Analýza rizik GDPR

1) Preambule

V návaznosti na již zpracovaný audit připravenosti spolku Polský kulturně-osvětový svaz v České republice z.s., zapsaného ve spolkovém rejstříku vedeném Krajským soudem v Ostravě v oddíle L, vložka 22, sídlem: Střelniční 209/28, 737 01 Český Těšín, identifikační číslo: 004 42 771 (dále jen „spolek“ či „PZKO“), na GDPR (General Data Protection Regulation), tedy pravidla ochrany osobních údajů stanovené v Nařízení evropského parlamentu a rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), ze dne 27. dubna 2016, jehož účinnost je dána 25. květnem 2018 (dále jen „nařízení“), je v tomto dokumentu zpracována analýza rizik, která obsahuje identifikaci zpracovaných osobních údajů, hrozeb a zranitelností ve spojitosti s osobními údaji, posouzení pravděpodobností a dopadů hrozeb na osobní údaje a identifikaci a ohodnocení rizik.

Cílem analýzy rizik je odhalit rizika a navrhnout účinná a efektivní opatření k minimalizaci potenciálních škod hrozících informačním aktivům v podobě osobních údajů.

2) Posouzení vlivu na ochranu osobních údajů

Dle ustanovení článku 35 nařízení platí, že *pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. Posouzení vlivu na ochranu osobních údajů je nutné zejména v těchto případech:*

a) *systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;*
b) *rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nařízení (citlivé osobní údaje, tedy údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů;*
c) *rozsáhlé systematické monitorování veřejně přístupných prostorů.*

V případě Spolku neprobíhá zpracování osobních údajů popsané výše (v čl.35 odst. 3 písm. a), b) nebo c) Nařízení).

3) Identifikace, zda je zpracování označené za rizikové dozorovým úřadem

Dle ustanovení článku 36 nařízení platí, že *správce* (v tomto případě Spolek) *konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů podle článku 35 vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.*

Zpracovávání osobních údajů Spolkem není dozorovým orgánem označeno za rizikové s ohledem na svou povahu – primárně jsou zpracovávány osobní údaje zaměstnanců z důvodu personálních a mzdových, sekundárně pak osobní údaje obchodních partnerů z důvodů obchodních.

Spolek zpracovává toliko následující osobní údaje:

a) osobní údaje svých členů

obecné osobní údaje	jméno a příjmení		ANO	~~NE~~	
	titul		~~ANO~~	NE	
	pohlaví		ANO	~~NE~~	
	datum narození		ANO	~~NE~~	
	rodné číslo		~~ANO~~	NE	
	osobní stav		~~ANO~~	NE	
	vzdělání		~~ANO~~	NE	
	lokalita/adresa bydliště		ANO	~~NE~~	
	číslo bankovního účtu		~~ANO~~	NE	
	IP adresa		~~ANO~~	NE	
	e-mailová adresa		ANO	~~NE~~	
	telefonní číslo		ANO	~~NE~~	
	identifikační údaje vydané státem		~~ANO~~	NE	Jaké:
	údaje o příjmech		~~ANO~~	NE	
	údaje o rodinných příslušnících nebo osobách blízkých		~~ANO~~	NE	Jaké:
	údaje o předchozím zaměstnání		~~ANO~~	NE	
	údaje o řidičském oprávnění		~~ANO~~	NE	
citlivé osobní údaje	údaje o rasovém či etnickém původu		~~ANO~~	NE	
	politických názorech		~~ANO~~	NE	
	náboženském nebo filozofickém vyznání		~~ANO~~	NE	
	členství v odborech		~~ANO~~	NE	
	o zdravotním stavu		~~ANO~~	NE	
	sexuální orientaci		~~ANO~~	NE	
	trestních deliktech či pravomocném odsouzení osob		~~ANO~~	NE	
	genetické údaje		~~ANO~~	NE	
	biometrické údaje	fotografický záznam, podobizna	~~ANO~~	NE	

