

Příloha 1: Analýza oblasti GDPR

Osobní údaje	Jsou identifikovány osobní údaje, zpracovávané organizací?
aplikováno	

Osobní údaje	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (opatření dle GDPR v závislosti na rizicích).
částečně aplikováno	

Osobní údaje	Při zpracování osobních údajů se využívá pseudonymizace.
neaplikováno	

Osobní údaje	Při zpracování osobních údajů se využívá šifrování osobních údajů.
neaplikováno	

Osobní údaje	Při zpracování osobních údajů je zajištěna neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb zpracování.
částečně aplikováno	

Osobní údaje	Při zpracování osobních údajů je zajištěna schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.
aplikováno	

Osobní údaje	Při zpracování osobních údajů je zajištěn proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
neaplikováno	

Osobní údaje	Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
neaplikováno	

Osobní údaje	Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.
částečně aplikováno	

OÚ - kodexy chování	Zpracovány kodexy chování v souvislosti se zpracováním osobních údajů.
nerelevantní	

OÚ - kodexy chování	Dodržovány schválené kodexy chování.
nerelevantní	

OÚ - kodexy chování	Vydáno osvědčení podle čl. 40 GDPR.
nerelevantní	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů - předání údajů nebo soubor předání, včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo daných třetích zemí - svoji právně závaznou povahu, a to interně i externě
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrná a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů; opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu, včetně práva nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování, práva podat stížnost u příslušného dozorového úřadu, právní ochrany a případně i práva na odškodnění v případě porušení závazných podnikových pravidel
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii; správce nebo zpracovatel se může této odpovědnosti zcela nebo zčásti zprostit, pouze pokud prokáže, že za okolnost, jež vedla ke vzniku škody, není daný člen odpovědný
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující způsob poskytování informací o závazných podnikových pravidlech, zejména o ustanoveních uvedených v písmenech d), e) a f) tohoto odstavce, subjektům údajů, vedle informací uvedených v článcích 13 a 14
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující úkoly všech pověřenců pro ochranu osobních údajů jmenovaných v souladu s článkem 37, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a sledování školení a vyřizování stížností
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující postupy pro vyřizování stížností
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly. Tyto mechanismy zahrnují audity ochrany údajů a metody zajištění opravných opatření pro ochranu práv subjektu údajů. Výsledky takového ověření by měly být oznámeny osobě nebo subjektu uvedenému v písmenu h) a radě řídicího podniku skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a na požádání by měly být zpřístupněny příslušnému dozorovému úřadu;
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů; mechanismus spolupráce s dozorovým úřadem, který zajistí dodržování pravidel každým členem skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, zejména zpřístupňování výsledků ověřování opatření uvedených v písmenu j) dozorovému úřadu;
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující mechanismy pro podávání zpráv příslušnému dozorovému úřadu o právních požadavcích, kterým je člen skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost podřízen ve třetí zemi a které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly
neaplikováno	

OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující vhodnou odbornou přípravu v oblasti ochrany údajů pro pracovníky, kteří mají k osobním údajům trvalý nebo pravidelný přístup.
neaplikováno	

OÚ - záznamy o zpracování	Vedeny záznamy o činnostech zpracování OÚ: - jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů; - účely zpracování; - popis kategorií subjektů údajů a kategorií osobních údajů; - kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
neaplikováno	

OÚ - záznamy o zpracování	Vedeny záznamy o činnostech zpracování OÚ: - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk
neaplikováno	

OÚ - záznamy o zpracování	Vedeny záznamy o činnostech zpracování OÚ: - je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů; - je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.
neaplikováno	

OÚ - záznamy o zpracování	Vedeny záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují: - jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů; - kategorie zpracování prováděného pro každého ze správců; - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk; - je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.
neaplikováno	

Osobní údaje	Vedeny záznamy o všech typech zpracování OÚ (např. i záznamy o přístupech ke čtení).
neaplikováno	

Osobní údaje	Provedeno posouzení vlivu na ochranu OÚ.
neaplikováno	

Osobní údaje	Přirazena role DPO (Data Protection Officer).
nerelevantní	

Osobní údaje	Jakým způsobem jsou evidovány a získávány souhlasy se zpracováním osobních údajů?
aplikováno	Souhlasy jsou získávány přes e-shop odsouhlasením.

