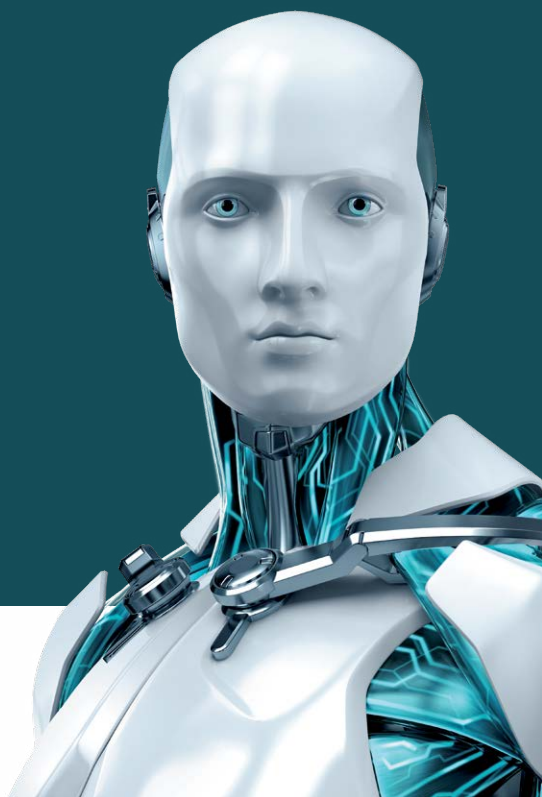
GDPR

marec 2017

GDPR

ČO BUDE PRE VÁŠ BIZNIS ZNAMENAŤ NOVÉ NARIADENIE NA OCHRANU OSOBNÝCH ÚDAJOV?

Viac informácií na tému GDPR
sifrovanie.eset.sk



ESET UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

ALLEN & OVERY

GDPR DESATORO

1. Povinnosť oznamovať porušenie ochrany osobných údajov regulátorovi ako aj jednotlivcom
2. Zmenené podmienky na nomináciu tzv. zodpovednej osoby
3. Zvýšenie pokút na likvidačnú úroveň
4. Striktnejšie podmienky na poskytovanie súhlasu pri spracúvaní osobných údajov
5. Nové „právo byť zabudnutý“
6. Nová povinnosť „privacy by design and by default“
7. Nové právo na prenosnosť údajov
8. Striktnejšie pravidlá pre sprostredkovateľov
9. Nové pravidlo „one-stop-shop“
10. Zmeny pri prenosoch osobných údajov do zahraničia

Obsah

GDPR desatoro 4
Oznamovanie porušenia osobných údajov 6
Nominácia zodpovednej osoby 7
Zvýšenie pokút na likvidačnú úroveň. 8
Striktnejšie požiadavky na súhlas pri spracúvaní osobných údajov 9
Právo byť zabudnutý (právo na výmaz) 11
„Privacy by design and by default“ 12
Právo na prenosnosť údajov 13
Nové zodpovednosti pre sprostredkovateľov 14
Nové pravidlo „one-stop-shop“ (jednotné kontaktné miesto) 15
Medzinárodné prenosy dát 17

GDPR DESATORO

Po štyroch rokoch kontroverzných diskusií ohľadne toho, ako by mala vyzerať nová právna úprava pre ochranu osobných údajov, bol text nového nariadenia **(GDPR)**[1] schválený a začne sa uplatňovať od 25. mája 2018. GDPR nahradí zákon č. 122/2013 Z.z. o ochrane osobných údajov, ktorý bude zrušený. Keďže ide o nariadenie, nemusí ho implementovať každá členská krajina EÚ a od dátumu účinnosti je priamo vykonateľné.

GDPR nie je iba ďalšou novelou v oblasti ochrany osobných údajov, ale znamená menšiu revolúciu v oblasti ochrany dát. Takáto posilnená ochrana však ide ruka v ruke s početnými novými povinnosťami pre spoločnosti, ktoré spracúvajú osobné údaje.

Aj keď GDPR bude mať najväčší dopad pre veľké spoločnosti, ktoré spracúvajú značné množstvo osobných údajov, ako sú napríklad banky, farmaceutické a telekomunikačné spoločnosti, nezanedbateľné množstvo nových povinností prinesie aj pre menšie a stredné podniky ako napríklad e-shopy alebo marketingové spoločnosti. Je to preto, že GDPR sa bude aplikovať na každého, kto spracúva osobné údaje. Dá sa povedať, že dnes už ťažko existuje spoločnosť, ktorá by osobné údaje nespracúvala. Ak máte zamestnancov alebo zákazníkov, je veľmi pravdepodobné, že osobné údaje spracúvate. Teda bude len malý počet spoločností, ktoré budú môcť text GDPR odignorovať.

Čo je „osobný údaj“

Definícia pojmu osobný údaj je už teraz veľmi široká a GDPR tento koncept do budúcna určite nezúži.

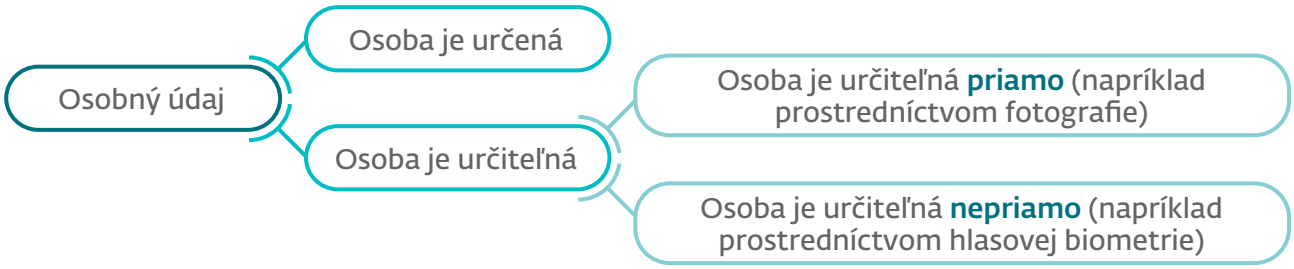
Zákon o ochrane osobných údajov definuje osobný údaj ako údaj týkajúci sa určenej alebo určiteľnej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Medzi osobné údaje podľa GDPR patria napríklad:

- *meno, priezvisko*
- *fotografia*
- *e-mailová adresa*
- *telefónne číslo*
- *číslo účtu*
- *odtlačok prsta*
- *hlas*
- *lokalizačné údaje*

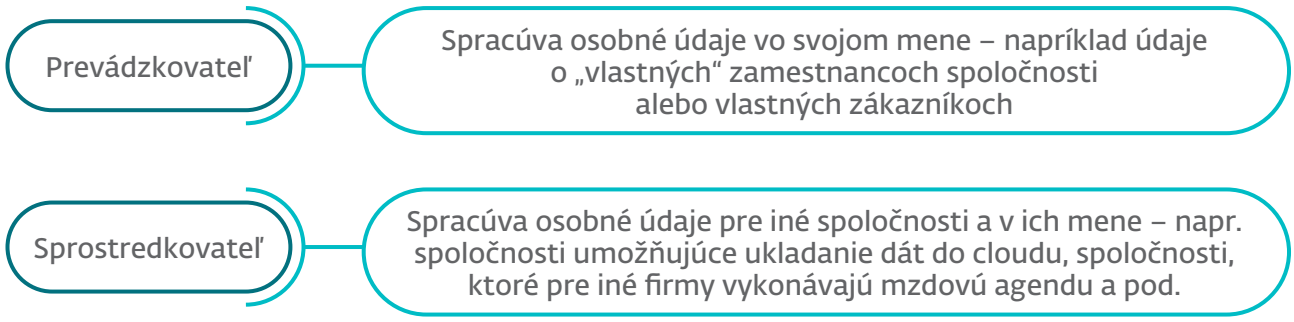
Ako bolo vyššie uvedené, GDPR tento koncept širokého poňatia definície osobného údaju nezmení. Okrem „tradičných“ osobných údajov, ktorými vieme fyzickú osobu priamo identifikovať, ako sú napríklad meno, priezvisko, fotografia či e-mailová adresa, sa GDPR bude vzťahovať aj na údaje, na základe ktorých možno identifikovať osobu nepriamo, prostredníctvom tretích osôb, napríklad telefónne číslo, číslo účtu, odtlačok prsta, hlas či lokalizačné údaje. Pseudonymizované údaje (ako napríklad kódované údaje využívajúce sa pri klinickom skúšaní) budú rovnako osobné údaje ak existuje možnosť, prostredníctvom tretích osôb, sa prepracovať k menu osoby (napríklad k menu pacienta, ktorý sa zúčastnil klinického skúšania). Údaje ako agregované štatistiky však budú mimo rámca GDPR.

1 Nariadenie Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).



GDPR sa bude týkať tak prevádzkovateľov ako aj sprostredkovateľov

Zákon o ochrane osobných údajov sa síce vzťahoval tak na spoločnosti, ktoré spracúvajú osobné údaje vo svojom mene - **prevádzkovatelia** (teda spracúvajú „vlastné" osobné údaje ako napríklad zamestnanci spoločnosti alebo vlastní zákazníci), ako aj na spoločnosti, ktoré spracúvajú dáta pre iné spoločnosti – **sprostredkovatelia** (napr. spoločnosti umožňujúce ukladanie dát do cloudu, spoločnosti ktoré pre iné firmy vykonávajú mzdovú agendu alebo outsourcované call centrá), avšak väčšina povinností (ako aj zodpovednosť) bola na prevádzkovateľoch.



GDPR toto nastavenie zásadne mení a sprostredkovatelia budú v ochrane osobných údajov zohrávať omnoho aktívnejšiu úlohu. Rovnako budú mať širšiu zodpovednosť za dáta, ktoré spracúvajú. Je teda na mieste povedať, že len málo spoločností GDPR „unikne".

Ako bolo vyššie uvedené, GDPR prinesie veľký počet zmien a tieto budú mať dosah takmer na každú firmu a organizáciu. V tejto analýze je obsiahnutých 10 najdôležitejších z týchto zmien:

1. Povinnosť oznamovať porušenie ochrany osobných údajov regulátorovi ako aj jednotlivcom
2. Zmenené podmienky na nomináciu tzv. zodpovednej osoby
3. Zvýšenie pokút na likvidačnú úroveň
4. Striktnejšie podmienky na poskytovanie súhlasu pri spracúvaní osobných údajov
5. Nové „právo byť zabudnutý"
6. Nová povinnosť „privacy by design and by default"
7. Nové právo na prenosnosť údajov
8. Striktnejšie pravidlá pre sprostredkovateľov
9. Nové pravidlo „one-stop-shop"
10. Zmeny pri prenosoch osobných údajov do zahraničia

1. OZNAMOVANIE PORUŠENIA OSOBNÝCH ÚDAJOV

1.1 Povinnosť oznámenia incidentu regulátorovi

Povinnosť oznamovať incidenty porušenia osobných údajov[2] spoločnosti spracúvajúce osobné údaje momentálne podľa zákona o ochrane osobných údajov nemajú[3]. Takúto povinnosť však prinesie GDPR. Povinnosť oznamovania incidentov sa však nebude vzťahovať iba na „zásadné" porušenia ako napríklad strata či únik údajov alebo krádež identity, ale bude zahŕňať takmer každé porušenie osobných údajov (napríklad aj výmenu obálok určených pre dve rôzne osoby bankou alebo prístup neoprávnenou osobou k databáze obsahujúcej osobné údaje), ibaže by bolo preukázané, že je nepravdepodobné, že incident spôsobí riziko pre práva a slobody jednotlivcov, ktorých sa týka.