		otisk prstu	~~ANO~~	NE
		podpis	ANO	~~NE~~
	osobní údaje dětí		~~ANO~~	NE

b) osobní údaje svých zaměstnanců

obecné osobní údaje	jméno a příjmení		ANO	~~NE~~	
	Titul		ANO	~~NE~~	
	Pohlaví		ANO	~~NE~~	
	datum narození		ANO	~~NE~~	
	rodné číslo		ANO	~~NE~~	
	osobní stav		~~ANO~~	NE	
	Vzdělání		ANO	~~NE~~	
	lokalita/adresa bydliště		ANO	~~NE~~	
	číslo bankovního účtu		ANO	~~NE~~	
	IP adresa		~~ANO~~	NE	
	e-mailová adresa		ANO	~~NE~~	
	telefonní číslo		ANO	~~NE~~	
	identifikační údaje vydané státem		~~ANO~~	NE	Jaké:
	údaje o příjmech		ANO	~~NE~~	
	údaje o rodinných příslušnících nebo osobách blízkých		ANO	~~NE~~	Jaké: Dětí, manžel/ka
	údaje o předchozím zaměstnání		ANO	~~NE~~	
	údaje o řidičském oprávnění		ANO	~~NE~~	
citlivé osobní údaje	údaje o rasovém či etnickém původu		~~ANO~~	NE	
	politických názorech		~~ANO~~	NE	
	náboženském nebo filozofickém vyznání		~~ANO~~	NE	
	členství v odborech		~~ANO~~	NE	
	o zdravotním stavu		~~ANO~~	NE	
	sexuální orientaci		~~ANO~~	NE	
	trestních deliktech či pravomocném odsouzení osob		~~ANO~~	NE	
	genetické údaje		~~ANO~~	NE	
	biometrické údaje	fotografický záznam, podobizna	~~ANO~~	NE	
		otisk prstu	~~ANO~~	NE	
		Podpis	ANO	~~NE~~	

	osobní údaje dětí	ANO	~~NE~~

c) osobní údaje externích subjektů:

obecné osobní údaje	jméno a příjmení	ANO	NE	
	Titul	ANO	NE	
	Pohlaví	ANO	NE	
	datum narození	ANO	NE	
	rodné číslo	ANO	NE	
	osobní stav	ANO	NE	
	Vzdělání	ANO	NE	
	lokalita/adresa bydliště	ANO	NE	
	číslo bankovního účtu	ANO	NE	
	údaje o platebních kartách	ANO	NE	
	údaje o jiných platebních prostředcích	ANO	NE	Jaké:
	IP adresa	ANO	NE	
	e-mailová adresa	ANO	NE	
	telefonní číslo	ANO	NE	
	identifikační údaje vydané státem (např. IČO)	ANO	NE	Jaké: IČO
	údaje o rodinných příslušnících nebo osobách blízkých	ANO	NE	Jaké:
citlivé osobní údaje	údaje o rasovém či etnickém původu	ANO	NE	
	politických názorech	ANO	NE	
	náboženském nebo filozofickém vyznání	ANO	NE	
	členství v odborech	ANO	NE	
	o zdravotním stavu	ANO	NE	
	sexuální orientaci	ANO	NE	
	trestních deliktech či pravomocném odsouzení osob	ANO	NE	
	genetické údaje	ANO	NE	
	biometrické údaje – fotografický záznam, podobizna	ANO	NE	
	biometrické údaje – otisk prstu	ANO	NE	
	biometrické údaje – Podpis	ANO	NE	

	osobní údaje dětí	ANO	NE

d) osobní údaje klientů:

obecné osobní údaje	jméno a příjmení	ANO	~~NE~~	
	Titul	~~ANO~~	NE	
	Pohlaví	~~ANO~~	NE	
	datum narození	~~ANO~~	NE	
	rodné číslo	~~ANO~~	NE	
	osobní stav	~~ANO~~	NE	
	vzdělání	~~ANO~~	NE	
	lokalita/adresa bydliště	ANO	~~NE~~	
	číslo bankovního účtu	~~ANO~~	NE	
	údaje o platebních kartách	~~ANO~~	NE	
	údaje o jiných platebních prostředcích	~~ANO~~	NE	Jaké:
	IP adresa	~~ANO~~	NE	
	e-mailová adresa	ANO	~~NE~~	
	telefonní číslo	ANO	~~NE~~	
	identifikační údaje vydané státem (např. IČO)	ANO	~~NE~~	Jaké: IČ
	údaje o rodinných příslušnících nebo osobách blízkých	~~ANO~~	NE	Jaké:
citlivé osobní údaje	údaje o rasovém či etnickém původu	~~ANO~~	NE	
	politických názorech	~~ANO~~	NE	
	náboženském nebo filozofickém vyznání	~~ANO~~	NE	
	členství v odborech	~~ANO~~	NE	
	o zdravotním stavu	~~ANO~~	NE	
	sexuální orientaci	~~ANO~~	NE	
	trestních deliktech či pravomocném odsouzení osob	~~ANO~~	NE	
	genetické údaje	~~ANO~~	NE	
	biometrické údaje – fotografický záznam, podobizna	~~ANO~~	NE	
	biometrické údaje – otisk prstu	~~ANO~~	NE	
	biometrické údaje – podpis	~~ANO~~	NE	

