasu bylo prokazatelně svobodné a nebylo podmíněno skutečnostmi, které nejsou pro zpracování relevantní. V případě neschopnosti GBR prokázat svobodné udělení souhlasu SOUÚ, se souhlas automaticky považuje za neplatný a DPO je povinen zpracování založené na tomto souhlasu bezodkladně ukončit.

Vzor záznamu je uveden v **příloze č. 13** – „**Souhlas se zpracováním OÚ**“.

5.3.2 Rodičovský souhlas

GBR provádí zpracování OÚ osob mladších 16 let pouze v rozsahu určených právní povinností správce dle kap. 5.2.1, písm. (c).

V případě mimořádného zpracování OÚ osoby mladší 16 let, musí před prvním zpracováním zajistit DPO rodičovský souhlas a prokázat, že tento souhlas je skutečně udělen osobou pověřenou výkonem práv dítěte.

5.4 Zpracování zvláštních OÚ

Zpracování zvláštních kategorií OÚ, specifikovaných v kap. 5.4.1 se s výjimkami podle kap. 4.5.2 v GBR zakazuje.

5.4.1 Specifikace zvláštních OÚ

Za zvláštní OÚ se považují informace o:

- Rasovém původu,
- etnickém původu,
- politických názorech,
- náboženském vyznání,
- filozofickém přesvědčení,
- členství v odborech,
- genetické údaje,
- biometrické údaje,
- zdravotním stavu,
- sexuálním životu,
- sexuální orientaci.

5.4.2 Výjimky pro zpracování zvláštních OÚ

V podmínkách GBR může docházet ke zpracování OÚ na jejichž základě by mohla vzniknout závažná rizika pro základní práva a svobody SOOÚ.

DPO připustí zpracování dalších zvláštních OÚ pouze v případě, že:

- SOOÚ udělil výslovný souhlas se zpracováním,
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo SOOÚ v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů SOOÚ nebo jiné fyzické osoby v případě, že SOOÚ není fyzicky nebo právně způsobilý udělit souhlas;
- zpracování se týká osobních údajů zjevně zveřejněných SOOÚ;
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků;
- zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo členského státu;
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance a lékařské diagnostiky.

5.5 Zpracování OÚ týkajících se rozsudků v trestních věcech

GBR nezpracovává OÚ týkajících se rozsudků v trestních věcech a trestných činů. V případě, že by se jednalo o mimořádný případ, který by vyžadoval předmětné zpracování, může tak být učiněno výhradně po výzvě a pod dozorem orgánu veřejné moci.

Majitel dílčího procesu zpracování musí požadavek orgánu veřejné moci oznámit DPO, prostřednictvím záznamu „**Interní sdělení**“, jehož vzor je specifikovaný v **příloze č. 8**. Celkové zpracování předmětných

OÚ bude s ohledem na vysoký stupeň možného ohrožení zájmů SOOÚ, prováděno pod metodickým dohledem DPO.

5.6 Neidentifikované zpracování OÚ

GBR nezpracovává OÚ, které nevyžadují identifikaci, ani osobní údaje SOOÚ, které není schopen identifikovat.

5.7 Transparentnost a postupy

Veškeré informace, které GBR poskytuje SOOÚ jsou založeny na současném splnění zásad:

- stručnosti,
- transparentnosti,
- srozumitelnosti,
- snadné přístupnosti
- jasných a jednoduchých jazykových prostředků

Poskytování všech informací omezuje GBR na **písemnou formu**, za níž se ve vhodných případech považuje i forma elektronická. Výhradně na žádost SOOÚ a po prokazatelném ověření identity SOOÚ mohou majitelé dílčích procesů zpracování nebo DPO poskytnout informace ústně. Ve všech případech jsou informace podávány **bezplatně**.

Lhůta na poskytnutí informací je stanovena na maximálně **1 kalendářní měsíc**. Překročení limitní lhůty je považováno za systémovou neshodu a musí být řešeno postupy stanovenými pro nápravná a preventivní opatření.

5.8 Poskytování informací a přístup k OÚ

OÚ pro zpracování jsou v GBR získávány přímo od SOOÚ nebo z jiných zdrojů např. databází. Podle zdroje OÚ jsou SOOÚ poskytovány povinné základní informace a to v rozsahu:

- totožnost a kontaktní údaje správce a jeho případného zástupce;
- kontaktní údaje DPO;
- účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
- oprávněné zájmy správce nebo třetí strany v případě, že je zpracování prováděno podle kap. 5.2.1, odst. f);
- případné příjemce nebo kategorie příjemců osobních údajů;
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci.

Na základě rozhodnutí DPO lze v oprávněných případech poskytovat SOOÚ i další informace sloužící pro zajištění spravedlivého a transparentního zpracování, zejména o:

- době, po kterou budou osobní údaje uloženy,
- existenci základních práv SOOÚ
- existenci práva odvolat kdykoli souhlas, pokud je zpracování založeno na souhlasu SOOÚ
- existenci práva podat stížnost u ÚOOÚ nebo žalobu u příslušného soudu;

- skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Vzor informací poskytovaných SOOÚ v případě, že tento SOOÚ je poskytovatelem OÚ, tvoří **přílohu č. 10** – „**Informace o zpracování a právech SOOÚ**".

Vzor informací poskytovaných SOOÚ v případě, že OÚ nejsou získány přímo od tohoto SOOÚ, tvoří **přílohu č. 11** – „**Informace o zpracování a právech SOOÚ**".

Majitelé dílčích procesů zpracování zajistí, aby SOOÚ obdržel povinné informace při první komunikaci se správcem, nebo nejpozději před prvním zpřístupněním OÚ třetí straně, případně nejpozději do 1 kalendářního měsíce od získání OÚ.

5.9 Práva SOOÚ

GBR deklarovala v koncepčním dokumentu „**Politika ochrany osobních údajů**" zajišťování práv SOOÚ jako jeden ze základních aspektů systémového přístupu o ochraně OÚ.

5.9.1 Právo SOOÚ na přístup k vlastním OÚ

Majitelé dílčích procesů zpracování, případně DPO mají povinnost poskytnout SOOÚ informaci, potvrzení nebo přístup k OÚ, která se ho týkají, pokud tím nebude porušeno právo jiného SOOÚ.
Informace, kterých se povinnost týká, jsou:

- účely zpracování;
- kategorie dotčených OÚ;
- příjemci nebo kategorie příjemců, kterým OÚ byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou OÚ uloženy,
- existence práva požadovat od správce opravu OÚ,
- existence práva požadovat od správce výmaz OÚ,
- právo vznést námitku proti zpracování OÚ,
- právo podat stížnost u ÚOOÚ nebo žalobu u příslušného soudu,
- veškeré dostupné informace o zdroji OÚ, pokud nejsou získány od SOOÚ,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování SOOÚ.

Pokud je SOOÚ požadována kopie OÚ, poskytne jí správce v prvním případě bezplatně. V dalších případech bude poskytnutí potvrzení zpoplatněno, přičemž cena bude stanovena jako součet nákladů na konkrétní administrativní úkon a dalších případných nákladů např. poštovného apod. DPO oznámí zpoplatnění i jeho důvod SOOÚ i ÚOOÚ.

5.9.2 Právo SOOÚ na opravu vlastních OÚ

Požadavek na opravu vlastních OÚ může SOOÚ uplatňovat u kteréhokoliv majitele dílčího procesu zpracování, který tento požadavek bez zbytečného odkladu oznámí DPO prostřednictvím řízeného záznamu v **příloze č. 6** – „**Protokol aktualizace OÚ**".

DPO bez zbytečného odkladu zajistí opravu nepřesného OÚ. Za nepřesné OÚ se považují i neúplné OÚ a požadavky na dodatečná prohlášení SOOÚ.

5.9.3 Právo SOOÚ na výmaz vlastních OÚ

Požadavek na výmaz vlastních OÚ může SOOÚ uplatňovat u kteréhokoliv majitele dílčího procesu zpracování, který tento požadavek bez zbytečného odkladu oznámí DPO prostřednictvím řízeného záznamu v **příloze č. 6 – „Protokol aktualizace OÚ**".

Je-li splněna alespoň jedna z dále uvedených podmínek, zajistí DPO bez zbytečného odkladu vymazání OÚ a oznámí tuto skutečnost SOOÚ.

Podmínky k provedení výmazu:

- OÚ již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- SOOÚ odvolá souhlas, na jehož základě byly údaje zpracovány a neexistuje jiný důvod pro zpracování;
- SOOÚ vznese námitky proti zpracování a neexistují převažující oprávněné důvody pro zpracování
- OÚ byly zpracovány protiprávně;
- OÚ musí být vymazány ke splnění právní povinnosti;
- OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti kap. 5.3.2.

Pokud byly předmětné OÚ zveřejněny, zajistí DPO v součinnosti s majiteli dílčích procesů zpracování, okamžité odstranění a současně v rámci svých možností informuje ostatní známé správce o žádosti SOOÚ požadující vymazání veškerých odkazů na OÚ, jejich kopie i replikace.

5.9.4 Právo SOOÚ na omezení zpracování vlastních OÚ

DPO omezí správce zpracování OÚ, pokud:

- SOOÚ popírá přesnost OÚ, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- zpracování je protiprávní a SOOÚ odmítá výmaz OÚ a žádá pouze o omezení jejich použití;
- OÚ již nejsou potřebné pro původní účely zpracování, ale SOOÚ je požaduje pro určení, výkon nebo obhajobu právních nároků;
- SOOÚ vznesl námitku proti zpracování a dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody SOOÚ.

V případě omezení zpracování OÚ zajistí majitelé dílčích procesů zpracování výhradně uložení OÚ a přesun vybraných OÚ do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům, dočasné odstranění zveřejněných údajů z internetových stránek apod. Omezení zpracování OÚ musí být v systémech/ činnostech zpracování jasně vyznačeno.

Výjimku povoluje DPO z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu EU nebo některého členského státu. V případě uplatnění výjimky z omezení upozorní správce SOOÚ, že omezení zpracování bylo zrušeno.

5.9.5 Právo SOOÚ na přenositelnost vlastních OÚ

Správce zajistí pro SOOÚ přenesení jeho vlastních OÚ k jinému správci, při současném splnění dvou podmínek:

- zpracování OÚ je založeno na souhlasu SOOÚ dle kap. 5.2.1, písm. a) nebo na smlouvě podle kap. 5.2.1, písm. b).
- zpracování OÚ se provádí automatizovaně a je možné je exportovat ve strojovém kódu.

O splnění podmínek pro přenesení OÚ rozhoduje DPO.

OÚ jsou správcem přenášeny výhradně v běžně užívaných otevřených formátech, zejména XML, JSON, CSV, spolu s upotřebitelnými metadaty v reálně dosažitelné rozlišitelnosti. Správce si současně vyhrazuje právo nepřenášet OÚ ve formátu PDF, neboť je pravděpodobné, že OÚ nebudou dostatečně strukturované a popisné, aby je bylo možné snadným způsobem opětovně použít.

Správce si vyhrazuje právo nepřenést OÚ v případě, že se datový soubor OÚ týká více SOOÚ a byla by tím dotčena jejich práva a svobody.

V případě, že je správce požádán nebo vyzván k převzetí OÚ od jiného správce, rozhodne DPO v součinnosti s majitelem příslušného dílčího procesu zpracování o akceptování tohoto požadavku. V případě odmítnutí DPO informuje SOOÚ o zamítnutí žádosti a toto rozhodnutí je považováno za konečné.

5.9.6 Právo SOOÚ vznést námitku

Námitku SOOÚ vznesenou proti zpracování podle kap. 5.2.1, písm. e) nebo f), vypořádává DPO. Součástí vypořádání námitky proti zpracování OÚ musí být písemný záznam dle vzoru v **příloze č. 8** – „**Interní sdělení**“, který jednoznačné prokáže, existenci závažných oprávněných důvody pro zpracování, které převažují nad zájmem nebo právem SOOÚ.

Správce neuplatňuje metody přímého marketingu, profilování ani zcela automatizovaného zpracování a tak případné námitky SOOÚ směřující do těchto oblastí nemohou být relevantní.

5.10 Automatizované individuální rozhodování

Správce neprovádí automatizované individuální rozhodování.

5.11 Profilování SOOÚ

Správce neprovádí profilování SOOÚ.

5.12 Zabezpečení/ ochrana OÚ

ŘG jmenovala DPO za osobu odpovědnou za zpracování zásad zabezpečení a ochrany OÚ při neautomatizovaném a částečně automatizovaném zpracování. V souladu s deklarací v **kap. 5.10** a **5.11** není plně automatizované zpracování v GBR prováděno.

Zásady zabezpečení a ochrany OÚ při neautomatizovaném zpracování jsou součástí interních postupů v souladu odpovědností jednotlivých zaměstnanců GBR za přidělené agendy poskytovaných služeb.

