Dobrý den, do rukou se Vám dostala praktická část diplomové práce, která má za cíl poskytnout základní předhled toho, jaké povinnosti se daného subjektu týkají, na co byste se měli zaměřit, co pro Vás či vaši firmu může být rizikové a základní přehled povinností.
Jedná se o základní příručku, to znamená, že pro určité subjekty, v závislosti na náležitostech zpracování či kategorii osobních údajů, které jsou více či méně specifické, tato příručka nebude kompletní a bude sloužit jako základní přehled a návod na to, na co se v implementaci GDPR zaměřit. V případě, že máte pochybnosti či otázky, doporučuji projít danou část v diplomové práci či přímo v nařízení nebo materiálech vydané Úřadem pro ochranu osobních údajů či Evropským sborem pro ochranu osobních údajů. Ve specifických případech konzultovat problematiku s odborníkem či právníkem.
Na tomto listě najdete pokyny, jak tento nástroj použít. Nástin celé problematiky můžete naleznout v diplomové práci, která obsahuje jak obecný přehled obsahu nařízení, srovnání s předchozí legislativou, tak i vysvětlení klíčových náležitostí a souvislostí, a naleznete v ní i celý návodný popis pro implementaci.
List analýza slouží k vyplnění specifikace organizace, zpracování, osobních údajů a subjektů údajů, použitých technologií a zabezpečení. Jednotlivé sekce jsou vizuálně označené a dané otázce jsou přiřazené dvě až čtyři odpovědi. Organizace by měla tento dokument vyplnit pro každý účel zpracování. K identifikaci jednotlivých účelů zpracování a lepší přehlednost, lze napsat název řešené oblasti do hlavičky dokumentu.

V hlavičce listu je také označení sloupců - A, B, C, D, které označují identifikátor odpovědi. Odpověď "A" se vyskytuje jen u vybraných otázek, která vždy identifikuje, že daná problematika se v organizaci nevyskytuje - tyto odpovědi jsou podbarvené šedivou barvou. Odpověď "B" označuje ve většině případů nízké hodnoty dané problematiky. Takové jsou podbarvené zelenou barvou. Pokud je pole podbarvené šedou, opět se jedná o v organizaci nepoužitou problematiku. Odpověď "C" označuje ve většině případů významné hodnoty pro danou problematiku, takové jsou podbarvené žlutě. Odpověď "D" ve většině případů označuje kritické hodnoty, sloupec je podbarven červeně. Přesto odpovědi v daných sloupcích mají různou úroveň těchto hodnot.
V případech, kdy otázka není rozlišena významností jsou odpovědi podbarvené stupni šedi. V případech, kdy naopak daná odpověd je značně významná a dané problematice by měla být zvýšená poroznost, zobrazí se na levé straně u specifikace problematiky barevný symbol. Červený v případě opravdu kritického způsobu zpracování či jiné specifikace, žlutý v případě významného problému. U takové problematiky by mělo být zváženo, jestli je takový druh zpracování opravdu nutný, případně problematiku řešit s odborníkem či právníkem.
Pro odpověď lze dané písmeno napsat či vybrat ze seznamu v sloupci "Odpověď". Tento sloupec je jedinou oblastí, která je v tomto listu editovatelná, aby nedošlo k jeho porušení. V případě, kdy odpovědí dochází k automatickému vyloučení některých odpovědí, změní se barva daných řádku na šedivou.
Sloupec "Má vliv:" ukazuje, jestli má daná odpověď vliv na rozhodnutí o tom, jestli má organizace povinnost vést záznamy o činnostech zpracování (ZČZ), provést posouzení vlivu na ochranu osobních údajů (DPIA) či jmenovat pověřence pro ochranu osobních údajů (DPO).
Listy Vyhodnocení a Doporučení pro zabezpečení pak obsahují přehled povinností, které je organizace nutna plnit spolu s jejich základním vysvětlením. Povinnosti a doporučení, které se organizace netýkají, jsou podbarvené šedě.
Poslední dva listy obsahují ukázku toho, jak lze vést záznamy o činnostech zpracování a posouzení vlivu na ochranu osobních údajů. První řádek v těchto ukázkových tabulkách obsahuje doplňkové informace.