Incidenty, ktoré bude potrebné oznámiť, budú zahŕňať takmer každé porušenie, bez ohľadu či sa jedná o veľkú spoločnosť, alebo o malý či stredný podnik. Teda v prípade, že spoločnostiam po máji 2018 dáta (respektíve ich časť) uniknú alebo ich stratia, alebo nastane iné porušenie osobných údajov, nebude môcť takúto situáciu riešiť spoločnosť iba interne ako tomu bolo doteraz, ale bude musieť informovať o takomto incidente príslušný dozorný orgán, ktorým je u nás Úrad na ochranu osobných údajov Slovenskej republiky (ďalej aj „**Úrad**").

Takáto informácia musí byť Úradu oznámená bez zbytočného odkladu, avšak nie dlhšie ako 72 hodín od momentu, keď sa spoločnosť o porušení dozvedela. Ak by táto lehota nemohla byť dodržaná, musí byť omeškanie oznámenia (teda dôvody, prečo nebolo možné oznámiť to do 72 hodín) zdôvodnené.

1.2 Povinnosť oznámenia incidentu jednotlivcom, ktorých dát sa incident týka

Okrem oznámenia porušenia osobných údajov Úradu budú musieť byť v niektorých prípadoch informovaní o porušení aj jednotlivci, ktorých dáta sú incidentom dotknuté. Bude to v prípadoch, kedy existuje vysoké riziko pre práva a slobody dotknutých osôb. Teda pokým oznámenie Úradu bude potrebné vykonať takmer pri každom porušení, oznámenie jednotlivcom bude potrebné vykonať len v tých najzávažnejších prípadoch.

Ak však existuje povinnosť oznámiť incident jednotlivcom, takéto oznámenie nemôže byť urobené komplikovaným technickým alebo právnym jazykom. Oznámenie musí byť pre jednotlivcov zrozumiteľné a musí obsahovať jednoducho formulovaný opis povahy porušenia.

Oznámenie jednotlivcom sa v niektorých prípadoch vyžadovať nebude (a to aj napriek tomu, že existuje vysoké riziko pre práva jednotlivcov). Sú to takéto prípady:

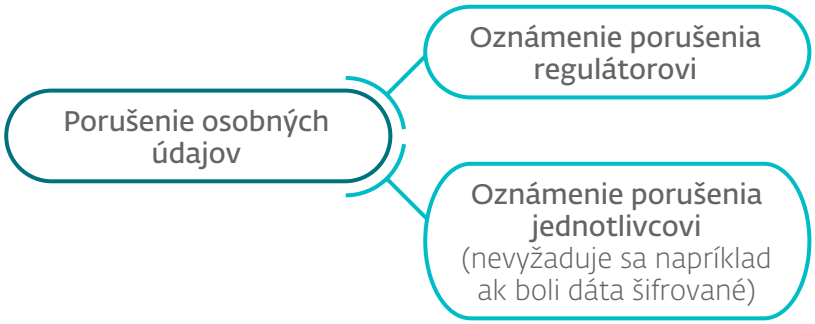
a. Incident sa stal napriek tomu, že boli implementované primerané technické a organizačné bezpečnostné opatrenia (ako je napríklad šifrovanie), a to najmä tie opatrenia na základe ktorých sú osobné údaje, ktoré sú súčasťou incidentu, nečitateľné pre akúkoľvek inú osobu;

b. Po incidente boli prijaté následné opatrenia, ktorými sa zabezpečilo, že vysoké riziko pre práva a slobody dotknutých osôb sa pravdepodobne nezmaterializuje;

2 „**Porušenie ochrany osobných údajov**" (angl. personal data breach) GDPR definuje ako porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

3 Istou výnimkou sú v tomto smere spoločnosti, ktoré spadajú pod reguláciu zákona č. 351/2011 Z.z. o elektronických komunikáciách, na základe ktorého povinnosť oznamovať niektoré incidenty existovala už predtým.

c. Oznámenie jednotlivcom by vyžadovalo neprimerané úsilie zo strany spoločnosti, kde porušenie nastalo. V takom prípade dôjde namiesto toho k verejnému oznámeniu o incidente alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.



1.3 Odporúčania

Každá spoločnosť by mala do mája 2018 vypracovať interný plán pre oznamovanie a následné riešenie incidentov, ktoré zahŕňajú porušenie ochrany osobných údajov[4].

2. NOMINÁCIA ZODPOVEDNEJ OSOBY

To, že spoločnosti musia mať zodpovednú osobu nie je novou povinnosťou, nakoľko s nominovaním zodpovednej osoby počíta v niektorých prípadoch aj zákon na ochranu osobných údajov. Podľa neho dokonca zodpovedná osoba musí absolvovať skúšku na Úrade[5]. Výhoda nominácie zodpovednej osoby (oproti stavu, kde spoločnosť zodpovednú osobu nemá) podľa zákona o ochrane osobných údajov bola, že spoločnosti nemuseli na Úrade oznamovať informačné systémy obsahujúce osobné údaje. Malo sa totižto za to, že na tieto informačné systémy dohliada zodpovedná osoba, a teda Úrad o nich nemusí mať znalosť.

2.1 Kedy je potrebné mať zodpovednú osobu?

GDPR však tieto podmienky mení. V porovnaní so súčasným stavom, veľa spoločností, ktoré predtým zodpovednú osobu mali, respektíve rozhodli sa ju nominovať, ju už nebudú musieť mať. Ďalšou zmenou je, že zodpovednou osobou môže byť aj právnická osoba. Zodpovedné osoby budú musieť nominovať nielen prevádzkovatelia (ako tomu bolo podľa zákona o osobných údajov), ale aj sprostredkovatelia.

