Implementace GDPR v Rakousku – Zákon mezi prvními

Od 25. května 2018 je účinné nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („GDPR“ - General Data Protection Regulation, "DSGVO - Datenschutz-Grundverordnung" v Rakousku). Jak jsou na tom s přípravou a implementací v oblasti nastavení nových pravidel a splnění požadavků upravující ochranu osobních údajů právě v sousedním Rakousku?

V červenci 2017 byl přijat rakouský zákon o ochraně osobních údajů („DSG – Datenschutzgesetz“, původní z roku 2000) a to v návaznosti na nové nařízení GDPR, které sjednocuje pravidla týkající se zpracování osobních údajů, práv subjektů a povinností odpovědných osob v celé EU. Dle § 18 DSG nového zákona je dozorčím orgánem v Rakousku se všemi pravomocemi včetně stanovení sankcí Úřad pro ochranu osobních údajů („Datenschutzbehörde Republik Österreich, dále jen „DSB““)[1].

Po srovnání nového zákona s nařízením GDPR jsou zvláště důležité následující změny resp. upřesnění, které nová legislativní úprava s účinností od 25. května 2018 přináší:

- ochrana údajů se dotýká nejen fyzických osob, ale zahrnuje i právnické osoby (zanecháno ze zákona DSG z roku 2000), přestože nařízení GDPR se týká výhradně ochrany fyzických osob,
- zpracování údajů týkající se trestné činnosti (podezření ze spáchání trestného činu, odsouzení za trestné činy nebo preventivní opatření) mohou být zpracovány na nezbytné účely oprávněných zájmů příslušného správce nebo třetí stranou (§ 4, odst. 3 DSG),
- vyslovení souhlasu u dětí se zpracováním osobních údajů byl snížen z 16 let stanovených v nařízení GDPR na 14 let (§ 4, odst. 4 DSG),
- stanovení zvláštních podmínek při ukládání sankcí právnickým osobám (§ 30 DSG) ,
- „odpuštění“ sankcí při porušení pravidel v souvislosti s ochranou osobních údajů a jejich nakládáním a zpracováním veřejným subjektům a orgánům veřejné moci (§ 30, odst. 5 DSG) tj. „Gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden“),
- zachování registru zpracování osobních údajů jen pro archivní účely do konce roku 2019 v rámci přechodného ustanovení (§69, odst. 2 DSG).

[1] Zdroj: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf

Stejným úřadem byla v červenci 2017 zveřejněna příručka[2] s cílem předat informace k novému nařízení GDPR, seznámení s terminologií a změnami, které nařízení přinese. Příručka obsahuje nejen stručné shrnutí nového nařízení, ale zároveň se blíže věnuje výkladu některých vybraných článků nařízení GDPR. Na závěr zodpovídá na otázky např. kdo musí mít pověřence a jeho povinnosti, za jakých podmínek mohou být uloženy sankce dozorčím orgánem, bezpečnost vs. cloudové služby, apod.

Prvotní informace ještě před schválením nařízení GDPR informoval úřad DSB o blížících se změnách prostřednictvím pravidelných čtvrtletních zpráv v Newsletter, blíže https://www.dsb.gv.at/newsletter.

Praktické návody v souvislosti se zaváděním GDPR v praxi jsou nejvíce uváděny Hospodářskou komorou Rakouska (Wirtschaftskammer Österreich, dále jen „WKO"), kde bylo mj. doporučeno, aby byly učiněny následující základní a nejdůležitější kroky tzv. Compliance-Schritte ještě před datem 25. května 2018[3]:

1) Příprava – stanovení osob zodpovědných za zavádění GDPR (interní/externí), časový harmonogram činností včetně vyčíslení finančních prostředků
2) Průzkum status quo (analýza aktuálního stavu) a potřebné úpravy (cílový stav) – v této fázi je nutné si zodpovědět zejména otázky např.

