

Posouzení vlivu na ochranu osobních údajů-DPIA.

Správce osobních údajů

EVERY REGARD s.r.o.

Ostrava-Slezská Ostrava, Záměstní 1155/27, PSČ 710 00

IČO: 5460034

DIČ: společnost není plátcem DPH ani nepřijímá platby v hotovosti

Telefon: +420 607 888 494

Email: easyrating@everyregard.one

Zastoupená: Miroslav Kalinský, jednající na základě plné moci

Preambule.

Pokud jsou při zpracování rozsáhlým způsobem ohrožena práva a svobody fyzických osob, musí správce vypracovat posudek vlivu na ochranu osobních údajů, (angličtině Data Protection Impact Assessment – DPIA), případně by měl zpracovat posouzení, proč DPIA není nutno zpracovávat. Společnosti jej budou muset vypracovat, pokud provádějí systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování. Posouzení vlivu na ochranu osobních údajů budou muset vypracovat společnosti poskytující věrnostní programy, online nebo telekomunikační služby založené na lokalizačních datech nebo cílenou behaviorální reklamu. Obdobnou povinnost pak budou mít všechny společnosti nebo instituce, které v rozsáhlém objemu zpracovávají citlivé osobní údaje anebo systematicky monitorují veřejně přístupné prostory. Zpracování osobních údajů podléhající posouzení vlivu na ochranu osobních údajů upravuje čl. 35 odst. 1 nařízení GDPR. Z tohoto článku vyplývá, že DPIA je správce údajů povinen provést v případě, kdy je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

V rámci uplatnění přístupu založeného na riziku je správce povinen již od počátku koncipování zpracování osobních údajů brát v potaz povahu, rozsah, kontext a účel jejich zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu přizpůsobit zabezpečení osobních údajů.

Pro určení míry rizikovosti je základním vodítkem výše uvedený čl. 35 odst. 3 GDPR, který demonstrativní výčtem uvádí některé vysoce rizikové operace s osobními údaji, jež zakládají povinnost provést DPIA. Zdůrazňuje zejména taková zpracování osobních údajů, při nichž dochází k:

- a) systematickému a rozsáhlému vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se
- b) zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
- c) rozsáhlému zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo rozsáhlému systematické monitorování veřejně přístupných prostorů.

Konkrétnější kritéria pro vyhodnocení, zda operace společnosti určité s osobními údaji podléhají procesu DPIA, tedy zda představují vysoké riziko pro práva a svobody fyzických osob, které vyžaduje čl. 35 nařízení GDPR ve svém prvním odstavci, stanoví Výkladové pokyny pracovní skupiny WP29 (WP 248). Tyto pokyny čl. 35 odst. 3 nařízení GDPR doplňují a jsou jimi:

- a) **vyhodnocování osobních aspektů subjektů údajů týkajících se zejména jejich pracovního výkonu,**
- b) ekonomické situace, zdravotního stavu, osobních zájmů, chování, lokace a pohybu (např.
- c) prověřování platebních schopností klientů banky nebo vytváření marketingového profilu internetových uživatelů)
- d) zpracování údajů založené na automatizovaném rozhodování, které má právní nebo podobné významné účinky pro subjekty údajů, například když takové zpracování vede k diskriminaci některých jednotlivců;
- e) systematické monitorování, tj. zpracování údajů za účelem sledování a kontroly
- f) subjektů údajů včetně systematického monitorování veřejně přístupných prostorů;
- g) zpracování citlivých údajů (např. zpracování záznamů o zdravotním stavu pacientů nemocnicí, zpracování lokalizačních údajů nebo zpracování finančních údajů, které mohou být zneužity);
- h) zpracování údajů velkého rozsahu vzhledem k počtu dotčených subjektů údajů, rozsahu
- i) zpracovávaných údajů, době zpracování a územnímu rozsahu (např. zpracování údajů klientů bankami či pojišťovny nebo zpracování údajů uživatelů internetu pro účely cílené reklamy);
- j) zpracování propojených nebo kombinovaných souborů osobních údajů, které pocházejí z více různých zpracování, pro účely nad rámec původního účelu;
- k) zpracování osobních údajů o „zranitelných“ osobách (např. údajů o dětech, zaměstnancích, uchazečích o azyl, důchodcích, pacientech atd.);
- l) zpracování údajů při použití nových technologických řešení a organizačních opatření (např. zavedení technologie umožňující zaměstnancům vstup na pracoviště na základě otisku prstu);
- m) předání osobních údajů mimo Evropskou unii;
- n) zpracování osobních údajů, které samo o sobě zabraňuje uplatnění práv nebo užívání služby ze strany subjektu údajů (např. zpracování údajů prováděné ve veřejném prostoru, kterému se nemohou subjekty údajů vyhnout, nebo prověřování platební schopnosti potenciálních zákazníků banky za účelem rozhodnutí, zda jim bude poskytnut úvěr či nikoliv).

Dle pokynů pracovní skupiny W29 se bude obvykle vyžadovat DPIA u takových zpracování osobních údajů, která splňují alespoň dvě výše uvedená kritéria.

K tomu:

- **Vzhledem k faktu, že Správce splňuje pouze jednu z podmínek uvedených výše a zároveň mu takové zpracování ukládá zákon, není nutné Posouzení vlivu zpracovávat.**
- **Podle článku 35 odst. 10 GDPR, pokud má zpracování osobních údajů podle článku 6 odst. 1 písm. c) GDPR, tj. splnění právní povinnosti, nebo písmene f) GDPR, tj. oprávněné zájmy, právní základ v právním řádu EU nebo ČR, je správce od posouzení vlivu na ochranu osobních údajů osvobozen.**

Viz:

- Stanovisko UOOU: <https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu-pravnich-predpisu-dpia/ds-5344>
 - (14) Podle článku 35 odst. 10 GDPR, pokud má zpracování osobních údajů podle článku 6 odst. 1 písm. c) GDPR, tj. splnění právní povinnosti, nebo písmene e) GDPR, tj. oprávněné zájmy, právní základ v právním řádu EU nebo ČR, je správce od posouzení vlivu na ochranu osobních údajů osvobozen. Podmínkou však je, aby posouzení vlivu na ochranu osobních údajů učinil stát. Toto posouzení vlivu na ochranu osobních údajů je přirozeně odlišné od posouzení vlivu na ochranu osobních údajů správcem, neboť to první je abstraktní, to druhé je konkrétní.
 - (15) Návrh § 10 zákona o zpracování osobních údajů stanoví: „Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.“

Analýzu zpracoval:

EVERY REGARD s.r.o., Slezská Ostrava, Záměstní 1155/27, 710 00, IČO: 05460034

Zpracovatel:

Kalinský Miroslav, jednající na základě plné moci


EVERY REGARD s.r.o.
Záměstní 1155/27
Ostrava-Slezská Ostrava, 710 00
IČO: 05460034, společnost není plátcem DPH

V Ostravě dne: 1.2.2022