Účel zpracování						
Problematika	**A**	**B**	**C**	**D**	**Odpověď**	**Má vliv na:**
Specifikace ekonomického subjektu						
Jedná se o	**FO**	**nekomerční sdružení (zájmové spolky, kluby či ostatní nevýdělečné organizace)**	**podnikající FO nebo PO**	**orgán veřejné moci či veřejný subjekt**		DPO
Počet zaměstnanců		**0**	**1-249**	**250+**		ZČZ
Organizace	**nezpracovává osobní údaje** v žádné části jakéhokoli procesu organizace nepřijde do styku s osobními údaji, neuchovává je, nenahlíží do nich, ani s nimi nijak nemanipuluje	**přijímá osobní údaje (příjemce)** osobní údaje jsou organizaci poskytnuty, ta ovšem zpracování ani neurčuje, ani neprovádí	**zpracovává osobní údaje jiných organizací (zpracovatel)** osobními údaji shromážděné jinou organizací provádí operace na základě pokynů	**určuje účely a prostředky zpracování (správce)** organizace nakládá s osobními údaji bez nutnosti souhlasu jiné organizace, osobní údaje využívá pro své potřeby, určuje jaké operace s osobními údaji budou prováděné, na základě jakého právního titulu zpracování probíhá a pro jaký účel		
Uchovávání osobních údajů						
Forma osobních údajů		**listinné**	**elektronické**	**obě varianty**		
Úložiště		**lokální - PC, mobil, tablet, papírové dokumenty**	**server organizace**	**on-line - služba (externí systém), cloud**		
Přístupy v rámci organizace		**pouze pro osoby pověřené zpracováním**	**omezenému počtu osob**	**neomezenému počtu osob**		
Specifikace subjektů údajů a osobních údajů						
Zdroj osobních údajů		**přímo od dané osoby (subjektu údajů)**	**jiný**	**obě varianty**		
Kategorie subjektu údajů		**běžné osoby** osoby bez zvláštní zranitelnosti	**osoba není identifikována** organizace nemá dostatek osobních údajů k jednoznačené identifikaci subjektu údajů	**zranitelné osoby** osoby, které mohou být zpracováním více poškozené - děti, pacienti, zdravotně postižení, žadatelé o azyl, sociálně slabí apod.		DPO
Kategorie osobních údajů		**běžné údaje** účast na běžných akcích, úroveň vzdělání, popis praxe, ostatní obecné vzhledové a osobnostní charakteristiky, prosté obrazové záznamy, nejedinečné údaje apod.	**významné údaje** údaje znamenající poškození cti či pověsti v případě úniku, přístupové údaje, pseudonym, zaznamenané přestupky/pokuty, účast na některých specifických akcích, jedinečné identifikační údaje např. jméno, příjmení, RČ, číslo OP apod.	**kritické údaje** údaje spadající do čl 9, 10, vysoce osobní povahy, historie navštívených stránek, finanční údaje, údaje o zařízení, o uskutečněných voláních		DPIA
Zvláštní kategorie osobních údajů - čl. 9		**nezpracovány**	**zpracovány**	**rozsáhle zpracovány**		DPIA, DPO, ZČZ
Údaje o trestních věcech - čl. 10		**nezpracovány**	**zpracovány**	**rozsáhle zpracovány**		DPIA, DPO, ZČZ
Kategorie subjektu údajů z pohledu zařazení do vymezené skupiny a možné ohrožení z okolního prostředí		**subjekty nejsou součástí vymezené skupiny**	**subjekty jsou součástí vymezené skupiny s omezenou zranitelností** časově omezená nebo situačně daná - subjekty jsou např. nemocní či staří lidé, děti, mladiství, studenti, či žadatelé vůči veřejné správě, příjemci zdravotních a sociálních služeb, odběratelé specifického zboží	**subjekty jsou součástí vymezené skupiny se stálou zranitelností** zranitelnost se není omezená časem či danou situací, subjekty, které jsou vymezné dle údajů spadajících do čl.9 - sexuální orientace, národnost apod.) či odsouzení pro trestný čin		DPIA
Specifikace zpracování						
Zpracování je:		**příležitostné**		**systematické a pravidelné** vyskytující se v souladu se systémem, předem naplánované, organizované nebo metodické, odehrávající se jako součást obecného plánu, provedené jako součást strategie, po určité období v určitých intervalech, opakované, nepřetržité		DPO