- Jaké osobní údaje jsou zpracovávány?
- Jaké datové aplikace existují – které jsou nyní aktuální a využívány?
- Proč jsou osobní údaje zpracovávány – stanovení cíle?
- Právní základ se zpracováním osobních údajů – vyslovení souhlasu
- Jaké jsou zpracovávány citlivé údaje?
- Poskytuje informační společnost službu přímo dětem?
- Splňuje poskytovaná informace náležitosti podle GDPR?
- Existují již přijatá opatření při nakládání s osobními údaji v dané společnosti/úřadu?
- Potřebuji pověřence pro ochranu osobních údajů?
- Předávání osobních údajů do třetích zemí – jak probíhá a na jakém právním základu?
- Ochrana osobních údajů zaměstnanců – pracovní smlouvy, služební předpisy?
- Jak mohu prokázat, že pravidla a zásady při zpracování osobních údajů jsou v souladu s nařízením GDPR? – povinnosti zpracovatele (tj. fyzická nebo právnická osoba, orgán veřejné moci, který zpracovává osobní údaje pro správce) – např. dokumentace k souhlasu se zpracováním osobních údajů, dokumentace o přijatých bezpečnostních opatřeních, dokumentace o posouzení rizik, dokumentace k mlčenlivosti zaměstnanců zpracovatele osobních údajů, apod.)
- Vymáhání práva a sankcí – nápravná opatření a sankce

[2] Zdroj: https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2
[3] Zdroj: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html

3) Plán opatření (dle analýzy skutečného stavu, bod 2) – stanovení priorit jednotlivých cílů včetně časového harmonogramu a rozpočtového výhledu, určení opatření a následná realizace

Současně WKO informuje o možnosti online zakoupení brožury k GDPR.[4] Tato brožura poskytuje kompaktní přehled základních požadavků v souvislosti s nařízením GDPR a rakouského zákona o ochraně osobních údajů, obsahuje kontrolní seznamy a vzorové dokumenty. Tyto vzorové dokumenty jsou rovněž ke stažení v elektronické podobě na stránkách WKO https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Musterdokumente-zur-EU-Datenschutzgrundverordnung.html.

Dále byl zveřejněn základní návod/vzor podle článku 30 GDPR „záznamy o činnostech zpracování", kde správce odpovídá, aby záznamy obsahovaly všechny stanovené údaje uvedené v odst. 1.[5] Vzorový dokument uvádí základní obsah záznamu při zpracování osobních údajů, tj. kategorie A. Kontaktní údaje o správci či pověřenci pro ochranu osobních údajů (jméno, email, tel. číslo, zástupce správce), B. Popis účelu zpracování osobních údajů (cíl, popis zpracování dat), C. Bližší specifikace k účelnosti zpracování osobních údajů (popis kategorie subjektů údajů; právní základ – prohlášení o souhlasu nebo jiné dokumenty; zpracování dat příjemců a jejich odeslání včetně výmazu a doby uchovávání; kategorie příjemců, kterým byly nebo budou údaje zpřístupněny), D. Popis technických, organizačních a bezpečnostních opatření (šifrování, pseudonymizace, důvěrnost, integrita, apod.).

Podobný vzor je uveden i pro zpracovatele, který dle článku 30 GDPR odst. 2 vede záznamy o všech kategoriích činností zpracování prováděných pro správce.[6] Dokument obsahuje doporučený rozsah kategorií činností zpracovávání prováděných pro správce, tj. kategorie A. Kontaktní údaje o zpracovateli či pověřenci pro ochranu osobních údajů (jméno, email, tel. číslo, zástupce zpracovatele), B. Kontaktní údaje o správci včetně uvedení zástupce správce, kategorie zpracování prováděného pro každého ze správců; informace k přenosu osobních údajů do třetích zemí, C. Popis technických, organizačních a bezpečnostních opatření.

A na závěr jedna zajímavost. Počátkem února 2018 se Rakousko ujalo předsednictví pracovní skupiny WP29 Rakousko a tím převzalo tuto významnou funkci po Francii, která ji zastávala 4 roky.

[4] Zdroj: https://webshop.wko.at/datenschutzanpassungsgesetz-2018.html
[5] Zdroj: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html
[6] Zdroj: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-auftragsverarbeite.html