Příloha č. 1 Kontrolní seznam o připravenosti na nařízení GDPR „Checklist“

Kategorie osobních údajů a subjektů údajů	**Prvky osobních údajů obsažené v každé kategorii dat**	**Zdroj osobních údajů**	**Účely, pro které jsou zpracovávány osobní údaje**	**Právní základ pro každý účel zpracování (nespecifické kategorie osobních údajů)**	**Zvláštní kategorie osobních údajů**	**Právní základ pro zpracování zvláštních kategorií osobních údajů**	**Doba uchování**	**Akce musí být v souladu s GDPR?**
Uveďte kategorie osob údajů a shromážděných a uchovávaných osobních údajů, např. Aktuální údaje o zaměstnancích; údaje o důchodcích zaměstnanců; údaje o zákaznících (informace o prodeji); marketingová databáze; CCTV záběry.	*Seznam všech typů osobních údajů obsažených v každé kategorii osobních údajů, např. Jméno, adresa, bankovní údaje, historie nákupů, historie procházení online, video a obrázky.*	*Uveďte zdroj (zdroje) osobních údajů, např. shromážděných přímo od jednotlivců; od třetí strany (jestliže třetí strana identifikuje správce údajů, protože tyto informace budou nezbytné k plnění povinností podle článku 14).*	*V rámci každé kategorie seznamů osobních údajů se shromažďují a uchovávají účely údajů, např. marketing, zlepšování služeb, výzkum, vývoj produktů, integrita systémů, záležitosti týkající se lidských zdrojů, reklama.*	*Pro každý účel zpracování osobních údajů uveďte právní základ, ze kterého vychází, např. souhlas, smlouva, právní závazek (článek 6).*	*Pokud jsou shromažďovány a uchovávány zvláštní kategorie osobních údajů, uveďte podrobnosti o povaze údajů, např. o zdravotních, genetických a biometrických datech.*	*Uveďte právní základ, na kterém jsou shromažďovány a uchovávány zvláštní kategorie osobních údajů, např. výslovný souhlas, legislativní základ (článek 9).*	*Pro každou kategorii osobních údajů uveďte dobu, po kterou budou data uchována, např. jeden měsíc? Jeden rok?* *Obecně platí, že údaje musí být uchovávány déle, než je nezbytné pro účel, pro který byly shromážděny.*	*Identifikujte akce, které jsou nutné k zajištění toho, aby všechny operace zpracování osobních údajů byly kompatibilní se standardem GDPR, např. to může zahrnovat smazání dat, kde není důvod pro uchovávání.*

Osobní data

	Otázka	Ano	Ne	Komentáře / Opatření
Zpracování údajů na základě souhlasu (články 7, 8 a 9 a další pokyny k dispozici na stránkách GDPRandYou.ie)	Provedli jste kontrolu procesů ve vaší organizaci v souvislosti se shromažďováním souhlasu, aby bylo zajištěno, že je svobodně dána, specifická a informovaná a že je jasným znamením, že se subjekt údajů rozhodl souhlasit se zpracováním svých údajů pomocí prohlášení nebo jasného souhlasného opatření?			
	Pokud osobní údaje, které v současné době držíte na základě souhlasu, nesplňují požadovaný standard podle GDPR, znovu jste požádali o souhlas s tím, abyste zajistili soulad s GDPR?			
	Existují postupy, které dokládají, že subjekt údajů souhlasil s tím, aby byly zpracovávány jeho údaje?			
	Jsou zavedeny postupy umožňující subjektu údajů stáhnout svůj souhlas se zpracováním svých osobních údajů?			
Osobní údaje dětí (článek 8)	Kde jsou služby poskytovány dítětem online, jsou zavedeny postupy pro ověření věku a získání souhlasu rodiče / zákonného zástupce, pokud je to nutné?			

Legitimní zpracování zájmů	Je-li legitimní zájem právním základem, na jehož základě jsou zpracovávány osobní údaje, byla provedena vhodná analýza, která zajistila, že použití tohoto právního základu je přiměřené? Tato analýza musí prokázat, že 1) existuje oprávněný zájem, 2) zpracování údajů je naprosto nezbytné pro dosažení oprávněného zájmu a 3) zpracování není narušeno právy subjektu údajů.			