ŘG určila EG, jakožto osobu odpovědnou za stanovení odpovídajících technických opatření k řádnému zabezpečení technických prostředků v prostředí IT.

EG je povinna prostřednictvím zaměstnanců GBR a externího dodavatele, schváleného v databázi ověřených dodavatelů, který je zároveň identifikován jako zpracovatel v **příloze č. 9 – „Seznam zpracovatelů a společných správců OÚ**“, zajistit, aby principy ochrany byly založeny na elementárních zásadách informační bezpečnosti, zejména:

- Důvěrnosti - informace je přístupná pouze těm, kteří mají povolený (autorizovaný) přístup,
- celistvosti - je zajištěna správnost, úplnost a kontinuita informací,
- dostupnosti - oprávnění uživatelé mají přístup k informacím v okamžiku, kdy je potřebují,

a to popisem v oblastech:

- Bezpečnostní politiky na dílčích stupních vč. důvodů, cílů a způsobů zabezpečení OÚ
- procesní organizace bezpečnosti informací vč. organizačního zajištění bezpečnosti OÚ,
- organizace činností jednotlivých správců a uživatelů vč. personální bezpečnosti,
- klasifikace a řízení informačních aktiv,
- řízení přístupu a přístupových práv k IT systémům,
- politiky mobilních zařízení a práce na dálku,
- technologie šifrování, krytování, pseudonimizace a anonymizace dat,
- zabezpečení pracovišť (např. zámky, mříže, kamerový systém, evidence vstupů, ostraha),
- zabezpečení zařízení IT vč. bezpečnosti prostředí (např. klimatizace serverovny)
- zásad bezpečnosti provozu,
- likvidace technických zařízení, která obsahují nebo mohou obsahovat data vč. osobních údajů,
- zásad servisu a předávání nefunkčních/ částečně funkčních zařízení mimo GBR,
- zásad bezpečnosti komunikací a přenos dat,
- údržby informačního systému a minimálních požadavků na vývoj a údržbu IT,
- zásad ověřování bezpečnosti dodavatelů a třetích stran,
- způsobů zvládání bezpečnostních incidentů,
- tvorby a aktualizace webových stránek,
- řízení kontinuity dat a procesů, v nichž dochází k jejich zpracování,
- souladu s interními a externími požadavky.
- BCM
- zajištění souladu s GDPR.

Podmínky a pravidla ochrany OÚ v prostředí IT budou zahrnovat minimálně informační aktiva v rozsahu:

- Datová aktiva
  - databáze,
  - dokumentace.
- DRP
  - Umístění a popis záloh OÚ,
  - pořadí a způsob obnovy jednotlivých komponent IT,
  - maximální časy obnovy,
  - kontaktní údaje servisních organizací,

  - metodiku testování plánů obnovy
  - postupy pro ověření zásad přesnosti OÚ obnovených ze záloh, zejména s ohledem na dříve odstraněné záznamy o zpracování OÚ i OÚ samotné.
  - způsob ověření úspěšného obnovení OÚ ze zálohy.
- SW aktiva
  - systémový software,
  - aplikační software,
  - vývojové nástroje.
- HW aktiva
  - počítače,
  - servery
  - ostatní infrastrukturu.
- Informační služby
  - veřejné registry,
  - cloudové služby.
- Ocenění významu aktiv pro GBR

Veškeré SW produkty využívané k zabezpečování provozní agendy GBR jsou výrobci vybaveny workflow, splňujícím požadavky GDPR, případně disponují značkou shody Ready GDPR. Jedná se především o SW MUZO, OK mzdy, TEMUS, Clavius a Demus.

Při každé významné změně podmínek a pravidel ochrany vztahujících se na prostředky IT zohlední EG změnu v interních postupech. EG následně informuje o provedených změnách DPO, který je bezodkladně začlení do relevantních interních předpisů, systémové dokumentace i operativních postupů při zpracování OÚ, které budou na straně správce zahrnovat:

- pseudonymizaci OÚ
- šifrování OÚ;
- schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- obnovu OÚ ze záloh;
- interní audity systému GDPR, zaměřené zejména na náhodné nebo protiprávní zničení, ztrátu, pozměnění, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Veškerá opatření budou realizována s ohledem na stav technických prostředků a předpokládaných nákladům na provedení tak, aby odpovídaly povaze, rozsahu, kontextu, účelům zpracování i rizikům pro práva a svobody SOOÚ.

Určení opatření provede DPO pro celý životní cyklus existence OÚ tzn., jak pro dobu před zpracováním, tak pro dobu samotného zpracování.

Stanovená technická a organizační opatření musí prokazatelně zajistit, aby se zpracovávaly pouze OÚ, jež jsou pro konkrétní účel daného zpracování nezbytné a to jak v množství shromážděných OÚ, tak i v rozsahu zpracování OÚ, době uložení OÚ a zajištění dostupnosti OÚ.

Obdobné podmínky jsou platné pro veškerá zpracování technologických osobních údajů, identifikovaných a specifikovaných v **příloze č. 5** – „**Analytická tabulka OÚ**“.

5.13 Společní správci

V návaznosti na provedenou analýzu zpracování ověřil DPO, že v aktuálním stavu systému GDPR není prováděno zpracování OÚ dalšími správci, kteří by stanovovali účely a prostředky zpracování a jednali tak v zájmu ochrany OÚ dotčených SOOÚ.

V případě vzniku mimořádné situace, kdy by vznikl sekundární správce OÚ, musí DPO, na základě písemné dohody s pověřenými zástupci společných správců stanovit podíly na odpovědnosti za plnění povinností při zpracování OÚ, zejména v oblasti výkonu práv SOOÚ a informační povinnosti podle **kap. 5.8**.

Bez ohledu na podmínky písemné dohody mezi společnými správci potom může SOOÚ vykonávat svá práva u každého ze správců i vůči každému z nich.

Na základě provedené identifikace by DPO bezodkladně zaznamenal identifikovaného společného správce do záznamu podle **přílohy č. 10** – „**Seznam zpracovatelů a společných správců OÚ**“

5.14 Zástupce správce mimo EU

GBR nejmenovala žádného zástupce, který by byl usazený mimo EU.

5.15 Zpracování OÚ pro správce

Výběr vhodného zpracovatele provádí DPO podle charakteru, účelu a potřebných prostředků zpracování OÚ. DPO je povinna prověřit potencionálního zpracovatele, aby bylo jisté nebo téměř jisté, že poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo veškeré požadavky správce a byla zajištěna ochrana práv SOOÚ.

Písemný smluvní vztah se zpracovatelem uzavírá ŘG na doporučení DPO. Předmětný dokument obsahuje minimálně:

- předmět a dobu trvání zpracování,
- povahu a účel zpracování,
- typ osobních údajů
- kategorie SOOÚ,
- povinnost ohlašovat správci porušení zabezpečení OÚ,
- ostatní povinnosti a práva, zejména:
  - zákaz předání OÚ do třetí země nebo mezinárodní organizaci,
  - závazek mlčenlivosti,
  - oznamovací/ schvalovací povinnost pro zapojení subzpracovatele,
  - povinnost vymazat OÚ vč. jejich kopií a replikací po ukončení zpracování,
  - závazek umožnit kontrolu, audit, inspekci nebo jiný úkon správce, auditora nebo ÚOOÚ.

Schválené zpracovatele eviduje správce prostřednictvím řízeného záznamu v **příloze č. 9** – „**Seznam zpracovatelů a společných správců OÚ**“.

K termínu účinnosti Obecného nařízení musí DPO zajistit doplnění dříve uzavřených obchodních smluv s externími dodavateli, kteří při plnění předmětu smlouvy používají OÚ, u nichž je GBR správcem, o ustanovení upravující práva a povinnosti externího dodavatele v oblasti zpracování a ochrany OÚ. Externí dodavatel je nadále v systému ochrany OÚ klasifikován jako zpracovatel.

Doplnění smluvních vztahů provádí DPO prostřednictvím dodatku dříve uzavřené smlouvy nebo samostatnou smlouvou o zpracování OÚ tzv. „Zpracovatelskou smlouvou“, vycházející ze standardizovaných smluvních doložek uvedených v **kap. 6** – „**Související dokumentace**“.

Vzor dodatku je uveden v **příloze č. 14** – „**Dodatek smluvních vztahů pro zpracování OÚ**“

5.16 Záznamy o zpracování

GBR vede pouze nezbytné řízené záznamy o:

- činnostech zpracování,
- kategoriích činností zpracování,

Rozsah záznamů, jejich formální stránku i věcný obsah určuje DPO, po dohodě s majiteli dílčích procesů zpracování OÚ.

Účelem řízených záznamů je dokladování a prokazování shody realizovaného systému ochrany OÚ s požadavky Obecného nařízení a to jak k ÚOOÚ, tak i k ostatním zainteresovaným stranám.

5.17 Spolupráce s ÚOOÚ, vč. ohlašování bezpečnostních incidentů

Veškerou komunikaci s ÚOOÚ zajišťuje DPO, která zároveň organizuje a koordinuje případnou spolupráci pracovníků GBR s ÚOOÚ.

Spolupráce s ÚOOÚ může představovat součinnost při kontrolní a dozorové činnosti nebo dotazování a konzultace z iniciativy správce. Konzultace správce vyplývající z DPIA nejsou realizovány.

V případě vzniku jakéhokoli porušení zabezpečení OÚ oznámí DPO bezpečnostní incident ÚOOÚ a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Oznámení DPO neprovádí v případě, že je jisté, že porušení zabezpečení nemá za následek riziko pro práva a svobody SOOÚ.

Vzor formuláře viz. **příloha č. 12** – „**Vzor hlášení porušení zabezpečení**“.

5.18 Oznámení porušení zabezpečení OÚ SOOÚ

Oznámení porušení zabezpečení OÚ se SOOÚ realizuje pouze v případě, že DPO vyhodnotí následek jako vysoké riziko pro práva a svobody SOOÚ a pokud:

- již nebyla zavedena potřebná technická a organizační ochranná opatření např. šifrování,
- správce dosud nepřijal následná nápravná a preventivní opatření, která zajistí, že se vysoké riziko již neprojeví,

- oznámení nevyžaduje nepřiměřené úsilí (v tomto případě postačuje veřejné oznámení nebo podobné opatření).

5.19 DPIA a konzultace s ÚOOÚ

GBR neprovádí zpracování, které vyžaduje DPIA. Z tohoto titulu nejsou prováděny konzultace výstupů DPIA s ÚOOÚ.

5.20 DPO

GBR ustanovuje funkci DPO podle čl. 37, odst. 4). Činností DPO je pověřena externí právnická osoba, jejíž způsobilost byla ověřena interními postupy.

Součástí smluvního vztahu mezi správcem a externím dodavatelem je určení konkrétního zaměstnance externího subjektu, zajišťujícího činnost DPO.

V návaznosti na ustanovení DPO v GBR provedl správce ohlášení všech relevantních údajů ÚOOÚ a prostřednictvím standardních komunikačních kanálů i ostatním zainteresovaným stranám.

Vzor ohlášení DPO je uveden v **příloze č. 15** – „**Ohlášení DPO**“.

5.21 Kodexy chování a osvědčení

GBR nevyužívá k prokazování shody systému řízení GDPR s Obecným nařízením žádné odvětvové kodexy chování nebo osvědčení.

5.22 Předávání OÚ třetím stranám

GBR v rámci žádné z činností zpracování nepředává OÚ třetím stranám, tzn. do zemí mimo EU, ani mezinárodním organizacím.

Smluvním ujednáním se zákaz této činnosti vztahuje i na veškeré zpracovatele a subzpracovatele GBR podle kap. 5.15.

5.23 Závazná podniková pravidla

Struktura GBR nezahrnuje organizace ve stejné skupině podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost. GBR z tohoto důvodu nestanovila žádná závazná podniková pravidla pro mezinárodní předávání OÚ.

5.24 Dozor nad systémem ochrany OÚ

Vzhledem k charakteru činnosti GBR, spočívajícím v možném poskytování služeb na území více států EU (kooperace se zahraničními partnery, galeriemi apod.) nebo pro obyvatele více států EU (cizozemští návštěvníci GBR), se může se vyskytnout potřeba konat z důvodu ochrany práv a svobod SOOÚ, zejména pokud hrozí, že výkon některého z práv SOOÚ by mohl být značně ztížen.

Dozorový úřad má možnost přijmout na svém území prozatímní opatření se stanovenou dobou platnosti, která by neměla být delší než tři měsíce. V případech s přeshraničním rozměrem je DPO povinna zajistit účinnou spolupráci s ÚOOÚ (vedoucím dozorovým úřadem) a dotčenými dozorovými úřady tak, aby dotčené dozorové úřady byly na dvoustranné nebo mnohostranné úrovni schopny poskytovat vzájemnou pomoc a provádět společné postupy, aniž by mechanismus jednotnosti použily.

