Legalion

GDPR SPRIEVODCA PRE FIRMY A PODNIKATEĽOV

Ochrana osobných údajov už dávno nie je len formalitou. Správne nastavené procesy sú kľúčom k dôvere klientov a obchodných partnerov. Navyše vás ochránia pred pokutami. Prevencia je totiž vždy lacnejšia ako uložená sankcia.

Náš GDPR sprievodca pre firmy a podnikateľov vám pomôže zorientovať sa v povinnostiach, predísť chybám a nastaviť efektívne riešenia v súlade s Nariadením GDPR. Praktický návod, ktorý spája odbornosť s podnikateľskou realitou.

Legalion

1. Úvod – bližšie priblíženie Nariadenia GDPR, jeho cieľov a významu ochrany osobných údajov

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679, známe pod skratkou GDPR (General Data Protection Regulation), je základným právnym predpisom EÚ v oblasti ochrany osobných údajov. Platí od 25. mája 2018 a nahradilo dovtedajšiu smernicu 95/46/ES.

Keďže ide o nariadenie, má priamu účinnosť vo všetkých členských štátoch Európskej únie, teda aj na Slovensku, bez potreby jeho transpozície do vnútroštátneho práva.

Medzi hlavné ciele Nariadenia GDPR patrí najmä:

- posilniť ochranu základných práv fyzických osôb v digitálnej dobe (najmä práva na ochranu osobných údajov a súkromia)
- stanoviť rovnaké pravidlá ochrany osobných údajov v celej EÚ
- zabezpečiť slobodný pohyb osobných údajov medzi členskými štátmi bez prekážok
- zvýšiť zodpovednosť firiem a štátnych orgánov, ktoré osobné údaje spracúvajú

Osobné údaje sú dnes jednou z najcennejších komodít – od údajov zákazníkov v e-shopoch, používateľov sociálnych sietí, cez údaje zamestnancov, až po údaje pacientov v zdravotníctve. GDPR preto reaguje na tieto výzvy modernej doby, kedy sa začalo masívne využívanie digitálnych technológií, sociálnych sietí, mobilných aplikácií či umelej inteligencie. Základom je princíp „accountability“ – zodpovednosti. Každá firma a každý podnikateľ musí nielen dodržiavať požiadavky Nariadenia GDPR, ale aj vedieť preukázať, že ich dodržiava.

Pre firmy a podnikateľov to znamená povinnosť zaviesť vnútorné procesy, pravidlá a dokumentáciu, ktoré zabezpečia, že spracúvanie osobných údajov je zákonné, transparentné a bezpečné.

Základné princípy ochrany osobných údajov (čl. 5 Nariadenia GDPR)

Nariadenie GDPR je postavené okolo niekoľkých základných princípov, ktoré definujú ochranu osobných údajov v Únii. Každá firma a podnikateľ musí spracúvať osobné údaje v súlade s týmito princípmi. Tieto princípy navyše fungujú aj ako výkladová pomôcka do praxe. Pokiaľ Nariadenie GDPR alebo prax firmy pripúšťa niekoľko výkladov alebo spôsobov spracúvania osobných údajov, je potrebné vybrať ten správny, a to pomocou základných princípov.

Legalion

Medzi základné princípy ochrany osobných údajov patrí:

- zákonnosť, spravodlivosť a transparentnosť – osobné údaje možno spracúvať len na základe právneho dôvodu uvedeného v Nariadení GDPR a dotknuté osoby musia byť o spracúvaní svojich osobných údajov jasne a jednoducho informované
- presnosť – údaje musia byť aktuálne a presné
- integrita a dôvernosť – údaje musia byť primerane chránené pred ich zmenou, poškodením, stratou alebo sprístupnením neoprávneným osobám
- obmedzenie účelu – osobné údaje sa môžu použiť iba na vopred určený účel,
- minimalizácia údajov – spracúvať sa majú len tie osobné údaje, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania
- obmedzenie uchovávania – osobné údaje je možné uchovávať len po dobu nevyhnutnú na daný účel spracúvania
- zodpovednosť (accountability) – prevádzkovateľ musí vedieť preukázať súlad so všetkými týmito zásadami

Význam Nariadenia GDPR pre prax

Pre firmy a podnikateľov, Nariadenie GDPR zavádza povinnosť vytvoriť interný systém riadenia ochrany údajov – teda nielen spracúvať osobné údaje zákonne, ale mať k tomu aj potrebnú dokumentáciu. Ako napríklad: zásady ochrany osobných údajov, záznamy o spracovateľských činnostiach, zmluvy so sprostredkovateľmi, interné smernice, poverenia a poučenia zamestnancov a iné. Týmto spôsobom firmy a podnikatelia preukazujú súlad spracúvaných osobných údajov s Nariadením GDPR. Ide o premietnutie princípu zodpovednosti za spracúvané osobné údaje.

Pre jednotlivcov, Nariadenie GDPR poskytuje v prvom rade ochranu ich osobných údajov pred ich neoprávneným použitím tretími osobami, ochranu súkromného a rodinného života. Súčasne im poskytuje široký súbor práv (prístup, oprava, vymazanie, prenosnosť údajov, možnosť namietať spracúvanie a pod.), čím posilňuje ich kontrolu nad vlastnými údajmi.

Pre dohľad, Nariadenie GDPR dáva dozorným orgánom (na Slovensku Úrad na ochranu osobných údajov SR) silné kompetencie – od právomoci viesť kontroly, až po ukladanie pokút (pokuty do výšky 20 miliónov eur alebo 4 % z celosvetového ročného obratu).

Legalion

Prečo považujeme tento úvod za dôležitý?

V praxi sa často stretávame s tým, že podnikatelia považujú ochranu osobných údajov za „ďalšiu administratívnu povinnosť.“

V skutočnosti je však cieľom nariadenia ochrana práv fyzických osôb (a teda každého jedného z nás) pred zneužívaním našich osobných údajov. Tento cieľ ochrany osobných údajov má preto nielen právny, ale aj celospoločenský význam. Správne nastavenie ochrany osobných údajov vo firme a v podnikaní nie je iba povinnosťou, ale aj konkurenčnou výhodou. Súlad s požiadavkami Nariadenia GDPR zvyšuje dôveryhodnosť firiem a podnikateľov a posilňuje vzťah so zákazníkmi, obchodnými partnermi či zamestnancami.

Navyše firmu a podnikanie chráni pred následkami v podobe kontrol a pokút zo strany Úradu na ochranu osobných údajov.

Teraz už vieme, čo je Nariadenie GDPR a aké ciele sleduje ochrana osobných údajov.

Poďme sa pozrieť na to, čo sú to vlastne osobné údaje.

2. Čo sú osobné údaje? Aké kategórie osobných údajov poznáme?

Podľa čl. 4 ods. 1 GDPR sú osobnými údajmi **akékoľvek informácie o identifikovanej alebo identifikovateľnej fyzickej osobe**. Tejto budeme ďalej hovoriť aj dotknutá osoba.

Identifikovaná osoba je napríklad pre zamestnávateľa zamestnanec, ktorý je označený menom a priezviskom, bydliskom a dátumom narodenia v pracovnej zmluve. Takáto dotknutá osoba je jednoznačne identifikovaná.

Identifikovateľná osoba je osoba, ktorú možno nepriamo identifikovať. Napríklad využitím kombinácie osobných údajov, ktoré o tejto osobe máme k dispozícii, ako dátum narodenia, adresa bydliska a IP adresa. Na základe týchto osobných údajov je možné v niektorých prípadoch presne identifikovať konkrétnu osobu.

Na prvý pohľad sa môže zdať, že akékoľvek informácie o osobe môžu viesť k jej presnej identifikácií. Stačí na to použiť dostatok prostriedkov (peňažných, ľudských, technologických a pod.).

Nariadenie GDPR (recitál 26) preto pracuje s testom **„prostriedkov, ktoré sú rozumne pravdepodobné“ na identifikáciu** (náklady, čas, technológia, dostupné zdroje, technologický vývoj).