GDPR ukladá povinnosť nominovať zodpovednú osobu v prípadoch, ak:

a. Spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt (okrem súdov). Odporúčanie Pracovnej skupiny 29[6] však uvádza, že aj tie spoločnosti, ktoré nie sú nevyhnutne orgánmi verejnej moci, ale vykonávajú úlohy vo verejnom záujme (ako napríklad verejná doprava alebo dodávka energie), by mali nominovať zodpovednú osobu.

4 Incident identification a incident response plan.

5 Táto skúška podľa GDPR nie je potrebná, avšak zodpovedná osoba musí mať na výkon svojej funkcie náležité odborné kvality a odborné znalosti nielen v oblasti vnútroštátneho, ale aj európskeho práva o ochrane osobných údajov a jeho praktickej aplikácie, ako aj podrobnú znalosť GDPR.

6 Pracovná skupina 29 je poradný orgán zložený zo zástupcov národných úradov na ochranu osobných údajov, kde sekretariátom je Európska komisia. Napriek tomu, že stanoviská Pracovnej skupiny nie sú právne záväzné a majú skôr formu odporúčaní, keďže boli generované expertmi zo všetkých úradov na ochranu osobných údajov členských štátov EÚ, majú vysokú presvedčovaciu silu, sú často citované v právnych stanoviskách a vo všeobecnosti predstavujú harmonizovaný výklad ustanovení na ochranu osobných údajov.

b. Hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je pravidelné alebo systematické monitorovanie[7] jednotlivcov vo veľkom rozsahu (napríklad na regionálnej, vnútroštátnej alebo nadnárodnej úrovni), ktoré by mohli ovplyvniť veľký počet osôb, respektíve týkajúce sa veľkého objemu údajov. Do tejto kategórie bude spadať napríklad činnosť internetového vyhľadávača pre účely cielenej (behaviorálnej) reklamy, úverové bodovanie, smart autá a podobne.

c. Hlavnou činnosťou prevádzkovateľa alebo sprostredkovateľa je spracúvanie citlivých údajov (ako napríklad údaje o zdravotnom stave alebo biometrické údaje) vo veľkom rozsahu alebo spracúvanie údajov týkajúcich sa uznania viny za trestné činy a priestupky.

Zodpovedná osoba ako taká nie je zodpovedná za prípadný nesúlad s GDPR. Je úlohou spoločnosti ako takej (teda prevádzkovateľa alebo sprostredkovateľa) zabezpečiť súlad s GDPR.

Zodpovedná osoba nesmie v súvislosti s plnením svojich úloh dostávať žiadne pokyny a musí vykonávať svoje úlohy nezávisle.

2.2 Odporúčania

Spoločnosti, ktoré podľa GDPR budú musieť nominovať zodpovednú osobu, by sa mali rozhodnúť, či túto úlohu zveria osobe (zamestnancovi) v rámci spoločnosti alebo budú túto úlohu outsourcovať externej fyzickej osobe/spoločnosti.

3. ZVÝŠENIE POKÚT NA LIKVIDAČNÚ ÚROVEŇ

Pokuty už podľa zákona o ochrane osobných údajov nie sú nízke a môžu byť udelené (za najvážnejšie porušenia) až vo výške do 200-tisíc eur. GDPR však tieto pokuty posúva ešte vyššie. Preto by sa súladom s GDPR mali zaoberať nielen nižšie, ale aj výkonné orgány spoločností (ako napríklad predstavenstvo alebo spoločníci).

Pokuty za porušenia podľa GDPR sú takéto:

a. Pokuta až do výšky **20 miliónov eur**, alebo v prípade spoločnosti až do výšky **4% celosvetového ročného obratu** v predchádzajúcom finančnom roku, podľa toho, ktorá suma je vyššia. Takáto pokuta bude uložená napríklad v takýchto prípadoch:

- **I.** keď neboli splnené podmienky súhlasu so spracovaním, alebo
- **II.** keď boli porušené zásady prenosu dát mimo územia Európskej únie.[8]

b. Pokuta až do výšky **10 miliónov eur**, alebo v prípade spoločnosti až do výšky **2% celosvetového ročného obratu** v predchádzajúcom finančnom roku, podľa toho, ktorá suma je vyššia. Takáto pokuta bude uložená napríklad v prípadoch:

- **I.** nedostatočná zmluva so sprostredkovateľom, ktorá nespĺňa podmienky podľa GDPR,
- **II.** nezabezpečenie dostatočnej bezpečnosti spracúvaných osobných údajov (**okrem iného napríklad aj šifrovaním**),

7 Napríklad sledovanie správania osoby prostredníctvom tracking alebo profiling (pre účely prijatia rozhodnutia týkajúceho sa tejto osoby alebo pre účely analýzy či predvídania osobných preferencií, správania a postojov tejto osoby) .

8 Resp. mimo krajín Európskeho hospodárskeho priestoru (**EHP**).

III. neoznámenie porušenia ochrany osobných údajov,

IV. nenominovanie zodpovednej osoby v tých prípadoch kde to GDPR vyžaduje.

Pri rozhodovaní o uložení pokuty a jej výške sa v každom jednotlivom prípade náležite zohľadnia viaceré skutočnosti. Týmito skutočnosťami sú napríklad povaha, závažnosť a trvanie porušenia, počet dotknutých osôb a úmyselný prípadne nedbanlivostný charakter porušenia. Ďalej bude zohľadnená miera zodpovednosti prevádzkovateľa alebo sprostredkovateľa so zreteľom na technické a organizačné opatrenia, ktoré prijali, ako aj akékoľvek kroky, ktoré prevádzkovateľ alebo sprostredkovateľ podnikol s cieľom zmierniť škodu, ktorú dotknuté osoby utrpeli.