6 Související dokumentace

- 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).
- Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.
- Rozhodnutí Komise 2001/497/ES, o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí
- Rozhodnutí Komise 2004/915/ES, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí
- Rozhodnutí Komise 2010/87/EU, o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích
- WP 242 rev. 01 - Vodítka k právu na přenositelnost údajů
- WP 243 rev. 01 – Vodítka pro posouzení vlivu na ochranu údajů a stanovení, zda je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko
- Doporučení Komise 2003/361/ES, o definici mikropodniků, malých a středních podniků
- ČSN ISO/IEC 19794-2:2013 (369860) Informační technologie - Formáty výměny biometrických dat - Část 2: Data markantů prstu,
- ČSN ISO/IEC 19794-3:2008 (369860) Informační technologie - Formáty výměny biometrických dat - Část 3: Spektrální data vzoru prstu.
- ČSN ISO/IEC 19794-4:2017 (369860) Informační technologie - Formáty výměny biometrických dat - Část 4: Data obrazu prstu.
- ČSN EN ISO/IEC 27000 (369790) - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN EN ISO/IEC 27001 (369797) - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky.
- ČSN EN ISO/IEC 27002 (369798) - Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN ISO/IEC 27005 (369790) - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.

- ČSN ISO/IEC 27032 (369790) - Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost.
- Zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů v platném znění.
- Zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy v platném znění.
- Zákon č. 89/2012 Sb., občanský zákoník v platném znění.
- Zákon č. 127/2005 Sb., o elektronických komunikacích v platném znění.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti v platném znění.

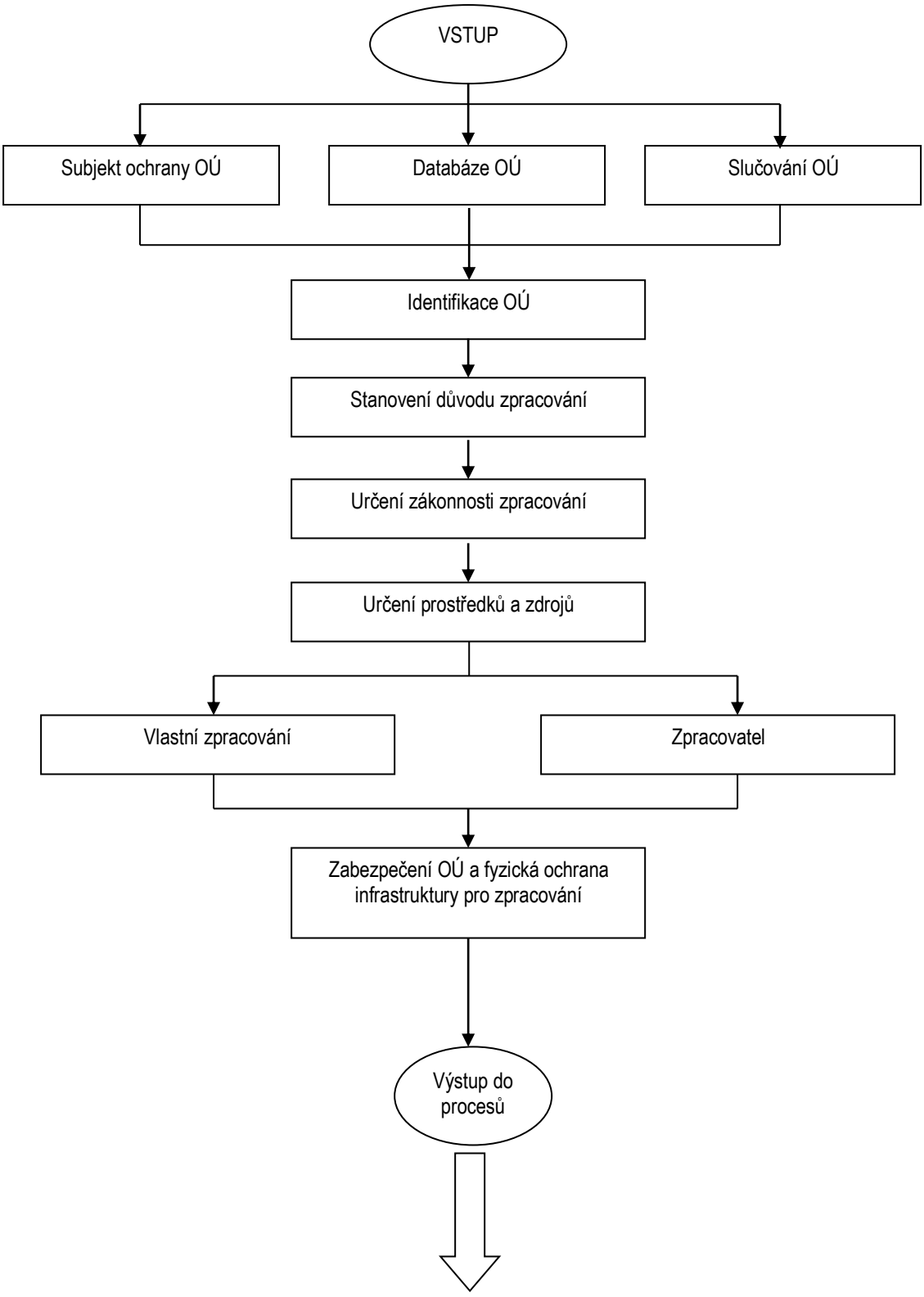
7 Seznam příloh

Vývojový diagram procesu „Realizace služeb“ - příloha č. 1

Řízeným záznamem z procesu realizace služeb je:

- příloha č. 1 - Vývojový diagram procesu
- Příloha č. 2 - Korelační tabulka
- Příloha č. 3 - Politika ochrany osobních údajů
- Příloha č. 4 - Seznam majitelů dílčích procesů zpracování
- Příloha č. 5 - Analytická tabulka
- Příloha č. 6 - Protokol aktualizace osobního údaje (vzor záznamu)
- Příloha č. 7 - Jmenovací dekret DPO (vzor záznamu)
- Příloha č. 8 - Interní sdělení (vzor záznamu)
- Příloha č. 9 - Seznam zpracovatelů a společných správců OÚ
- Příloha č. 10 - Informace o zpracování a právech SOOÚ (vzor záznamu A)
- Příloha č. 11 - Informace o zpracování a právech SOOÚ (vzor záznamu B)
- Příloha č. 12 - Vzor hlášení porušení zabezpečení
- Příloha č. 13 - Souhlas se zpracováním OÚ
- Příloha č. 14 - Dodatek smluvních vztahů pro zpracování OÚ
- Příloha č. 15 - Ohlášení DPO

Majitel procesu: DPO



- Nápravná a preventivní opatření
- Řízení infrastruktury a lidských zdrojů

Směrnice		**Obecné nařízení**
Číslo kap.	**název kap.**	**číslo čl.**
1	ÚČEL	2
2	ROZSAH PLATNOSTI	3
3	ZKRATKY A DEFINICE	4
4	VÝVOJOVÝ DIAGRAM A KONCEPČNÍ DOKUMENTY	-
5	POPIS PROCESU A ODPOVĚDNOST	24
5.1	Identifikace SOOÚ a zásady zpracování OÚ	1, 5
5.2	Zákonnost zpracování OÚ	6
5.2.1	Vymezení zákonnosti zpracování OÚ	6
5.3	Souhlas se zpracováním OÚ	7
5.3.1	Podmínky souhlasu se zpracováním OÚ	7
5.3.2	Rodičovský souhlas	8
5.4	Zvláštní OÚ	9
5.4.1	Specifikace zvláštních OÚ	9
5.4.2	Výjimky pro zpracování zvláštních OÚ	9
5.5	Zpracování OÚ týkajících se rozsudků v trestních věcech	10
5.6	Neidentifikovatelné zpracování OÚ	11
5.7	Transparentnost a postupy	12
5.8	Poskytování informací a přístup k OÚ	13, 14, 77, 79
5.9	Práva SOOÚ	-
5.9.1	Práva SOOÚ na přístup k vlastním OÚ	15, 77, 79
5.9.2	Právo SOOÚ na opravu k vlastních OÚ	16
5.9.3	Právo SOOÚ na výmaz vlastních OÚ	17
5.9.4	Právo SOOÚ na omezení zpracování vlastních OÚ	18
5.9.5	Právo SOOÚ na přenositelnost vlastních OÚ	20
5.9.6	Právo SOOÚ vznést námitku	21
5.10	Automatizované individuální rozhodování	22
5.11	Profilování SOOÚ	22
5.12	Zabezpečení/ ochrana OÚ	25, 32
5.13	Společní správci	26
5.14	Zástupce správce mimo EU	27

Směrnice		**Obecné nařízení**
Číslo kap.	**název kap.**	**číslo čl.**
5.15	Zpracování OÚ pro správce	28, 29, 33
5.16	Záznamy o zpracování	30
5.17	Spolupráce s ÚOOÚ vč. ohlašování bezpečnostních incidentů	31, 33, 36
5.18	Ohlašování porušení zabezpečení OÚ SOOÚ	34
5.19	DPIA a konzultace s ÚOOÚ	35, 36
5.20	DPO	37, 38, 39
5.21	Kodexy chování a osvědčení	40, 41, 42, 43
5.22	Předávání OÚ třetím stranám	44, 45, 46
5.23	Závazná podniková pravidla	47
5.24	Dozor nad systémem ochrany OÚ	55, 56

Motto: „**Ochrana osobních údajů všech fyzických osob je součástí firemní kultury, která je jedním z hlavních pilířů naší dlouhodobé strategie a trvalým závazkem ke všem zainteresovaným stranám**“

Výkonné vedení **Galerie Benedikta Rejta** považuje za prioritní rozhodnutí vytvořit, dokumentovat, uplatňovat a udržovat systém řízení osobních údajů fyzických osob **s cílem plnit na vysoké úrovni požadavky jejich důvěrnosti a ochránit jejich zájmy, práva i svobody.**

Veškeré činnosti při zpracování osobních údajů jsou realizovány s přihlédnutím k sociální odpovědnosti založené na důsledné vzájemné prospěšnosti ekonomické i sociální a při důsledném respektování řízení změn, který **Galerie Benedikta Rejta vnímá jako kontinuální, nikdy nekončící závazek**.

Výkonné vedení **Galerie Benedikta Rejta** deklaruje, že řízení osobních údajů podle 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, chápe jako dlouhodobý proces s nutností neustálého zlepšování jeho efektivnosti a osobní angažovanosti.

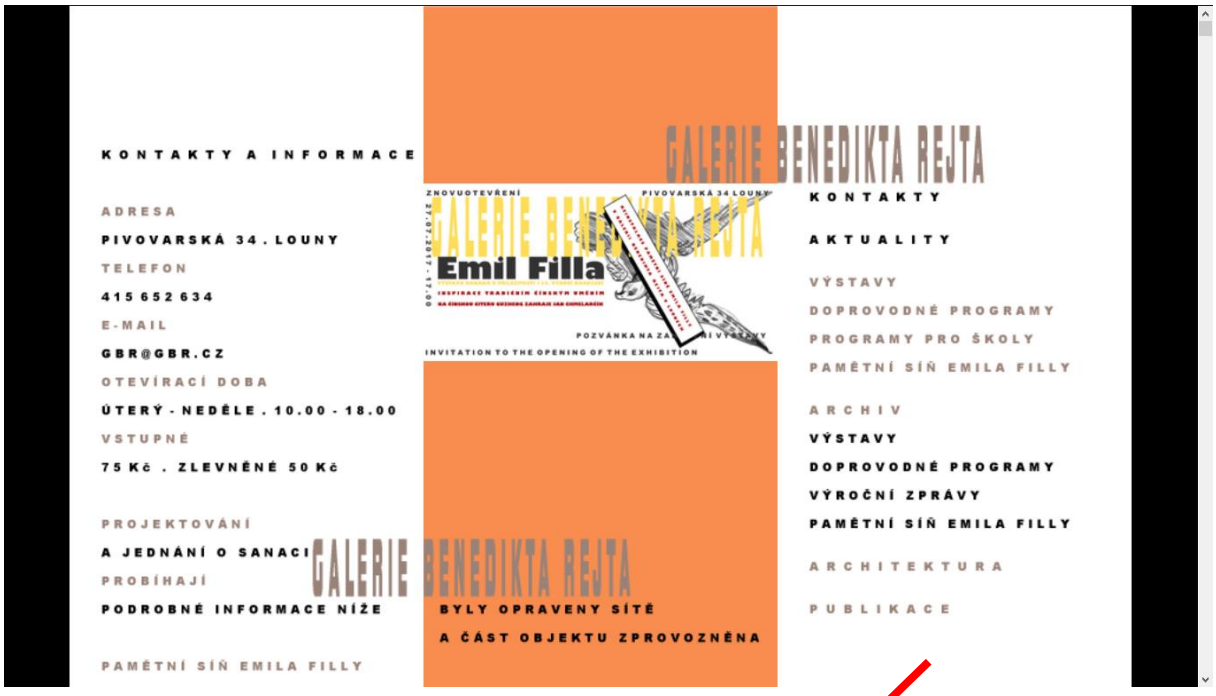
Výkonné vedení **Galerie Benedikta Rejta** bude poskytovat zdroje pro zajištění vysoké úrovně ochrany osobních údajů a vytvářet podmínky pro neustálé zlepšování systému jejich zpracování.

