Hlavné zmeny v právnej úprave ochrany osobných údajov

Od 25.05.2018 prichádza do platnosti Nariadenie GDPR a zákon o ochrane osobných údajov nadobúdajú účinnosť k rovnakému dňu. Úlohou novej právnej úpravy je zabezpečiť jednotnú právnu reguláciu nakladaní s osobnými údajmi, zaistiť ochranu fyzických osôb, ochranu osobných údajov, s ktorými sa nakladá a taktiež kontrolu nad spracovateľmi týchto údajov. Cieľom regulácie GDPR, je zvýšiť ochranu osobných údajov a posilniť práva fyzických osôb. Všetky povinnosti prevádzkovateľa a sprostredkovateľa vyplývajú priamo z tohto nariadenia, nariadenie sa vzťahuje na každého, kto spracúva osobné údaje na území Európskej únie, ale i mimo nej, ak spĺňa nariadením stanovené podmienky.

V tomto dokumente si Vás dovoľujeme informovať aké dôležité a zásadné zmeny prichádzajú s novou legislatívou.

PRÁVNE ZÁKLADY OCHRANY SÚKROMIA ZAMESTNANCA A OCHRANY OSOBNÝCH ÚDAJOV

Všeobecný právny rámec v oblasti ochrany práva na súkromný a rodinný život v rámci pracovnoprávnych vzťahov predstavuje:

- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679**
  z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov (GDPR);

- **Smernica Európskeho parlamentu a Rady (EÚ) 2016/680** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV – účinnosť od 25.05.2018 – tzv. policajná smernica;

- **Zákon č. 18/2018 Z .z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**;
- Osobitné právne predpisy – **Ústava SR, Občiansky zákonník, Obchodný zákonník, Zákonník práce** a ďalšie;

- Nariadenie Európskeho parlamentu a Rady (EÚ) o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách) – e-Privacy – platnosť cca o 2 roky;

- Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (NIS) 2016/1148 z 06.07.2016 – tzv. kyberbezpečnosť;

- Materiály pracovnej skupiny WP 29 – zverejnené na webovej stránke Úradu na ochranu osobných údajov Slovenskej republiky
- **Smernica na ochranu osobných údajov**
- **Smernica na oznamovanie porušenia ochrany osobných údajov**

ČO JE OSOBNÝ ÚDAJ PODĽA ČL 4. BOD 1 NARIADENIA

- Podľa GDPR sa za osobné údaje bude považovať nielen, že osoba je identifikovaná priamo alebo nepriamo, ale bude sa považovať osobný údaj ako je identifikátor **- odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor.** Za online identifikátor sa považuje **cookies, IP adresa alebo štítky na rádiofrekvenčnú identifikáciu.** Tieto môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi a inými informáciami získanými zo serverov môžu použiť na vytvorenie profilov fyzických osôb a na ich identifikáciu.

OSOBITNÁ KATEGÓRIA OSOBNÝCH ÚDAJOV PODĽA NARIADENIA ČL.9

- **Údaje týkajúce sa zdravia –** sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave (recitál bod 35 Nariadenia), napríklad o chorobe, zdravotnom postihnutí, riziku ochorenia, anamnéze, klinickej liečbe, alebo o fyziologickom alebo biomedicínskom stave dotknutej osoby bez ohľadu na zdroj týchto informácií, či už pochádzajú od lekára alebo od iného zdravotníckeho pracovníka, z nemocnice alebo vykonania diagnostického testu in vitro.