	osobní údaje dětí	~~ANO~~	NE

e) osobní údaje získané prostřednictvím kamerových systémů

Kancelář ekonoma v sídle spolku na adrese Střelniční 209/28, 737 01 Český Těšín je střežena mimo jiné kamerovým systémem. Kamerový systém může pořídit záznam jednotlivých zaměstnanců nebo externích subjektů pokud se objeví před objektivem. Kamera funguje v režimu trvalého záznamu. Systém ovládající kamery a uchovávající záznamy je provozován zaměstnancem spolku na pozici správce sítě.

Záznamy kamerového systému se uchovávají po dobu 14 dnů. K záznamu kamer má přístup pouze zaměstnanec spolku na pozici správce sítě.

Kamerový systém funguje na lokální síti a přesup je zabezpečený heslem. Servis kamerového systému provádí zaměstnanec spolku na pozici správce sítě.

4) Identifikace hrozeb spojených se zpracováním (např. porušení zabezpečení údajů, zpracování údajů v rozporu se základními zásadami GDPR apod.) – závěry srovnávací analýzy (Auditu připravenosti)

Za hrozby spojené se zpracováním osobních údajů není považováno pouze porušení zabezpečení údajů, ale také různé hrozby, které může vyvolávat sám správce, například zpracováním údajů v rozporu se základními zásadami Nařízení. Mezi tyto hrozby může patřit např.:

a) zpracování osobních údajů v rozporu se zásadou zákonnosti,
b) nevhodné zpracování osobních údajů, které přesahuje rozumné očekávání subjektu údajů či které jde nad rámec obvyklého očekávání ve společnosti,
c) nezákonné překročení stanoveného účelu zpracování,
d) rozpor se zásadou minimalizace údajů, tzn. excesivní shromažďování či jiné zpracování osobních údajů,
e) zpracování či uchovávání osobních údajů, které jsou nepřesné či neaktuální,
f) uchovávání osobních údajů po dobu delší, než je nutná,
g) narušení integrity či důvěrnosti osobních údajů,
h) znemožnění či ztížení možnosti uplatnit práva subjektů údajů.

Správce by přitom neměl posuzovat pouze újmu, kterou může způsobit zpracováním on sám, ale také újmu, která může subjektům údajů vzniknout následným jednáním třetí strany, např. po předání či zveřejnění osobních údajů.

V rámci srovnávací analýzy byl posuzován stav procesů, stav dokumentace, jak rovněž stav technického zabezpečení Spolku, přičemž dospěl k následujícím závěrům.

1.1. Zákonnost zpracování OÚ

Správce jednoznačně splňuje minimálně jednu z podmínek pro naplnění zákonnosti zpracování ÓU. Jedná se zejména o splnění právní povinnosti vztahující se na organizaci (zaměstnavatel vede záznamy pro vyplácení mzdy zaměstnanců, zajišťuje odvody na zdravotní/sociální/důchodové pojištění atd.).

Nad rámec Správce vedle uvedeného zpracovává osobní údaje na základě souhlasu subjektu údajů pro jeden či více konkrétních účelů.