Pro zajištění uvedených strategických rozhodnutí a deklarací, výkonné vedení **Galerie Benedikta Rejta** vyhlašuje ve své působnosti tyto závazné zásady:

1. **Plnit na vysoké úrovni požadavky legislativních předpisů** v oblasti ochrany osobních údajů.
2. Na základě stávajících zkušeností **vytvořit**, **dokumentovat** a **uplatňovat** systém řízení ochrany osobních údajů.
3. Systematicky uplatňovat a rozvíjet **odpovědný přístup** k osobním údajům fyzických osob.
4. Firemní kulturu založit na třech klíčových oblastech: **komunikaci**, **řízení procesů** a **infrastruktuře**.
5. Zajišťovat a **neustále zlepšovat** úroveň ochrany osobních údajů a odbornou způsobilost zaměstnanců **Galerie Benedikta Rejta** pro jejich zpracování.
6. Udržovat a **rozvíjet vztahy** se způsobilými zpracovateli osobních údajů, založené na jasném vymezení účelů a prostředků zpracování a vysoké náročnosti na kvalitu i perspektivu spolupráce.
7. Vytvářet v **Galerii Benedikta Rejta** vědomí závažnosti a důležitosti pochopení a plného přijetí požadavků vytvářeného a etapovitě uplatňovaného systému řízení ochrany osobních údajů.
8. Rozpracovávat shora uvedené závazné zásady ochrany osobních údajů do konkrétních a měřitelných cílů ochrany osobních údajů se specifikovanou odpovědností a termíny jejich plnění.
9. Přezkoumávat systém ochrany osobních údajů v **Galerii Benedikta Rejta** ve stanovených termínech s cílem jeho stálého zlepšování, aktualizace i zajištění potřebných zdrojů na jeho udržování.

V Lounech, dne 25. 5. 2018

PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
Galerie Benedikta Rejta



GALERIE BENEDIKTA REJTA

Motto: **„Ochrana osobních údajů všech fyzických osob je součástí firemní kultury, která je jedním z hlavních pilířů naší dlouhodobé strategie a trvalým závazkem ke všem zainteresovaným stranám"**

Výkonné vedení **Galerie Benedikta Rejta** považuje za prioritní rozhodnutí vytvořit, dokumentovat, uplatňovat a udržovat systém řízení osobních údajů fyzických osob **s cílem plnit na vysoké úrovni požadavky jejich důvěrnosti a ochránit jejich zájmy, práva i svobody**.

Veškeré činnosti při zpracování osobních údajů jsou realizovány s přihlédnutím k sociální odpovědnosti založené na důsledné vzájemné prospěšnosti ekonomické i sociální a při důsledném respektování řízení změn, který **Galerie Benedikta Rejta vnímá jako kontinuální, nikdy nekončící závazek**.

Výkonné vedení **Galerie Benedikta Rejta** deklaruje, že řízení osobních údajů podle 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, chápe jako dlouhodobý proces s nutností neustálého zlepšování jeho efektivnosti a osobní angažovanosti.

Výkonné vedení **Galerie Benedikta Rejta bude** poskytovat zdroje pro zajištění vysoké úrovně ochrany osobních údajů a vytvářet podmínky pro neustálé zlepšování systému jejich zpracování.

Pro zajištění uvedených strategických rozhodnutí a deklarací, výkonné vedení **Galerie Benedikta Rejta** vyhlašuje ve své působnosti tyto závazné zásady:

1. **Plnit na vysoké úrovni požadavky legislativních předpisů** v oblasti ochrany osobních údajů.
2. Na základě stávajících zkušeností **vytvořit**, **dokumentovat** a **uplatňovat** systém řízení ochrany osobních údajů.
3. Systematicky uplatňovat a rozvíjet **odpovědný přístup** k osobním údajům fyzických osob.
4. Firemní kulturu založit na třech klíčových oblastech: **komunikaci**, **řízení procesů** a **infrastruktuře**.
5. Zajišťovat a **neustále zlepšovat** úroveň ochrany osobních údajů a odbornou způsobilost zaměstnanců **Galerie Benedikta Rejta** pro jejich zpracování.
6. Udržovat a **rozvíjet vztahy** se způsobilými zpracovateli osobních údajů, založené na jasném vymezení účelů a prostředků zpracování a vysoké náročnosti na kvalitu i perspektivu spolupráce.
7. Vytvářet v **Galerii Benedikta Rejta** vědomí závažnosti a důležitosti pochopení a plného přijetí požadavků vytvářeného a etapovitě uplatňovaného systému řízení ochrany osobních údajů.
8. Rozpracovávat shora uvedené závazné zásady ochrany osobních údajů do konkrétních a měřitelných cílů ochrany osobních údajů se specifikovanou odpovědností a termíny jejich plnění.
9. Přezkoumávat systém ochrany osobních údajů v **Galerii Benedikta Rejta** ve stanovených termínech s cílem jeho stálého zlepšování, aktualizace i zajištění potřebných zdrojů na jeho udržování.

V Lounech, dne 25. 5. 2018

PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
Galerie Benedikta Rejta

Identifikované procesy zpracování OÚ a majitelé dílčích procesů zpracování
(vzor záznamu)

Dílčí proces zpracování	Odpovídá	Spolupracuje

Dílčí procesy zpracování OÚ zahrnují i činnosti nezbytné k jejich nastavení, případně přenastavení a změnám. Jsou-li činnosti přípravy dílčího procesu zpracování natolik zásadní a náročné (např. na poskytnuté zdroje, zejména čas, pracovníky apod.), že by svými parametry převyšovaly dílčí proces zpracování, musí být vyčleněny do samostatného procesu, který však nemusí být relevantní pro systém řízení a zpracování OÚ (GDPR).

č.	**Osobní údaje**	**Účel záznamu**	**Zákonnost**	**Zdroj**	**Nezbytnost** (pouze u záznamů se souhlasem subjektu)	**Způsob aktualizace**	**Doba uložení**	**Umístění záznamu**	**….**
1.	Jméno rodné								
2.	Jméno křestní								
3.	Příjmení								
4.	Datum narození								
5.	Rodné číslo								
6.	Místo trvalého pobytu								
7.	Adresa bydliště								
8.	Občanství								
9.	Státní příslušnost								
10.	Podpis								
11.	Fotografie								
12.	Občanský průkaz								
13.	Řidičský průkaz vč. EŘP								
14.	Cestovní pas (osobní, služební, diplomatický)								
15.	Zbrojní průkaz (vč. EZP)								
16.	Ostatní osobní průkazy (ID karta)								
17.	Nemocenské (zdravotní) pojištění								
18.	Důchodové (penzijní) pojištění								
19.	Další identifikační údaje vydané státní správou								
20.	Číslo bankovního účtu								
21.	Informace o vzdělání								
22.	Profesní certifikáty								
23.	Profesní osvědčení								
24.	Komerční pojištění								
25.	Životní pojištění								
26.									
…									
124.									

Jméno rodné	Nedědičné osobní jméno, které spolu s děděným příjmením tvoří povinné oficiální dvoučlenné (popř. vícečlenné) osobní jméno, sloužící k občanskoprávní identifikaci každého subjektu ochrany osobních údajů.
Jméno křestní	Plní funkci rodného jména, jeho udělením při křtu.
Příjmení	Identifikátor subjektu osobních údajů, který je zbaven významu slova. Ustáleně označují nositele, jsou dědičná zpravidla po otci, přecházejí v přechýlené podobě na manželku a na dcery. Podle příjmení tak mohou být zprostředkovaně identifikované další subjekty ochrany osobních údajů (rodinní příslušníci).
Datum narození	Vyjadřuje den, měsíc a rok narození subjektu ochrany osobních údajů.
Rodné číslo	Devítimístný nebo desetimístný číselný identifikátor přidělovaný obyvatelům České republiky. Rodné číslo je upraveno zákonem č. 133/2000 Sb., o evidenci obyvatel. Z rodného čísla lze odvodit datum narození a pohlaví subjektu ochrany osobních údajů. Prvních šest číslic vyjadřuje datum narození ve formátu „rrmmdd“, přičemž pro ženy se k měsíci narození připočte 50 nebo 70. Koncovka rodného čísla za lomítkem odlišuje osoby stejného pohlaví narozené ve stejný den. Pro osoby narozené do roku 1953 včetně za lomítkem následují tři číslice, od roku 1954 čtyři číslice. Formát rodného čísla přestane být uplatňován v roce 2054. Desetimístná rodná čísla jsou beze zbytku dělitelná jedenácti.
Místo trvalého pobytu	Adresa pobytu subjektu osobních údajů v České republice, kterou si zvolí. Subjekt může mít jen jedno místo trvalého pobytu, a to ve způsobilé nemovitosti. Tento objekt musí být označen popisným, evidenčním nebo orientačním číslem a musí být přímo určen pro bydlení, ubytování nebo alespoň pro individuální rekreaci. Trvalý pobyt má pouze evidenční charakter kvůli potřebám státu a nemusí být proto totožný s reálným bydlištěm. Právní úprava místa trvalého pobytu je obsažena v § 10–12 zákona č. 133/2000 Sb., o evidenci obyvatel.
Adresa bydliště	Právní pojem označující místo, kde se subjekt ochrany osobních údajů trvale zdržuje. V českém právu se soukromoprávní pojem „adresa bydliště“ odlišuje od veřejnoprávního pojmu „trvalý pobyt“, který má jen evidenční charakter, ačkoli často může jít o stejnou adresu. Definice bydliště je obsažena v ustanovení § 80 NOZ.
Občanství	Časově relativně trvalý, místně neomezený právní svazek subjektu ochrany osobních údajů a daného České republiky.
Státní příslušnost	Pojem státní příslušnost je významově obdobný jako občanství, ale je obsahově širší, neboť i právnické osoby příslušné k ČR.
Podpis	Je vyjádřením souhlasu subjektu ochrany osobních údajů s projevenou vůlí (s výjimkou podpisového vzoru). Je umísťován na konci textu, aby dovršil dané právní jednání, text následující až za podpisem nemá právní následky. Za podpis se považuje signatura, parafa, famílie, autogram ad.).
Fotografie	Trvalý obrazový záznam subjektu ochrany osobních údajů, provedený digitálně prostřednictvím čipu nebo chemickým procesem prostřednictvím světlocitlivého materiálu, v černobílé, monochromatické, barevné, infračervené či jiné podobě, umožňující přímou nebo zprostředkovanou (např. prostřednictvím metadat) identifikaci subjektu ochrany osobních údajů. Při posuzování nezáleží na důvodu pořízení fotografie např. amatérská, profesionální, komerční, pracovní, umělecká, vědecká, forenzní atd. Kromě ochrany osobních údajů podléhá fotografie i regulaci autorských práv a výjimkám tzv. licencím (např. novinářská).
Občanský průkaz	Státní správou vydávaný identifikační doklad subjektu ochrany osobních údajů, podle zákona č. 328/1999 Sb., o občanských průkazech a podle vyhlášky č. 400/2011 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech. Od roku 2018 začne být pouze vydáván elektronický OP splňující podmínky nařízení eIDAS s novým typem čipu.
Řidičský průkaz vč. EŘP	Státní správou vydávaný identifikační doklad subjektu ochrany osobních údajů, prokazující řidičské oprávnění k řízení motorových vozidel.
Cestovní pas (osobní, služební, diplomatický)	Cestovní pas je identifikační doklad subjektu ochrany osobních údajů, který pro něj vydává vláda státu, jehož je občanem. Je základním dokumentem, který je potřeba pro vstup a projíždění jinými státy. Cestovní pasy obvykle obsahují fotografii držitele, podpis, datum narození, národnost a někdy další znaky identifikující člověka, proto je lze používat jako průkaz totožnosti.
Zbrojní průkaz (vč. EZP)	Veřejná listina, která subjektu ochrany osobních údajů opravňuje k nabývání vlastnictví a držení zbraně nebo střeliva do těchto zbraní v rozsahu oprávnění stanovených pro jednotlivé skupiny zbrojního průkazu a v rozsahu těchto oprávnění k jejich nošení dle zákona č. 119/2002 Sb., o zbraních. Řízení osobních údajů vyplývajících z jejich evidence ve zbrojním průkazu se vztahuje i na osobní údaje uvedené v Evropském zbrojním průkazu, pokud tato povinnost správci vyplyne ze vztahů se subjektem ochrany osobních údajů.
Ostatní osobní průkazy (ID karta)	Ostatní osobní, identifikační průkazy, které jsou vydávány za účelem prokázání totožnosti a zamezení podvodů se záměnou totožnosti, pokud obsahují chráněné údaje o subjektu ochrany osobních údajů, obvykle zejména jeho celé jméno, fotografii, datum narození, rodné číslo, povolání, adresu bydliště, vyznání národnost nebo biometrické údaje apod. V podmínkách ČR půjde zejména o zdravotní kartu občana EU, průkaz pro veřejnou dopravu, školní a závodní jídelny, veřejné knihovny, přístup do objektu (vstup na pracoviště, do garáže apod.
Nemocenské (zdravotní) pojištění	Osobní údaje subjekty ochrany vyplývající ze zákona č.187/2006 Sb., o nemocenském pojištění v platném znění.
Důchodové (penzijní) pojištění	Osobní údaje subjekty ochrany vyplývající ze zákona č. 155/1995 Sb., o důchodovém pojištění