- Zakazuje sa spracovanie osobných údajov, ktoré odhaľujú **rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách a spracúvanie genetických údajov, biometrických údajov, na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života a sexuálnej orientácie.**
  Od 25.5.20018 ***všeobecne použiteľný identifikátor – rodné číslo*** *sa nepovažuje za osobitnú kategóriu osobných údajov. GDPR to volá* ***národné identifikačné číslo*** *a nariadenie ustanovuje, že každý členský štát má právo si upraviť vo svojom vnútroštátnom predpise podmienky spracovania RČ.*

- *Po novom sú 3 typy osobných údajov:*
- ***1.) osobné údaje***
- ***2.) osobitná kategória osobných údajov***
- ***3.) rodné číslo, ktoré sa považuje za citlivé dáta***

- Podľa GDPR spracúvanie fotografickej podobizne alebo grafického zobrazenia podpisu bez získavania biometrických údajov sa nepovažuje za **spracúvanie osobitných kategórií osobných údajov.**

Rodné číslo podľa § 78 ods. 4 zákona č. 18/2018

- Pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby **všeobecne použiteľný identifikátor** podľa osobitného predpisu len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracovania. Súhlas so spracovaním všeobecne použiteľného identifikátora musí byť výslovný a nesmie ho vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje: to neplatí, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba.

- RČ nebude osobitná kategória OÚ, ale stále platí, že ho **môžeme spracovať, len ak je to nevyhnutné na dosiahnutie účelu.** RČ nemôžeme sprístupniť, zverejniť, môžeme ho spracovávať, ak to vyplýva z osobitného predpisu alebo, ak je to nevyhnutné na dosiahnutie účelu alebo, ak nám dotknutá osoba dala súhlas. Stále platí sprísnený režim *Rozdiel medzi zákonom č. 122/2013 a novým zákonom č.18/2018 je v tom, že podľa nového zákona* ***si môže dotknutá osoba zverejniť vlastné RČ .***

VYSVETLENIE POJMOV

- **Prevádzkovateľ** - každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene.
- **Spoloční prevádzkovatelia** – ***novinka***, ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.(*napr. že dá sa dohodnúť, že dve firmy si povedia, že my určíme účel a prostriedky spracúvania. Nedá sa to aplikovať na personalistiku, na účtovníctvo tento inštitút sa dá uplatniť napr. na marketing alebo na kamery, viacej firiem sa dohodne, že bude mať spoločné kamery*
- **Sprostredkovateľ -** každý, kto spracúva osobné údaje v mene prevádzkovateľa. *Medzi prevádzkovateľom a sprostredkovateľom musí byť písomne uzavretá zmluva. Nová sprostredkovateľská zmluva sa uzatvára v zmysle GDPR - Čl. 28 ods.3 od 25.5.2018 boli definované náležitosti zmluvy.*
- **Dotknutá osoba** - každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
- **Príjemca** - každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci.
- **Tretia strana** - každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje. *Najčastejšie je to iný subjekt, ktorý si ďalej spracúva osobné údaje vo vlastnom mene (napr. Sociálna poisťovňa, Zdravotná poisťovňa, Daňový úrad, Inšpektorát práce, Doplnkové dôchodkové poisťovne, exekútor, banky, polícia, súdy, orgány činné v trestnom konaní).*

NOVÉ POJMY PODĽA NARIADENIA

- **Profilovanie -** akákoľvek forma automatizovaného spracúvanie osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom. *Sledovanie správania sa dotknutej osoby v online prostredí hlavne, že profilujeme zamestnanca v súvislosti s výkonom práce, je potrebné ho o tom informovať, v niektorých prípadoch má právo namietať. Na určenie toho, či spracovateľskú činnosť možno považovať za „sledovanie správania sa dotknutej osoby, by sa malo zistiť, či sú fyzické osoby sledované na internete vrátane prípadného následného využitia technologických riešení spracúvania osobných údajov, ktoré spočívajú v profilovaní fyzickej osoby na účely prijatia rozhodnutia týkajúceho sa tejto osoby alebo na účely analýzy predvídania osobných preferencií, správania a postojov tejto osoby.*
- **Pseudonymizácia je:** spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe. *Inak povedané, pseudonymizácia znamená zmenu identifikátorov (rodného čísla, mena a priezviska, dátumov narodenia, trvalého bydliska a pod.) na nové označenie, prednostne formou zakódovania tak, aby príjemca údajov nemohol určiť konkrétnu osobu.*
- Toto nariadenie sa neuplatňuje na osobné údaje zosnulých osôb. § 78 ods.7 nového zákona o OOÚ – „ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba vyslovila nesúhlas“ (§ 116 Občianskeho zákonníka).
- **Právo na zabudnutie -** dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, **ak je splnený niektorý z týchto dôvodov**:
    - osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
    - dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), a ak neexistuje iný právny základ pre spracúvanie;
    - dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2;
    - osobné údaje sa spracúvali nezákonne;
    - osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;
    - osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1.