Rozsah zpracování		**malý** méně než 5000 / 0,5% populace do 2 přistupujících 1-4 míst zpracování obec	**střední** 5 001-10 000/0,5-1% populace 2-20 přistupujících 5-20 míst zpracování region, kraj	**velký** od 10 001 / 1,0% populace více než 20 přistupujících osob více než 20 míst zpracování státní		DPIA, DPO
Zpracování probíhá na základě		**plnění právní povinnosti**	**plnění smluvních povinností, oprávněný zájem správce, ochrana životně důležitých zájmů**	**souhlas, plnění úkolu prováděného ve veřejném zájmu**		
Možnost subjektu údajů ovlivnit specifikace zpracování a uplatňování svých práv (právo na výmaz, právo vznést námitku apod.)		**vysoká** subjekt bez problému prosazuje svá práva daná nařízením	**omezená** svá práva může uplatňovat jen částečně, v omezeném časovém úseku nebo za vymezených podmínek – zpracování k uplatnění práv a povinností vyplývající ze zákona – uzavírání smluvních vztahů	**minimální či žádná** svá práva může uplatňovat jen dílčím způsobem či vůbec nelze ovlivnit prosazení práv daná nařízením		DPIA
Přístupnost osobních údajů mimo hranice organizace		**nejsou veřejně přístupné - přístupné pouze správci nebo zpracovateli (a orgánům veřejné moci na základě právních předpisů)**	**omezenému počtu subjektů - dostupné pouze předem vymezené skupině**	**neomezenému počtu subjektů - např. na základě právních předpisů**		DPIA
Předávání osobních údajů						
Využívá organizace zpracovatele?		**ne**	**ano, vazby jsou jednoznačně vymezené**	**ano, vazby nejsou jednoznačně vymezené**		DPIA
Předání třetím stranám		**ne**	**ano, subjekt údajů je informován**	**ano, subjekt údajů není informován**		
Předání do třetích zemí a mezinárodním organizacím		**ne**	**ano, do zemí zajišťující institucionální bezpečnost**	**ano, do ostatních zemí**		
Monitorování						
Monitorování veřejně přístupných prostor		**neprobíhá**	**ano** probíhá na pozemcích majitele, bytových domech, průmyslových objektech, prodejnách, 1-1,5m veřejného prostranství, či těsně přilehlé k monitorovanému objektu	**ano, rozsáhlé** kamerové systémy monitorující ve velkém rozsahu veřejná prostranství, např. letiště		DPIA
Monitorování subjektu údajů	**neprobíhá**	**monitorované** monitorování prostřednictvím jedinečných identifikačních údajů – záznam životních funkcí pacientů, docházkové systémy, zvukové záznamy, záznamy z činnosti subjektů na síti	**rozpoznatelné** monitorování ve formě obrazových záznamů za účelem ochrany majetku a zvýšení bezpečnosti jako běžný kamerový systém	**lokalizovatelné** monitorování fyzického pohybu nebo pobytu identifikovatelných SÚ, lokalizace subjektu, nepatří sem zvukové záznamy pro smluvní účely		DPIA
Využívaná řešení						
Používané IT systémy jsou vyvinuté a spravované:		**přímo společností**	**externím dodavatelem**	**obě varianty**		
Využití nových technologických nebo organizačních řešení		**již nasazené řešení známého zpracování**	**nové řešení již známého zpracování**	**zcela nové řešení, doposud nerealizované zpracování**		DPIA
Použitý systém pro zpracování		**jednoduchý nebo složitý systém bez propojení na jiná zpracování** zřetězení operací s proměnlivými nebo vícenásobnými vazbami	**s propojením na jiná zpracování stejným správcem** zejména zpracování se slučováním/sdružováním údajů získaných za různými účely	**automatizované expertní systémy** analýza, profilování, veškeré automatizované zpracování		DPIA
Využití marketingu		**ne**	**ano, pasivní**	**ano, aktivní, profilovaný (na míru)**		
Využití webových stránek	**ne**	**pouze informativní webové stránky, bez formulářů či sledování uživatele resp. bez identifikace**	**jednoduché formuláře pro kontaktování pomocí e-mailu, žádné statistiky či cizí scripty, pokud cookies, tak pouze výkonnostní či relační**	**lze se zaregistrovat, použití analytik anebo cizích skriptů, cookies i reklamní a trvalá**		
Využití e-shopu		**ne**	**ano, bez historie, bez registrace**	**ano, historie - předchozí nákupy, návštěvy, remarketing**		