	v platném znění, upravujícím hmotné zabezpečení pojištěnců pro případ stáří, poklesu pracovní schopnosti z důvodu dlouhodobě nepříznivého zdravotního stavu (tj. invalidity) a úmrtí živitele prostřednictvím důchodů. Zpracování osobních údajů v předmětné kategorii se týká všech správců, pro všechny skupiny pojištěnců, tj. zaměstnance, osoby ve služebním poměru, členy družstev, osoby samostatně výdělečně činné a další skupiny pojištěnců.
Číslo bankovního účtu	Číslo finančního účtu v bance, který zaznamenává finanční transakce subjektu ochrany osobních údajů a sleduje tak jeho finanční účtu. Jedná se o bankovní účty v celém rozsahu jejich typu, tzn. kreditní, debetní, depozitní, úvěrové účty či podle určení tzn. běžné, termínované, spořící úvěrové, zahraniční, ale i např. notářskou úschovu. V souladu s nařízením Evropského parlamentu a Rady (ES) č. 924/2009 a (EU) č. 260/2012 se jedná pouze o vnitrostátní formát bankovního účtu nebo o formát IBAN (do osobních údajů již nezahrnujte čísla bankovních účtů ve formátu BBAN.
Informace o vzdělání	Informace o souhrnu znalostí, dovedností a schopností, které subjekt ochrany osobních údajů získával prostřednictvím vzdělávání, výuky a studia, výhradně však jako uznané výsledky vzdělávání nebo učení (stupeň vzdělání), popřípadě kvalifikace uvedená v Národní soustavě kvalifikací.
Profesní certifikáty	Doklad o profesní kvalifikaci, která stanovuje standardy pro vzdělávání, odbornou přípravu a odborné kompetence. Většinou pokud byla zakončena profesní zkouškou.
Profesní osvědčení	Doklad o profesní kvalifikaci, která stanovuje standardy pro vzdělávání, odbornou přípravu a odborné kompetence. Většinou pokud není zakončena profesní zkouškou a vystavuje se například pouze na základě absolvování a účasti na odborném, doškolovacím nebo jiném kurzu, semináři apod.
Komerční pojištění	Údaje subjektu ochrany osobních údajů vyplývající ze závazku pojistitele, potvrzeného pojistnou smlouvou s pojistníkem, který sjednává pojištění ve prospěch pojištěného (pojištěnce), vůči pojištěnci tlumit dopad (škodu) z určených negativních škodních událostí, případně důchodové připojištění nebo životní pojištění.
Životní pojištění	Údaje subjektu ochrany osobních údajů vyplývající z pojistné smlouvy mezi pojistníkem a pojistitelem, ve které se pojistitel zavazuje zaplatit určenou peněžní částku pojištěné osobě v případě pracovní neschopnosti, doby nezbytného léčení úrazu, za trvalé následky úrazu, za hospitalizaci následkem úrazu, v případě invalidity 1., 2. nebo 3. stupně, závažných onemocnění a dalších připojištění nebo tuto částku zaplatit oprávněné osobě v případě úmrtí pojištěného, avšak pouze v případě, že pojistník umožňuje daňové úlevy na dani z příjmu, za podmínek stanovených zákonem a správce (např. zaměstnavatel) s relevantními údaji pracuje např. při zpracování daňového přiznání k dani z příjmu fyzických osob. Jsou-li součástí smlouvy i osobní údaje oprávněné osoby (obmyšlené osoby), musí správce chránit i tyto osobní údaje.
Doplňkové penzijní spoření	Údaje subjektu ochrany osobních údajů vyplývající z realizovaného doplňkového penzijního připojištění, podle zákona č. 427/2011 Sb., o doplňkovém penzijním spoření v platném znění, v případě, že je realizováno s příspěvkem zaměstnavatele nebo pokud správce zpracovává pro subjekt ochrany osobních údajů daňové přiznání k příjmu fyzických osob a ten uplatňuje legislativně určené daňové zvýhodnění.
Telefonní číslo	Slouží k jednoznačné identifikaci subjektu ochrany osobních údajů v telefonní síti. Jedná se výhradně o telefonní číslo ve veřejné telefonní síti a v úplném formátu podle národní číslovacího plánu vč. telefonního čísla bez mezinárodní předvolby. Telefonní čísla ve firemní telefonní síti nejsou osobními údaji ve smyslu GDPR, nap. 474 55*6 789* je osobním údajem podle GDPR, interní linka 6789 nikoliv. Telefonní číslo subjektu ochrany osobních údajů zaznamenané v adresáři, v seznamu kontaktů či v jiném umístění podléhá ochraně osobních údajů podle GDPR. Telefonní číslo hot-line např. informační linky ČEZ, RWE ad. nepodléhá ochraně osobních údajů podle GDPR a to i přesto, že je linka obsluhována zaměstnanci příslušné organizace, kteří se při přijetí hovoru představují vlastním jménem a příjmením. Základním hlediskem podřízenosti obecného telefonního čísla řízení podle GDPR je schopnost správce nebo zpracovatele dohledat prostřednictvím běžných a nekomplikovaných postupů konkrétní subjekt ochrany osobních údajů. Běžné a nekomplikované postupy mohou zahrnovat využití vlastní databáze ostatních zpracovávaných osobních údajů nebo běžné webové aplikace pro dohledání neznámých telefonních čísel, které identifikují telefonní číslo, neuložené v seznamu kontaktů např. Number Finder, Search & Locate Number on Map ad.
E-mail	Internetový systém elektronické pošty založený na protokolu SMTP (Simple Mail Transfer Protocol). Ochrana GDPR se nevztahuje na osobní údaje v intranetových poštovních systémech, které umožňují zasílání a přijímání zpráv uživatelům uvnitř jedné společnosti nebo organizace (tyto systémy často používají nestandardní protokoly, mívají ovšem bránu, která jim dovoluje posílat a přijímat e-maily z internetu). Postup je obdobný jako u telefonních čísel. Je nezbytné rozlišovat e-mailové adresy, jednoznačně implikující konkrétní fyzickou osobu a e-mailové adresy částečně nebo zcela obecného formátu. Při analýze je nezbytné zvažovat schopnost správce nebo zpracovatele identifikovat konkrétní subjekt ochrany osobních údajů, pokud se tak děje „…běžnými a technicky nekomplikovanými postupy, odpovídajícím standardní technologické úrovni obvyklé v místě a čase…“. Pokud je po zadání e-mailu do vyhledávače (Seznam, Google…) nebo jiným způsobem vstupní identifikátor spárován s konkrétním subjektem ochrany osobních údajů nebo jiným identifikátorem, který až následně umožní sprárování s konkrétním subjektem ochrany osobních údajů, podléhá řízení osobního údaje GDPR.

Facebook	V případě, že správce nebo zpracovatel komunikuje se subjekty ochrany osobních údajů prostřednictvím oficiální firemní stránky (Pages) nebo prostřednictvím osobních profilů subjekty ochrany osobních údajů, kteří mohou být jejich příznivci (Likers). Např. pokud dochází k zasílání reklamy (informace o výrobcích, službách, aktivitách, událostech, místech a to i v kombinacích např. PPC), pokud jsou umísťovány příspěvky do profilů uživatelů (Wall) atd.
WhatsApp	V případě, že správce nebo zpracovatel komunikuje se subjekty ochrany osobních údajů prostřednictvím multiplatformní aplikace umožňující výměnu zpráv a multimediálních souborů mezi vlastníky smartphonů pomocí internetu a zasílá nebo získává textové zprávy fotografie, videosoubory, audiosoubory a polohu subjektu ochrany osobních údajů apod.
Messenger	Jakožto obecný systém umožňující komunikaci správce nebo zpracovatele osobních údajů se subjektem ochrany osobních údajů, prostřednictvím výměny textových zpráv, video přenosu, chatu, sdílení fotografií, hlasového volání ad.
Skype	Peer-to-peer (P2P) program podporující internetovou telefonii (VoIP) a videohovory, instant messaging i přenos datových souborů. Komunikace probíhá decentralizovaně přes různé počítače zapojené v síti Skype, centrální server pouze ověřuje veřejný klíč uživatele při přihlášení do sítě. Komunikace je šifrována na 256 bitů, ale součástí přenosu je odeslání MAC adresy a sériového čísla základové desky počítače. Komunikační protokol ani zdrojové kódy programu nejsou veřejně dostupné. Pro zajištění ochrany osobních údajů nesmí být povoleno ovládán vnějších aplikací přes API (Application Programming Interface - rozhraní pro programování aplikací).
Linked It	Pokud správce nebo zpracovatel využívá pro součinnost osobní údaje z profesní sociální sítě, kde se v profilu uživatele se nachází jeho životopis obsahující osobní údaje, popis kariéry, pracovní místa, vzdělání ad. a kde je uživatel zapojen prostřednictvím vlastních kontaktů i do kontaktů svých kontaktů, čímž vzniká provázaná síť uživatelů nebo pokud správce nebo zpracovatel využívá profesní sociální síť k vyhledávání nových obchodních partnerů či uveřejnění možností spolupráce.
Webmail	Umožňuje uživatelům přistupovat k jejich e-mailovým schránkám prostřednictvím webového prohlížeče. Webmail je používán jako alternativa ke klasickým aplikacím e-mailových klientů (např. Microsoft Outlook, Mozilla Thunderbird ad.). Webmail poskytují téměř všechny internetové portály a poskytovatelé webových služeb (např. Gmail, Yahoo! Mail, Hotmail, AOL, Seznam, Centrum ad.
Viber	Peer-to-peer (P2P) program podporující internetovou telefonii (VoIP) a videohovory, instant messaging i přenos datových souborů. Je dostupný pro většinu operačních systémů (Android, iOS, Windows Phone, Linux). Po spuštění se vstupním identifikátorem stává telefonní číslo subjektu ochrany osobních údajů a aplikace automaticky synchronizuje kontakty z telefonu a automaticky provádí rešerši, který ze sdílených kontaktů službu využívá.
Osobní profily na jiných sociálních sítích	Jakékoliv profily na sociálních sítích, které nejsou uvedeny mezi výše uvedeným demonstrativním výčtem. Sociální sítě je potřeba v analýze přesně vymezit a stanovit, jakého zpracování osobních údajů se používání sociální sítě týká.
Blog	Osobní údaje subjektu ochrany ve webové aplikaci (blogu), pokud je editor (bloger) zároveň správcem osobních údajů a tyto používá v příspěvcích, bez ohledu na to, zda se jedná o textovou nebo administrační část. Osobním údajem bude i přezdívka na blogu, je-li podle ní fyzická osoba identifikovatelná. Způsob zpracování (řízení ochrany osobních údajů) bude rozdílný v případech, že se jedná o uzavřenou skupinu nebo formu, kde je například nabízen přehled nejnovějších příspěvků prostřednictvím RSS (Rich Site Summary), obsahujícím metadata.
Chat	Osobní údaje subjektu ochrany účastnícího se komunikace prostřednictvím komunikační sítě na základě specifických protokolů (IRC, TS, XMPP ad.), v reálném čase a to bez ohledu na skutečnost, zda se jedná o psaný text, audiochat, videochat nebo hybridní formy.
Rodinný stav	V souladu s ELDP (Evidenčním listem důchodového pojištění) dle § 16 odst. 4 a 5 zákona č. 155/1995 Sb., o důchodovém pojištění – vztahuje se pouze k osobním údajům subjektu ochrany v rozsahu svobodný/á, ženatý/vdaná, vdova, vdovec, rozvedený/á.
Jméno rodné manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Jméno křestní manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Příjmení manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Datum narození manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Rodné číslo manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Místo trvalého pobytu manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Adresa bydliště manželky	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.