1.2. Procesy ochrany OÚ v jejich životním cyklu

1.2.1.Shromažďování OÚ

Oblast	Stav	Poznámka	Proces
Právní základ zpracování	Ze zákonných důvodů; se souhlasem subjektu údajů.	Prováděno rutinní činností personálního oddělení, obchodního oddělení, či jiných pověřených oddělení.	Není popsán, není definován
Uložení dat/zpracování (kde všude se OÚ vyskytují)	Přehled mají předseda a pracovníci na základě pracovního zařazení.	V zamykatelné skříni a archivu. Není klasifikace dat. Není klasifikace dat. Osobní údaje se vyskytují v systému POHODA, v Office, v listinné podobě.	
Přenos/předání interní	Jednotliví pracovníci na základě vlastního povědomí a rutinních postupů.	Není dokumentováno, co nesmí, co je zakázáno a jakým způsobem se má provádět.	
Získávání souhlasu	Probíhá, je formalizován.	Souhlas není vždy a za všech okolností získán. V případě zákonného získávání není nezbytně nutné. Souhlasy získány od zaměstnanců v pracovních smlouvách. U obchodních partnerů ještě nutno dořešit, pokud jde o FO.	
Informovanost subjektů (před a po)	Je prováděno ad hoc, není formalizováno.	Není dokumentováno, jak mají jednotliví pracovníci postupovat v jednotlivých případech.	

1.2.2.Ukládání a zpracování OÚ

Oblast	Stav	Poznámka	Proces
Úložiště (např. e-maily, sdílená úložiště, lokální ukládání dat)	OÚ se mohou nacházet v celém IS (e-maily, sdílená úložiště, lokální ukládání dat, databáze). Zejména se však jedná o oddělení HR a finance.	Uživatelé nejsou pravidelně školeni o ochraně dat.	Není popsán, není definován
Šifrování (transparentní, ad-hoc, řízení klíčů, hesel)	Není zavedeno.	Není uvedeno explicitně.	

Přístupy (identifikace osoby provádějící zpracování)	Přístupy jsou přidělovány na základě pracovního zařazení, případně požadavku předsedy.	Postup zřízení přístupu není formalizován a nejsou vytvářeny záznamy.	
Oprávnění manipulovat s OÚ	Na základě pracovní smlouvy, zařazení na odpovídající oddělení.	Není uvedeno explicitně.	
Auditní záznamy (logování, přístup k logům, ochrana proti změnám, lhůty)	Provádí se ad hoc v případě potřeby (chyba, havárie, incident).	Není stanoven postup pro monitorování a práci se záznamy.	
Pravidla sdílení	Pokud ke sdílení dat dochází, je na základě zařazení nebo požadavku předsedy. Je prováděno rutinně.	Není formalizovaný a dokumentovaný postup, nejsou generovány záznamy.	
Postupy v případě změny	Je prováděno ad hoc.	Není zaveden proces řízení změn jako takový.	

1.2.3.Zálohování OÚ

Oblast	Stav	Poznámka	Proces
Redundance, záložní systémy, replikace, datová centra	Je prováděno zálohování.	Nejsou prováděny testy obnovy, nejsou definovány parametry RTO a RPO, není zpracován zálohovací plán.	Není popsán, není definován
Bezpečné úložiště záloh/zabezpečení médií	Vše je umístěno v jedné lokalitě.		

1.2.4.Likvidace OÚ

Oblast	Stav	Poznámka	Proces
Převzetí požadavku na výmaz OÚ	Je možné jen neformalizovaným způsobem. Není vytvořen záznam. Je prováděn individuálně jednotlivými pracovníky na základě jejich rutin.	Není popsán postup, definovány povinnosti.	Není popsán, není definován
Posouzení oprávněnosti (vyjádření výsledku správce údajů do 1. kalendářního měsíce)	Je možné jen neformalizovaným způsobem. Není vytvořen záznam. Je prováděn individuálně jednotlivými pracovníky na základě jejich rutin.	Není popsán postup, definovány povinnosti.	