Obecné zásady pro zpracování osobních údajů

Podmínky vyjádření souhlasu
Souhlas je vždy přiřazený k určitému účelu.
Je odvolatelný.
Odvoláním souhlasu není dotčeno zpracování před jeh
Odvolání souhlasu musí být stejně snadné jako jeho po
Souhlas musí být jasně odlišitelný, srozumitelný a snad
Pokud jsou povinnosti a náležitosti souhlasu porušeny

SÚ, které nejsou identifikované
V případě, že by správce musel vyvinout nepřiměřené ú pro jejich identifikaci a následné plnění ostatních povin

Informace, které musí společnost sdělit subjektu údaj
bez ohledu na zdroj
od subjektu údajů
jiný zdroj

Zpracovatel
Zpracovatelská smlouva musí obsahovat

Všeobecné zásady zpracování osobních údajů zaměst
Jako právní důvod by neměl být využíván souhlas
Zpracování během přijímacího řízení
Zpracování při prověřování v průběhu zaměstnání
Dohled nad užíváním ICT
Předávání zaměstnaneckých údajů třetím stranám

Záznamy činností zpracování (ZČZ)
Musí obsahovat:

Pověřenec pro ochranu osobních údajů (DPO)
Správce sdělí:
DPO má za úkol:

Posouzení vlivu na ochranu osobních údajů (DPIA)
Je vhodné zkontrolovat, jestli dané zpracování, v stanovených ÚOOÚ. Seznam takový
Vyžaduje:
V minimálním rozsahu musí obsahovat:
Udává povinnost vést záznamy o činnostech zpracován

Podmínky pro předávání do třetích zemí bez institucio
Pouze pokud jsou splněny tyto podmínky:

Automatizované rozhodování
Pro subjekt údajů neplatí právo nebýt předmětem automatizovaného rozhodování, pokud je zpracování:

Zpracování rizikových údajů či subjektů údajů
Zpracování zvláštní kategorie osobních údajů je povoleno jen pokud se jedná o zpracování:

Zpracování OÚ o trestních věcech lze pouze:

zákonnost, korektnost a transparentnost
účelové omezení
minimalizace údajů
přesnost
omezení uložení
integrita a důvěrnost
odpovědnost

o odvoláním, o čemž musí být subjekt údajů informován.
skytnutí.
no přístupný.
či nedodrženy, není platný.

úsilí, nařízení neukládá správci povinnost získávat další údaje o subjektech
nností GDPR

ů
Identifikační a kontaktní údaje na správce (a DPO)
Účely zpracování a zákonné tituly
Každý příjemce nebo kategorie příjemců
Přesun dat do třetích zemí a poskytnuté záruky
Doba uchování
Existence práv subjektu údajů
Právo na odstoupení od smlouvy kdykoli je to relevantní
Právo na podání stížnosti dozorovému orgánu
Informace o existenci automatizovaného rozhodování včetně možných důsledků
zákonný nebo smluvní závazek, důsledek neposkytnutí osobních údajů
oprávněné zájmy správce nebo případné třetí strany
kategorie osobních údajů
zdroj (veřejně přístupný?)