Informácie o identifikovateľnej osobe sú preto osobnými údajmi iba v prípade, ak je takáto osoba **identifikovateľná pri použití prostriedkov, ktoré je rozumne možné použiť na jej identifikáciu.** Ak identifikácia konkrétnej osoby na základe nepriamych informácií vyžaduje neprimerane veľa úsilia, nákladov, času, technológií a dostupných zdrojov, nemožno predpokladať, že tieto informácie povedú k identifikácii tejto osoby.

Potom platí, že tieto údaje nie sú osobnými údajmi.

Z rozhodovacej praxe Súdneho dvora EÚ napríklad platí, že:

- Breyer (C-582/14) - dynamická IP adresa je osobný údaj, ak má prevádzkovateľ reálne prostriedky (priamo či cez tretiu stranu) osobu identifikovať,
- Nowak (C-434/16) - skúšobná písomka a poznámky hodnotiteľa sú osobné údaje študenta,
- Buivids (C-345/17) - videozáznam osoby je osobný údaj, ak je osoba identifikovateľná.

Osobné údaje sú teda akékoľvek informácie o fyzickej osobe, ktorá je jednoznačne identifikovaná alebo je možné ju na základe týchto informácií identifikovať.

Údaje sú osobnými údajmi iba vtedy, ak ide o informácie, ktoré sa týkajú konkrétnej osoby. O osobné údaje ide vtedy, ak je splnená aspoň jedna z týchto 3 podmienok:

- obsah - informácia priamo opisuje osobu (meno, zdravotná diagnóza, fotka),
- účel - informácia sa používa na hodnotenie alebo rozhodovanie o osobe (scoring, profil),
- výsledok (dopad) - informácia má vplyv na práva alebo postavenie osoby (napr. red flag „rizikový zákazník“).

Praktický príklad: Aj hodnotiace úsudky a komentáre (napr. poznámka personalistu „kandidát je málo flexibilný“) sú osobné údaje, lebo sa vzťahujú k identifikovanej osobe a majú na jej postavenie dopad

Dôležité je, že ochrane podľa Nariadenia GDPR podliehajú len údaje o fyzických osobách. Údaje o právnických osobách (napr. IČO, obchodné meno) sa za osobné údaje nepovažujú, pokiaľ nie je možné podľa nich určiť konkrétnu fyzickú osobu (napr. živnostník uvádzajúci svoje meno a adresu).

V minulosti na Slovensku nebolo úplne jasné, či sa za osobné údaje považujú aj osobné údaje fyzických osôb, ktoré podnikajú (živnostníci, slobodné povolania a pod.). Túto otázku jednoznačne vyriešil Úrad na ochranu osobných údajov vo svojom metodickom usmernení.

Nariadenie GDPR sa vzťahuje aj na fyzické osoby, ktoré podnikajú ako živnostníci, slobodné povolania alebo akokoľvek inak.

Kategórie osobných údajov

Nariadenie GDPR rozdeľuje osobné údaje na 2 kategórie: bežné osobné údaje a osobitnú kategóriu osobných údajov (tzv. citlivé údaje).

Bežné osobné údaje sú údaje, ktoré bežne používame všetci a poskytujeme ich firmám a podnikateľom.

Patria sem najmä:

- identifikačné údaje: meno, priezvisko, adresa, rodné číslo, číslo OP,
- kontaktné údaje: telefónne číslo, e-mail,
- online identifikátory: IP adresa, cookies, užívateľské mená.

Legalion

Osobitné kategórie osobných údajov sú vymedzené v čl. 9 Nariadenia GDPR. Ide o osobné údaje, ktoré sú príliš citlivé na to, aby sa s nimi zaobchádzalo tak, ako s bežnými osobnými údajmi. Preto pre ich spracúvanie platia prísnejšie pravidlá.

Ide o údaje, ktoré majú zvýšený potenciál zasiahnuť do súkromia, a preto ich spracúvanie je zakázané, okrem výnimiek uvedených v čl. 9 ods. 2 GDPR.

Patria sem:

- údaje o rasovom alebo etnickom pôvode,
- politické názory,
- náboženské alebo filozofické presvedčenie,
- členstvo v odborových organizáciách,
- genetické údaje,
- biometrické údaje na účely identifikácie,
- údaje o zdraví,
- údaje o sexuálnom živote alebo sexuálnej orientácii.

Spracúvanie týchto osobných údajov **si vyžaduje zvláštny právny základ** (napr. výslovný súhlas, plnenie zákonnej povinnosti, ochrana životne dôležitých záujmov, pracovnoprávne povinnosti, zdravotná starostlivosť), pričom vyžadujú vyššiu mieru ochrany pred ich neoprávneným sprístupnením tretím osobám.

Okrem týchto 2 kategórií osobných údajov pracuje Nariadenie GDPR ešte osobitne s **osobnými údajmi o trestných činoch a priestupkoch**. Osobitosti sú uvedené v čl. 10 Nariadenia GDPR.

Spracúvanie osobných údajov o trestných činoch a priestupkoch je možné len pod kontrolou orgánu verejnej moci alebo, ak to umožňuje právo členského štátu (napr. v oblasti zamestnávania, compliance alebo bezpečnostných previerok).

Praktické príklady:

- *meno a priezvisko zákazníka v e-shope = bežný osobný údaj*
- *zdravotná dokumentácia pacienta = osobitná kategória údajov*
- *záznam o treste v registri trestov = údaj o trestných činoch a priestupkoch*
- *IP adresa používateľa na webstránke = osobný údaj, pokiaľ je možné identifikovať konkrétneho užívateľa v spojení s inými osobnými údajmi tohto užívateľa*

Legalion

Za osobné údaje sa považujú aj **pseudonymizované údaje** a v niektorých prípadoch aj **anonymizované údaje**.

Pseudonymizované údaje (hash, náhodný identifikátor) sú stále osobné údaje, nakoľko v praxi takmer vždy existuje spojovací kľúč alebo rozumne pravdepodobné prostriedky spätného priradenia. S pseudonymizovanými údajmi je preto potrebné nakladať ako s osobnými údajmi v súlade s Nariadením GDPR.

Anonymizované údaje v zásade už nie sú osobné údaje, len ak je de-identifikácia prakticky nezvratná pri zohľadnení rozumných prostriedkov identifikácie dnes aj v dohľadnej budúcnosti. To znamená, že na základe anonymizovaných údajov nie je možné dnes a ani v blízkej budúcnosti identifikovať konkrétnu osobu. V opačnom prípade sú aj anonymizované údaje osobnými údajmi.

3. Spracúvanie osobných údajov a právne základy

V tejto časti sa najprv pozrieme na to, čo všetko sa považuje za spracúvanie osobných údajov a následne na právne základy, ktoré nás oprávňujú osobné údaje spracúvať.

3.1. Definícia spracúvania osobných údajov

Podľa čl. 4 ods. 2 GDPR je spracúvaním **akákoľvek operácia alebo súbor operácií vykonávaných s osobnými údajmi, a to automatizovane alebo manuálne.**

Spracúvaním osobných údajov je teda akýkoľvek úkon, ktorý firma alebo podnikateľ robí s osobnými údajmi.

Medzi spracúvanie preto patrí:

- zhromažďovanie a získavanie (napr. vyplnenie formulára na webe),
- zaznamenávanie a štruktúrovanie (napr. vytvorenie databázy klientov),
- uchovávanie, usporadúvanie,
- zmena, kombinovanie,
- vyhľadávanie, nahliadanie, používanie,
- poskytovanie tretej strane (napr. odovzdanie účtovných dokladov účtovníkovi),
- zverejňovanie (napr. fotky zamestnancov na webovej stránke),
- vymazanie alebo zničenie.

Aj obyčajné uchovávanie osobných údajov (napr. archív papierových zmlúv v šanóne) je spracúvanie.