Pokuty však nie sú jediným dôvodom, pre ktorý by spoločnosti mali dbať na zabezpečenie súladu s GDPR. Aj keby sa Úrad rozhodol v konkrétnom prípade pokutu neudeliť, má ďalšie právomoci, ktoré môžu byť v konkrétnom prípade pre spoločnosť ešte závažnejšie ako udelenie pokuty. Jedná sa napríklad o nasledujúce právomoci Úradu:

a. nariadiť dočasné alebo trvalé obmedzenie vrátane zákazu spracúvania;
b. nariadiť vymazanie osobných údajov;
c. nariadiť prevádzkovateľovi, aby porušenie ochrany osobných údajov oznámil dotknutej osobe;
d. nariadiť pozastavenie toku údajov príjemcovi v tretej krajine.

3.2 Odporúčania

Spoločnosť by mala výšku takýchto pokút dať do pozornosti výkonným orgánom spoločnosti, aby prípadne tieto orgány vedeli prerozdeliť rozpočet na zabezpečenie súladu s GDPR informovaným spôsobom.

4. STRIKTNEJŠIE POŽIADAVKY NA SÚHLAS PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Podmienky udelenia platného súhlasu sa podľa GDPR sprísnia[9]. Súhlas podľa GDPR je slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týkajú. Nemení sa fakt, že súhlas musí byť preukázateľný, a teda prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.

9 Je to aj napriek tomu, že definícia súhlasu podľa GDPR sa oproti definícii podľa zákona o ochrane osobných údajov markantne nezmení. GDPR však k tejto definícii pridáva mnoho ďalších podmienok.

4.1 Ktorý súhlas bude možné považovať za platný?

Súhlas by sa mal poskytnúť jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním osobných údajov. Súhlas môže byť poskytnutý napríklad:

a. písomným vyhlásením. Ak dá dotknutá osoba súhlas v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, súhlas musí byť predložený tak, aby bol jasne odlíšiteľný od iných skutočností. Zároveň musí tento súhlas byť v zrozumiteľnej a ľahko dostupnej forme a formulovaný jasne a jednoducho[10]. Ak tak prevádzkovateľ neučiní, súhlas bude neplatný;

b. ústnym vyhlásením[11],

c. označením (zakliknutím) políčka[12],

d. akýmkoľvek iným vyhlásením či úkonom, ktorý jasne znamená, že dotknutá osoba súhlasí s navrhovaným spracúvaním jej osobných údajov.

Mlčanie, vopred označené políčka (pre-ticked boxes), nebudú považované za súhlas.

GDPR obsahuje špecifické podmienky pre **súhlas udelený dieťaťom** pri poskytovaní služieb informačnej spoločnosti. Ak má dieťa menej než 16 rokov, spracúvanie je zákonné iba za podmienky, že súhlas vyjadril alebo schválil rodič[13].

Ako je uvedené vyššie, jednou z podmienok platnosti súhlasu je, aby bol poskytnutý slobodne. V tejto súvislosti vzniká otázka, ako bude posudzovaný súhlas v prípade, ak medzi postavením dotknutej osoby a prevádzkovateľom existuje jednoznačný nepomer, najmä v **zamestnaneckom kontexte**[14]. Preto v týchto prípadoch často nebude možné použiť súhlas ako základ pre spracúvanie osobných údajov, ale vhodnejším právnym základom bude napríklad pracovná zmluva.

Pre spracúvanie citlivých osobných údajov[15] sa podmienky súhlasu v zásade nemenia, tak zákon na ochranu osobných údajov ako GDPR vyžadujú výslovný súhlas.

4.2 Možnosť odvolania súhlasu

Dotknutá osoba má podľa GDPR právo kedykoľvek svoj súhlas odvolať, čo jej musí byť pred poskytnutím súhlasu špecificky oznámené. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie. Odvolanie súhlasu však nebude mať vplyv na zákonnosť spracúvania pred jeho odvolaním.

10 Napríklad súhlas v cudzom jazyku, ktorému jedinec nerozumie, nebude spĺňať predpoklady GDPR.

11 Takéto ústne prehlásenie však musí spĺňať podmienku preukázateľnosti. To by bolo možné napríklad nahraním telefonického rozhovoru. Telefonický rozhovor však možno nahrať len s predchádzajúcom súhlasom osoby, ktorá má poskytnúť súhlas.

12 Ticking a box.

13 Alebo iný nositeľ rodičovských práv a povinností. Členské štáty môžu právnym predpisom stanoviť na tieto účely nižšiu vekovú hranicu za predpokladu, že takáto nižšia veková hranica nie je menej než 13 rokov.

14 Alebo ak je prevádzkovateľ orgánom verejnej moci.

15 Citlivé osobné údaje GDPR definuje ako tie, 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 alebo sexuálnej orientácie fyzickej osoby.

4.3 Odporúčania

Získať súhlas, ktorý spĺňa všetky atribúty GDPR nebude také jednoduché ako podľa zákona o ochrane osobných údajov. Súčasné súhlasy budú môcť byť považované za platné len do tej miery, pokiaľ budú reflektovať nové požiadavky GDPR. V opačnom prípade bude **potrebné vyžiadať si nové súhlasy**.

Nakoľko súhlasy podľa zákona o ochrane osobných údajov nemuseli obsahovať toľko informácií ako podľa GDPR, je dôvodný predpoklad, že veľa súhlasov bude musieť byť získaných opätovne. Nakoľko takýto postup môže byť administratívne a časovo náročný, a to najmä pre spoločnosti s veľkými databázami dát, spoločnosti by sa mali zamyslieť nad možnými inými možnosťami, ako spracúvať osobné údaje[16].

