Audit připravenosti na GDPR – srovnávací analýza spolku Polský kulturně-osvětový svaz v České republice z.s.

1. Úvod

Spolek Polský kulturně-osvětový svaz v České republice z.s., zapsaný 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“), je spolkem, založeným dle právního řádu České republiky.

Statutárním orgánem spolku je předseda:

Mgr. HELENA LEGOWICZ
dat. nar. 3. listopadu 1954
Trvale bytem: Obecní 186, 735 43 Albrechtice
Bydliště: 43-400 Cieszyn, powiat Cieszyn, Górna 20, Polská republika

Účelem (cílem) spolku dle zápisu ve spolkovém rejstříku je zachování národní identity Poláků žijících v České republice, zejména:
a) Ochrana a reprezentace práv a zájmů Poláků žijících v České republice,
b) sdružování Poláků žijících v České republice,
c) podporování kultury a osvěty navazováním na tradice polské kultury a kultury Těšínského Slezska a účast na multikulturním rozvoji České republiky a Evropy,
d) zachování obecného užívání polského jazyka a propagace polské kultury v ČR,
e) podpora polských společenských, kulturních a hospodářských aktivit.

Orgány PZKO jsou:

- Sjezd delegátů PZKO - nejvyšší orgán spolku
- Hlavni výbor PZKO - výkonný a administrativní orgán spolku
- Konvent předsedů - přijímá usnesení, jež jsou pro hlavní výbor závazná, v období mezi sjezdy delegátů
- Revizní komise PZKO - kontrolní orgán spolku

Hlavní výbor PZKO má následující oddělení:

- Ekonomické oddělení
- Sekretariát
- Redakce Zwrot

Ke dni provedení auditu Spolek eviduje 69 pobočných spolků.

Spolek provozuje v rámci své činnosti následující webové stránky: www.pzko.cz a www.zwrot.cz.

2. GDPR

GDPR neboli General Data Protection Regulation je Nařízení evropského parlamentu a rady (EU), jehož účinnost je dána 25. květnem 2018. GDPR je přímo závazné pro jednotlivé členské země Evropské unie a nahradí jednak směrnici 95/46/ES, která upravuje ochranu osobních údajů na úrovni Evropské unie, ale i český zákon č. 101/2000 Sb., o ochraně osobních údajů.

Hlavním cílem je důslednější ochrana osobních údajů občanů EU. Osobním údajem je myšlen jakýkoli údaj s potenciálem identifikovat konkrétní osobu. Osobním údajem je tedy třeba i telefonní číslo, bydliště, GPS lokace, nebo dokonce informace o tom, že má dotyčná osoba tetování.

Regulace ukládá v oblasti osobních dat povinnosti společnostem a definuje práva občanů EU na dostupnost informací.

V případě porušení/nedodržení povinností nebo odmítnutím spolupráce se státním kontrolním orgánem, se zpracovatel dat vystavuje sankci až do hodnoty 20 mil. EUR případně do 4% celosvětového ročního obratu společnosti. Sankci je samozřejmě možné uložit opakovaně.

3. Použité pojmy a zkratky

Analýza rizik (risk analysis)	proces identifikování bezpečnostních rizik, stanovící jejich závažnost a identifikující oblasti, která vyžadují ochranná opatření;
Bezpečnost	bezpodmínečný stav bezpečí;
Bezpečnost IT (IT security)	všechny aspekty souvisící s definováním, dosažením a udržováním důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti;
Bezpečnostní opatření (safeguard)	praxe, postup nebo mechanismus, který snižuje riziko;
Důvěrnost (confidentiality)	vlastnost, že informace není dostupná nebo přístupná neautorizovaným jednotlivcům, entitám, nebo procesům (ISO 7498-2:1989);
IDS (Intrusion Detection System)	systém detekce narušení bezpečnostní politiky, sleduje síťové prostředí nebo konkrétní počítač s cílem identifikovat útočníka;
IDS/IPS	kombinace IDS a IPS prostředků, používáno také jako označení kategorie produktů detekujících narušení bezpečnostní politiky;
IPS (Intrusion Prevention System)	systém prevence narušení bezpečnostní politiky (vyvinul se z IDS), sleduje síťové prostředí nebo konkrétní počítač s cílem zabránit útoku útočníka;
Politika bezpečnosti IT (IT security policy)	pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejích systémů IT;
Riziko (risk)	potenciální možnost, že daná hrozba využije zranitelností aktiv nebo skupiny aktiv a způsobí tak ztrátu nebo zničení aktiv;