3.2. Právne základy spracúvania osobných údajov

Každé spracúvanie osobných údajov musí mať právny základ. Právny základe môžeme vnímať ako oprávnenie na spracúvanie konkrétnych osobných údajov. Nariadenie GDPR pozná šesť hlavných právnych základov:

Súhlas dotknutej osoby [čl. 6 ods. 1 písm. a) Nariadenia GDPR]
Osobné údaje je možné spracúvať na základe súhlasu dotknutej osoby. Dotknutá osoba musí vyjadriť svoj súhlas slobodne a na konkrétny účel. Súhlas teda nemôže byť podmienkou uzatvorenia zmluvy. Súčasne je potrebné, aby bola dotknutá osoba informovaná o svojich právach, najmä práve súhlas kedykoľvek odvolať.

Súhlas dotknutej osoby nemôže firma alebo podnikateľ iba skryť v zmluve alebo obchodných podmienkach. Súhlas musí byť udelený jednoznačne, a to aktívnym konaním dotknutej osoby. V praxi sa na to využívajú tzv. check-boxy (či už v zmluvách alebo na webstránkach).

Príklad: newsletter pre osoby, ktoré nie sú zákazníkmi alebo klientmi je možné zasielať iba, ak tieto osoby súhlasili s jeho zasielaním, napr. zaškrtli „chcem dostávať novinky“

Plnenie zmluvy [čl. 6 ods. 1 písm. b) Nariadenia GDPR]
Firmy a podnikatelia môžu spracúvať osobné údaje dotknutých osôb aj z dôvodu, že to je potrebné na plnenie zmluvy medzi nimi a dotknutou osobou. Toto oprávnenie sa pritom vzťahuje aj na predzmluvnú komunikáciu. Každá zmluva musí totiž obsahovať identifikáciu zmluvných strán v rozsahu meno a priezvisko, bydlisko a dátum narodenia.

Je tomu tak preto, že:

- firma a podnikateľ musia poznať s kým zmluvu uzatvárajú, a súčasne
- sú tieto údaje potrebné v prípade súdneho konania (bez týchto údajov totiž nie je možné podať žalobu na súde).

Ak by zmluva neobsahovala údaj o dátume narodenia, firma alebo podnikateľ nevedia túto osobu pred súdom jednoznačne identifikovať, a súd im žalobu nepripustí a zamietne.

Na druhej strane v zásade platí, že iné osobné údaje nie sú pre plnenie zo zmluvy potrebné. Samozrejme tu existujú určité výnimky (e-mail alebo telefónne číslo – ak je potrebné na plnenie zmluvy alebo komunikáciu s druhou zmluvnou stranou a pod.).

Príklad: e-shop potrebuje adresu kupujúceho, aby doručil tovar a jeho dátum narodenia, aby si mohol svoje prípadné práva uplatniť voči kupujúcemu na súde

Právna povinnosť prevádzkovateľa [čl. 6 ods. 1 písm. c) Nariadenia GDPR]
Firmy a podnikatelia sú oprávnení spracúvať osobné údaje aj vtedy, ak im ich spracúvanie prikazuje zákon alebo iný právny predpis.

Ideálnym príkladom sú údaje zamestnanca, ktoré zamestnávateľ potrebuje na jeho prihlásenie do Sociálnej poisťovne, zdravotnej poisťovne a na daňový úrad.

Príklad: zamestnávateľ odovzdáva osobné údaje zamestnancov a v niektorých prípadoch aj ich rodinných príslušníkov Sociálnej poisťovni, zdravotnej poisťovni a daňovému úradu, a to podľa zákona

Ochrana životne dôležitých záujmov osoby [čl. 6 ods. 1 písm. d) Nariadenia GDPR]
Tento právny základ nie je pomerne častý, ale o to dôležitejší. Najčastejšie ho používajú zdravotnícke zariadenia a nemocnice pri ochrane pacienta v ohrození života alebo na ochranu jeho zdravia. Typické je to však práve pre urgentné situácie, kedy nie je možné spracúvať osobné údaje na základe iných právnych základov.

Príklad: lekár a nemocnica spracúvajú údaje pacienta v bezvedomí, aby mu poskytli neodkladnú zdravotnú starostlivosť

Neskôr, kedy je možné založiť spracúvanie osobných údajov pacienta na inom právnom základe, sú lekár a zdravotnícke zariadenie povinní nájsť iný právny základ – napríklad plnenie zmluvy.

Verejný záujem alebo výkon verejnej moci [čl. 6 ods. 1 písm. e) Nariadenia GDPR]
Tento právny základ spracúvania osobných údajov sa týka štátnych orgánov, iných orgánov verejnej moci a subjektov, ktorým bol prenesený výkon verejnej moci.

Na spracúvanie osobných údajov týmito orgánmi a subjektmi je vždy potrebné zákonné oprávnenie, vyplývajúce buď zo zákona alebo práva Únie.

Príklad: mestský úrad vedie evidenciu obyvateľov a na tento účel je oprávnený spracúvať osobné údaje

Oprávnený záujem prevádzkovateľa [čl. 6 ods. 1 písm. f) Nariadenia GDPR]
V mnohých prípadoch nie je možné použiť iný právny základ ako je oprávnený záujem prevádzkovateľa (firmy, podnikateľa). Ide o najflexibilnejší právny základ spracúvania osobných údajov, ale zároveň aj ten najrizikovejší.

Jeho podstatou je oprávnený záujem firmy alebo podnikateľa na spracúvaní určitých osobných údajov dotknutých osôb. Napríklad, firma si nainštaluje kamerový systém do skladu. Firma má totiž oprávnený záujem chrániť zdravie zamestnancov v sklade a svoj majetok, ktorý je v sklade umiestnený.

Na druhej strane tu však máme záujem dotknutých osôb (zamestnancov) na ochrane osobných údajov, svojej podobizne a svojho súkromia.

Preto sa pri použití tohto právneho základu vyžaduje vykonať **test proporcionality** (niekedy sa používa aj pojem balančný test). Ním firma alebo podnikateľ vlastne zisťujú, či ich oprávnený záujem (mať kamerový systém) neprevyšuje nad oprávneným záujmom zamestnancov na ochrane ich osobných údajov, podobizne a súkromia.

Test proporcionality **pozostáva z 3 krokov**, respektíve menších testov:

Test oprávnenosti záujmu
Týmto testom firma alebo podnikateľ zisťujú, či je ich záujem oprávnený (legitímny). Teda, či ich záujem skutočne existuje, a to v čase spracúvania osobných údajov. Tento záujem môže byť rôzny – právny, hospodársky, spoločenský alebo bezpečnostný.

Podstatné je, že oprávnený záujem firmy alebo podnikateľa nemôže byť v rozpore so zákonom alebo iným právnym predpisom.

Príklady legitímnych záujmov:

- ochrana majetku spoločnosti pred krádežou (kamerový systém),
- prevencia podvodov pri online platbách,
- priamy marketing voči existujúcim klientom (recitál 47 GDPR).

Test nevyhnutnosti
Pri teste nevyhnutnosti musíme zodpovedať otázku, či je spracúvanie osobných údajov na účely oprávneného záujmu firmy alebo podnikateľa skutočne nevyhnutné. Či sa týmto spracúvaním dosiahne záujem prevádzkovateľa.

Spracúvanie osobných údajov musí byť teda primerané a adekvátne na dosiahnutie sledovaného účelu. Súčasne nesmie existovať iný spôsob spracúvania, ktorý je menej invazívny a firma ním rovnako dosiahne sledovaný cieľ alebo účel.

Dôležitým faktorom je aj rešpektovanie princípu minimalizácie spracúvaných osobných údajov. Inak povedané, firma alebo podnikateľ nesmú spracúvať nadmerné množstvo osobných údajov, ktorých spracúvanie nesúvisí so sledovaným účelom.

Príklad:

- ak je cieľom ochrana majetku, kamerový záznam vstupu do budovy môže byť primeraný,
- ale kamerový systém na toaletách by bol neprimeraný – cieľ sa dá dosiahnuť inak.