Informování příjemců (zpracovatelů, třetích stran)	Je možné jen neformalizovaným způsobem. Není vytvořen záznam. Je prováděn individuálně jednotlivými pracovníky na základě jejich rutin.	Není popsán postup, definovány povinnosti.	
Implementace do IS - zvláštní (omezený režim) zpracování OÚ – příznak	Je omezeno technickými možnostmi aplikací. Je možné na základě manuálního postupu.	Není návod na jednotné označování.	
Implementace do IS - výmaz části nebo všech OÚ	Je omezeno technickými možnostmi aplikací. Je možné na základě manuálního postupu.	Není návod na postup, pravidla a parametry.	
Implementace do IS - příznak požadavku (na výmaz, nesouhlas s dalším zpracováním)	Je omezeno technickými možnostmi aplikací. Je možné na základě manuálního postupu.	Není návod na jednotné označování.	
Bezpečná skartace dat a médií	Není prováděno, neexistují záznamy.	Není návod na postup.	

V návaznosti na uvedené je nutno k jednotlivým hrozbám spojeným se zpracováním osobních údajů uvést následující.

a) Zpracování osobních údajů v rozporu se zásadou zákonnosti.
Spolek nyní nezpracovává osobní údaje v souladu se zásadou zákonnosti, neboť minimálně nemá formalizován postup získávání souhlasů subjektů osobních údajů s jejich zpracováním.

b) Nevhodné zpracování osobních údajů, které přesahuje rozumné očekávání subjektu údajů či které jde nad rámec obvyklého očekávání ve společnosti.
V této souvislosti by hrozbou mohlo být zpracování osobních údajů subjektů, širším okruhem osob, než je bezpodmínečně nutné, což je dáno zejména absencí uceleného vnitřního předpisu, který by stanovil pravidla pro přístup k osobním údajům, jejich uchovávání, zálohování a likvidaci.

c) Nezákonné překročení stanoveného účelu zpracování.
Zato hrozba úzce souvisí s hrozbou nevhodného zpracování osobních údajů.

d) Rozpor se zásadou minimalizace údajů, tzn. excesivní shromažďování či jiné zpracování osobních údajů.
Tato hrozba úzce souvisí s hrozbou nevhodného zpracování osobních údajů – viz výše (zejména jsou osobní údaje shromažďovány bez adekvátního odůvodnění duplicitně v různých informačních systémech, jak rovněž v listinné podobě).

e) Zpracování či uchovávání osobních údajů, které jsou nepřesné či neaktuální.
Tato hrozba je dána zejména absencí uceleného vnitřního předpisu.

f) Uchovávání osobních údajů po dobu delší, než je nutná.
Tato hrozba je dána zejména absencí uceleného vnitřního předpisu.

g) Narušení integrity či důvěrnosti osobních údajů.
Tato hrozba je dána absencí uceleného systému zabezpečení osobních údajů (zejména šifrování, pseodonymizace, jak rovněž fyzického zabezpečení osobních údajů uchovávaných v listinné podobě).

h) Znemožnění či ztížení možnosti uplatnit práva subjektů údajů.
Spolek nemá zavedeny mechanizmy pro zajištění práv subjektů (právo na informace, právo na zapomenutí, právo na přenositelnost dat, informovanost v případě bezpečnostního incidentu, atd.).

1.3. Technická opatření na ochranu dat

1.3.1. Role pověřence pro ochranu OÚ

Dle ustanovení článku 37 a násl. nařízení GDPR platí, že *správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:*

a) *zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;*
b) *hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;*
c) *hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v Článku 9 (rasový a etnický původ, politické názory, náboženství, zdravotní stav, sexuální orientace atd.) a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.*

Spolek nemá povinnost zřídit a personálně obsadit roli pověřence pro ochranu osobních údajů, neboť pokud jsou zpracovávány citlivé osobní údaje, nejsou zpracovávaný či monitorovány rozsáhle, pravidelně a systematicky.

1.3.2. Implementace vhodných technických a organizačních opatření

Technická a organizační opatření ochrany osobních údajů jsou nutná, a to ve všech kategoriích uvedených výše v bodu 1.2., tedy v kategoriích Shromažďování OÚ, Ukládání a zpracování OÚ, Zálohování OÚ a Likvidaci OÚ.

Konkrétně by mělo jít o následující opatření:

- Způsob autentizace – autentizace pomocí jména a hesla je korektní, problémem může být stávající politika hesel, která umožňuje uživatelům nekonečné opakování stejného hesla a nebrání útoku hrubou silou.
- Řízení identit uživatelů – není implementován nebo nastaven proces řízení identit, což může vést k existenci neřízených účtů s vysokými oprávněními nebo k „zapomenutí“ účtů.

