



ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

INTERNÍ PRAVIDLA A POSTUPY SPOLEČNOSTI PG group a.s. NA OCHRANU OSOBNÍCH ÚDAJŮ

Níže uvedené informace jsou poskytnuty v souladu s nařízením 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 95/46ES.

SPECIFIKACE SPRÁVCE/ZPRACOVATELE OSOBNÍCH ÚDAJŮ

TOTOŽNOST SPRÁVCE

PG group, a.s. se sídlem U Slávie 1540/2a, Praha 10, PSČ: 100 00, IČ: 645 81 241, zapsaná v obchodním rejstříku B 9074 vedená u Městského soudu v Praze (dále je „PGG“)

KONTAKTNÍ ÚDAJE SPRÁVCE

PG group, a.s., U Plynárny 1450/2a, Praha 4, PSČ: 140 00, email: gdpr@pgrgroup.cz, t: +420 731 431 815

KONTAKTNÍ ÚDAJE ODPOVĚDNÉHO PRACOVNÍKA

Jiří AUGUSTA, email: gdpr@pgrgroup.cz (dále je „odpovědný pracovník“)

PŘEDMĚT ČINNOSTI SPRÁVCE

Grafické práce, poradenství v marketingu, marketing

ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Marketingové a obchodní účely

1. BLÍŽE K DOKUMENTU

Cílem interních pravidel a postupů je jednoznačně, přehledně a funkčně stanovit pravidla a postupy ochrany osobních údajů, nakládání s osobními údaji, jejich uchování, udržování aktuálnosti a odstraňování tak, aby byla vyloučena nebo snížena na přijatelnou minimální úroveň možnost jejich zneužití, úniku nebo neoprávněného nakládání s nimi.

V dalším textu se používá termín správce osobních údajů a zpracovatel osobních údajů, vyjadřuje se tím organizace/zaměstnavatel, resp. ti její zaměstnanci či představitelé, kteří získání, uchování nebo zpracování osobních údajů provádějí, řídí, kontrolují či mají k těmto údajům přístup.

Tento souhrn interních pravidel byl zpracován na základě aktuálně platné legislativy a s přihlédnutím k převažujícímu (obvyklému) výkladu, po posouzení rizik spojených se získáváním uchováváním a zpracováním osobních údajů, a to s vynaložením přiměřené odborné péče tak, aby vyjadřoval zásady záměrné a standardní ochrany osobních údajů.

2. OSOBNÍ ÚDAJE

Osobní údaje jsou základní údaje o žijící fyzické osobě, a to bez ohledu na to, zda je tato osoba podnikající či nikoli. Osobním údajem se tedy typicky rozumí údaje identifikující fyzickou osobu v postavení zaměstnance, zájemce o zaměstnání, bývalého zaměstnance, obchodního partnera, bývalého obchodního partnera, zájemce o obchodní vztah, ale i osobní údaje třetích osob dodané klientem v rámci zakázky.

Za osobní údaje se nepovažují údaje o zemřelých osobách a anonymizované údaje. Osobními údaji též nejsou údaje o právnických osobách.

Osobním údajem je především jméno, příjmení, pohlaví, věk, datum narození, rodné číslo, osobní stav, občanství, fotografie, bydliště, ale i jakékoli další údaje identifikující dotyčnou osobu jako telefonní číslo, e-mailová adresa, adresa zaměstnání nebo jiné ověřovací identifikační údaje.

Dále je zavedena zvláštní kategorie osobních údajů (citlivých údajů), které je možné zpracovávat jen výjimečně, pouze z důvodů vyjmenovaných v nařízení, jako rasový nebo etnický původ, náboženské vyznání, politické



názory, sexuální orientace, údaje o zdravotním stavu, členství v odborech, údaje o trestních deliktech, genetické a biometrické údaje apod.