Případné ostatní osobní údaje manželky	Jedná se např. o zdravotní stav, zdravotní hendikepy, znevýhodnění atd., pokud se přímo vztahuje zpracování osobních údajů subjekt ochrany, s nímž má správce nebo zpracovatel přímý vztah.
Jméno rodné dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Jméno křestní dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Příjmení dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Datum narození dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Rodné číslo dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Místo trvalého pobytu dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Adresa bydliště dítěte	Osobní údaj je zpracováván ve stejném režimu jako příslušný osobní údaj subjektu ochrany osobních údajů, s nímž má správce nebo zpracovatel přímý vztah.
Případné ostatní osobní údaje dětí	Jedná se např. o zdravotní stav, zdravotní hendikepy, znevýhodnění atd., pokud se přímo vztahuje zpracování osobních údajů subjekt ochrany, s nímž má správce nebo zpracovatel přímý vztah.
Členství v odborech	Týká se výhradně sdružování v odborových organizacích v České republice, podle obecné úpravy o sdružování podle zákona č. 89/2012 Sb., občanský zákoník. Odbory musí být sdružením zaměstnanců, založeným s cílem prosazovat jejich pracovní, hospodářské, politické, sociální a jiné zájmy. Pouze tak mohou odbory jednat jménem pracovníků, které zastupují, pokud jednají se zaměstnavatelem nebo státem, například ohledně výše mezd nebo pracovních podmínek.
Záznamy o probíhajícím trestním stíhání	Informace o trestní stíhání subjektu ochrany osobních údajů v rámci trestního řízení, a to od zahájení stíhání usnesením, až do právní moci rozsudku či jiného rozhodnutí, kterým se trestní řízení končí. Trestním stíháním přechází trestní řízení z fáze prověřování okolností, zda trestný čin spáchán vůbec byl, do fáze vyšetřování spáchaného trestného činu, a je proto zahajováno navíc až poté, co je dostatečně odůvodněn závěr, že jej spáchal subjekt ochrany osobních údajů. Ochrana osobních údajů se týká i informací v rámci odložení věci. Chráněnými osobními údaji je usnesení o zahájení, přerušení i zastavení trestního stíhání, popis vyšetřovaného skutku, zákonné označení trestného činu a identifikace subjektu ochrany osobních údajů.
Trestní záznamy	Informace o subjektu ochrany osobních údajů uvedené zejména v rejstříku trestů vedeném Ministerstvem vnitra České republiky, podle zákona č. 269/1994 Sb., o rejstříku trestů, v němž se vede evidence osob pravomocně odsouzených soudy v trestním řízení a dále evidenci jiných skutečností významných pro trestní řízení. Údaje z evidence slouží správcům osobních údajů především pro potřebu trestního, občanskoprávního nebo správního řízení a k prokazování bezúhonnosti.
Soudní rozhodování nebo rozhodnutí	Například, pokud správce nebo zpracovatel využívá ke své činnosti obecná stanoviska kolegia nejvyššího soudu nebo tzv. Zelenou knihu (Sbírku soudních rozhodnutí a stanovisek), jakožto významného prostředku pro předvídatelnost rozhodování českých soudů. Mimo tyto případy i veškeré informace o podání obžaloby na subjekt ochrany osobních údajů, zahájení a průběhu hlavního líčení a pravomocném i nepravomocném rozsudku.
Exekuční záznamy	Veškeré záznamy vztahující se k subjektu ochrany údajů, uvedené v oficiální exekuční databázi vedené a spravovaná Exekutorskou komorou ČR, podle zákonného zmocnění daného ustanovením § 125 zákona č. 120/2001 Sb.
Mzdové záznamy	Zahrnuje např. obsah existujících mzdových listů a výkazů, patřících k pracovním poměrům jednotlivých subjektů ochrany osobních údajů, vyplývajících z povinností správců zaměstnavatelů (správců), zejména podle zákon č. 586/1992 Sb., o daních z příjmů a zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení (v platných zněních)
Zdravotní stav	Osobní údaje mohou zahrnovat např. informace o invaliditě, o změnách stupně invalidity, o dlouhodobě nepříznivém zdravotním stavu, o neschopnosti vykonávat z důvodu zdravotního stavu výdělečnou činnost, o zdravotním znevýhodnění, o pohyblivosti a orientaci subjektu ochrany osobních údajů pro účely řízení o přiznání průkazu osoby se zdravotním postižením, o nárocích na zvláštní pomůcky při vadách nosného nebo pohybového ústrojí, o sluchovém postižením, o zrakovém postižení, o mentální retardací, o stupně závislosti subjektu ochrany osobních údajů ad. Vždy se musí jednat o oficiální dokumenty nebo záznamy lékaře nebo zdravotnického zařízení, zpracované přímo pro subjekt ochrany osobních údajů nebo pro okresní správu sociálního zabezpečení za účelem posouzení zdravotního stavu a pracovní schopnost, zejména pro účely sociálního zabezpečení, pro účely poskytnutí sociálních dávek, vydání průkazu osoby se zdravotním postižením atd. Osobní údaje zahrnují i informace pro účely nemocenského pojištění, kontrolu správnosti posuzování zdravotního stavu a dočasné pracovní neschopnosti ošetřujícími lékaři, posuzování pracovní schopnost dočasně práce neschopných pojištěnců před i po uplynutí podpůrčí doby atd.

Zdravotní postižení	Informace o subjektu ochrany osobních údajů specifikující zdravotní postižení tj. jakoukoliv odchylkou ve zdravotním stavu, která jej omezuje v určité činnosti (uplatnění v zaměstnání, uplatnění ve společnosti, pohyb, kvalita života ad.). Podle typu správce je nezbytné správně identifikovat a provádět zpracování na základě zákonné povinnosti správce. Toto analytická část bude zpracována důsledně podle oborové příslušnosti správce (jiná bude u komerční organizace, jiná u školského zařízení atd.). Definice zdravotního postižení jsou uvedeny v příslušných legislativních předpisech: - zákon č. 108/2006 Sb., o sociálních službách specifikuje zdravotní postižení jako „tělesné, mentální, duševní, smyslové nebo kombinované postižení, jehož dopady činí nebo mohou činit osobu závislou na pomoci jiné osoby“. - zákon č. 435/2004 Sb., o zaměstnanosti vymezuje osoby se zdravotním postižením jako fyzické osoby, které jsou orgánem sociálního zabezpečení uznány jako invalidní ve třetím stupni (tj. osoby s těžším zdravotním postižením) nebo v prvním či druhém stupni. Mezi osoby se zdravotním postižením se navíc řadí i fyzické osoby, které byly orgánem sociálního zabezpečení posouzeny, že již nejsou invalidní, a to po dobu 12 měsíců ode dne tohoto posouzení. Naopak osobami se zdravotním postižením již nejsou fyzické osoby, které byly podle předchozí a nyní už neúčinné právní úpravy rozhodnutím úřadu práce uznány jako zdravotně znevýhodněné. - V oblasti zdravotního pojištění se v ČR pojem postižení definuje jako stav závažného a trvalého snížení funkční schopnosti vzniklého v důsledku úrazu, nemoci či vrozené vady. - V oblasti vzdělávání, upravené zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávaní (školský zákon), lze za osoby s postižením považovat „všechny děti, mladé lidi a dospělé, kteří jsou v učení, sociálním chování, v komunikaci a řeči nebo v psychomotorických schopnostech tak omezeni, že jejich spoluúčast na životě ve společnosti je podstatně ztížena“ a potřebují speciální pedagogickou podporu. - Listina základních práv Evropské unie (někdy též Charta základních práv) je dokument zakotvující základní práva při uskutečňování norem evropského práva. Listina byla vyhlášena jako samostatný dokument, který má dle čl. 6 Smlouvy o Evropské unii stejnou právní sílu jako zakládající smlouvy a tvoří součást primárního práva Evropské unie. Osob se zdravotním pojištěním se týká čl. 26. - Úmluva OSN o právech osob se zdravotním postižením (Convention on the Rights of Persons with Disabilities) přijata v roce 2006, s účinností od 3. května 2008 definuje subjekty se zdravotním postižením jako osoby mající dlouhodobé fyzické, duševní, mentální nebo smyslové postižení, které v interakci s různými překážkami může bránit jejímu plnému a účinnému zapojení do společnosti na rovnoprávném základě s ostatními.
Lékařské nálezy	Záznamy, které vyplňuje lékař nebo zdravotnické zařízení a které vyjadřují stav subjektu ochrany osobních údajů z cíleného nebo komplexního vyšetření. Může se jednat o jakoukoliv formu lékařského nálezu, který správce zpracovává tzn. fyziologický nález (výsledek vyšetření, který je v souladu se stavem organismu ve zdraví a při němž nebylo zjištěno nic chorobného patologického), objektivní nález (výsledek vyšetření, které lékař provádí při fyzikálním vyšetření), patologický nález (výsledek fyzikálního, laboratorního či přístrojového vyšetření, který upozorňuje na nějakou chorobu, např. nádorové ložisko, zánět, vyrážka na kůži, otok kloubu aj), anamnézy subjektu ochrany osobních údajů vč. rodinné anamnézy, výsledky průběžného stanovování diagnózy atd.
Lékové předpisy	Informace o předepsaných lécích, které subjekt ochrany osobních údajů užívá pro zajištění zdraví nebo předcházení nepříznivým zdravotním stavům. Relevantní jsou léky, které jou nezbytné pro výkon povolání, léky, které jsou nezbytné pro děti v rámci školních aktivit ad.
Náboženské vyznání	Příslušnost subjektu ochrany osobních k náboženství, jakožto soustavě jednání, symbolů a představ, jimiž různá společenství a církve vyjadřují reálný, životní či osobní vztah k transcendentní zkušenosti či transcendentním představám.
Filozofické vyznání	Informace o subjektu ochrany osobních údajů vyjadřující specifické osobní hledisko k určité skutečnosti, přirozené různosti, pluralitě názorů a soustavnému, racionálnímu a kritickému zkoumání skutečností, světa, člověka i toho, co je přesahuje.
Kulturní preference	Osobní údaje identifikující motivaci, hodnoty a další faktory, které ovlivňují preference a spotřební chování subjektu ochrany osobních údajů v kulturním sektoru. Může se především jednat o statistické techniky, které dovedou měřit významnost faktorů ovlivňujících spotřební chování subjektů ochrany v kultuře a může sloužit správcům nebo zpracovatelům k efektivnějším manažerským a strategickým rozhodnutím, týkajícím se subjektů ochrany. Osobní údaje v položce č. 69 mají úzkou vazbu na osobní údaje v položce č. 73.
Sexuální orientace	Informace o sexuálním zaměření a sexuálních preferencích subjektu ochrany osobních údajů, zejména náklonnosti k mužům, ženám či oběma pohlavím, věkovým skupinám nebo typům jiných objektů sexuální touhy. Sexuální orientace ve vztahu k pohlaví je pojímána buď jako souvislé spektrum od výhradně heterosexuální, po výhradně homosexuální nebo bisexuální.