Škodlivý software	počítačový program nebo kód, jehož spuštění představuje bezpečnostní hrozbu pro výpočetní systém – příkladem jsou viry, červi, trojské koně apod.;
Uživatel	zaměstnanec, který využívá informační technologie k plnění pracovních úkolů;
Zranitelnost (vulnerability)	zahrnuje slabé místo aktiva nebo skupiny aktiv, které může být využito hrozbou;
Osobní údaj (OÚ)	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;
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 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 SÚ	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;
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;
Závazné podnikové 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;
Přeshraniční zpracování	buď: 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;
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.

4. Osobní údaje

Spolek pracuje s několika zdroji osobních údajů, které jsou od sebe odděleny, a to s osobními údaji svých členů, svých zaměstnanců, s osobními údaji svých obchodních partnerů – dodavatelů (případně jejich zaměstnanců) a s osobními údaji svých klientů. Osobní údaje jsou získávány rovněž pomocí kamerového systému umístěného v sídle.

a) Osobní údaje členů

Spolek ke dni vyhotovení tohoto auditu eviduje 9900 členů. Údaje a informace, které jsou získávány o členech, jsou primárně uchovávány v účetním programu Microsoft Access, jak rovněž v listinné podobě. Údaje jsou získávány přímo od subjektu údajů vyplněním přihlášky do spolku, jak rovněž v průběhu členství. Po přijetí za člena jsou osobní údaje členů zavedeny do informačního systému, po jeho odchodu jsou vymazávány.

Data jsou uložena programu MS Access. Program používá vlastní autentizační mechanismus založený na kombinaci jména a hesla. K databázi systému má přístup pouze předseda a zaměstnanec na pozici ekonom.

Listinné dokumenty obsahující osobní údaje jsou umístěny v zamykatelné skříni, do které má přístup pouze předseda a zaměstnanec na pozici ekonom. Po skončení členství člena jsou dokumenty obsahující jeho osobní údaje skartovány.

V rámci interního zpracování jsou osobní údaje zaměstnanců dále zpracovány zaměstnanci Ekonomického oddělení, a to výlučně za účelem vedení evidence členů.

Nedochází k externímu zpracování osobních údajů členů.

Data a informace, které jsou sbírány:

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 zaměstnanců

Spolek ke dni vyhotovení tohoto auditu zaměstnává 10 zaměstnanců. Údaje a informace, které jsou získávány o zaměstnancích, jsou primárně uchovávány v účetním programu POHODA, jak rovněž v listinné podobě. Údaje jsou získávány po celou dobu kontaktu a případně vztahu se zaměstnanci či potencionálními zaměstnanci, tedy již v rámci prvního kontaktu s uchazeči o zaměstnání (dotazníky), v průběhu nástupního pohovoru, jak rovněž v průběhu pracovního poměru. Po nástupu do zaměstnání jsou osobní údaje zaměstnanců zavedeny do informačního systému, po jeho odchodu jsou nadále uchovávány.

Data jsou uložena v účetním programu POHODA. Program používá vlastní autentizační mechanismus založený na kombinaci jména a hesla. K databázi systému má přístup pouze předseda a zaměstnanec na pozici ekonom.

Listinné dokumenty obsahující osobní údaje jsou umístěny v zamykatelné skříni, do které má přístup pouze zaměstnanec na pozici ekonom. Po skončení pracovního poměru zaměstnance jsou dokumenty obsahující jeho osobní údaje přesunuty do uzamykatelného archívu.

V rámci interního zpracování jsou osobní údaje zaměstnanců dále zpracovány zaměstnanci Ekonomického oddělení, a to za účelem vedení evidence zaměstnanců, vedení evidence docházky zaměstnanců, za účelem vyplácení mezd a odměn zaměstnanců a vedení evidence pracovních smluv. Osobní údaje zaměstnanců jsou po odchodu zaměstnance skladovány a archivovány po dobu 30 let.