Osobní údaje mohou být zpracovávány jen ze zákonných důvodů a zákonem stanoveným způsobem. Není-li pro uchování nebo zpracování osobních údajů zákonný důvod, je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. U dětí do 16 let (pokud vnitrostátní úprava nestanoví věk nižší) je nutný souhlas rodiče (zákonného zástupce).

3. ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ

PGG získává osobní údaje o dvou základních okruzích fyzických osob, a to o zaměstnancích a o obchodních partnerech/zákaznících/klientech (dále jen klientech).

Údaje o zaměstnancích jsou získávány při vstupu zaměstnance do zaměstnání (získání osobních dat nezbytných pro splnění povinností ukládaných státem formou zákonů zejména při odvodu daní a zákonného pojištění). Tyto údaje jsou s ohledem na účel zpracování zpracovávány bez souhlasu subjektu údajů a jsou průběžně aktualizovány při každé objektivní změně osobního údaje, a to nahlášením ze strany zaměstnance. Při ukončení pracovní-právního vztahu jsou všechny osobní údaje zaměstnance vymazány s výjimkou těch, které je zaměstnavatel po dobu stanovenou zákonem povinen uchovávat (zejména pro účely daňové kontroly, kontroly správy sociálního zabezpečení, kontroly zdravotní pojišťovny apod.).

Osobní údaje uchazečů o zaměstnání, kteří se následně nestali zaměstnanci správce, lze zpracovávat pouze na základě souhlasu subjektu údajů, jinak musí být po skončení příslušného výběrového řízení likvidovány.

PGG provozuje systém tzv. trackování času zaměstnanců, při kterém se sleduje využití času zaměstnanců v pracovní době pro řešení jednotlivých úkolů. Pokud je smluvně sjednáno, PGG sleduje využití času i fyzických osob, kteří jsou ve vztahu k PGG jako dodavatelé.

Údaje o klientech jsou získávány při uzavírání smluvního vztahu a dále v průběhu smluvního vztahu. Tyto údaje zahrnují údaje o všech fyzických osobách, ať už v postavení zaměstnance, zaměstnavatele, pověřené osoby a podobně, ale i osobní údaje předané klientem o třetích osobách. Ke zpracování osobních údajů poskytnutých v souvislosti s obchodním vztahem není třeba zvláštní souhlas. Pokud však jsou osobní údaje uchovávány po skončení smluvního vztahu nad rámec zákonných povinností (např. po lhůtě pro případné provedení daňové kontroly nebo reklamace, po skončení doby trvání oprávněného zájmu spočívajícího v možném oslovení klienta s nabídkou podobného produktu, jaký si zakoupil), má PGG k dispozici souhlas dotyčné fyzické osoby, který je jasně formulován, s označením PGG, přehledem získaných údajů a účelu, pro který se údaje získali. Souhlas není získán předem zaškrtnutým políčkem v internetovém či

listinném formuláři. Stejně tak PGG přistupuje k získání souhlasu dotyčné osoby při uchování či zpracování jejích osobních údajů pro další oslovení např. zasláním newsletteru nebo jiného informačního sdělení.

Při získání osobních údajů PGG dotyčnou fyzickou osobu informuje o své totožnosti a kontaktních údajích, o účelu zpracování a právním základu pro zpracování, o kategorii dotčených osobních údajů a o případných dalších příjemcích osobních údajů. To neplatí, pokud byly osobní údaje získány přímo od dotyčné fyzické osoby a tato osoba již výše uvedené informace má.

Při předávání osobních údajů jiné právnické nebo fyzické osobě pro její potřeby (např. sdílení klientů mezi firmami) PGG zajistí nezbytný konkrétní souhlas fyzické osoby, jejíž osobní údaje jsou předávány, s uvedením identifikace těch, kterým jsou osobní údaje předávány, a účelu, pro který se údaje předávají.

4. UCHOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

Osobní údaje jsou uchovávány v listinné podobě v uzamčené skříni. Přístup k listinným osobním údajům má pouze odpovědný pracovník a osoby písemně pověřené k nakládání s příslušnými osobními údaji. Listiny obsahující osobní údaje nejsou volně přístupné (položené na stole bez přítomnosti osoby, která má k osobním údajům povolený přístup a která odpovídá za to, že osobní údaje neuniknou k nepovolané osobě). V nepřítomnosti pověřených osob musí být skříň uzamčena.

Osobní údaje jsou dále uchovávány v elektronické formě na počítačích, přístup k nim je zabezpečen heslem, které zná jen odpovědný pracovník, které jsou písemně pověřeny k nakládání s příslušnými osobními údaji. Pokud tato osoba nemá bezprostřední kontrolu nad počítačem, je od počítače odhlášena. Počítače jsou umístěny v prostoru firmy, který je v nepřítomnosti pověřených osob uzamčen.

Některá osobní data mohou být umístěna na počítačích dodavatele IT služeb v jeho prostorách. S IT dodavatelem je uzavřeno písemné ujednání o ochraně osobních údajů, ochrana osobních údajů je zajištěna nejméně na stejné úrovni jako v PGG. Některá osobní data jsou též umístěna na přenosných počítačích. Pokud se tyto přenosné počítače nacházejí mimo prostory firmy, jsou pod trvalým dohledem pověřené osoby nebo jsou zabezpečeny stejným způsobem jako v prostorách firmy (zamčená skříň nebo zamčená místnost).

Data se zásadně nepřenášejí uvnitř subjektu ani vně subjektu prostřednictvím nezašifrovaného přenosu dat (otevřený e-mail, skype apod.). Při nutnosti přenosu dat se používá šifrovaný přenos nebo fyzické předání např. na flash paměti.

Pravidla a postupy pro uchovávání osobních údajů platí i pro externí zpracovatele osobních údajů (např. účetní firma, firma zajišťující externí cloudové úložiště apod.), znalost a přihlášení se k těmto pravidlům a postupům musí



být vyjádřeny písemnou formou. Zabezpečení takových osobních údajů uložených u zpracovatelů zajišťují dotčení zpracovatelé.

Pokud pomine právní důvod pro uchovávání osobních údajů (souhlas fyzické osoby nebo jiný právní důvod jako plnění smlouvy, trvání pracovně-právního vztahu, oprávněný zájem atd.), příslušná osobní data, která není povinna PGG uchovávat ze zákona, vymaže či zlikviduje.

Na žádost fyzické osoby je PGG jako správce údajů povinna její osobní údaje smazat či přestat uchovávat (pokud netrvá povinnosti je uchovávat ze zákonných důvodů). Fyzická osoba má právo na přístup ke svým osobním údajům. Na základě její žádosti je tedy PGG povinna sdělit, jaké osobní údaje o ní uchovává, či potvrdit, že o ní žádné osobní údaje neuchovává. Dále má fyzická osoba právo na opravu chybných osobních údajů o ní uchovávaných. PGG je povinna reagovat na podnět takové fyzické osoby co nejdříve, nejpozději však do 30 dnů. V případě, že její žádosti nevyhoví, je povinna to zdůvodnit. Vždy je však nejprve třeba ověřit totožnost dotčené fyzické osoby.

Jsou-li osobní údaje fyzické osoby uchovávány pro účely přímého marketingu, bude dotčená fyzická osoba upozorněna na právo kdykoli bezplatně požadovat ukončení uchovávání a zpracování osobních údajů o své osobě. Požadavek na ukončení uchovávání osobních údajů bude proveditelný stejně snadno jako udělení souhlasu, tedy například proklikem v zaslaném newsletteru, jímž se dotčená osoba odhlásí z odběru a její osobní údaje se vymažou z distribučního seznamu.