- Řízení záznamů (logů) – není implementován nástroj a proces, který by umožňoval zpracovávat a vyhodnocovat záznamy informačních systémů. V případě jakéhokoliv incidentu je pak velmi obtížné identifikovat kořenovou příčinu a tuto odstranit tak, aby se incident již nemohl opakovat.
- Kontrola správců/administrátorů – není implementován nástroj a proces, který by umožňoval kontrolovat činnost správců/administrátorů. Tito mají pro výkon své funkce vysoká oprávnění, která jim umožňují získat přístup k datům pomocí systémových prostředků a nástrojů.

1.3.3. Implementace pseudonimizace dat

GDRP uvádí jako základní prostředek/opatření pro zajištění ochrany OÚ implementaci pseudonymizaci. Spolek nemá implementovánu pseudonymizaci dat jako takovou. Ochrana OÚ je založena na kontrole přístupu k aplikacím, jenž data zpracovávají a tím k omezenému množství pracovníků, kteří mohou s daty manipulovat. Je doporučeno nasazení pseudonymizace.

1.3.4. Schopnost obnovit dostupnost OÚ po havárii nebo bezpečnostním incidentu

Spolek má nasazeny základní technologie pro obnovu dat a informačních systémů. Tyto technologie však nejsou doplněny odpovídajícími procesy a dokumentovanými postupy jako jsou havarijní plány a postupy a proces řízení bezpečnostních incidentů.

1.3.5. Pravidelné testování, posuzování a hodnocení účinnosti nasazených opatření

Spolek neprovádí pravidelné testování a hodnocení účinnosti nasazených opatření. Není zaveden interní předpis, který by potřebné procesy zahrnoval.

Shrnutí

Spolek pracuje s osobními údaji svých zaměstnanců a s osobními údaji zákazníků a obchodních partnerů (dodavatelé). Získání osobních údajů je zákonné. Nejsou zavedeny odpovídající procesy, které by umožnily naplnit požadavky GDPR:

- Právo být zapomenut (Right to be forgotten)
- Snazší přístup k datům (Easier access to one's data)
- Právo na přenositelnost dat (Right to data portability)
- Informovanost v případě bezpečnostního incidentu (The right to know when one's data has been hacked)
- Ochrana dat jako základní požadavek na design a výchozí stav (Security by design and by default)
- Snazší vymahatelnost práva (Stronger enforcement of the rules)

5) Identifikace potenciální újmy dotčených osob spojené se zpracováním jejich osobních údajů (fyzická, hmotná nebo nehmotná újma způsobená správcem nebo třetí stranou)

Různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či

společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů.

S ohledem na uvedené se jako reálné potenciální újmy dotčených osob spojené se zpracováním osobních údajů ze strany Spolku jeví následující:

a) diskriminace,
b) krádež,
c) finanční ztráta,
d) poškození pověsti,
e) jiné významné hospodářské či společenské znevýhodnění v situaci, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají členství v odborech, údaje o zdravotním stavu nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření,
f) jiné významné hospodářské či společenské znevýhodnění v situaci, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, a místa pobytu a pohybu.

6) Zhodnocení pravděpodobnosti, že újma vznikne (posouzení slabých míst systémů a procesů zpracování oproti povaze hrozby)

Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelům zpracování. Riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko. Míra pravděpodobnosti vzniku újmy závisí na konkrétních faktorech, jakými jsou např.:

a) počet osob zapojených do zpracování,
b) zapojení třetích stran do zpracování,
c) rozdílné právní požadavky dopadající na zpracování osobních údajů (např. při předání osobních údajů do zahraničí),
d) slabá místa v procesech a systémech zpracování a nedostatky ve správě osobních údajů obecně nebo
e) historie předchozích incidentů, při nichž došlo ke vzniku újmy.

Z hlediska povahy zpracovávaných osobních údajů, způsobu a účelu jejich zpracování, jak rovněž zhodnocení výše zmíněných faktorů je u Spolku nutno dospět k závěru, že míra pravděpodobnosti vzniku újmy není vysoká, jelikož Spolek, primárně zpracovává osobní údaje na základě zákonné

zmocnění a dále v souvislosti s výkonem své činnosti, kdy však klíčovými obchodními partnery jsou obchodní korporace, nikoli subjekty osobních údajů.

