Advokátní kancelář Růžha ve spolupráci se společností ORSYS s.r.o. si v souvislosti s blížícím se datem nabytí účinnosti obecného nařízení Evropského parlamentu a Rady EU o ochraně osobních údajů (2016/679; „**GDPR**“) dovoluje v rámci informačního servisu stručně nastínit některé požadavky nařízení, jejichž implementaci do příslušných vnitřních předpisů, procesů a webové prezentace bude ve vztahu ke zpracovávání osobních údajů třeba zajistit.

GDPR v návaznosti na stávající právní úpravu vychází zejména ze zásady minimalizace rozsahu zpracování osobních údajů (tedy zpracovávat je třeba pouze osobní údaje nezbytné pro dosažení sledovaného účelu a toliko po nezbytně dlouhou dobu), zásady transparentnosti a zásady přístupu založeného na riziku (účinnější a propracovanější opatření je třeba požadovat po subjektu zpracovávajícím velké množství osobních údajů, příp. zvláštní kategorie osobních údajů - např. údaje o zdravotním stavu).

1) Transparentní informace

S ohledem na principy zakotvené v příslušné právní úpravě je předně třeba zmínit, že důraz bude kladen především na účinnou ochranu práv subjektu údajů. GDPR **posiluje informační povinnost správce osobních údajů** (kterým je každý subjekt zpracovávající data subjektů údajů - typicky zaměstnanců, smluvních partnerů - podnikajících fyzických osob, nebo zákazníků, kteří předávají správci své osobní údaje, tedy typicky zákazníků nakupujících prostřednictvím internetového obchodu) vůči subjektům údajů, přičemž subjektem údajů se rozumí identifikovaná **fyzická osoba** (nikoliv tedy např. s.r.o.).

Subjektu údajů je třeba v rámci srozumitelné a přehledné informace sdělit zejména následující skutečnosti:

(i) totožnost správce údajů (tedy údaje o Vás/Vaší společnosti),
(ii) kontaktní údaje správce,
(iii) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování (typicky se bude jednat o plnění smluvní povinnosti - zpracování za účelem dodání objednaného zboží; ve vztahu k zaměstnancům pak plnění zákonné povinnosti v souvislosti s povinnými odvody a hlášeními příslušným orgánům),
(iv) případné příjemce nebo kategorie příjemců osobních údajů (např. přepravní společnost, externí mzdová účetní apod.),
(v) dobu, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (v této souvislosti lze odkázat na archivační a skartační řád) a
(vi) informaci o právech subjektu údajů (právo na přístup k osobním údajům, právo na přenositelnost osobních údajů, právo podat stížnost u dozorujícího úřadu apod.).

Informační povinnost lze splnit např. **vyvěšením informace v provozovně** (zejm. ve vztahu k zaměstnancům), případně (např. vůči smluvním partnerům a/nebo zákazníkům internetového obchodu) **zveřejněním na Vašem webu** (např. internetového obchodu).

2) Vyžadování souhlasu se zpracováním osobních údajů pouze v odůvodněných případech

Přístup, který v současné době ze strany správců osobních údajů převládá, tedy vyžadování souhlasu se zpracováním osobních údajů za všech okolností, nelze považovat za souladný ani se stávající právní úpravou ochrany osobních údajů. GDPR na současnou úpravu navazuje - platí tedy, že souhlas není třeba, resp. je **nežádoucí**, v případě, že osobní údaje subjektu jsou zpracovávány pouze k plnění zákonné nebo smluvní povinnosti - v případě internetového obchodu typicky pro dodání objednaného zboží, uchovávání osobních údajů po dobu záruční lhůty pro účely reklamace, přímý marketing – zasílání obchodních sdělení po provedení předchozího nákupu apod. Existuje-li proto jiný titul pro zpracování osobních údajů (plnění smluvní/zákonné povinnosti, oprávněný zájem apod.), **nemělo by být udělení souhlasu vyžadováno**.

Získání samostatného souhlasu se zpracováním osobních údajů naproti tomu bude nezbytné v případě, že osobní údaje subjektu údajů mají být zpracovávány k jiným účelům - např. je-li ve vztahu k zákazníkovi prováděno tzv. profilování (vyhodnocování aktivity zákazníka na příslušné internetové stránce a přizpůsobování nabídek získaným informacím ohledně zákaznických preferencí).

Souhlas musí být **aktivní** (uvedenou podmínku nesplňuje např. předem zaškrtnutá kolonka souhlasu se zpracováním osobních údajů), **prokazatelný**, **svobodný**, **konkrétní** a **informovaný** (subjekt údajů tedy musí být přehledným způsobem informován o účelu a době zpracování a dalších skutečnostech specifikovaných v bodu 1) - postačuje samozřejmě možnost „prokliku“ na příslušnou informační stránku). GDPR pamatuje i na souhlas udělený ze strany subjektu údajů před účinností GDPR - takový souhlas bude nadále účinný za předpokladu, že splňuje shora uvedené podmínky; v opačném případě bude třeba získat nový souhlas subjektu údajů.