5. PRÁVO BYŤ ZABUDNUTÝ (PRÁVO NA VÝMAZ)

Aj keď nové "právo byť zabudnutý" bolo prezentované ako jedna z noviniek, ktorú GDPR priniesla, nejedná sa o úplne nový inštitút, ktorý by zákon o ochrane osobných údajov predtým vôbec nepoznal. Ten poznal právo na výmaz. Právo byť zabudnutý však nie je iba nový názov pre právo na výmaz osobných údajov. Právo byť zabudnutý podľa GDPR je koncipované širšie ako právo na výmaz a je detailnejšie upravené.

5.1 V ktorých prípadoch možno žiadať o "zabudnutie"?

Toto právo nebude môcť jednotlivec využiť vo všetkých prípadoch, keď je výmaz podľa jeho posúdenia vhodný. Právo na výmaz sa môže uplatniť ak sú dáta, ktoré sa jednotlivca týkajú, spracúvané protizákonne (napríklad už nie sú potrebné pre účel, na ktorý boli získané), alebo keď osoba odvolá súhlas na spracúvanie. Výmaz dát musí prevádzkovateľ vykonať bez zbytočného odkladu, avšak do jedného mesiaca od obdržania žiadosti[17].

Špecifický režim pre „zabudnutie" majú dáta, ktoré boli už zverejnené. Keď prevádzkovateľ dostane od jednotlivca žiadosť o výmaz (zabudnutie) údajov, ktoré boli už zverejnené, musí okrem toho, že žiadosť posúdi sám, informovať aj iných prevádzkovateľov, ktorí tieto osobné údaje spracúvajú, o tom, že dotknutá osoba žiada ich vymazanie. Táto povinnosť sa uplatní nielen pre „pôvodné" osobné údaje, ale aj na akékoľvek kópie alebo linky, kde sa dáta jednotlivca nachádzajú. Pri rozhodovaní o takejto žiadosti sa však musí brať do úvahy dostupná technológia a náklady (cena) tak, aby bola splnená podmienka primeranosti a proporcionality. Teda ak by vyhovenie žiadosti o zabudnutie malo byť spojené s neprimeranými nákladmi alebo komplexnými technickými prostriedkami, takejto žiadosti nebude nutné vyhovieť.

Napriek tomu sa predpokladá, že zabezpečenie súladu so žiadosťou o zabudnutie nebude pre spoločnosti jednoduché. Bude skôr obtiažne identifikovať (vzhľadom na fakt, že dáta sú zverejnené), ktorým ďalším prevádzkovateľom musí „pôvodný" prevádzkovateľ oznámiť, že jednotlivec žiada o zabudnutie. Rovnako posúdenie, ktorá žiadosť znamená neproporčné náklady resp. neprimerané technické prostriedky je subjektívne posúdenie.

16 Napríklad spracúvanie osobných údajov na základe zmluvy alebo na základe legitímnych záujmov prevádzkovateľa alebo inej strany.

17 V nevyhnutných prípadoch, ak je žiadosť komplexná alebo sa týka veľkého počtu dotknutých osôb, táto lehota môže byť predĺžená o ďalšie 2 mesiace.

Právo byť zabudnutý však nie je absolútnym právom jednotlivca. Neznamená to, že akonáhle osoba zašle žiadosť o vymazanie, prevádzkovateľ musí automaticky dáta mazať. Ak by napríklad právo byť zabudnutý kolidovalo so slobodou prejavu alebo právom na informácie (napríklad právo byť zabudnutý by vyúsťovalo do cenzúry tlače), takejto žiadosti nemusí byť vyhovené. Rovnako nemusí prevádzkovateľ žiadosti vyhovieť, ak je spracúvanie dát, ktoré je predmetom žiadosti o vymazanie, potrebné z dôvodov verejného záujmu v oblasti verejného zdravia alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

5.2 Odporúčania

Spoločnosti, ktoré by mohli dostávať veľký počet takýchto žiadostí (napríklad internetové vyhľadávače, sociálne siete, internetové blogy a pod.) by si mali stanoviť, ako budú v budúcnosti narábať s takýmito žiadosťami formou interných smerníc a zaškoliť zamestnancov. Ak sa počíta s veľkým počtom takýchto žiadostí, zjednodušením by mohlo byť aj vytvorenie jednotného formulára pre takéto žiadosti. Rovnako treba rátať aj s faktom, že GDPR sa nebude vzťahovať len na spoločnosti usídlené v EÚ, ale v niektorých prípadoch aj pre spoločnosti usídlené mimo územia EÚ[18].

6. „PRIVACY BY DESIGN AND BY DEFAULT“

Povinnosť zabezpečiť „privacy by design and by default“ momentálne v zákone o ochrane osobných údajov nie je obsiahnutá. Ten rovnako špecificky neobsahuje požiadavku, že ochrana súkromia musí byť komplexne zvažovaná už pri koncipovaní projektov od ich raného štádia.

So zreteľom na povahu, na rozsah a účel spracúvania ako aj na riziká, ktoré sú so spracúvaním spojené, prevádzkovateľ musí určiť primerané technické a organizačné opatrenia pre každú formu spracúvania. Tieto opatrenia musia byť prevádzkovateľom vybraté na základe najnovších poznatkov a technológií, avšak aj s prihliadnutím na ich cenu. Takýmito opatreniami sú okrem iného:

a. **Pseudonymizácia[19] údajov** (čo je napríklad kódovanie údajov[20]) tam, kde je to vhodné;
b. **Minimalizácia údajov**, čo znamená, že prevádzkovateľ implementuje primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne jeho systémy budú spracúvať len osobné údaje, ktoré sú nevyhnutne potrebné (a žiadne iné) pre každý konkrétny účel spracúvania. Rovnako tieto systémy musia zabezpečiť, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu. Rovnako musia takéto opatrenia zabezpečiť, aby osobné údaje neboli štandardne prístupné neobmedzenému počtu zamestnancov prevádzkovateľa, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom.