Údaje získané tzv. trackováním času zaměstnanců jsou uchovávány nejvýše po dobu 24 měsíců. Údaje získané tzv. trackováním času dodavatelů jsou uchovávány po nezbytně nutnou dobu potřebnou pro případné zákonné povinnosti (lhůta pro provedení případné daňové kontroly nebo reklamace, aj.). K záznamům o sledování času zaměstnanců má přístup pouze statutární ředitel a písemně pověřený zaměstnanec.

5. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Osobní údaje je možné zpracovávat jen se souhlasem fyzické osoby, o které se osobní údaje zpracovávají, nebo na základě zákonného důvodu pro zpracování osobních údajů.

V případě hromadného zpracování osobních údajů PGG vyhodnotí možná rizika a při vysoké rizikovosti zpracování osobních údajů zpracuje posouzení dopadů/vlivu zpracování osobních údajů.

PGG nemusí vést záznamy o činnostech zpracování, neboť je malým nebo středním podnikem, na které se tato povinnost obecně nevztahuje. Pokud by však zpracování osobních údajů probíhalo pravidelně nebo ohrožovalo práva a svobody osob, povede PGG záznamy o činnostech zpracování.

PGG nezpracovává a ani nebude zpracovávat zvláštní kategorii osobních údajů (citlivých údajů) jako je rasový nebo etnický původ, náboženství, údaje o zdravotním stavu zaměstnanců, sexuální orientace apod.

Záznamy obsahují název a kontaktní údaje PGG, důvod zpracování údajů, popis kategorií subjektů údajů a osobních údajů, kategorie organizací, které údaje obdrží, případný přenos údajů do jiné země či organizace, lhůtu pro odstranění údajů a popis bezpečnostních opatření uplatňovaných při zpracovávání.

Výše uvedená pravidla platí i při zpracování osobních údajů externím dodavatelem. V takovém případě je externí dodavatel (zpracovatel) vázán písemným smluvním vztahem, ve kterém je specifikován předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování, typ údajů a kategorie osob, jejichž osobní údaje jsou zpracovávány, a riziko pro práva těchto osob. Po dokončení zpracování osobních údajů externí dodavatel dotčené osobní údaje vrátí nebo smaže, pokud není pro další uchovávání osobních údajů právní důvod.

6. VZDĚLÁVÁNÍ, KONTROLA A PŘEZKOUMÁNÍ, ÚČINNOST

Všichni zaměstnanci PGG jsou prokazatelně proškoleni z pravidel a postupů do 7 dnů od zařazení pravidel a postupů při ochraně osobních údajů do závazných vnitřních předpisů. Zaměstnanci jsou také seznámeni s tím, že za porušení ochrany osobních údajů je možné uložit zaměstnavateli sankci až do výše 20 mil. eur (cca 500 mil. Kč).

Zaměstnanci PGG mají povinnost dodržovat pravidla a postupy ochrany osobních údajů. Zjistí-li porušení stanovených pravidel a postupů, jsou povinni to oznámit odpovědnému pracovníkovi, jenž přijme příslušná nápravná opatření, která odvrátí či minimalizují způsobenou škodu a zajistí, že se pochybení nebude opakovat.

Závažné porušení ochrany dat PGG jako správce osobních údajů nahlásí do 72 hodin Úřadu pro ochranu osobních údajů a fyzické osobě, jíž se porušení pravidel a postupů při nakládání s osobními údaji týká. Ohlášení bude obsahovat popis porušení zabezpečení osobních údajů, jméno odpovědné nebo pověřené osoby, popis důsledků porušení zabezpečení osobních údajů a popis přijatých nápravných opatření.

Odpovědný pracovník má za povinnost průběžně kontrolovat dodržování stanovených pravidel a postupů při ochraně osobních údajů.

Pravidla a postupy podléhají pravidelnému přezkumu, který probíhá nejpozději do 12 měsíců od minulého přezkumu nebo od zavedení pravidel a postupů.

Tato pravidla a postupy nabývají účinnosti dnem 25. 5. 2018, od tohoto data jsou závazná pro všechny zaměstnance PGG.