Sexuální identita	Identifikace subjektu ochrany osobních údajů v návaznost na sebepojetí, které určuje, zda se považuje za muže či ženu a nemusí vždy být v souladu s biologickým pohlavím a skutečnou sexuální orientací, stejně tak ani se sexuálním chováním. Řízenými údaji mohou být informace o transsexualitě (neztotožněním se s biologickým pohlavím) a transvestitismu (touha podobat se opačnému pohlaví jen v některých vnějších projevech) apod.
Rasový původ	Příslušnost subjektu ochrany osobních údajů ke skupině fyzických osob sdílejících stejnou genetickou výbavu, společné tradicí, jazyk, společenský řád, umění, postoje, vymoženosti dané skupiny nebo jiné znaky. Rasový původ může mít přímou vazbu na další vstupní identifikátory, zejména náboženské vyznání (položka č. 67), filozofické vyznání (položka č. 68), kulturní preference atd.
Etnický původ	Informace o příslušnosti subjektu ochrany osobních údajů k určitému etniku tzn. skupině fyzických osob, které spojuje pocit sounáležitosti, víra ve společný původ a dějiny, společné označení sama sebe neboli kulturní prvky odlišující je od jiných etnik.
Informace o politických názorech	Přímé názory a zájmy nebo blízké názory subjektů ochrany osobních údajů na programy politických stran, hnutí či uskupení, včetně preferencí vyjádřených volbou, účastí ve volbách nebo jen podporou politických subjektů (položka nebude zohledněna za předpokladu, že je správce nebo zpracovatel politickým subjektem).
DNA (občasné označení DNK)	Osobní údaje ve formě záznamů DNA (Deoxyribonukleová kyselina, deoxyribonucleic acid,) tj. biologické makromolekuly – polymeru v podobě řetězce nukleotidů, složených z cukru deoxyribózy, fosfátové skupiny a jedné ze čtyř nukleových bází. Informační funkci (osobní údaje) vykonávají právě báze, jimiž může být adenin (A), guanin (G), cytosin (C) nebo thymin (T). Pro oblast GDPR se může jednat zejména o záznamy z oblasti lékařství, kriminality, biologie atd. Osobní údaj musí splňovat požadavky ČSN ISO/IEC 19794-14:2014 (369860) Informační technologie - Formáty výměny biometrických dat - Část 14: Data DNA
Otisk prstů	Struktura kožních papilárních liniích na prstech (výjimečně na celých dlaních), která je charakteristická pro každý subjekt ochrany osobních údajů. Údaj bude relevantní především pokud správce provozuje docházkový nebo přístupový systém, založený na snímání otisku prstu nebo pokud využívá zařízení, na nichž je identifikace uživatele prováděna otiskem prstu (mobilní zařízení, tablety, telefony atd.). Osobní údaj musí splňovat požadavky ČSN ISO/IEC 19794-2:2013 (369860) Informační technologie - Formáty výměny biometrických dat - Část 2: Data markantů prstu, ČSN ISO/IEC 19794-3:2008 (369860) Informační technologie - Formáty výměny biometrických dat - Část 3: Spektrální data vzoru prstu a ČSN ISO/IEC 19794-4:2017 (369860) Informační technologie - Formáty výměny biometrických dat - Část 4: Data obrazu prstu.
Scan tváře	Osobní údaje generované systémy pro scan tváře (čtečka tváře – Face ID). Účel a řízení osobních údajů bude obdobné jako u položky č. 77 vč. případů, kdy by docházelo k modelování získaných dat např. prostřednictvím 3D tiskárny – osobním údajem by byl i výsledný produkt, za předpokladu, že by bylo dosaženo vysoké shody marketů se subjektem osobních údajů. Osobní údaj musí splňovat požadavky ČSN ISO/IEC 19794-5:2013 (369860) Informační technologie - Formáty výměny biometrických dat - Část 5: Data obrazu obličeje.
Scan oční duhovky	Osobní údaje subjektu ochrany založené na zpracování 266 příznaků obrazců oční duhovky, tvořenými kolagenovými vlákny. Účel a řízení osobních údajů bude obdobné jako u položky č. 77. Osobní údaj musí splňovat požadavky ČSN ISO/IEC 19794-6 (369860) Informační technologie - Formáty výměny biometrických dat - Část 6: Data obrazu duhovky.
Snímek sítnice	Osobní údaje subjektu ochrany založené na zpracování obrazu žilního systému sítnice, pořízeného v infračerveném spektru. Účel a řízení osobních údajů bude obdobné jako u položky č. 77.
Hlasový záznam	Osobním údajem jsou audio záznamy subjektů ochrany provedené prostřednictvím technických zařízení (analogových i digitálních), pořízené především pro dokumentování uskutečněných událostí. Do položky spadají i nahrávané telefonické rozhovory. Pokud budou audio záznamy sloužit ke speciálním účelům např. rozpoznávání emocí a následné profilování chování subjektů ochrany, je nezbytné provést posouzení vlivu na ochranu osobních údajů (DPIA). Je nezbytné posoudit vazbu na položku č. 89 Metadata.
Ostatní biometrické údaje	Mimo položky č. 76 až č. 80 se jedná zejména o tvar dlaně a prstu, žilní systém dlaně a prstu, termální snímek tváře a dlaně, dentální snímek, tvar ucha, dynamiku chůze, dynamiku psaní na klávesnici a podpis (nejedná se o podpisový vzor v položce č. 97).
Údaje dětí (mimo děti zaměstnanců)	Osobní údaje dětí, mimo údaje v kategorii „Rodinné údaje“. Např. údaje dětí účastnících se veřejně dostupných akcí a aktivit např. dětské kempy a tábory, dětské dny, Mikulášské nabídky, sportovní utkání ad. Osobní údaje mohou být zpracovávány pouze na základě zákonného důvodu např. rodičovského souhlasu, novinářské licence apod.
Elektronický podpis (podpisový certifikát)	Algoritmus digitálních dat nahrazující vlastnoruční ověřený podpis subjektu ochrany osobních údajů, který slouží k připojení v datovém souboru. Osobní údaj musí splňovat požadavky nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu a o zrušení směrnice Evropské unie 1999/93/EC (eIDAS).

IP adresa	Osobní údaj, který se váže k subjektu ochrany údajů od prvního použití IP adresy v provozu (viz. rozsudek Soudního dvora Evropské unie, ze dne 19. října 2016). **IP adresa** je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. V současné době je nejrozšířenější IPv4, která používá 32bitové IP adresy, které jsou zapisovány dekadicky po jednotlivých oktetech (tj. po osmicích bitů), například 192.168.0.2. Z důvodu nedostatku adres je IPv4 nahrazován protokolem IPv6, který používá 128bitové IP adresy zapsané hexadecimálně, například 2001:db8:0:1234:0:567:8:1
MAC adresa	MAC adresa (Media Access Control) je jednoznačný identifikátor síťového zařízení. Je přiřazována síťové kartě bezprostředně při její výrobě (u starších karet je uložena v EPROM) a proto se jí také někdy říká fyzická adresa. MAC adresa se skládá ze 48 bitů a podle standardu se píše jako šestice dvojciferných hexadecimálních čísel oddělených dvojtečkami např. 01:23:45:67:89:ab).
Cookies	Jako cookie se v protokolu HTTP označuje data, distribuovaná www serverem na počítač uživatele. Při následných návštěvách téhož serveru pak prohlížeč tato data posílá zpět na server, čímž se snižují nároky na vzájemný přenos dat. Cookies tak běžně slouží k rozlišování jednotlivých subjektů ochrany osobních údajů a k ukládání jejich uživatelských preferencí a následnému přizpůsobení obsahu, cílení a měření reklam. Pokud správce osobních údajů využívá cookies např. z Google Alalytics, Facebooku ad, provádí cílené směřování reklamy subjektům ochrany osobních údaj. Například Facebook prodává cookies dalším stranám (příjemcům), které inzerují v rámci této platformy a které je dále využívají ve svých službách. Třetí strany používají cookies ve spojení s Facebook službami také na vlastních webech a ve vlastních aplikacích. Nakládání s cookies bude definitivně vyřešeno v navazujícím evropském nařízení ePrivacy. Předpokládá se, že ukládání cookies bude primárně (implicitně) zakázané a budou se v systému uživatelsky (explicitně) povolovat.
Kamerový záznam	Veškeré záznamy z dílčích kamer nebo kamerových systému se záznamem i bez něj, pokud umožňují identifikaci subjektů ochrany osobních údajů. Předmětem zpracování je audio i video složka pořizovaných záznamů. Pokud správce používá kamerový systém při kontrolách docházky zaměstnanců, dodržování technologických postupů, ochraně majetku, snižování krádeží a kriminality obecně, nebo při zajištění bezpečnosti a ochrany zdraví doporučujeme provést posouzení vlivu na ochranu osobních údajů (DPIA). Pokud je systém určen pro monitorování veřejných prostranství a pohybu osob, je provedení DPIA povinné. Je nezbytné posoudit vazbu na položku č. 89 Metadata.
IMEI	Osobní údaj subjektu ochrany – uživatele smartphone, obdoba MAC adresy u PC nebo Ntb. IMEI (International Mobile Equipment Identity). Unikátní patnáctimístné číslo přidělené výrobcem mobilnímu telefonu. IMEI ukládá mobilní operátor do registru mobilních zařízení (EIR). IMEI je zapsán ve formátu ZZnnnn-MM-nnnnnn-X. První skupina je tzv. type approval code (TAC) uvozený dvěma číslicemi kódu země (ZZ). Druhá skupina (MM) je kód výrobce, třetí skupina je sériové číslo telefonu. Poslední cifra (X) je využívána pro kontrolní součet. Vyvolání - *#06#
Metadata	Jedná se o soubory dat, poskytujících informaci o jiných datech. Příkladem jsou např. digitální fotografie, které obvykle obsahují metadata ve formátu EXIF, s informací o vzniku fotografie (datum, čas pořízení, použitá ohnisková vzdálenost, použití blesku, typ a výrobce fotoaparátu, aktuální software, čas expozice, digitální zoom, komprese, údaje GPS o poloze apod. Zvukové soubory obsahují metadata s informací o názvu, autorovi, albu, použitém kodeku, datovém toku apod. Např. v souborech formátu *.mp3 se metadata ukládají do ID3 tagu. V e-learningových aplikacích se používá standardní formát metadat dle IMS Global Learning Consortium. Ministerstvo školství, mládeže a tělovýchovy České republiky v rámci Státní informační politiky ve vzdělávání užívá standard metadat EDUCZ, který vychází ze standardu Dublin Core. Digitální mapy obsahují metadata s verzí mapového podkladu, přesností polohy, podmínek šíření a používání, výrobce atd. Metadata jsou strukturovaná často pomocí tagované reprezentace a někdy hierarchicky. Struktura metadat (a formát) je v mnoha oblastech a aplikacích dohodnut až standardizován.
IPTC	IPTC-NAA-Standard slouží k ukládání textových informací do obrazových souborů (např. autorská práva, jméno autora, titulek fotografie, klíčová slova pro vyhledávání atd. S pomocí softwaru je správa fotografií jednodušší.IPTC-NAA-Standard vyvinul IPTC (International Press Telecommunications Council) spolu s NAA (Newspaper Association of America) v zásadě pro všechny druhy médií (text, fotografie, grafiky, audio i video).
Přístupová jména a hesla	Osobní údaje subjektu údajů, ve formě hesel, PIN, přístupových kódů, přístupových jmen, čísel z GRID karet ad. Rozsah je specifický podle aplikací, které správce používá. Zpracování se týká i samostatných programů pro evidenci přístupových údajů, trezorů hesel ad . (např. True Key, Sticky Password
Evidence docházky	Osobní údaje subjektu údajů, využívané v individuálních systémech evidence docházky. Rozsah je specifický podle konkrétního způsobu evidence, který správce používá. Do zpracování je však potřeba zahrnout veškeré údaje v souladu s ustanovením § 96, zákona č. 262/2006 Sb., zákoník práce, zejména odpracované směny, práci přesčas, noční práce, dobu pracovní pohotovosti ad.
Lokační údaje osob	Osobní údaje uživatelů firemních zařízení vybavených GSM a/nebo GPS modulem, např. tablety, smartphone ad. Osobní údaje budou zpracovávány především ve formátech pro geografii nebo vizualizaci prostorově umístitelných dat.

Lokační údaje vozidel	Osobní údaje uživatelů firemních vozidel, kteří je využívají i pro soukromé účely. Zdrojem osobních údajů budou především sledovací zařízení GSM a GPS vč. údajů z mobilních i zabudovaných navigací, uchovávaných ve formátech pro geografii nebo vizualizaci prostorově umístitelných dat. Je nezbytné posoudit vazbu na položku č. 96 Kniha jízd.
Data sdílených služeb (sdílená ekonomika)	Digitální služby, aplikace a firmware v oblasti komunikace, zábavy, obchodování, vzdělávání např. AirBnB, Uber atd.
Kniha jízd	Evidence údajů o využívání firemních vozidel. Osobní údaje je budou týkat řidičů a posádek vozidel.
Podpis (podpisový vzor)	Vlastnoruční podpis subjektu osobních údajů ve statická i dynamické formě, přičemž statická forma porovnává vizuální podobu vzoru a dynamická forma se navíc zaměřuje i na další markanty např. změnu přítlaku pera apod.
Údaje psychické identity	Např. psychotesty řidičů
SPZ vozidla	Je-li soukromé vozidlo využíváno k plnění pracovních povinností.
Číslo osvědčení o registraci vozidla	„Malý“ TP. Je-li soukromé vozidlo využíváno k plnění pracovních povinností.
Číslo technického průkazu vozidla	„Velký“ TP. Je-li soukromé vozidlo využíváno k plnění pracovních povinností.
Číslo mezinárodní pojišťovací karty	„Zelená karta“. Je-li soukromé vozidlo využíváno k plnění pracovních povinností.
Evidence v centrálních evidencích MVČR	Osobní údaje zahraničních subjektů ochrany, např. VISAPOINT (v případě zaměstnanců z třetích zemí apod.).
Evidence v centrálních evidencích MZV	Osobní údaje subjektů ochrany, jsou-li správcem zadávány např. do evidence DROZD, v případě jejich vysílání do zahraničí.
Číslo havarijního pojištění	Je-li soukromé vozidlo využíváno k plnění pracovních povinností.
Informace o půjčkách a úvěrech	Je¨li vyžadováno potvrzení o mzdě nebo záruky zaměstnavatele.
Informace z katastru nemovitostí	Např. existuje-li možnost home office apod.
Firemní navštívenky	Na základě souhlasu subjektu.
Ověřovací funkcionality na webu	Pokud správce používá funkcionalitu např. pro ověření certifikátů a osvědčení na webu apod.
Záznam z jednání	Např. je-li součástí hlasový nebo obrazový záznam apod. Vazba na položku č. 89 Metadata
Osobní údaje pro leteckou přepravu	Směrnice č. 2016/681 (nerelevantní pro organice neprovozující leteckou přepravu, CK a CA)
Etnologie, kulturní a sociální antropologie	V běžném režimu se bude jednat především o osobní údaje subjektů ochrany provázané s položkou č. 11 (fotografie). Typickým příkladem může být fotografie subjektu ochrany, na níž nebude rozpoznatelná vizuální identita subjektu (obličej), ale může dojít k identifikovatelnosti např. prostřednictvím specifického tetování.
Údaje autonomních dopravních systémů	Osobní údaje subjektů ochrany pořízené autonomními dopravními prostředky např. snímání vizuální podoby (autonomní vozidlo neodveze malé dítě, pokud nebude prokazatelně provázeno další osobou, u níž lze předpokládat dostatečný duševní potenciál k rozpoznání účelu cesty a důsledků dopravy do konkrétního místa nebo autonomní dopravní prostředek rozpozná podle vizuální podoby, specifických znaků nebo vzorců chování turisty a upozorní je, že jsou přepravováni do lokality se zvýšenou kriminální činností např. mimo turistické letovisko do okrajových částí města (ghetta) apod. Stejně tak se jedná o data, která autonomní systémy sbírají pro svůj provoz (např. kamery).