18 GDPR sa bude vzťahovať na spracúvanie osobných údajov dotknutých osôb prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v EÚ ak spracúvanie súvisí: a) s ponukou tovaru alebo služieb osobám v EÚ bez ohľadu na to, či sa vyžaduje platba, alebo b) so sledovaním ich správania, pokiaľ ide o ich správanie na území EÚ.

19 „**Pseudonymizácia**“ je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na netechnické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

20 Kódovanie údajov sa často vykonáva napríklad v prípade klinického skúšania na „anonymné“ označenie pacientov, ktorí sú zahrnutí do programu. Identifikácia (priama) nie je možná, avšak dodatočne je možné dopracovať sa ku konkrétnemu kódu, ktorým sa následne identifikuje meno konkrétneho pacienta.

Inherentnou súčasťou „privacy by design and by default" je aj povinnosť v niektorých prípadoch vypracovať takzvané „**posúdenie vplyvu na ochranu osobných údajov**" (**impact assesment**). Takého hodnotenie vplyvov je potrebné na posúdenie rizík, ktoré niektoré formy spracúvania osobných údajov môžu obnášať, s cieľom vyhodnotiť najrizikovejšie projekty[21]. Takýto dokument bude obsahovať opis plánovaných spracovateľských operácií a účely spracúvania, posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu, ako aj posúdenie rizika pre práva a slobody jednotlivcov. Takýto dokument musí obsahovať aj opatrenia na riešenie identifikovaných rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov.

Spoločnosť môže využiť nový certifikačný mechanizmus, ktorý zavádza GDPR[22] ako napríklad schválené pečate a značky na preukázanie súladu s požiadavkami „privacy by design and by default".

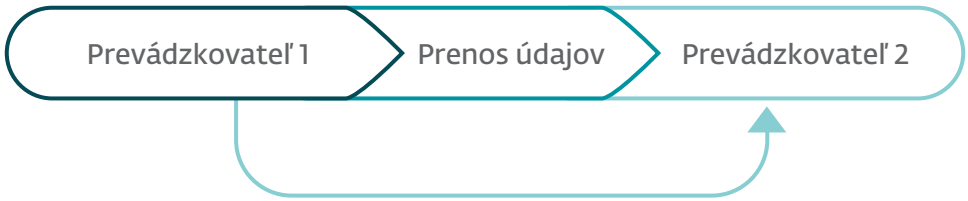
6.2 Odporúčania

Spoločnosti by si mali interne prejsť, či ich systémy nespracúvajú viac dát ako je potrebné[23] alebo či nie sú tieto dáta uchovávané príliš dlhú dobu. Rovnako bude potrebné zvážiť, či by nebolo vhodné dáta zakódovať (pseudonymizovať) a pracovať s takto upravenými dátami. Tímy pracujúce na projektoch, ktoré zahŕňajú spracovanie osobných údajov, by mali zahŕňať odborníkov z oblasti ochrany osobných údajov, a to už od raných štádií projektu (a nielen v ich finálnej fáze).[24]

7. PRÁVO NA PRENOSNOSŤ ÚDAJOV

Právo na prenosnosť údajov je úplne novým právom podľa GDPR, ktoré v zákone na ochranu osobných údajov nebolo obsiahnuté. Do istej miery obsahuje črty práva na prístup k údajom, avšak je omnoho širšie.

Podľa tohto nového práva, dotknutá osoba bude mať právo získať osobné údaje, ktoré sa jej týkajú, a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi. Takémuto prenosu nesmie „pôvodný" prevádzkovateľ brániť a dokonca musí jednotlivca špecificky upozorniť, že takéto právo má (a to najmä pri zatvorení účtu).



21 Posúdenie vplyvu je potrebné v prípade (i) systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania, a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby; (ii) spracúvania citlivých osobných údajov vo veľkom rozsahu, alebo (iii) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

22 Certifikačné mechanizmy na účely preukázania súladu s GDPR.

23 T.z. či sú spracúvané iba „must have" dáta (a nie „nice to have" dáta).

24 Právo na prenosnosť bude však zahŕňať len tie dáta, ktoré boli poskytnuté na základe súhlasu jednotlivca alebo na základe zmluvy s jednotlivcom.

V praxi sa bude jednať o mnoho situácií, kedy budú chcieť jednotlivci takéto právo využiť na presun svojich dát. Bude to napríklad pri presune existujúcich e-mailov (e-mail box) od jedného prevádzkovateľa k inému, respektíve pri presune transakcií platieb od súčasnej banky jednotlivca do novo vybranej banky. Takýto e-mail box, respektíve jednotlivé transakcie, bude musieť pôvodný prevádzkovateľ presunúť k subjektu, ktorý určí jednotlivec, a bude tak musieť urobiť bez zbytočného odkladu, avšak najneskôr v lehote 1 mesiaca od obdržania žiadosti[25] a zdarma[26]. Presun bude musieť byť v takom formáte, ktorý bude novým providerom použiteľný (teda napríklad pre presun e-mail boxu nie v pdf formáte, ale vo formáte, ktorý uchováva metadáta).

Niektoré dáta však evidentne nebudú spadať do rozsahu práva na prenosnosť. Budú to napríklad dáta, ktoré vytvoril sám prevádzkovateľ (aj keď na základe dát, ktoré poskytol jednotlivec)[27].

7.1 Odporúčania

Takéto právo sa s najväčšou pravdepodobnosťou nestretne s veľkým nadšením u viacerých spoločností, a to najmä tých, ktorých databázy obsahujú veľké množstvo osobných údajov. Okrem administratívnej záťaže, ktorú toto nové právo prinesie, je potrebné rátať aj s tým, že „pôvodný" prevádzkovateľ bude zodpovedať za akt prenosu k novému prevádzkovateľovi. Je teda potrebné zabezpečiť, aby prenos (transfer) dát ako taký bol bezpečný (**napríklad formou šifrovania**)[28]. Rovnako treba vziať do úvahy, že niektoré prenosy môžu byť z územia EÚ/EHP do krajiny mimo územia EÚ/EHP, kde prevádzkovatelia budú musieť prijať špecifické záruky pre takýto prenos.