Práva subjektů údajů

	Otázka	Ano	Ne	Komentáře / Opatření
Přístup k osobním údajům (článek 15)	Existuje zdokumentovaná politika / postup pro zpracování žádostí o přístup k tématu (SAR)?			
	Je vaše organizace schopna odpovědět na SAR do jednoho měsíce?			
Přenositelnost dat (článek 20 a další pokyny k dispozici na GDPRandYou.ie)	Existují postupy pro poskytování osobních údajů jednotlivcům ve strukturovaném, běžně používaném a strojově čitelném formátu?			
Vymazání a opravy (články 16 a 17)	Existují kontroly a postupy, které umožňují vymazání nebo opravu osobních údajů (případně)?			

Právo na omezení zpracování (článek 18)	Existují kontroly a postupy, které zastaví zpracování osobních údajů, pokud se na základě platných důvodů subjekt údajů snaží o omezení zpracování?			
Právo vznést námitky proti zpracování (článek 21)	Jsou subjekti údajů informováni o svém právu vznést námitky proti určitým druhům zpracování, jako je přímý marketing, nebo pokud je právní základ pro zpracování legitimními zájmy nebo nezbytným pro úkol vykonávaný ve veřejném zájmu?			
	Existují kontroly a postupy pro zastavení zpracování osobních údajů, pokud subjekt údajů vznesl námitky proti zpracování?			
Profilování a automatizované zpracování (článek 22 a další pokyny k dispozici na GDPRandYou.ie)	Má-li automatizovaný rozhodovací proces, který má právní nebo významný podobný dopad na subjekt údajů, založen na souhlasu, byl shromážděn výslovný souhlas?			
	V případě automatického rozhodnutí, které je nezbytné pro uzavření nebo plnění smlouvy nebo na základě výslovného souhlasu subjektu údajů, existují postupy, které usnadňují právo subjektu údajů získat lidský zásah a napadnout rozhodnutí?			

Omezení práv subjektů údajů (článek 23)	Byly zdokumentovány okolnosti, v nichž mohou být práva na ochranu osobních údajů právně omezena? Poznámka: Irský zákon o ochraně údajů stanoví další podrobnosti týkající se provádění článku 23.			

Přesnost a zachování

	Otázka	Ano	Ne	Komentáře / Opatření
Omezení účelu	Jsou osobní údaje používány pouze pro účely, pro které byly původně shromažďovány?			
Minimalizace dat	Shromažďované osobní údaje jsou omezeny na to, co je nezbytné pro účely, pro které jsou zpracovávány?			
Přesnost	Jsou zavedeny postupy pro zajištění aktuálnosti a přesnosti osobních údajů a pokud je požadována oprava, jsou nezbytné neprodleně provedené změny?			
Zachování	Existují postupy uchovávání údajů a postupy, které zajistí, že údaje nebudou uchovávány déle, než je nezbytné pro účely, pro které byly shromažďovány?			

Jiné právní závazky týkající se zadržení	Je vaše organizace předmětem jiných pravidel, která vyžadují minimální dobu uchovávání (např. zdravotní záznamy / daňové záznamy)?			
	Máte zavedené postupy pro zajištění bezpečného zničení dat v souladu s vašimi pravidly uchovávání údajů?			
Duplikace záznamů	Existují postupy, které zajistí, že nebude existovat zbytečná nebo neregulovaná duplikace záznamů?			

Požadavky na průhlednost

	Otázka	Ano	Ne	Komentáře / Opatření
Transparentnost vůči zákazníkům a zaměstnancům (články 12, 13 a 14 a další pokyny k dispozici na stránkách GDPRandYou.ie)	Jsou uživatelé / zaměstnanci služeb plně informováni o tom, jak pomocí jasných a srozumitelných údajů využíváte jejich údaje v stručné, transparentní, srozumitelné a snadno přístupné formě?			
	Pokud jsou osobní údaje shromažďovány přímo od jednotlivců, existují postupy pro poskytování informací uvedených v článku 13 GDPR?			

	Pokud nejsou osobní údaje shromažďovány od subjektu, ale od třetí strany (např. získané v rámci fúze), existují postupy pro poskytování informací uvedených v článku 14 GDPR?			
	Při interakci se subjekty údajů, například při poskytování služby, prodeji dobrého sledování nebo sledování kamerovým systémem, existují postupy pro aktivní informování subjekty údajů o jejich právech GDPR?			
	Jsou informace o tom, jak organizace usnadňuje subjektům údajů uplatňovat jejich práva GDPR zveřejněná ve snadno přístupném a čitelném formátu?			