Nedochází k externímu zpracování osobních údajů zaměstnanců.

Data a informace, které jsou sbírány:

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	
	biometrické údaje – otisk prstu	~~ANO~~	NE	
	biometrické údaje – Podpis	ANO	~~NE~~	
	osobní údaje dětí	ANO	~~NE~~	

c) Osobní údaje externích subjektů

Údaje a informace, které jsou získávány o externích subjektech, primárně dodavatelích, jejichž pomocí vykonává spolek svou činnost, jsou primárně uchovávány v účetním programu POHODA, jak rovněž

v listinné podobě. Spolek ke dni vyhotovení tohoto auditu spolupracuje přibližně se 100 dodavateli zboží a služeb. Zvláštní skupinou dodavatelů jsou osoby spontánně zasílající články k uveřejnění v měsíčníku ZWROT nebo na webových stránkách tohoto měsíčníku. Údaje vstupují do systému jednak z kontraktačního jednání, z osobního jednání s partnery a z veřejných zdrojů (Internet). Údaje jsou získávány individuálně předsedou či jednotlivými pracovníky spolku, kteří s dodavatelem jednají. Data jsou využívána pro zpracování smlouvy a dále v průběhu celého trvání smluvního vztahu k jeho vedení (účetní operace, kontrola výkonu činnosti, atd.). Životní cyklus jednotlivých takto získaných osobních údajů je zcela pod kontrolou předsedy a Ekonomického oddělení spolku.

Data jsou uložena v účetním programu POHODA. Program používá vlastní autentizační mechanismus založený na kombinaci jména a hesla. K databázi systému má přístup pouze předseda a zaměstnanec na pozici ekonom.

V rámci interního zpracování jsou osobní údaje externích subjektů dále zpracovány pracovníky Ekonomického oddělení, a to za účelem vedení evidence dodavatelů a obchodněprávních smluv. Osobní údaje externích subjektů jsou po ukončení obchodněprávního vztahu skladovány a archivovány dle zákonných lhůt.

Listinné dokumenty obsahující osobní údaje jsou umístěny v uzamykatelné místnosti, do které má přístup pouze zaměstnanec Ekonomického oddělení. Po skončení obchodněprávního vztahu jsou dokumenty obsahující jeho osobní údaje přesunuty do uzamykatelného archívu.

Data a informace, které jsou sbírány:

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

d) Osobní údaje klientů

Klienty spolku jsou odběratelé měsíčníku ZWROT. Spolek ke dni vyhotovení tohoto auditu eviduje přibližně 2000 klientů - odběratelů. Osobní údaje klientů jsou získávány primárně při platbách kartou a dále v souvislosti pořizováním kamerového záznamu za účelem zabezpečení objektu. Údaje vstupují do systému přímým získáním od subjektu údajů při vyplňování objednávky předplatného v listinné či elektronické podobě. Údaje a informace, které jsou získávány o klientech, jsou uchovávány v programu Microsoft Access, účetním programu POHODA, jak rovněž v listinné podobě.

Data jsou využívána pro zpracování smlouvy a dále v průběhu celého trvání smluvního vztahu k jeho vedení (zasílání měsíčníku, účetní operace, atd.). Životní cyklus jednotlivých takto získaných osobních údajů je zcela pod kontrolou předsedy a Redakce Zwrot.

Data jsou uložena v účetním programu POHODA a MS Access. Program POHODA používá vlastní autentizační mechanismus založený na kombinaci jména a hesla. K databázi systému má přístup pouze předseda a zaměstnanec na pozici ekonom. MS Access s databází klientů je umístěn na počítači, jenž používá autentizační mechanismus založený na kombinaci jména a hesla. K databázi má přístup pouze předseda a zaměstnanci Redakce ZWROT.

V rámci interního zpracování jsou osobní údaje klientů dále zpracovány pracovníky Ekonomického oddělení, a to za účelem vedení evidence smluv a objednávek, jak rovněž k vystavování faktur. Databáze adres klientů je používána oddělením Redakce ZWROT k zasílání měsíčníků. Osobní údaje klientů jsou po ukončení obchodněprávního vztahu skladovány a archivovány dle zákonných lhůt.