3) Prokazování splnění povinností, záznamy o činnostech zpracování

V případě kontroly Úřadu pro ochranu osobních údajů (**ÚOOÚ**) bude třeba plnění povinností při zpracování osobních údajů ze strany správce prokázat, a to zejména předložením příslušných interních dokumentů stanovujících vnitřní bezpečnostní aj. pravidla pro zpracování osobních údajů.

Pro stanovení okruhu dokumentů, které je v zájmu plnění povinností dle GDPR třeba mít k dispozici, a jejich obsahu je nejprve nezbytné určit, **jaké osobní údaje** (např. jméno, příjmení, rodné číslo/datum narození, adresa pobytu) a **pro jaké účely** jsou ze strany správce zpracovávány; v případě zaměstnanců se jedná obvykle o zpracování pro účely plnění smluvní povinnosti - výplaty mzdy - a zákonných povinností v souvislosti s příslušnými odvody a hlášeními, v případě smluvních partnerů - fyzických osob (případně spotřebitelů) jsou osobní údaje obvykle zpracovávány v souvislosti s plněním smluvních povinností. Rozsah zpracovávaných osobních údajů a účel, za kterým jsou osobní údaje zpracovávány, je však třeba zkoumat v každém konkrétním případě. Zároveň je třeba zamyslet se nad skutečností, zda je pro dosažení zamýšleného účelu skutečně nezbytné zpracovávat osobní údaje v daném rozsahu, nebo zda by postačovalo méně osobních údajů (např. datum narození namísto rodného čísla apod.) - tedy v zásadě provést alespoň základní audit stávajícího zpracování osobních údajů.

(i) Základní shora uvedený dokument představují tzv. **záznamy o činnostech zpracování**, které blíže specifikují způsob, důvod a dobu zpracování osobních údajů, jejich zabezpečení a instrukce pro hlášení případných bezpečnostních incidentů. Jedná se tedy o formu komplexnější vnitřní směrnice, která obsahuje závazné postupy pro procesy související se zpracováním osobních

údajů. Záznamy o činnostech zpracování je obecně třeba mít připraveny bez ohledu na skutečnost, zda je třeba získat souhlas subjektu se zpracováním osobních údajů, nebo nikoliv.

(ii) K prokázání plnění povinností s ohledem na stanovení nezbytné doby, po kterou jsou osobní údaje zpracovány, lze doporučit přijetí **archivačního a skartačního řádu** pro stanovení nejzazších lhůt k archivaci osobních údajů a následného postupu likvidace příslušných dokumentů.

S ohledem na přístup založený na riziku lze rovněž provést analýzu rizik ve vztahu k činnostem, při nichž dochází ke zpracování osobních údajů, pro nastavení odpovídajících opatření.

4) Hlášení případů porušení zabezpečení osobních údajů

Jakékoliv *(významnější)* porušení zabezpečení osobních údajů je správce osobních údajů povinen bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, hlásit ÚOOÚ. Samozřejmě není třeba hlásit každý drobný bezpečnostní incident, ale pouze takový, u něhož není nepravděpodobné, že by příslušné porušení mělo za následek riziko pro práva a svobody fyzických osob. Povinnost se tedy vztahuje zejména na hlášení porušení zabezpečení, v jehož důsledku došlo ke ztrátě zpracovávaných osobních údajů; součástí hlášení je rovněž popis pravděpodobných důsledků porušení zabezpečení osobních údajů.

Ve zvlášť závažných případech (je-li pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob) je porušení zabezpečení nezbytné oznámit rovněž subjektu údajů, jehož osobní údaje byly ohroženy.

Závěrečné shrnutí

Shora uvedená informace má za cíl představit Vám některé základní povinnosti a procesy související s nabytím účinnosti GDPR, které bude třeba implementovat. Lze shrnout, že GDPR v řadě ohledů pouze zpřesňuje stávající právní úpravu, zároveň však v některých případech zavádí zcela nové instituty, na které bude třeba reagovat. GDPR je proto třeba vnímat zejména jako motivaci k přehlednému nastavení vnitřních procesů v souvislosti se zpracováním osobních údajů, archivací a skartací dat.

V případě zájmu Vám rádi budeme nápomocni při zpracování základních dokumentů k prokázání plnění povinností uložených GDPR, které jsou popsány výše, tak, abyste byli na novou právní úpravu v souvislosti se svou obchodní činností připraveni.