Test vyváženia záujmov firmy a dotknutých osôb
Posledným krokom je samotný balančný test. Jeho podstatou je zistiť, či prevyšuje oprávnený záujem firmy alebo podnikateľa na spracúvaní osobných údajov dotknutých osôb nad ich právom na ochranu osobných údajov alebo prevyšuje záujem dotknutých osôb na ochranu nad oprávneným záujmom firmy.

Pri tomto teste musíme posudzovať nasledovné faktory:

rozumné očakávania dotknutej osoby – osoba môže oprávnene očakávať, že údaje budú spracúvané na daný účel?
- áno: zákazník môže očakávať priamy marketing od e-shopu, kde nakúpil
- nie: neočakáva, že jeho údaje budú predané tretej strane na neznáme účely

dopad na práva osôb – môže spracúvanie viesť k diskriminácii, stigmatizácii, finančnej strate alebo obmedzeniu základných práv?

povaha údajov – ide o bežné údaje (kontakt) alebo citlivé kategórie (zdravie, biometria)? Čím citlivejšie údaje, tým vyššie riziko zásahu

spôsob spracúvania – je invazívne, rozsiahle, dlhodobé? Krátkodobé a obmedzené spracúvanie je menej rizikové než systematické profilovanie.

bezpečnostné záruky a opatrenia – existujú mechanizmy, ktoré dopad zmierňujú (transparentné informovanie, možnosť namietať čl. 21 GDPR, technické a organizačné opatrenia napr. skrátenie retenčnej lehoty, pseudonymizácia)?

Po posúdení jednotlivých faktorov je možné dospieť k záveru, koho záujem prevyšuje. Ak záujem dotknutých osôb na ochrane osobných údajov neprevyšuje oprávnený záujem firmy alebo podnikateľa, potom je možné osobné údaje dotknutých osôb spracúvať na tento konkrétny účel.

Na základe oprávneného záujmu však nie je možné spracúvať osobitné kategórie osobných údajov. Na ich spracúvanie sa totiž vyžaduje právny základ uvedený v čl. 9 ods. 2 Nariadenia GDPR – výslovný súhlas, pracovnoprávne povinnosti, zdravotná starostlivosť, verejný záujem v oblasti verejného zdravia.

Praktický príklad – kamerový systém v kancelárii
***Účel**: ochrana majetku a bezpečnosti zamestnancov → legitímny záujem existuje.*
***Nevyhnutnosť**: kamery pri vstupe a na chodbe → primerané; kamery v šatniach → neprimerané.*
***Balančný test**: zamestnanci môžu rozumne očakávať monitoring v priestoroch, kde sa pohybujú verejne; očakávajú však súkromie v oddychovej zóne.*
***Záruky**: oznamy o monitoringu, limitovaná doba uchovávania záznamov (napr. 15 dní), prístup len oprávneným osobám, možnosť spracúvanie namietať.*
***Výsledok**: oprávnený záujem prevažuje, spracúvanie je zákonné.*

Praktické príklady (pre lepšiu orientáciu):

e-shop:
- *plnenie zmluvy → meno a priezvisko, adresa, dátum narodenia, e-mail na doručenie*
- *právna povinnosť → uchovávanie faktúr pre daňový úrad*
- *súhlas → zasielanie newsletterov*

zamestnávateľ:
- *právna povinnosť → odvody do Sociálnej poisťovne*
- *oprávnený záujem → kamera pri vstupe do budovy alebo v sklade*
- *súhlas → použitie fotografie zamestnanca na webovej stránke*

nemocnica:
- *právna povinnosť → vedenie zdravotnej dokumentácie*
- *ochrana životne dôležitých záujmov → urgentná zdravotná starostlivosť, osobitná kategória (čl. 9) → spracúvanie zdravotných údajov na účely liečby*

Výber právneho základu spracúvania osobných údajov

Firma alebo podnikateľ sú povinní si vybrať správny právny základ pre spracúvanie osobných údajov.

Teda, ak firma uzatvára zmluvu so zákazníkom, na účely plnenia zmluvy môže spracúvať osobné údaje zákazníka v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia, prípadne aj email (ak je potrebný na komunikáciu).

Naopak, ak firma plánuje zaviesť kamerový systém, nemôže použiť právny základ – plnenie zmluvy. Kamerový systém nie je potrebný na plnenie zmluvy so zákazníkom. Rovnako by nemala použiť súhlas – súhlas je totiž možné kedykoľvek odvolať. Potom sa ľahko môže stať, že firma nebude mať súhlas od všetkých zamestnancov, ale kamerový systém bude ich osobné údaje spracúvať.

Pre kamerový systém je preto najvhodnejší právny základ – oprávnený záujem spoločne s testom proporcionality.

Vo všeobecnosti môžeme povedať, že najčastejšími právnymi základmi sú práve plnenie zmluvy a plnenie zákonnej povinnosti. Ak nie je možné spracúvanie osobných údajov podriadiť pod tieto právne základy, musíme skúmať, či nemáme oprávnený záujem. Ak sa ukáže, že ani oprávnený záujem nie je správnym právnym základom, zostáva nám súhlas.

Súhlas je teda taká posledná možnosť, ako spracúvať osobné údaje. Môžeme ho však použiť naozaj len v prípade, ak neexistuje iný vhodnejší právny základ spracúvania osobných údajov.

4. Prevádzkovateľa a sprostredkovateľa, ich úlohy a zodpovednosť

Doteraz sme v texte používali pojem firma a podnikateľ. Nariadenie GDPR však používa svoje vlastné pojmy ako prevádzkovateľ (ten kto spracúva osobné údaje) a sprostredkovateľ (ten kto pre iného spracúva osobné údaje).

Poďme sa teda pozrieť na to, kto je prevádzkovateľ, kto sprostredkovateľ a aké majú povinnosti.

4.1. Kto je prevádzkovateľ (controller)

Podľa čl. 4 ods. 7 Nariadenia GDPR je prevádzkovateľom **fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určuje účely a prostriedky spracúvania osobných údajov**.

Prevádzkovateľ je teda akási pomyselná hlava spracúvania osobných údajov. Prevádzkovateľ je totiž ten, kto skutočne spracúva osobné údaje. Rozhoduje tiež o tom, prečo ich spracúva (uzatvorenie zmluvy) a akými prostriedkami bude osobné údaje spracúvať.

Môže ísť o kohokoľvek - firmu, ktorá uzatvára zmluvy so svojimi zákazníkmi, štátny orgán, ktorý vedie register, školu, nemocnicu, obec, občianske združenie, ale aj fyzickú osobu, ktorá si chráni svoj majetok kamerovým systémom.

Prevádzkovateľ je preto ten, kto nesie hlavnú zodpovednosť za spracúvanie osobných údajov a aj plnenie požiadaviek Nariadenia GDPR.

Príklad: e-shop, ktorý vedie databázu zákazníkov, je prevádzkovateľom, pretože určuje účel (predaj, doručenie tovaru) aj prostriedky (IT systém, kuriér)

4.2. Kto je sprostredkovateľ (processor)

Podľa čl. 4 ods. 8 Nariadenia GDPR je sprostredkovateľom subjekt, ktorý spracúva údaje v mene prevádzkovateľa.

Inak povedané, sprostredkovateľ je ten, kto síce spracúva osobné údaje, ale nie pre seba ale pre iného – štandardne pre prevádzkovateľa. Sprostredkovateľ teda nekoná pre seba, vo vlastnom mene, ale pracuje pre prevádzkovateľa a s osobnými údajmi, ktoré mu prevádzkovateľ poskytne.

Príklad: účtovná firma, ktorá spracúva mzdovú agendu pre klienta (prevádzkovateľa) – spracúva osobné údaje zamestnancov výlučne pre účely klienta

4.3 Vzťah prevádzkovateľ ↔ sprostredkovateľ

Medzi prevádzkovateľom a sprostredkovateľom existuje už nejaký zmluvný vzťah, bez ohľadu na to, či je písomný alebo nie.