Další povinnosti správce údajů

	Otázka	Ano	Ne	Komentáře / Opatření
Dohody o dodavatelích (články 27 až 29)	Dohody s dodavateli a dalšími třetími osobami, které zpracovávají osobní údaje ve vašem zastoupení, byly přezkoumány, aby byly zajištěny všechny vhodné požadavky na ochranu údajů?			
Pracovníci ochrany údajů (osoby odpovědné za ochranu údajů), (články 37 až 39 a další pokyny k dispozici na stránkách GDPRandYou.ie)	Potřebujete jmenovat pověřence pro ochranu osobních údajů podle článku 37 GDPR?			
	Pokud se rozhodne, že pověřenec pro ochranu osobních údajů není požadován, zdokumentovali jste důvody proč?			
	Kde je jmenován pověřenec pro ochranu osobních údajů? Jsou zavedeny linky eskalace a podávání zpráv? Jsou tyto postupy zdokumentovány?			
	Zveřejnili jste kontaktní údaje vašeho DPO, abyste usnadnili svým zákazníkům / zaměstnancům kontakt s ním? (Poznámka: Po 25. květnu 2018 budete také muset informovat orgán ochrany osobních údajů o vašich kontaktních osobách pro ochranu údajů)			

Posouzení dopadů ochrany údajů (DPIA), (článek 35 a další pokyny k dispozici na stránkách GDPRandYou.ie)	Pokud je zpracování údajů považováno za vysoké riziko, máte proces identifikace potřeby a vedení DPIA? Jsou tyto postupy zdokumentovány?			

Bezpečnost dat

	Otázka	Ano	Ne	Komentáře / Opatření
Příslušná technická a organizační bezpečnostní opatření (článek 32)	Vyhodnotili jste rizika spojená se zpracováním osobních údajů a zavedete opatření k jejich zmírnění?			
	Existuje zdokumentovaný bezpečnostní program, který specifikuje technické, administrativní a fyzické záruky osobních údajů?			
	Existuje zdokumentovaný proces řešení stížností a problémů souvisejících s bezpečností?			
	Existuje určená osoba, která je odpovědná za prevenci a vyšetřování narušení bezpečnosti?			
	Používají se standardní šifrovací technologie pro přenos, ukládání a přijímání citlivých osobních údajů subjektu údajů?			

	Jsou osobní údaje systematicky zničeny, smazány nebo anonymizovány, když již není zákonem požadováno, aby byly zachovány.			
	Může být v případě fyzického nebo technického incidentu včas obnoven přístup k osobním údajům?			

Přerušení dat

	Otázka	Ano	Ne	Komentáře / Opatření
Povinnosti týkající se odezvy na porušení údajů (články 33 a 34 a další pokyny k dispozici na stránkách GDPRandYou.ie)	Má organizace dokumentovaný plán reakce na ochranu osobních údajů a bezpečnostních incidentů?			
	Jsou plány a postupy pravidelně kontrolovány?			
	Existují postupy, které umožňují informovat úřad pro ochranu údajů o porušování údajů?			
	Existují postupy, které mají subjekty údajů informovat o porušení údajů (případně)?			

	Jsou všechna porušení údajů plně dokumentována?			
	Existují postupy spolupráce mezi správci údajů, dodavateli a dalšími partnery, kteří se zabývají narušením údajů?			

Mezinárodní přenosy dat - *případně*

	Otázka	Ano	Ne	Komentáře / Opatření
Mezinárodní přenosy údajů (články 44 až 50)	Jsou osobní údaje převedeny mimo EHP, např. Do USA nebo do jiných zemí?			
	Zahrnuje to nějaké zvláštní kategorie osobních údajů?			
	Jaký je účel přenosu?			
	Do koho je převeden?			
	Jsou uvedeny všechny převody - včetně odpovědí na předchozí otázky (např. povaha údajů, účel zpracování, ze které země jsou data vyvážena a která země obdrží údaje a kdo je příjemcem převodu?)			
Zákonnost mezinárodních převodů	Existuje právní základ pro převod, např. Rozhodnutí Komise o přiměřenosti; standardní smluvní doložky. Jsou tyto základny zdokumentovány?			
Průhlednost	Jsou dotyčné osoby plně informovány o zamýšlených mezinárodních převodech jejich osobních údajů?			