Osobní údaje	Jsou souhlasy uchovávány a aktualizovány?
částečně aplikováno	Uchovávány ano, ale aktualizovány ne.

Osobní údaje	Garantují Vaši dodavatelé bezpečnost zpracovávaných osobních údajů?
neaplikováno	

Osobní údaje	Máte dnes již osobní údaje kategorizovány? Rozdělujete osobních údaje?
neaplikováno	

Osobní údaje	Zaznamenáváte/monitorujete práce s osobními daty?
neaplikováno	

Osobní údaje	Uchovávejte data získaná z Call centra?
nerelevantní	Společnost nemá Call centrum.

Osobní údaje	V jakém znění jsou dnes souhlasy udělovány? Jsou udělovány v souladu s GDPR?
neaplikováno	

Osobní údaje	Řešíte smluvně dodavatelský řetězec? Bezpečnost Vašich dat u Vašich dodavatelů?
neaplikováno	

Osobní údaje	Dokumentujete nakládání s osobními daty Vašich zákazníků?
neaplikováno	

Osobní údaje	Zálohujete data na více než 2 samostatné zálohy?
aplikováno	Ano.

Osobní údaje	Vedete záznamy o hromadném zpracování dat?
nerelevantní	Společnost data hromadně nezpracovává.

Osobní údaje	Rozesíláte marketingové letáky, upozornění?, marketingové newslettery jen s písemným souhlasem k nakládání s osobními údaji?
aplikováno	Ano, pouze se souhlasem.

Osobní údaje	Disponujete s marketingovými bázemi? Vlastními?
aplikováno	Ano.

Osobní údaje	Jsou osobní údaje v databázi zákazníků? Pokud jsou, vykonáváte správu dle smluvních ujednání?
částečně aplikováno	Ano, OÚ jsou v databázi zákazníků.

Osobní údaje	Zpracováváte osobní údaje jen ve Vašem vlastním systému, na kterém máte přijatá bezpečnostní opatření?
částečně aplikováno	Ano, zpracovává se ve vlastním systému.

Osobní údaje	Jsou osobní údaje evidovány pouze a výhradně ve Vašem vlastním systému?
aplikováno	

Osobní údaje	Plníte zavedená pravidelná školení pro práci s osobními daty?
neaplikováno	

Osobní údaje	Jakým způsobem řešíte dokumentaci k osobním datům - ISMS zavedeno nebo jiné směrnice?
neaplikováno	

Osobní údaje	Provádíte bezpečnostní audit IS, kde jsou osobní data obsažena?
neaplikováno	

Osobní údaje	Testujete bezpečnostní opatření? Kontrolujete své partnery, jakým způsobem pracují s osobními daty?
neaplikováno	

Osobní údaje	Máte k dispozici havarijní plány při porušení ochrany osobních údajů?
neaplikováno	

Osobní údaje	Evidujete údaje o nákupech, využívaných službách? Nebo jsou to data zákaznická, a vy jste v roli zpracovatele osobních údajů...(údaj o nákupu je osobním údajem) - řešíte tuto oblast dokumentačně a z pohledu bezpečnosti osobních údajů?
aplikováno	

Osobní údaje	Shromažďujete data o IP adresách?
aplikováno	

Osobní údaje	Referencujete tato data s referencemi na konkrétní profily, kde jsou dodací údaje nebo platební údaje zákazníka?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Probíhá u Vás automatické zpracování dat a profilování zákazníků? - systematické a rozsáhlé zpracování
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Pracujete s kategoriemi zvláštních údajů (rasové, etnické, trestní, registry dlužníků apod.)
nerelevantní	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Prověřujete platební schopnosti Vašich klientů?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Vytváříte marketingové profily svých zákazníků (např. dle jejich lokace)
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte údaje na základě automatizovaného rozhodování? - může vést k diskriminaci některého ze zákazníků
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Monitorujete adresné chování zákazníků?
aplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte lokalizační nebo platební údaje (i historie), které by mohly být zneužity?
aplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte rozsáhlé údaje - např. z důvodu cílení reklamy v e-shopech?
aplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte/evidujete údaje dle územního rozsahu?
částečně aplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte údaje propojených či kombinovaných souborů nebo databází, které osobní údaje obsahují? Kde původem je více zdrojů? - zpracování nad rámec původního účelu?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte data o zaměstnancích, zdravotně postižených nebo o nezletilých?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Máte interně zaveden systém otisku prstu pro vstup na pracoviště?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Předáváte data mimo EU?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Dochází k přeshraničnímu předávání dat vč. dat osobních?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Prověření zákazníků, kde se zákazník nemůže vyhnout nakládání s jeho daty - např. prověřování platební schopnosti či jeho ověření platební karty či totožnosti.
nerelevantní	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Po jakou dobu uchovávejte data z Call centra - z hovorů.
nerelevantní	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Kde probíhá zálohování a archivace těchto dat? Probíhá ve Vaší společnosti?
aplikováno	Ano, ve společnosti.