7) Zhodnocení závažnosti potenciální újmy, pokud by vznikla (z hlediska citlivosti nebo objemu osobních údajů apod.)

Faktory, které určují závažnost újmy, jsou zejména následující:

a) citlivost osobních údajů (přičemž se nelze omezit pouze na zvláštní kategorie osobních údajů, ale je nutné zvažovat skutečnou citlivost údajů – např. platební údaje do této kategorie nespadají, ale velmi citlivé bezpochyby jsou),
b) objem zpracovaných osobních údajů,
c) zranitelnost dotčených fyzických osob,
d) možný dopad zpracování na významné události v životě fyzických osob,
e) možný dopad zpracování na finanční a ekonomickou situaci fyzických osob.

Vedle uvedeného je nutné posoudit benefity, které může určité zpracování – byť rizikové – pro subjekt údajů znamenat. V některých případech může být výhoda natolik velká, že ospravedlní zbytkové riziko, které není možné dostatečně zmírnit.

Spolek zpracovává největší objem osobních údajů na základě zákonného zmocnění z titulu plnění povinností zaměstnavatele a plnění povinností vést evidenci členů Spolku.

Osobní údaje zpracované mimo zákonné zmocnění, tedy na základě souhlasu subjektů osobních údajů, jsou toliko obecné osobní údaje, uvedené výše pod bodem 3., které se týkají zejména plnění účelu Spolku.

S ohledem na uvedené je tedy možno konstatovat, že potencionální újma, pokud by vznikla, je vyšší u osobních údajů zaměstnanců a členů. U osobních údajů zpracovávaných na základě souhlasu subjektů osobních údajů, je míra závažnosti potencionální újmy, pokud by vznikla, neporovnatelně nižší.

8) Vyhodnocení rizika

Právní úprava požaduje, aby způsob zajišťování souladu s jeho pravidly vždy odpovídal riziku, které prováděné zpracování představuje pro práva a svobody fyzických osob. Tímto pravidlem se musí správce řídit při přijímání organizačních a technických opatření s cílem zajistit provádění všech zásad pro zpracování, jako je minimalizace údajů, přesnost, omezení uložení či důvěrnost a integrita, ale také např. při zavádění procesů pro výkon práv subjektů údajů nebo při výběru vhodných zpracovatelů. Riziko pro práva a svobody fyzických osob se v Nařízení objevuje zároveň také jako kritérium, na němž závisí uplatnění nebo míra uplatnění řady institutů. S posuzováním rizika se úzce pojí provádění principu odpovědnosti, kvůli kterému musí být správce schopen doložit soulad s Nařízením. Správce by tak měl všechna provedená posouzení rizik a následné zvolení vhodných opatření k jejich zmírnění pečlivě odůvodnit a přiměřeně zdokumentovat pro potřeby prokazování souladu.

Nařízení obecně rozpoznává tři druhy rizika pro práva a svobody, které mají odraz v uplatnění či míře uplatnění jednotlivých výše uvedených povinností.

a) Riziko – Riziko je obecným měřítkem zavádění technických a organizačních opatření k plnění povinností v Nařízení. Posouzení rizika je komplexní analýza zaměřená na zjištění možné újmy pro subjekty údajů a pravděpodobnosti, s jakou újma může vzniknout. Na základě analýzy musí správce následně přijmout taková opatření, aby riziko co nejvíce zmírnil. Kromě institutů, u nichž je výslovně zmíněno, je nutné je uplatňovat všude, kde je na správci, aby zavedl nějaký systém pro soulad s Nařízením. Příkladem může být např. zásada přesnosti. Je na správci, aby posoudil, jak často je s ohledem na riziko nutné přesnost osobních údajů ověřovat. Stejně tak musí správce s ohledem na riziko vyvinout vhodné způsoby pro uplatňování práv subjektů údajů.