Listinné dokumenty obsahující osobní údaje jsou umístěny v uzamykatelné místnosti, do které má přístup pouze zaměstnanec Ekonomického oddělení. Po skončení obchodněprávního vztahu jsou dokumenty obsahující jeho osobní údaje přesunuty do uzamykatelného archívu.

Data a informace, které jsou sbírány:

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

e) Osobní údaje a kamerové systémy

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.

5. Ochrana dat a informačního systému

Všechny listinné dokumenty obsahující osobní údaje jsou uzamčeny v zamykatelné skříni nebo zamykatelném archívu spolku.

Spolek nemá IT oddělení. Jeho funkci vykonává zaměstnanec spolku na pozici správce sítě. Data jsou uložena na serveru, jenž se nachází v EU nebo EHP. Popis ochranných opatření přijatých k zabezpečení informačního systému:

- Monitoring a evidence přístupů do systému.

Do administrační části serveru mam má přístup pouze správce IT.

- Přístup na SQL disky, sdílené disky.

Přístup na sdílené disky mají všichni zaměstnanci. Přístup je chráněný heslem. Spolek nemá SQL databáze s osobními údaji. Spolek má lokální (MS Access) databáze uložené na sdílených discích.

- Šifrování a pseudonymizace dat.

Data nejsou šifrovaná. Databáze jsou zaheslovány.

- Šifrování webového klienta?

Data nejsou šifrovaná.

- Šifrována data na stanicích a jejich zabezpečení.

Kazda stanice má své heslo. Data nejsou šifrována.

- Jak jsou zabezpečeny práva a role uživatelů v systému?

Spolek nemá hromadné (centrální) řízeni prav a roli.

- Jaké jsou bezpečnostní politiky a jejich vynucování u mobilních zařízení?

Bezpečnostní politiky nejsou vynucovány.

Spolek nemá smluvenou bezpečností agenturu pro zajištění fyzické bezpečnosti.

Vlastní role bezpečnostního manažera ať už pro fyzickou nebo informační bezpečnost není vytvořena a obsazena.

6. Posouzení aktuálního stavu s požadavky GDPR

a) Zákonnost zpracování OÚ

Spolek jednoznačně splňuje minimálně jednu z podmínek pro naplnění zákonnosti zpracování osobních údajů, kdy jde o splnění právních povinností vztahujících se k její podnikatelské činnosti (spolek jakožto zaměstnavatel, je povinna vést záznamy pro vyplácení mezd zaměstnanců, zajišťuje odvody na zdravotní/sociální/důchodové pojištění atd.). Nad rámec uvedeného spolek zpracovává osobní údaje na základě souhlasu subjektu údajů pro jeden či více konkrétních účelů – jedná se minimálně o osobní údaje smluvních partnerů – FO, zaměstnanců či pověřených osob smluvních partnerů, jejichž prostřednictvím tito plní své závazky vůči spolku, osobní údaje návštěvníků areálu spolku, atd.

b) Procesy ochrany osobních údajů v jejich životním cyklu

Shromažďování OÚ

Oblast	Stav	Poznámka	Proces
Právní základ zpracování	Ze zákonných důvodů viz. výše; se souhlasem subjektu údajů.	Prováděno rutinní činností předsedy a zaměstnanců.	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	Předseda a 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. 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 či spolupracovníci postupovat v jednotlivých případech.	

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.	Protože není zavedeno, není zpracována související dokumentace pro řízení.	
Přístupy (identifikace osoby provádějící zpracování)	Přístupy jsou přidělovány na základě pracovního či funkčního zařazení, případně požadavku předsedy.	Postup zřízení přístupu není formalizován a nejsou vytvářeny záznamy.	
Oprávnění manipulovat s OÚ	Na základě zařazení.	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.	