NOVÉ PRÁVNE ZÁKLADY PODĽA GPDR

- Prevádzkovateľ v prípade spracúvania osobných údajov bude musieť použiť iný primeraný právny základ „**oprávnený záujem**“ alebo „**zákonná povinnosť**“, alebo **„súhlas dotknutej osoby.**
- Dotknutá osoba má právo kedykoľvek odvolať svoj súhlas. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním. Pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie.
- Novinkou je, že dotknutá osoba môže v niektorých prípadoch udeliť **výslovný súhlas** so spracúvaním osobných údajov na jeden alebo viacero určených účelov.
- INFORMOVANIE DOTKNUTÝCH OSOB
- Čl. 13 všeobecného nariadenia o ochrane údajov ustanovuje tzv. **informačnú povinnos**ť prevádzkovateľa a určuje informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby.
- V prípade, že prevádzkovateľ od dotknutej osoby získava osobné údaje je povinný poskytnúť jej všetky tieto informácie**:**
  a) **Totožnosť a kontaktné údaje** prevádzkovateľa;
  b) Kontaktné údaje zodpovednej osoby;
  c) **Účely spracovania**, na ktoré sú osobné údaje určené;
  d) **Právny základ** spracúvania osobných údajov;
  e) Ak sa spracúvanie zakladá na právnom titule **oprávneného záujmu** prevádzkovateľa, ktoré sleduje prevádzkovateľ alebo tretia strana;
  f) **Príjemcov** alebo kategórie príjemcov osobných údajov;
  g) V relevantnom prípade informáciu o tom, že prevádzkovateľ zamýšľa **preniesť osobné údaje do tretej krajiny;**
  h) **Dobu uchovávania** osobných údajov, alebo ak to nie je možné kritéria na jej určenie;
  i) **Existenciu práva** požadovať od prevádzkovateľa **prístup** k osobným údajom týkajúcim sa dotknutej osoby a **práva na ich opravu** alebo **vymazanie**, alebo **obmedzenie spracúvania**, alebo **práva namietať proti spracúvaniu**, ako aj **práva na prenosnosť údajov**;
  j) Ak je spracúvanie založené na súhlase dotknutej osoby, existencia práva kedykoľvek **svoj súhlas odvolať** bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
  k) Právo **podať návrh na začatie konania** Úradu na ochranu osobných údajov SR;
  l) To či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou**,** alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a to či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia;
  m) Existenciu **automatizovaného individuálneho rozhodovania vrátane profilovania** týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

PRÁVA DOTKNUTEJ OSOBY

Novou právnou úpravou sa rozšírili a spresnili jednotlivé práva dotknutých osôb, a to:

- právo na opravu;
- právo na výmaz;
- právo na obmedzenie spracúvania;
- právo na prenosnosť údajov;
- právo namietať;
- právo namietať automatizované individuálne rozhodovanie a profilovanie.

- Zakotvila sa nová oznamovacia povinnosť prevádzkovateľa v súvislosti s opravou alebo vymazaním alebo obmedzením spracúvania osobných údajov dotknutých osôb, a to tak voči príjemcom, ktorým osobné údaje boli poskytnuté, ako aj voči samotnej dotknutej osobe.