Okrem toho Nariadenie GDPR vyžaduje upraviť vzťah medzi prevádzkovateľom a sprostredkovateľom písomnou zmluvou - zmluvou o poverení so spracúvaním osobných údajov. V tejto zmluve si prevádzkovateľ a sprostredkovateľ presne dohodnú, aké úlohy bude sprostredkovateľ plniť s osobnými údajmi, ktoré spracúva prevádzkovateľ a aké osobné údaje a na aký účel budú sprostredkovateľovi sprístupnené.

Zmluva musí obsahovať najmä:

- predmet a trvanie spracúvania,
- povahu a účel spracúvania,
- typ osobných údajov a kategórie dotknutých osôb,
- povinnosti a práva prevádzkovateľa,
- záväzky sprostredkovateľa (mlčanlivosť, bezpečnostné opatrenia, zákaz ďalšieho sprostredkovateľa bez súhlasu, asistencia pri uplatňovaní práv dotknutých osôb, povinnosť po skončení zmluvy údaje vymazať alebo vrátiť).

Táto „zmluva o spracúvaní“ je kľúčový dokument pre správne nastavenie vzťahov medzi sprostredkovateľom a prevádzkovateľom.

Na Slovensku Úrad na ochranu osobných údajov pri kontrolách opakovane zdôrazňuje, že zmluva so sprostredkovateľom je jedným z prvých dokumentov, ktoré si vyžiada. Prevádzkovatelia by preto mali disponovať štandardizovanými vzormi týchto zmlúv, ktoré následne prispôsobujú konkrétnemu typu služby alebo dodávateľa.

4.4 Spoloční prevádzkovatelia (joint controllers)

Vzťahy medzi podnikateľmi sú však často zložitejšie ako len vzťah prevádzkovateľa a sprostredkovateľa. Do úvahy totiž prichádza aj možnosť, že 2 firmy sú spoloční prevádzkovatelia.

Ak dve alebo viac firiem spoločne určujú účely a prostriedky spracúvania, ide o spoločných prevádzkovateľov podľa čl. 26 GDPR.

Aj tu platí povinnosť uzavrieť medzi prevádzkovateľmi zmluvu. V tejto zmluve sa musí transparentne určiť rozdelenie zodpovednosti, najmä pokiaľ ide o plnenie informačnej povinnosti a uľahčenie výkonu práv dotknutých osôb. Podstatná časť tejto zmluvy pritom musí byť dotknutým osobám poskytnutá.

Príklad: banka a poisťovňa spoločne prevádzkujú vernostný program so spoločnou databázou klientov

4.5 Zodpovednosť a sankcie

Prevádzkovateľ si nesie plnú zodpovednosť za dodržiavanie všetkých požiadaviek Nariadenia GDPR. Medzi také požiadavky patrí aj to, aby si vybral zodpovedného sprostredkovateľa, ktorý si riadne plní svoje povinnosti v oblasti ochrany osobných údajov.

Sprostredkovateľ pritom zodpovedá len v rozsahu, v akom poruší povinnosti, ktoré mu priamo ukladá Nariadenie GDPR alebo ktoré vyplývajú zo zmluvy s prevádzkovateľom.

Spoločná zodpovednosť (čl. 82 ods. 4 Nariadenia GDPR) prevádzkovateľa a sprostredkovateľa prichádza do úvahy, ak dôjde k porušeniu, ktoré je možné pričítať obom. Prevádzkovateľ aj sprostredkovateľ teda môžu byť spoločne zodpovední a dotknutá osoba si môže náhradu škody uplatniť voči ktorémukoľvek z nich.

Praktické odporúčania:

- *prevádzkovatelia by mali mať mapu všetkých sprostredkovateľov a evidenciu ich zmlúv*
- *pred výberom sprostredkovateľa je vhodné preveriť jeho technické a organizačné opatrenia (due diligence)*
- *pri dlhodobých zmluvných vzťahoch je dobré nastaviť pravidelné audity alebo aspoň právo prevádzkovateľa na kontrolu*
- *v praxi sa odporúča vytvoriť štandardnú šablónu zmluvy o spracúvaní, ktorá sa prispôsobuje podľa typu služby*
- *ideálne je zapracovať ustanovenia o spracúvaní osobných údajov do VOP alebo priamo do zmluvy so sprostredkovateľom (šetrí to čas a znižuje počet zmlúv)*

5. Dokumentačné povinnosti prevádzkovateľa

Ako sme spomínali v úvode, jedným z hlavných pilierov ochrany osobných údajov je princíp zodpovednosti (accountability). Podľa neho musí prevádzkovateľ nielen dodržiavať požiadavky Nariadenia GDPR, ale vedieť aj preukázať, že ich dodržiava. To v praxi znamená, že nestačí mať nastavené procesy, ale je potrebné ich aj dokumentovať.

Prvou a najzásadnejšou dokumentačnou povinnosťou je **vedenie záznamov o spracovateľských činnostiach podľa čl. 30 Nariadenia GDPR**. Prevádzkovateľ má totiž povinnosť uchovávať záznamy o všetkých spracovateľských operáciách, ktoré vykonáva.

Tieto záznamy musia obsahovať minimálne nasledovné údaje:

- meno a kontaktné údaje prevádzkovateľa a prípadne zodpovednej osoby,
- účely spracúvania,
- opis kategórií dotknutých osôb,
- opis kategórií osobných údajov,
- kategórie príjemcov,
- predpokladané lehoty uchovávania, a
- ·opis prijatých bezpečnostných opatrení.

.

Záznam o spracovateľských činnostiach je úplným základom, aby prevádzkovateľ poznal, aké osobné údaje spracúva a na aké účely. Tento záznam postačí viesť v elektronickej podobe, pričom je to jeden z prvých dokumentov, ktoré v prípade kontroly predkladáme.

Ďalším významným dokumentom je **interná smernica o ochrane osobných údajov**. Ide o súbor interných pravidiel, ktoré definujú spôsob, akým prevádzkovateľ spracúva osobné údaje, aké opatrenia prijíma na ich ochranu a kto nesie aké zodpovednosti. V menších firmách sa tieto pravidlá môžu prejaviť formou kratších dokumentov, no vo väčších spoločnostiach často ide o komplexné interné predpisy, vrátane bezpečnostných smerníc na ochranu údajov.

Prevádzkovateľ má okrem toho aj povinnosť zabezpečiť, aby mal k dispozícii všetky zmluvy o poverení so spracúvaním osobných údajov uzavreté so sprostredkovateľmi podľa čl. 28 Nariadenia GDPR. Tieto zmluvy sú základným dokumentom, ktorý preukazuje, že spracúvanie prebieha v súlade s požiadavkami Nariadenia GDPR a že sprostredkovateľ prijal primerané záruky.

Samostatnú kategóriu tvoria **záznamy o súhlase dotknutých osôb**. Ak je právnym základom spracúvania súhlas, prevádzkovateľ musí byť schopný preukázať, že súhlas bol udelený platne, teda že bol slobodný, informovaný a jednoznačný. Preto sa odporúča viesť evidenciu o tom, kedy a akým spôsobom bol súhlas udelený, a zabezpečiť technickú možnosť jeho odvolania.

V prípadoch, keď to povaha spracúvania vyžaduje, je potrebné vypracovať aj **posúdenie vplyvu na ochranu údajov (Data Protection Impact Assessment – DPIA)** podľa čl. 35 Nariadenia GDPR. Ide o proces, v ktorom prevádzkovateľ analyzuje plánované spracúvanie, identifikuje riziká pre práva a slobody dotknutých osôb a prijíma opatrenia na ich zmiernenie. DPIA je povinné najmä pri spracúvaní vo veľkom rozsahu, pri systematickom monitorovaní osôb alebo pri spracúvaní osobitných kategórií údajov.