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Disponujete kapacitami a plánem na zpracování procesu a technologických opatření, která vyplynou z tvorby dokumentace doporučení DPIA?
neaplikováno	

Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Disponujete přesným popisem procesů, jakým jako správce musíte prokazovat vůči UOOU?
neaplikováno	

Osobní údaje	Provádíte pravidelné bezpečnostní audity IS a s nimi provázaných dat?
neaplikováno	

Osobní údaje	Jsou ve Vámi vlastněných a využívaných IS data bezpečně zpracovávána, uchovávána?
částečně aplikováno	

Přenositelnost údajů	Data aktivní a vědomě poskytnutá vs. data poskytnutá zákazníkem na základě využití služby.
neaplikováno	

Osobní údaje	Máte kompletní přijímací dokumentaci zpracovanou?
neaplikováno	

Osobní údaje	Disponujete "papírovými osobními údaji"? Přístupujete k osobním údajům v nestrojové podobě jako k těm strojovým?
neaplikováno	

Příloha 2: Matice zranitelnosti

Zranitelnost [V]		Zdroj	INFORMAČNÍ					HARDWAROVÁ					SOFTWAREOVÁ							SLUŽBY																			
			server		server cloud IP kamera								server pc, ntb, mob							sídl	sklad M.	sklad Č.	kancelář	mobil. zař.	sídl	sklad M.	sklad Č.	kancelář											
Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zálohy dat		Server	Pracovní stanice	Notebooky	Mobilní zařízení	Pasivní síťové prvky	Aktivní síťové prvky	Firewall	Operační systémy		Exchange server	Software měřicího zařízení	Účetní software	Software IP kamer	VPN klient	Antivirový software	Spam filter	Internetové připojení						Elektrická energie					Doménové služby	E-shop	www	Dohled výměníkové stanice	Služba záloh	VPN připojení	Služba IP kamer
A	5	4	5	5	4	2	5	3	3	3	5	5	5	4	3	5	3	5	2	4	5	2	4	4	3	4	4	4	4	4	2	4	2	3	4	4	2		
Hrozba	T																																						
Požár	2							3	4	3	2	4	3	3									3						3										
Poškození vodou	1							2	3	3	3	1	2	2									2					2											
Zničení zařízení nebo médií	3							3	2	3	4	2	2	2									2					1											
Povodeň	1							1	5	3	3	5	5	5									5					5											
Přerušení dodávky elektřiny	3	4	4	4	2	3	2	2	3	1	1	4	4	4									4	4	4	4		5				2			1	2	4	2	
Selhání telekomunikačních zařízení	4	4	4	4	4	3		2	3	3	3	2	2										5	3	2	5					3			3	2	4			
Vzdálená špionáž	1	4	4	4	4	4	1		2	3	4	1	3	3	1	1	3	1	3	1		3										1	3	2	2	4		1	
Odposlech	1																						4	2	2	3	4					1			2	3	1	1	
Krádež médií nebo dokumentů	3	4	2	4	1	2	1																																
Krádež zařízení	4							1	3	4	5		3	3																									
Vyzrazení	5	3	3	4	3																																		
Falšování pomocí aplikačního prog. vybavení	4				1	1	1									1	1	2	1	1	1																		
Odhalení pozice	3									1	3																												
Selhání zařízení	3							3	2	2	1	1	3	3																									
Chybné fungování zařízení	3							3	2	2	2	2	3	3																									
Chybné fungování aplikačního prog. vybavení	3														3	3	3	1	4	1	3	3	3																
Chyba údržby	3							3	2	2	2		2	2	2	1	3	3	3	2	3	3	1													3			
Neoprávněné použití zařízení	3							2	3	3	4	3	2	2																									
Podvodné kopírování aplikačního prog. zařízení	1														1	2	1	2	2	1	1	1	1																
Použití padělaného nebo zkopírovaného prog. vyb.	1														1	1	1	1	1	1	1	1																	
Poškození dat	2	3	3	3	3	3	3																									2	1	3					
Nezákonné zpracování dat	1	3	3	3	3	3	3									4		4	3		2											3	1						
Chyba používání	3	3	3	3	3	3	2	2	3	3	3	4	3	3	3	3	3	2	4	1	3	4	4	2	2	2	2	2	2	2	2					3			
Zneužití oprávnění	4	3	3	3	3	3	2	4	4	4	4		3	3	3	3	3	1	4	1	3	3	3																
Odepření činnosti	3							3	2	2	2		3	3	3	3	3	2	2	3	5	4	3	4	3	3	4	3				3	4	1	3	3	5	2	
Nedostatek personálu	4																		3																				