předmět, doba trvání, povaha a účel zpracování a kategorie subjektů údajů a osobních údajů, povinnosti a práva správce

nanců
Pouze v situaci, kdy souhlas je dle pravidel nařízení - především souhlasu - zaměstnanec musí mít skutečnou volbu rozhodnutí
Zpracovávání osobních údajů pouze v potřebném rozsahu po nezbytně nutnou dobu
Zaměstnavatel má omezené možnosti zpracování údajů ze sociálních sítí - nemá legitimní důvod požadovat přístup k informacím sdílených na sociálních sítí
Nutnost zvážit proporcionalitu opatření - zájmy organizace nemohou převažovat nad zásadami ochrany soukromí
Důraz na zásadu přiměřenosti zpracovávaných kategorií osobních údajů

Nepovinné
Jméno a kontaktní údaj organizace

Jméno a kontaktní údaj DPO
Informace o předání údajů do třetí země či mezinárodní organizace
Obecný popis opatření
Účely zpracování
Popis kategorií subjektů údajů
Popis kategorií osobních údajů
Plánované lhůty pro likvidaci jednotlivých kategorií osobních údajů
Kategorie zpracování pro každého správce

Nepovinné
Jméno, příjmění a kontaktní údaje pověřence veřejně (např. na webových stránkách nebo úřední desce
Jméno, příjmění a kontaktní údaje pověřence Úřadu pro ochranu osobních údajů - prostřednictvím datové schránky, písemně, e-mailem (posta@uoou.cz)
Úloha pomocníka a konzultanta ochrany osobních údajů
zaštiťování komunikace s ÚOOÚ (popř. ostatními dozorovými úřady)
Kontaktní místo pro záležitosti spojené s GDPR
Poskytování informací správci a zpracovateli
Monitorování souladu s GDPR

Nepovinné
jehož souvislosti je vyžadován posudek DPIA, nezpadá do výjimek ch výjimek je dostupný na webových stránkách Úřadu.
Posudek DPO
Systematický popis zamýšlených operací zpracování, účely zpracování, popř. zájmy správce
Posouzení nezbytnosti a přiměřenosti operací zpracování
Posouzení rizik pro práva a svobody subjektu údajů
Plánovaná opatření pro prevenci či zmírnění rizik
í, jelikož je spojena s rizikem pro práva a svobody SÚ

nální ochrany
Informování subjektu údajů o možných rizicích
Výslovný souhlas subjektu údajů
Nezbytnost pro smluvní plnění
Nezbytnost z důležitých důvodů veřejného zájmu, právních nároků, k ochraně životně důležitých důvodů

Nezbytnost k uzavření nebo smlouvy
Povoleno právem
Založené na výslovném souhlasu subjektu údajů

S výslovným souhlasem subjektu pokud zpracování není v přímém rozporu s právem
Nezbytné pro účely plnění povinností a výkon zvláštních práv, pokud to není v rozporu s právem EU či členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu.
Nutné pro ochranu životně důležitých zájmů daného subjektu nebo jiné FO

Zpracování provádí nadace, sdružení nebo jiný neziskový subjekt, který sleduje dané kategorie údajů, zpracování vztahuje pouze na členy takového subjektu (jak současné, tak bývalé) nebo na osoby, které s nimi udržují pravidelné styky, osobní údaje mohou být zpřístupňovány mimo tento subjekt pouze se souhlasem subjektu údajů.
Osobní údaje zjevně zveřejněné subjektem údajů.
Nezbytné pro určení, výkon či obhajobu právních nároků, či pokud soudy jednají v rámci svých pravomocí.
Zpracování je nezbytné pro významný veřejný zájem ovšem musí být přiměřené ke sledovanému cíli.
Účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky či poskytování zdravotní či sociální péče, řízení systémů a služeb zdravotní či sociální péče, povinnost mlčenlivosti.
Veřejné zdraví
Nezbytné pro archivaci ve veřejném zájmu, vědeckého či historického výzkumu nebo statistické účely
pod dozorem orgánu veřejné moci
pokud je oprávněné dle práva EU nebo členského státu EU