Významnú dokumentačnú povinnosť predstavuje aj **bezpečnostná dokumentácia**, najmä opis technických a organizačných opatrení prijatých na zabezpečenie osobných údajov (napr. šifrovanie, pseudonymizácia, obmedzenie prístupu, školenie zamestnancov). Úrad na ochranu osobných údajov pri kontrolách často skúma, či sú tieto opatrenia primerané povahe spracúvaných údajov a rizikám. Bezpečnostná dokumentácia môže byť súčasťou internej smernice prevádzkovateľa o spracúvaní osobných údajov, ale pri väčších spoločnostiach ide o samostatný dokument, ktorý presne eviduje prijaté bezpečnostné opatrenia na ochranu údajov.

Napokon, prevádzkovateľ by mal mať pripravené aj **záznamy o porušeniach ochrany osobných údajov.** Každé porušenie, bez ohľadu na to, či bolo oznámené úradu alebo nie, musí byť riadne zdokumentované. Záznam má obsahovať opis incidentu, jeho následkov a prijatých nápravných opatrení. Tieto záznamy slúžia nielen na splnenie zákonnej povinnosti, ale aj ako nástroj na zlepšenie vnútorných procesov.

Celkovo možno povedať, že dokumentačné povinnosti predstavujú chrbtovú kosť GDPR compliance. Nejde o formalizmus, ale o praktický nástroj, ktorý umožňuje prevádzkovateľovi preukázať, že si splnil svoje povinnosti a že osobné údaje spracúva transparentne, bezpečne a zákonne.

6. Informačná povinnosť voči dotknutým osobám

Jedným zo základných princípov ochrany osobných údajov je aj transparentnosť spracúvania. Tá vo svojej podstate znamená hlavne povinnosť prevádzkovateľa informovať dotknuté osoby o spracúvaní ich osobných údajov.

Prevádzkovateľ musí zabezpečiť, aby dotknuté osoby dostali jasné, zrozumiteľné a včasné informácie o tom, ako sa ich osobné údaje spracúvajú. Táto povinnosť je zakotvená v článkoch 12 až 14 Nariadenia GDPR a tvorí základný predpoklad toho, aby dotknuté osoby mohli účinne uplatňovať svoje práva.

Nariadenie GDPR pritom rozlišuje dve základné situácie. **Ak sa osobné údaje získavajú priamo od dotknutej osoby, uplatní sa čl. 13 Nariadenia GDPR**. Prevádzkovateľ je v takom prípade povinný poskytnúť dotknutej osobe informácie najneskôr v okamihu ich získania. Ide napríklad o situáciu, keď zákazník vyplní registračný formulár na webovej stránke.

Druhým prípadom je situácia, keď prevádzkovateľ získava údaje z iného zdroja – napríklad z verejne dostupného registra alebo od iného subjektu. Vtedy platí čl. 14 Nariadenia GDPR, podľa ktorého musí prevádzkovateľ poskytnúť informácie najneskôr do jedného mesiaca, alebo pri prvom kontakte s dotknutou osobou, ak k nemu dôjde skôr.

Rozsah informácií, ktoré sa majú poskytnúť, je pomerne široký. Prevádzkovateľ musí vždy uviesť svoju totožnosť a kontaktné údaje, ako aj kontaktné údaje zodpovednej osoby, ak je ustanovená. Musí objasniť účely, na ktoré sa údaje spracúvajú, a uviesť právny základ spracúvania. Ak sa spracúvanie zakladá na oprávnenom záujme, je potrebné tento záujem presne špecifikovať. Ďalej sa uvádzajú kategórie príjemcov, prípadne informácia o prenose do tretích krajín a o primeraných zárukách.

Dotknutá osoba musí byť informovaná aj o dobe, po ktorú sa údaje budú uchovávať, alebo o kritériách, podľa ktorých sa táto doba určuje. Okrem toho Nariadenie GDPR vyžaduje, aby bola dotknutá osoba informovaná o svojich právach – právo na prístup k údajom, opravu, vymazanie, obmedzenie spracúvania, prenosnosť údajov, právo namietať a právo podať sťažnosť dozornému orgánu. Ak je spracúvanie založené na súhlase, musí sa uviesť aj právo tento súhlas kedykoľvek odvolať.

Z hľadiska formy musia byť informácie podané stručne, transparentne, zrozumiteľne a ľahko prístupným spôsobom, pričom sa odporúča používať jasný a jednoduchý jazyk, najmä ak sú adresované deťom. V praxi sa preto často využívajú viacvrstvové informačné texty, kde je v prvej vrstve uvedené stručné zhrnutie najdôležitejších informácií a v druhej vrstve detailnejšie právne a technické vysvetlenie.

Legalion

Ak si prevádzkovateľ nesplní svoju informačnú povinnosť, vystavuje sa riziku nielen vysokých sankcií, ale aj strate dôvery zo strany klientov, zamestnancov či partnerov. Správne a transparentné informovanie sa preto vníma nielen ako právna povinnosť, ale aj ako dôležitý prvok budovania dôveryhodnosti firmy a podnikania.

7. Práva dotknutých osôb

Ako sme uvádzali v predchádzajúcom bode, dotknuté osoby majú podľa Nariadenia GDPR rozsiahle práva. Nariadenie GDPR tým chce posilniť kontrolu jednotlivcov nad ich osobnými údajmi. Preto nariadenie priznáva dotknutým osobám široký súbor práv, ktoré sú zakotvené najmä v článkoch 15 až 22 Nariadenia GDPR.

Tieto práva nie sú len formálnymi ustanoveniami, ale predstavujú praktické nástroje, prostredníctvom ktorých môže jednotlivec dohliadať na to, ako firmy a podnikatelia nakladajú s jeho údajmi.

Prvým a najzákladnejším je **právo na prístup podľa čl. 15 Nariadenia GDPR**. Dotknutá osoba má právo vedieť, či prevádzkovateľ spracúva jej osobné údaje, a ak áno, má právo získať k nim prístup. Okrem samotných údajov musí prevádzkovateľ poskytnúť aj sprievodné informácie – účely spracúvania, kategórie údajov, kategórie príjemcov, dobu uchovávania a informácie o právach. V praxi to znamená, že ak sa jednotlivec obráti na prevádzkovateľa so žiadosťou o prístup, tento mu musí poskytnúť kópiu údajov a príslušné vysvetlenie.

Ďalším právom je **právo na opravu podľa čl. 16 Nariadenia GDPR**. Ak sú osobné údaje nesprávne alebo neúplné, dotknutá osoba má právo požadovať ich opravu alebo doplnenie. Prevádzkovateľ je povinný konať bez zbytočného odkladu, aby údaje boli vždy aktuálne a presné.

S tým súvisí aj právo na vymazanie, známe aj ako **„právo byť zabudnutý“ podľa čl. 17 Nariadenia GDPR**. Dotknutá osoba môže požadovať vymazanie svojich údajov, ak už nie sú potrebné na účel, na ktorý sa spracúvali, ak odvolala svoj súhlas, ak namieta proti spracúvaniu alebo ak bolo spracúvanie nezákonné. Toto právo však nie je absolútne – neplatí napríklad v prípadoch, keď je uchovávanie údajov potrebné na splnenie zákonnej povinnosti alebo na uplatňovanie právnych nárokov.

Ďalším významným právom je **právo na obmedzenie spracúvania podľa čl. 18 Nariadenia GDPR**. Dotknutá osoba môže žiadať, aby prevádzkovateľ dočasne „zmrazil“ spracúvanie údajov, napríklad ak sa spochybňuje ich presnosť alebo ak sa preveruje oprávnený záujem prevádzkovateľa. V takom prípade sa údaje nesmú ďalej spracúvať, len uchovávať.

Podľa čl. 20 Nariadenia GDPR má dotknutá osoba aj **právo na prenosnosť údajov**. To znamená, že údaje, ktoré poskytla prevádzkovateľovi na základe súhlasu alebo zmluvy a ktoré sa spracúvajú automatizovane, si môže vyžiadať v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte. Zároveň má právo, aby sa tieto údaje preniesli priamo k inému prevádzkovateľovi, ak je to technicky možné. Toto právo má v praxi veľký význam najmä v sektore telekomunikácií, bankovníctva či online služieb.