Příloha 3: Matice rizik

Riziko [R]		Zdroj	INFORMAČNÍ					HARDWAROVÁ					SOFTWAREOVÁ								SLUŽBY																			
			server			server		cloud	IP kamera						server		pc, ntb, mob							sídl	sklad M.	sklad Č.	kancelář	mobil. zař.	sídl	sklad M.	sklad Č.	kancelář								
			Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zálohy dat		Server	Pracovní stanice	Notebooky	Mobilní zařízení	Pasivní síťové prvky	Aktivní síťové prvky	Firewall	Operační systémy		Exchange server	Software měřicího zařízení	Účetní software	Software IP kamer	VPN klient	Antivirový software	Spam filtr	Internetové připojení						Elektrická energie					Doménové služby	E-shop	www	Dohled výměňíkové stanice	Služba záloh
A	5	4	5	5	4	2	5	3	3	3	5	5	5	4	3	5	3	5	2	4	5	2	4	4	3	4	4	4	4	4	4	4	2	4	2	3	4	4	2	
Hrozba	T																																							
Požár	2						30	24	18	12	40	30	30										24					24												
Poškození vodou	1						10	9	9	9	5	10	10										8					8												
Zničení zařízení nebo médií	3						45	18	27	36	30	30	30										24					12												
Povodeň	1						5	15	9	9	25	25	25										20					20												
Přerušení dodávky elektřiny	3	60	48	60	30	36	12	30	27	9	9	60	60	60									48	48	36	48		60				12			9	24	48	12		
Selhání telekomunikačních zařízení	4	80	64	80	80	48		40	36	36	36	40	40										80	48	24	80					24			36	32	64				
Vzdálená špionáž	1	20	16	20	20	16	2		6	9	12	5	15	15	4	3	15	3	15	2		15									2	12	4	6	16		2			
Odposlech	1																						96																	
Krádež médií nebo dokumentů	3	60	24	60	15	24	6																																	
Krádež zařízení	4						20	36	48	60		60	60																											
Vyzrazení	5	75	60	100	75																																			
Falšování pomocí aplikačního prog. vybavení	4				20	16	8									20	12	40	8	16	20																			
Odhalení pozice	3								9	27																														
Selhání zařízení	3						45	18	18	9	15	45	45																											
Chybné fungování zařízení	3						45	18	18	18	30	45	45																											
Chybné fungování aplikačního prog. vybavení	3													36	27	45	9	60	6	36	45	18																		
Chyba údržby	3						45	18	18	18		30	30	24	9	45	27	45	12	36	45	6														36				
Neoprávněné použití zařízení	3						30	27	27	36	45	30	30																											
Podvodné kopírování aplikačního prog. zařízení	1													4	6	5	6	10	2	4	5	2																		
Použití padělaného nebo zkopírovaného prog. vyb.	1													4	3	5	3	5	2	4	5	2																		
Poškození dat	2	30	24	30	30	24	12																										16	4	18					
Nezákonné zpracování dat	1	15	12	15	15	12	6									20		20	6		10											12	2							
Chyba používání	3	45	36	45	45	36	12	30	27	27	27	60	45	45	36	27	45	18	60	6	36	60	24	24	24	18	24	24	24	24	24					36				
Zneužití oprávnění	4	60	48	60	60	48	16	80	48	48	48		60	60	48	36	60	12	80	8	48	60	24																	
Odepření činnosti	3						45	18	18	18		45	45	36	27	45	18	30	18	60	60	18	48	36	27	48	36				18	48	6	27	36	60	12			
Nedostatek personálu	4																	60																						