Důvěrnost
Zabezpečení vstupu
Zabezpečení přístupu
Zabezpečení přístupových oprávnění
Oddělené zpracování
Pseudonymizace
Anonymizace
Šifrování

Integrita
Zabezpečení zpřístupňování údajů
Možnost zpětného ověření

Dosputnost a odolnost systémů
Ochrana před zničením či ztrátou
Obnovení dostupnosti údajů

Technická opatření
Fyzická bezpečnost
Využití nástrojů pro ochranu integrity
Aplikační bezpečnost
Využití nástrojů pro ověřování identity
Využití nástrojů na ochranu před škodlivým kódem

Bezpečnost systémů od externích dodavatelů
Blokace účtu při neúspěšných pokusech o přihlášení
Logování úspěšných přihlášení
Logování neúspěšných pokusů o přihlášení
Logování činností s OÚ
Zálohování systému
Šifrování záloh
Šifrování hesel uživatelů (ideálně SHA-2 o délce min 8 znaků)
Instrukce pro případ napadení systému
Řešení problémů v přiměřené reakční době

Bezpečnost listinných dokumentů
Ochrana osobních údajů se týká:
Fyzické zabezpečení

Zabezpečení před přístupem neoprávněných osob do vyhraněných prostor - vstupní karty, klíče, bezpečnostní služby, vrátnice, alarm
Zabezpečení systému před použitím neoprávněnými osobami - hesla, automatické zamykání, dvoufaktorové ověřování, šifrování médií
Autorizační komponenty, přístupové práva dle pracovního zasazení
Pokud je to v silách organizace, mělo by zpracování jednotlivých účelů probíhat odděleně
Využití s ohledem na technické možnosti a specifikace zpracování (např. citlivost údajů)

Omezení přístupu k datům v průbehů přenosu nebo přepravy
Přiřazení osob k jednotlivým operacím s daty a údaji (založení, mazání, úpravy)

Zálohování, využití vhodných nástrojů (antivirová ochrana, firewall) či zařízení (nepřerušitelné zdroje napájení)
Schopnost obnovit dostupnost údajů v co nejkratším času

Organizační opatření
Řízení a dokumentace přístupů k údajům
Školení zaměstnanců
Mlčenlivost
Bezpečnost lidských zdrojů
Řízení rizik

Bezpečnost systémů na interním serveru
Umístění serveru v odděleném uzamykatelném prostoru s omezeným
Šifrování dat uložených na serveru
Pravidelná aktualizace operačního systému
Antivirový software, firewall
Administrátorské účty jsou oddělené
Přístup k datům přes SFTP či jiný šifrovaný kanál
Administrátory jsou zodpovědné osoby (správce IT, majitel, …)

pouze evidence FO
uzamykatelný prostor s omezeným přístupem

Řešená oblast	Osobní údaj	Kategorie osobního údaje
Zaměstnanci	pro každý zpracovávaný osobní údaj zvlášť	běžné, významné, kritické

Účel zpracování	Kdo OÚ zpracovává	Příjemce ve třetích zemích nebo mezinárodní organizace
souhlas, plnění právních povinností, …	zpracovatel, správce,	ano/ne

Doba uchování	Riziko zpracování údajů
nejčastěji dle zákona, popř. po dobu platnosti účelu zpracování	běžné, významné, kritické

Bezpečnostní opatření	Způsob zpracování
technická a organizační opatření	shromáždění, uložení, nahlížení, oprava

Úložiště	Osobní údaje	Přístupová práva
Databáze, listinné faktury	jméno, příjmení, kamerový záznam	osoby, které mají k údajům přístup

Riziko úniku	Pravděpodobnost úniku
minimální, malé, střední, velké	fyzické narušení, hackerský útok, únik hesla

Prevence rizika	Postup při zjištění porušení zabezpečení
politika hesel, fyzické zabezpečení	1. Informovat jednatele, 2. Do 72 hodin informovat dozorový úřad, 3. Je-li to potřeba informovat i subjekt údajů (zákazníka / zaměstnance)