Veľmi dôležité je aj právo **namietať podľa čl. 21 Nariadenia GDPR**. Dotknutá osoba môže kedykoľvek namietať proti spracúvaniu, ktoré sa zakladá na oprávnenom záujme prevádzkovateľa alebo ktoré sa vykonáva na účely priameho marketingu. V prípade námietky musí prevádzkovateľ spracúvanie ukončiť, ak nepreukáže závažné oprávnené dôvody, ktoré prevažujú nad právami dotknutej osoby.

Napokon, Nariadenie GDPR zavádza aj **právo nepodliehať výlučne automatizovanému rozhodovaniu vrátane profilovania podľa čl. 22 Nariadenia GDPR**. Jednotlivec má právo, aby o jeho právach alebo povinnostiach nerozhodoval výlučne automatizovaný systém bez ľudského zásahu, ak by takéto rozhodnutie malo pre neho významné právne alebo obdobné účinky. Typickým príkladom je automatické vyhodnotenie bonity klienta v banke.

Pre všetky tieto práva platí spoločný procesný rámec. Dotknutá osoba ich môže uplatniť prostredníctvom žiadosti, prevádzkovateľ musí reagovať bez zbytočného odkladu, najneskôr však do 1 mesiaca, a poskytovanie informácií a úkonov musí byť spravidla bezplatné. Len vo výnimočných prípadoch, ak sú žiadosti zjavne neopodstatnené alebo neprimerané, môže prevádzkovateľ účtovať primeraný poplatok alebo žiadosť odmietnuť.

Tieto práva predstavujú účinný mechanizmus, ktorý umožňuje jednotlivcom aktívne kontrolovať, čo sa deje s ich osobnými údajmi. Pre prevádzkovateľa sú zároveň výzvou, pretože musí mať vytvorené vnútorné procesy a nástroje, aby dokázal žiadosti vybaviť v zákonom stanovených lehotách.

Praktický postup vybavovania žiadostí dotknutých osôb

Pre jednoduchšie použitie sme pripravili aj krátky praktický postup, ako správne vybaviť žiadosti dotknutých osôb.

1. Prijatie žiadosti
Prevádzkovateľ musí umožniť, aby dotknutá osoba mohla podať žiadosť viacerými spôsobmi – písomne, elektronicky (e-mail, webový formulár) alebo aj osobne.
Nariadenie GDPR nevyžaduje žiadnu osobitnú formu žiadosti, preto prevádzkovateľ nesmie odmietnuť napríklad ani žiadosť podanú e-mailom bez elektronického podpisu alebo osobne.

Vhodné je mať na webe alebo v interných dokumentoch štandardizovaný formulár, ktorý žiadateľom pomôže špecifikovať, ktoré právo chcú uplatniť, prípadne samostatnú e-mailovú schránku pre podávanie takýchto žiadostí.

Pozor si treba dať na to, že nie je podstatné, kam dotknutá osoba pošle e-mail. Dotknutá osoba môže poslať e-mail aj zamestnancovi prevádzkovateľa, s ktorým bežne komunikuje. Stále však platí, že žiadosť dotknutej osoby sa dostala k prevádzkovateľovi a ten ju musí vybaviť.

2. Overenie totožnosti žiadateľa
Prevádzkovateľ je povinný zabezpečiť, aby údaje poskytol naozaj len oprávnenej osobe. Ak má pochybnosti o totožnosti žiadateľa, môže si vyžiadať dodatočné informácie (napr. kópiu dokladu totožnosti, overenie cez e-mail alebo SMS).

Overenie musí byť primerané – nesmie ísť nad rámec toho, čo je potrebné na identifikáciu.

3. Zaevidovanie žiadosti
Každá žiadosť by mala byť zapísaná do interného registra žiadostí dotknutých osôb. Tento register by mal obsahovať dátum prijatia žiadosti, totožnosť žiadateľa, druh uplatneného práva a osobu zodpovednú za vybavenie.

Vedenie registra je súčasťou princípu zodpovednosti – pri kontrole zo strany úradu firma preukáže, že má nastavený systém na vybavovanie žiadostí.

4. Posúdenie žiadosti
Zodpovedná osoba (napr. osoba poverená ochranou osobných údajov, určený zamestnanec alebo externý subjekt) preskúma, ktoré údaje sa spracúvajú a či sú splnené podmienky na uplatnenie konkrétneho práva.

Ak je žiadosť nejasná, prevádzkovateľ môže kontaktovať žiadateľa a požiadať ho o spresnenie.

5. Realizácia opatrení
Ak je žiadosť oprávnená, prevádzkovateľ musí prijať potrebné opatrenia:

- pri práve na prístup – poskytnúť kópiu údajov,
- pri oprave – opraviť alebo doplniť údaje,
- pri vymazaní – vymazať údaje alebo anonymizovať,
- pri obmedzení spracúvania – označiť údaje ako „blokované“ a nepoužívať ich,
- pri prenosnosti – pripraviť údaje v strojovo čitateľnom formáte,
- pri námietke spracúvania – zastaviť spracúvanie, ak neexistujú závažné dôvody,
- pri automatizovanom rozhodovaní – zabezpečiť ľudský zásah do procesu.

6. Odpoveď žiadateľovi
Prevádzkovateľ musí poskytnúť odpoveď bez zbytočného odkladu, najneskôr do 1 mesiaca od prijatia žiadosti.

V odôvodnených prípadoch možno lehotu predĺžiť o ďalšie 2 mesiace, ak je žiadostí veľa alebo sú zložité. O predĺžení však musí byť žiadateľ vopred informovaný do 1 mesiaca od prijatia žiadosti.

Odpoveď musí byť poskytnutá v zrozumiteľnej forme, rovnakým spôsobom, akým bola žiadosť podaná (ak žiadateľ nepožiada inak).

7. Evidencia a archivácia
Po vybavení žiadosti sa výsledok zapíše do registra žiadostí.

Uchovávať sa má aj kópia komunikácie so žiadateľom – slúži to ako dôkaz, že firma splnila povinnosti podľa Nariadenia GDPR.

8. Odmietnutie žiadosti
Ak je žiadosť zjavne neopodstatnená alebo neprimeraná (napr. opakuje sa neustále bez dôvodu), môže ju prevádzkovateľ odmietnuť.

V takom prípade musí žiadateľovi vysvetliť dôvody odmietnutia a poučiť ho o práve podať sťažnosť dozornému orgánu.

V týchto prípadoch môže prevádzkovateľ účtovať primeraný poplatok (najmä na pokrytie administratívnych nákladov).

Praktické odporúčania:

- *vypracovať internú smernicu o vybavovaní práv dotknutých osôb, kde bude popísaný celý proces krok za krokom*
- *určiť zodpovednú osobu (alebo tím), ktorá bude žiadosti prijímať a vybavovať, prípadne tým môžete poveriť externý subjekt*
- *mať pripravené štandardizované vzory odpovedí pre jednotlivé práva – čo zrýchli proces a zabezpečí konzistentnosť*
- *pravidelne školiť zamestnancov, aby vedeli, ako postupovať, ak klient alebo zamestnanec uplatní svoje právo*

8. Poverenie a poučenie zamestnancov

Nariadenie GDPR síce priamo nepoužíva pojem „poverenie zamestnanca," no z jeho zásad vyplýva, že osobné údaje môžu spracúvať len tie osoby, ktoré na to majú oprávnenie od prevádzkovateľa alebo sprostredkovateľa. Tento princíp je odvodený z čl. 29 Nariadenia GDPR, podľa ktorého každý, kto spracúva osobné údaje v mene prevádzkovateľa alebo sprostredkovateľa, tak môže robiť výlučne na ich pokyn.

Na tento účel sa v praxi využíva jednoduché poverenie a poučenie zamestnancov, ktorí pracujú s osobnými údajmi.