POVINNOSŤ DODRŽIAVAŤ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

- Každé spracúvanie osobných údajov musí byť zabezpečené **zákonným, spravodlivým a transparentným** spôsobom**,** aby nedošlo k porušeniu základných práv dotknutej osobe.
- **Obmedzenie účelu** - osobné údaje získavať len na konkrétne určený, výslovne uvedený a oprávnený účel, aby bolo z neho jasné, aké spracovateľské operácie budú a nebudú prebiehať. Ak neboli získané na oprávnený účel je potrebné **zastaviť i**ch spracúvanie.
- **Minimalizácia údajov –** povinnosť dôsledne posúdiť a zvážiť primeraný a obmedzený rozsah osobných údajov, ktoré oprávnená osoba zamýšľa spracúvať na daný účel, v čase vymedzenia účelu spracúvania. Na tento účel využívať **pseudonymizáciu** údajov.
- **Správnosť –** povinnosť spracúvať správne a podľa potreby aktualizované údaje, zabezpečiť opravy nesprávnych osobných údajov z hľadiska ich účelu, na ktorý sú spracované alebo zabezpečiť ich **bezodkladné** vymazanie. Povinnosť overovať správnosť a aktualizáciu osobných údajov.
- **Minimalizácia uchovávania** – povinnosť realizovať uchovávanie osobných údajov vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. **Dodržiavať určené lehoty,** ktoré zodpovedajú potrebe uchovávať osobné údaje aj po skončení účelu ich spracúvania.
- **Integrita a dôvernosť (bezpečnosť)** – dodržiavať primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním osobných údajov a náhodnou stratou, zničením alebo poškodením.

- **Zásada zodpovednosti –** každá oprávnená osoba je zodpovedná za dodržiavanie základných zásad spracúvania osobných údajov a súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov**.** Na požiadanie úradu je povinná preukázať súlad so zásadami spracúvania osobných údajov.

DOKUMENTÁCIA

- Nová právna úprava zakotvila povinnosť ustanoviť zodpovednú osobu vo vybraných prípadoch;
- Na účely preukázania súladu s nariadením viesť a uchovávať záznamy **záznam o spracovateľských činnostiach prevádzkovateľa a záznam o kategóriách spracovateľských činností sprostredkovateľa;**
- **Poverenie fyzických osôb** (poučenie oprávnenej osoby**)** podľa nariadenia **čl. 32 ods.4** - oprávnená osoba na základe poverenia prevádzkovateľa pri spracúvaní osobných údajov postupuje v súlade s pokynmi prevádzkovateľa, nariadením a zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi predpismi a rešpektuje príslušné povinnosti určené prevádzkovateľom.

BEZPEČNOSTNÉ OPATRENIA PODĽA NARIADENIA

- K bezpečnostným opatreniam je potrebné zradiť najmä prijatie **primeraných, technických, organizačných** a **personálnych bezpečnostných opatrení** a **záruk** zo strany prevádzkovateľa ako aj sprostredkovateľa.
- Posúdenie vplyvu na ochranu osobných údajov čl. 35 nariadenia: „Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania, pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov“.

OZNÁMENIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV

- Ochrana osobných údajov je vecou každého z nás. Každý zamestnanec je bez zbytočného odkladu povinný nahlásiť porušenie ochrany osobných údajov. Postup oznámenia bol uvedený **v Smernici na oznamovanie porušenia ochrany osobných údajov**
- V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k vysokému riziku pre práva a slobody fyzických osôb.
- Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

- Spoločnosť spracúva osobné údaje iba za účelom plnenia zákonných povinností, ochrany oprávnených záujmov prevádzkovateľa, ak je spracúvanie nevyhnutné na plnenie zmluvy na základe súhlasu dotknutej osoby.

- Pred každým novým systematickým spracúvaním alebo zmenou spracúvania osobných údajov je príslušný vedúci zamestnanec povinný konzultovať toto spracúvanie so Zodpovednou osobou (Data protection officer) .