b) Vysoké riziko. Pokud na základě posouzení rizika správce zjistí, že při zpracování hrozí vysoké riziko, aktivuje se pro něj povinnost provést posouzení vlivu na ochranu osobních údajů dle čl. 35 Nařízení, povinnost provést předchozí konzultace s dozorovým úřadem dle čl. 36 Nařízení a v případě porušení zabezpečení osobních údajů povinnost notifikovat subjekty údajů dle čl. 34 Nařízení. Za vysoce rizikové zpracování bude považováno např. zpracování, které v souladu s dosaženou úrovní technických znalostí využívá nových technologií, jakož i jiných operací zpracování, které představují vysoké riziko pro práva a svobody subjektů údajů, zejména v případech, kdy je pro subjekty údajů s ohledem na tyto operace obtížnější uplatnit svá práva.

c) Nízké riziko – Nízké riziko aktivuje některé výjimky z povinností dle Nařízení. Nízké riziko tak může správce zprostit povinnosti ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 Nařízení a správce ze třetí země mimo EU může nízké riziko zprostit povinnosti jmenovat zástupce v EU dle čl. 27 Nařízení.

V případě zpracování osobních údajů na základě zákonného zmocnění z titulu plnění povinností zaměstnavatele a zpracování osobních údajů na základě zákonného zmocnění z titulu plnění povinností vést evidenci členů Spolku, je nutno konstatovat, že existuje riziko pro práva a svobody subjektů údajů.

V případě zpracování osobních údajů zpracovaných mimo zákonné zmocnění, tedy na základě souhlasu subjektů osobních údajů, je možno s ohledem na jejich množství, způsob zpracování a jejich povahu konstatovat, že riziko pro práva a svobody subjektů údajů je nízké.

9) Závěr analýzy rizik

Z provedené analýzy rizik vyplývá nutnost přijmout následující opatření

Opatření	Druh opatření	Typ
Dokumentovat proč jsou OÚ sbírány a zpracovávány - info, které bude k dispozici SÚ, před tím než údaje poskytnou.	Dokument	Politika/směrnice/info
Zpracovat a dokumentovat proces pro vymazání OÚ a to jak v elektronické, tak v papírové podobě. Stejně tak pro případ omezeného zpracování.	Dokument	Politika/směrnice/info
Zpracovat a dokumentovat proces pro získání souhlasu se získáním a zpracováním OÚ a to jak v elektronické podobě (email, web dotazníky, osobně nebo telefonicky).	Dokument	Politika/směrnice/info
Implementace šifrování	Technologie	

Implementace pseudonymizace	Technologie	
Zpracovat a dokumentovat proces získání OÚ od externího subjektu, zajištění souhlasu se získání OÚ.	Dokument	Politika/směrnice
Dokumentovat proč jsou sbírány a zpracovávány citlivé OÚ - info, které bude k dispozici SÚ, před tím než údaje poskytnou.	Dokument	Politika/směrnice/info
Zpracovat doložku mlčenlivosti pro všechny zaměstnance pracující s OÚ	Dokument	
Zpracovat a dokumentovat proces informování SÚ o zpracovávání OÚ. Jedná se jak o údaje v elektronické, tak v papírové podobě.	Dokument	Politika/směrnice
Zpracovat dokument informující SÚ o všech jeho právech a o postupech při práci s jeho OÚ.	Dokument	Politika/směrnice/info
Zpracovat a dokumentovat proces pro posouzení požadavků SÚ, proces zpětného informování. A to jak v elektronické podobě (email, web dotazníky, osobně nebo telefonicky).	Dokument	Politika/směrnice
Zpracovat a dokumentovat proces pro poskytnutí přístupu SÚ k jeho OÚ. Nesmí být v rozporu s bezpečností a analýzou rizik.	Dokument	Politika/směrnice
Zavedení vhodných technologických opatření	Technologie	
Zpracovat kodex chování pro pracovníky s přístupem k OÚ	Dokument	Politika/směrnice/info
Definovat a obsadit roli firemního zmocněnce pro oblast ochrany OÚ (nikoli však pověřence ve smyslu nařízení GDPR), jak rovněž stanovit jeho práva a povinnosti	Personální Dokument	Role/politika/směrnice
Zpracovat a dokumentovat proces vytváření záznamů při práci a manipulaci s OÚ.	Dokument	Politika/směrnice
Generovat záznamy při práci a manipulaci s OÚ.	Dokument	Záznamy
Zpracovat postupy incident managementu	Dokument	Politika/směrnice