Podstatou poverenia je to, že prevádzkovateľ udeľuje konkrétnemu zamestnancovi oprávnenie spracúvať v jeho mene osobné údaje. Samozrejmosťou je to, aby bol zamestnanec oprávnený spracúvať iba tie osobné údaje, ktoré sú potrebné na plnenie jeho pracovných povinností.

Nie je preto vhodné, aby bol každý zamestnanec poverený spracúvať akékoľvek a všetky osobné údaje, ktoré prevádzkovateľ spracúva.

Poverenie má presne určiť:

- ktoré osobné údaje môže zamestnanec spracúvať,
- na aký účel,
- v akom rozsahu (napr. len čítanie, alebo aj oprava a mazanie údajov),
- aké technické a organizačné pravidlá musí dodržiavať,
- ako má postupovať v prípade incidentu alebo porušenia ochrany údajov.

Okrem toho je potrebné zamestnancov aj riadne poučiť o ich povinnostiach.

Povinnosť mlčanlivosti

Každý zamestnanec, ktorý prichádza do styku s osobnými údajmi, musí byť zaviazaný povinnosťou mlčanlivosti. Táto povinnosť môže vyplývať priamo zo zákona (napr. v prípade advokátov či zdravotníckeho personálu), ale vo väčšine prípadov by mala byť výslovne dohodnutá v pracovnej zmluve, dohode alebo v osobitnom vyhlásení o mlčanlivosti.

Školenia a zvyšovanie povedomia

Nariadenie GDPR kladie dôraz na princíp „privacy by design a by default“. To znamená, že ochrana údajov má byť zakotvená už vo vnútorných procesoch organizácie. Kľúčovú úlohu v tom zohrávajú práve zamestnanci. Prevádzkovateľ by im mal pravidelne poskytovať školenia o ochrane osobných údajov a v konkrétnych prípadoch aj o kybernetickej bezpečnosti, aby vedeli, ako správne pracovať s údajmi a aké chyby môžu viesť k porušeniu ochrany údajov.

Interné politiky a postupy

Zamestnanci by mali mať k dispozícii jasné interné smernice – napríklad ako spracúvať mzdové údaje, ako postupovať pri komunikácii s klientmi alebo ako riešiť situácie, keď dôjde k strateniu USB kľúča so súbormi. Interné politiky musia byť zrozumiteľné a dostupné pre každého zamestnanca.

Kontrola a audit

Prevádzkovateľ má povinnosť zabezpečiť, aby zamestnanci vykonávali spracúvanie v súlade s Nariadením GDPR. To znamená pravidelne overovať, či zamestnanci dodržiavajú stanovené pravidlá, či majú prístup len k údajom, ktoré nevyhnutne potrebujú, a či nedochádza k neoprávnenému spracúvaniu. V praxi sa na to používajú prístupové práva v informačných systémoch a pravidelné audity.

Sankcie a zodpovednosť

Ak zamestnanec poruší povinnosti pri spracúvaní osobných údajov, zodpovedá za to v prvom rade prevádzkovateľ, keďže on je nositeľom primárnej zodpovednosti. Zamestnanec však môže niesť pracovnoprávnu zodpovednosť (napr. disciplinárne opatrenia, náhrada škody podľa Zákonníka práce).

Legalion

9. Posudzovanie vplyvu na ochranu osobných údajov (DPIA)

DPIA (Data Protection Impact Assessment) je proces, ktorý má prevádzkovateľom pomôcť vopred identifikovať a zhodnotiť riziká, ktoré môže konkrétne spracúvanie osobných údajov priniesť pre práva a slobody dotknutých osôb.

Tento nástroj je zakotvený v čl. 35 Nariadenia GDPR a je povinný všade tam, kde by spracúvanie mohlo viesť k vysokému riziku.

DPIA sa musí vykonať najmä v prípadoch, keď:

dochádza k systematickému a rozsiahlemu profilovaniu alebo automatizovanému rozhodovaniu s právnymi účinkami

sa spracúvajú osobitné kategórie údajov (citlivé údaje, napr. zdravotné) vo veľkom rozsahu

dochádza k systematickému monitorovaniu verejne prístupných priestorov vo veľkom rozsahu (napr. kamerové systémy v obchodných centrách)

Úrad na ochranu osobných údajov SR k tomu vydal zoznam konkrétnych spracovateľských činností, pri ktorých je DPIA povinné (tzv. „**čierny zoznam**“), a odporúča ho vykonať aj v iných prípadoch, kde existuje riziko.

Cieľom DPIA je:

- identifikovať, aké osobné údaje sa budú spracúvať,
- vyhodnotiť účel spracúvania a jeho zákonnosť,
- zhodnotiť, aké riziká spracúvanie prináša pre práva a slobody jednotlivcov,
- navrhnúť a prijať opatrenia, ktoré riziká znížia na prijateľnú úroveň.

Legalion

Ako vykonať DPIA krok po kroku:

Opis spracovateľskej operácie – aké údaje sa spracúvajú, kto je prevádzkovateľ, kto sú príjemcovia, aké technológie sa používajú.

Analýza nevyhnutnosti a proporcionality – preveriť, či je spracúvanie naozaj potrebné na dosiahnutie účelu a či nejde nad rámec tohto účelu.

Identifikácia rizík – zhodnotiť, aké riziká môžu vzniknúť (únik údajov, neoprávnený prístup, neopodstatnené profilovanie, diskriminácia).

Vyhodnotenie závažnosti rizík – posúdiť pravdepodobnosť a dopad na práva dotknutých osôb.

Opatrenia na zmiernenie rizík – návrh technických a organizačných opatrení (šifrovanie, pseudonymizácia, obmedzenie prístupu, interné procesy).

Záver – rozhodnutie, či je možné spracúvanie vykonávať, alebo je potrebné spracúvanie osobných údajov prepracovať.

Ak aj po vykonaní DPIA ostáva vysoké riziko a prevádzkovateľ ho nevie primerane zmierniť, má povinnosť konzultovať spracúvanie s dozorným orgánom (na Slovensku Úrad na ochranu osobných údajov). **Bez tejto konzultácie by spracúvanie ani nemalo začať.**

Praktické odporúčania:

- *vytvoriť si štandardizovanú šablónu DPIA, aby sa posudzovanie robilo jednotne*
- *zapájať do procesu nielen právnikov a zodpovednú osobu, ale aj IT odborníkov a manažment*
- *DPIA nevnímať len ako formálnu povinnosť, ale ako nástroj riadenia rizík, ktorý chráni nielen dotknuté osoby, ale aj reputáciu a bezpečnosť firmy*
- *dokumentovať celý proces – ak príde kontrola, preukázať, že DPIA bolo vykonané riadne a systematicky*

Legalion

Tohto sprievodcu sme pripravili na základe všetkých našich skúseností s prípravami GDPR dokumentácie. Naša advokátska kancelária má totiž rozsiahle skúsenosti s implementáciou GDPR pre spoločnosti rôzneho zamerania.

Klienti pritom oceňujú, že dokumentáciu pripravujeme tak, aby spĺňala zákonné požiadavky, bola praktická a obstála aj pri kontrolách.

GDPR je dynamická oblasť, ktorá sa vyvíja spolu s legislatívou aj technológiami. Našim klientom preto poskytujeme nielen počiatočnú dokumentáciu, ale aj kontinuálnu právnu podporu, aby boli pripravení na **zmeny**, **ktoré prinášajú moderné technológie ako napríklad AI.**

Staňte sa naším klientom a získajte spoľahlivého partnera v oblasti ochrany osobných údajov.

Radi vám pomôžeme nastaviť procesy tak, aby ste sa mohli naplno sústrediť na svoje podnikanie.

Kontaktujte nás a dohodnite si konzultáciu k nastaveniu GDPR vo vašej spoločnosti

JUDR. ALEXANDER UJ

+421 948 253 977

alexander.uj@legalion.sk

BBC 1, Plynárenská 1, 821 09 Bratislava

www.legalion.sk