Zálohování OÚ

Oblast	Stav	Poznámka	Proces
Redundance, záložní systémy, replikace, datová centra	Je prováděno zálohování.	Nejsou prováděny testy obnovy, nejsou definovány	Není popsán,

		parametry RTO a RPO, není zpracován zálohovací plán.	není definován
Bezpečné úložiště záloh/zabezpečení médií	Vše je umístěno v jedné lokalitě.		

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.		

c) Technická opatření na ochranu dat

GDPR jasně hovoří v určitých případech o nutnosti role pověřence, tato role není ve spolku definována a není ani obsazena *(dle ustanovení článku 37 a násl. nařízení GDPR platí, že správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:*

- *zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;*
- *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;*
- *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 s ohledem na charakter osobních údajů a rozsah jejich zpracování povinnost zřídit a personálně obsadit roli pověřence pro ochranu osobních údajů.

Nelze jednoznačně prokázat, že stávající technická a organizační opatření jsou vhodná. GDPR přisuzuje vhodnost uváděných prostředků na základě zpracování analýzy rizik. Analýza rizik identifikující a hodnotící hrozby a zranitelnosti následně stanovuje, která opatření a za jakých podmínek jsou vhodná. Technická a organizační opatření ochrany osobních údajů jsou s ohledem na stávající stav panující ve spolku nutná, a to ve všech kategoriích uvedených výše pod písm. b), tedy v kategoriích Shromažďování OÚ, Ukládání a zpracování OÚ, Zálohování OÚ a Likvidaci OÚ.

GDRP uvádí jako základní prostředek/opatření pro zajištění ochrany osobních údajů implementaci šifrování a pseudonymizaci. Spolek nemá implementováno šifrování dat v jejich úložištích a ani pseudonymizaci dat jako takovou, a tak není možné zajistit jejich ochranu před diskreditací. Ochrana osobních údajů je založena na kontrole přístupu k aplikacím, jenž data zpracovávají. Vhodnost nasazení šifrování nelze podložit analýzou rizik.

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. Vedle uvedeného spolek neprovádí pravidelné testování a hodnocení účinnosti nasazených opatření. V rámci nově zaváděných interních předpisů bude nutno stanovit kontrolní mechanizmy, včetně jejich periodicity – nabízí se pravidelné kvartální hodnocení. Samozřejmostí je stanovení osoby, která bude za předmětné testování, posuzování a hodnocení odpovědná.

Implementace technických a organizačních opatření na ochranu dat jsou podle GDPR definována na základě analýzy rizik. Protože analýza rizik jako taková není doposud zpracována, je reálné nebezpečí, že v některých případech mohou být stávající opatření vyhodnocena jako nedostatečná (opatření neodpovídá míře rizika) a bude nutné uvažovat o jejich implementaci. Z pohledu implementace technologií je při znalosti stávajícího stavu nutno upozornit na:

- 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 záznamů (logů) – není implementován nástroj a proces, který by umožňoval zpracovávat a vyhodnocovat záznamy systému. V případě jakéhokoliv incidentu je pak velmi obtížné identifikovat kořenovou příčinu a tuto odstranit tak, aby se incident již nemohl opakovat.
- Kontrola zaměstnanců – není implementován nástroj a proces, který by umožňoval kontrolovat činnost zaměstnanců na jejich počítači. Tito mají přístup k osobním údajům, přičemž následně nedochází ke kontrole, jak zaměstnanci nakládají s osobními údaji.

7. Shrnutí

Spolek pracuje s osobními údaji svých členů, zaměstnanců a s osobními údaji obchodních partnerů. 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)

Spolek tak v současné době neplní požadavky GDPR, kdy pro dosažení shody s nimi je nutné učinit nezbytné kroky jak v oblasti organizačních opatření, tak i v oblasti zabezpečení informačního systému.

8. Doložka

Tento audit byl vypracován pro konkrétní případ a jeho další použití ve vztahu k jakýmkoliv orgánům státní moci nebo jiným třetím osobám, které nejsou účastníky daného případu, vyžaduje předchozí souhlas jednatelů Advokátní kanceláře HAJDUK & PARTNERS s.r.o.

V případě nejasností či potřeby ujasnění údajů shora uvedených mne neváhejte bez dalšího kontaktovat.

Vypracoval: Mgr. Richard Koliba, advokát