Komu: DPO
Od: (uvést majitele dílčího procesu zpracování)

Datum: ……

Jméno SOOÚ: ……

Původní OÚ:

Aktualizovaný OÚ:

Návrh způsobu řešení:

Zákonnost zpracování: ……

Termín prvního zpracování: ……

Navrhl:

Datum: Podpis:

Schválil:

Datum: Podpis:

Jmenovací dekret

Jmenuji **sl. Pavlínu Krotkou do funkce Manažera ochrany osobních údajů** (DPO), v příspěvkové organizaci Galerie Benedikta Rejta, s interní odpovědností za činnosti vyplývající z požadavků 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.

Práva a povinnosti DPO:

- poskytovat informace a poradenství v oblasti ochrany osobních údajů správci, jeho statutárnímu orgánu a smluvním zpracovatelům,
- poskytovat informace a poradenství pro konkrétní činnosti zpracování osobních údajů zaměstnancům správce,
- monitorovat soulad činností v oblasti ochrany osobních údajů s požadavky Obecného nařízení, Politikou ochrany osobních údajů i dalšími legislativními v EU a ČR u správce a všech zpracovatelů,
- hodnotit riziko spojené s operacemi zpracování osobních údajů a zohledňovat povahu, rozsah, kontext a účel zpracování,
- navrhovat statutárnímu orgánu správce rozdělení odpovědnosti zaměstnanců za zpracování osobních údajů,
- navrhovat statutárnímu orgánu zdroje nezbytné k zajišťování zpracování a ochrany osobních údajů,
- zvyšovat povědomí a zajišťovat odbornou přípravu zaměstnanců provádějících zpracování osobních údajů,
- prověřovat plnění konkrétních a měřitelných cílů ochrany osobních údajů a předkládat o něm zprávu statutárnímu orgánu,
- provádět nebo zajišťovat interní audity v oblasti ochrany osobních údajů,
- provádět případné posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování,
- vést záznamy o činnostech zpracování osobních údajů a o souladu činností s požadavky Obecného nařízení,
- spolupracovat s Úřadem pro ochranu osobních údajů (ÚOOÚ),
- účastnit se případných kontrol, inspekcí a auditů v oblasti ochrany osobních údajů,
- působit jako kontaktní místo pro všechny zainteresované strany, včetně ÚOOÚ.
- vykonávat další činnosti při ochraně osobních údajů v Galerii Benedikta Rejta.

V Lounech, dne 25. 5. 2018

.....

PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
Galerie Benedikta Rejta

Komu: DPO

Od koho: Jméno: ……

Datum: ……

Definování činnosti zpracování (námitka, neshoda, preventivní opatření apod.):
(vyplní zaměstnanec)

Podpis:

Návrh způsobu řešení:
(vyplní majitel dílčího procesu zpracování)

Podpis:

Rozhodnutí o způsobu řešení:
(vyplní DPO)

- způsob řešení:
- odpovědný zaměstnanec:
- termín realizace:

Podpis:

Obchodní jméno zpracovatele	IČ zpracovatele	Předmět zpracování	Číslo zpracovatelské smlouvy

Obchodní jméno společného správce	IČ společného správce	Předmět zpracování, sdílené OÚ	Číslo smlouvy o aktualizaci OÚ

Informace pro zaměstnance

Informace poskytovaná v souladu s čl. 13, Nařízení Evropského parlamentu a Rady (EU) 2016/679

Identifikace správce osobních údajů:
Galerie Benedikta Rejta, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01

Kontaktní údaje DPO:
Galerie Benedikta Rejta, Pavlína Krotká, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01
e-mail: gbr@gbr.cz
telefon: +420 415 652 634, +420 739 931 335

Účel zpracování a právní základ pro zpracování:
……
……

Zpracování založeno na oprávněném zájmu správce nebo třetí strany:
Ne
Ano Určení oprávněného zájmu: ……

Příjemce osobních údajů:
Ne
Ano Určení příjemce: ……

Předání osobních údaje do třetí země nebo mezinárodní organizaci:
Ne
Ano Specifikace: ……

Rozhodnutí Komise o odpovídající ochraně
Ne
Ano

Doba uložení osobních údajů: ……..

Poučení: V průběhu zpracování osobních údajů má zaměstnanec právo požadovat od správce přístup k osobním údajům, právo na jejich opravu nebo výmaz, právo na omezení zpracování, právo vznést námitku proti zpracování, právo na přenositelnost údajů k jinému správci, právo odvolat kdykoli souhlas se zpracováním, právo podat stížnost u dozorového úřadu a právo podat žalobu k soudu;

Prohlášení správce: V rámci zpracování osobních údajů nedochází k automatizovanému rozhodování, ani profilování. Osobní údaje jsou používány pouze pro výše definovaná zpracování.

PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
Galerie Benedikta Rejta
v.r.

Informace pro zaměstnance

Informace poskytovaná v souladu s čl. 13, Nařízení Evropského parlamentu a Rady (EU) 2016/679

Identifikace správce osobních údajů:
Galerie Benedikta Rejta, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01

Kontaktní údaje DPO:
Galerie Benedikta Rejta, Pavlína Krotká, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01
e-mail: gbr@gbr.cz
telefon: +420 415 652 634, +420 739 931 335

Účel zpracování a právní základ pro zpracování:
……
……

Kategorie dotčených osobních údajů:
……
……

Příjemce osobních údajů:
Ne
Ano Určení příjemce: ……

Předání osobních údaje do třetí země nebo mezinárodní organizaci:
Ne
Ano Specifikace: ……

Rozhodnutí Komise o odpovídající ochraně
Ne
Ano

Doba uložení osobních údajů: ……..

Poučení: V průběhu zpracování osobních údajů má zaměstnanec právo požadovat od správce přístup k osobním údajům, právo na jejich opravu nebo výmaz, právo na omezení zpracování, právo vznést námitku proti zpracování, právo na přenositelnost údajů k jinému správci, právo odvolat kdykoli souhlas se zpracováním, právo podat stížnost u dozorového úřadu a právo podat žalobu k soudu;

Prohlášení správce: V rámci zpracování osobních údajů nedochází k automatizovanému rozhodování, ani profilování. Osobní údaje jsou používány pouze pro výše definovaná zpracování.

PhDr. Alica Štefančíková
ředitelka příspěvkové organizace
Galerie Benedikta Rejta
v.r.

Řízený záznam Hlášení porušení zabezpečení je veden ve formátu editovatelného formuláře PDF a tvoří nedílnou součást Směrnice č. 1 - Ochrana osobních údajů podle Nařízení EPaR (EU) 2016/679.

Souhlas se zpracováním osobních údajů
podle Nařízení Evropského parlamentu a Rady (EU) 2016/679

1. Já, níže podepsaný (á),
   tímto uděluji tímto souhlas příspěvkové organizaci **Galerie Benedikta Rejta**, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01 („Správce"), aby podle 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 (dále jen „Nařízení") zpracovával tyto mé osobní údaje:
   - Jméno, příjmení, datum narození, telefonní číslo, číslo bankovního účtu.
2. Osobní údaje dle bodu (1) jsou zpracovávány za účelem:
   - Jméno, příjmení, datum narození ……
   - Telefonní číslo ……
   - Číslo bankovního účtu ……
3. Osobní údaje budou správcem uloženy pouze po dobu nezbytnou ke zpracování resp. po dobu nezbytnou ke splnění vzájemných závazků a povinností:
   - Jméno, příjmení, datum narození ……
   - Telefonní číslo ……
   - Číslo bankovního účtu ……
4. Zpracování osobních údajů je prováděno Správcem a zpracovatelem:
   - ……
     ……

Výše uvedenému rozumím, na základě všech informací jsem zvážil(a) míru rizika a **se zpracováním uděluji výslovný souhlas**, který je mou svobodnou vůlí.

Poučení o právech osoby, jejíž osobní údaje jsou zpracovávány:
- odvolat souhlas se zpracováním osobních údajů,
- přistupovat k osobním údajům,
- požadovat opravu osobních údajů,
- požadovat výmaz osobních údajů,
- požadovat přenesení vlastních osobních údajů k jinému správci,
- vznést námitku proti zpracování osobních údajů,
- obrátit se na Úřad pro ochranu osobních údajů.

…… ……

Datum a jméno hůlkovým písmem

Podpis
(rodičovský souhlas u osoby mladší do 16 let)

Pro zajištění povinností podle nařízení EPaR(EU) č. 2016/679 bude do stávající nebo nové smlouvy vloženo následující ujednání, které může být i obsahem dodatku ke stávající smlouvě např. pro oblast zpracování mezd a personální agendy:

Čl. ……
Ochrana osobních údajů

- Smluvní strany specifikované v čl. ….. zastávají roli správce osobních údajů (objednatel) a zpracovatele osobních údajů (zhotovitel).
- Osobní údaje předávané správcem zpracovateli se týkají všech zaměstnanců správce, kteří požívají ochrany osobních údajů jakožto subjekty ochrany osobních údajů.

- *Předávané osobní údaje se týkají výhradně zpracování mezd a personální agendy zpracovatelem.*
- *Předmětem předání jsou i zvláštní kategorie osobních údajů nezbytné k provádění srážek ze mzdy ve prospěch exekučních úřadů a vedení povinných záznamů o exekucích i osobní údaje týkající se zdravotních postižení dotčených subjektů ochrany osobních údajů.*
- *Základní procesy zpracování na straně zpracovatele budou výhradně shromáždění, zaznamenávání, uspořádání, strukturování, uložení, vyhledání, nahlédnutí, použití, zpřístupnění, seřazení, omezení.*
- *Ostatní procesy zpracování na straně zpracovatele, zejména pozměnění, zkombinování, výmaz či zničení budou prováděny pouze na příkaz správce nebo pod jeho dohledem.*

nebo alternativně pro oblast BOZP a PO:

- *Předávané osobní údaje se týkají výhradně zpracování při zajišťování bezpečnosti a ochrany zdraví při práci a požární ochrany.*
- *Předmětem předání jsou i zvláštní kategorie osobních údajů nezbytné k provedení kategorizace prací a stanovení rizik na pracovištích a vedení povinných záznamů o školeních i osobní údaje týkající se zdravotních postižení dotčených subjektů ochrany osobních údajů.*
- *Základní procesy zpracování na straně zpracovatele budou výhradně uspořádání, strukturování, uložení, vyhledání, použití a seřazení.*
- *Ostatní procesy zpracování na straně zpracovatele, zejména shromáždění, zaznamenávání, nahlédnutí, zpřístupnění, pozměnění, zkombinování, omezení, výmaz či zničení budou prováděny pouze na příkaz správce nebo pod jeho dohledem.*

- Správce i zpracovatel se dohodly, že bude-li jedna ze stran shledána odpovědnou za porušení povinností při správě osobních údajů, kterého se dopustí druhá strana, druhá strana nahradí první straně v rozsahu, ve kterém je odpovědná, veškeré náklady, poplatky, škody, výdaje nebo ztráty, které první straně vznikly.

Pozn.: Obdobným způsobem musí být zpracován i pro jiné kategorie subjektů ochrany, jiné kategorie osobních údajů i pro jiné kategorie způsobů zpracování.

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
e-mail: posta@uoou.cz,
datová schránka: qkbaa2n

Věc: **Oznámení pověřence**

Příspěvková organizace **Galerie Benedikta Rejta**, IČ: 003 60 724, se sídlem Louny, Pivovarská 29, PSČ 440 01, zastoupená ředitelkou organizace **oznamuje** v souladu s článkem 37, odst. 7 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, **jmenování pověřence pro ochranu osobních údajů**, podle čl. 37, odst. 4, kterým je sl. **Pavlína Krotká**.

Kontaktní údaje pověřence pro ochranu osobních údajů:

- Telefon: **+420 415 652 634**
  +420 739 931 335
- e-mail: **gbr@gbr.cz**
- pošta: **Galerie Benedikta Rejta, příspěvková organizace**
  Pivovarská 29
  440 01Louny

Za správce PhDr. Alica Štefančíková, ředitelka příspěvkové organizace Galerie Benedikta Rejta:

.....
razítko a podpis