8. NOVÉ ZODPOVEDNOSTI PRE SPROSTREDKOVATEĽOV

Podľa zákona o ochrane osobných údajov, väčšinu zodpovedností mali prevádzkovatelia, nakoľko sa jednalo o „ich" údaje (respektíve údaje „ich" klientov alebo zamestnancov). Prevádzkovatelia boli zodpovední za súlad so zákonom o ochrane osobných údajov, a to aj v prípadoch, ak niektoré činnosti (v ich mene) outsourcovali na iné spoločnosti (sprostredkovateľov). GDPR túto situáciu markantne mení a sprostredkovatelia majú po prvýkrát na základe GDPR priame povinnosti ochrany osobných údajov, a to napriek tomu, že nespracúvajú osobné údaje vo vlastnom mene, ale pre niektorého zo svojich klientov. Sú to okrem iných tieto povinnosti:

a. Sprostredkovatelia budú v niektorých prípadoch povinní nominovať zodpovednú osobu rovnako ako prevádzkovatelia.

b. Sprostredkovatelia budú povinní viesť zoznamy spracovateľských operácií, a to pre každého klienta (prevádzkovateľa) zvlášť.

c. V prípade porušenia ochrany osobných údajov musia sprostredkovatelia informovať prevádzkovateľa.

25 V nevyhnutných prípadoch, ak je žiadosť komplexná alebo sa týka veľkého počtu dotknutých osôb, táto lehota môže byť predĺžená o ďalšie 2 mesiace.

26 Ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, prevádzkovateľ môže buď požadovať primeraný poplatok alebo odmietnuť konať. Prevádzkovateľ znáša bremeno preukázania zjavnej neopodstatnenosti alebo neprimeranosti žiadosti.

27 Napríklad informácia o bonite klienta (credit score), resp. posúdenie celkového zdravotného profilu, ktoré vytvoril prevádzkovateľ.

28 Pracovná skupina 29, stanovisko ohľadne prenosnosti údajov z 13. decembra 2016, str. 15. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

8.2 Nové požiadavky pre zmluvu so sprostredkovateľom

Rovnako GDPR reguluje, čo má obsahovať spracovateľská (sprostredkovateľská) zmluva (zmluva medzi prevádzkovateľom a sprostredkovateľom). Obsah tejto zmluvy bude odlišný od požiadaviek zákona o ochrane osobných údajov[29], a teda bude potrebné prepracovať (doplniť) väčšinu spracovateľských zmlúv, ktoré boli uzavreté podľa zákona o ochrane osobných údajov. Nad rámec štandardných požiadaviek[30] spracovateľskej zmluvy bude potrebné do každej takejto zmluvy zahrnúť:

a. že sprostredkovateľ implementoval primerané bezpečnostné opatrenia na ochranu osobných údajov (napríklad pseudonymizáciu, šifrovanie, pravidelné skúšanie a hodnotenie účinnosti technických a organizačných opatrení, či schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu),

b. detaily ohľadne subdodávok, a to najmä v tom zmysle, že ak sprostredkovateľ zapojí ďalšieho sprostredkovateľa, „pôvodný" sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa,

c. záväzok, že po ukončení poskytovania služieb sprostredkovateľ všetky osobné údaje prevádzkovateľa vymaže, alebo vráti prevádzkovateľovi a vymaže existujúce kópie,

d. záväzok sprostredkovateľa, že poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností podľa GDPR a umožní mu vykonať audit.

8.3 Odporúčania

Sprostredkovatelia by mali prejsť celým spektrom svojich činností, ktoré zahŕňajú spracovanie osobných údajov a identifikovať oblasti, na ktoré sa bude vzťahovať GDPR (a predtým sa nevzťahoval zákon o ochrane osobných údajov). Sprostredkovatelia môžu rovnako očakávať zvýšené nároky o súlad s GDPR zo strany svojich klientov ako prevádzkovateľov. Nakoľko spracovateľské zmluvy podľa zákona o ochrane osobných údajov nemusia obsahovať také množstvo detailov ako podľa GDPR, bude potrebné väčšinu z nich revidovať.

9. NOVÉ PRAVIDLO „ONE-STOP-SHOP" (JEDNOTNÉ KONTAKTNÉ MIESTO)

Keď Európska komisia v roku 2012 prišla s prvým textom GDPR, toto znenie obsahovalo princíp „one-stop-shop". Tento pôvodný návrh reflektoval na komplexnosť zabezpečenia súladu so zákonom pri nadnárodných spoločnostiach. Tieto spoločnosti, napriek tomu, že boli členom jednej skupiny a mali jednotné vnútorné procesy a systémy, v každom štáte spadali pod dohľad iného dozorného orgánu. To bránilo efektívnej centralizácii v týchto spoločnostiach a znamenalo vysoké

29 Zákon o ochrane osobných údajov vyžaduje, aby (písomná) spracovateľská zmluva obsahovala: (a) identifikačné údaje zmluvných strán; (b) deň, od ktorého je poskytovateľ cloudových služieb (sprostredkovateľ) oprávnený začať so spracúvaním osobných údajov v mene klienta (prevádzkovateľa) a podmienky spracúvania osobných údajov vrátane zoznamu povolených operácií s osobnými údajmi; (c) účel spracúvania osobných údajov; (d) názov informačného systému; (e) zoznam osobných údajov, ktoré sa budú presúvať do cloudu (pokiaľ to bude vhodnejšie, zoznam možno nahradiť rozsahom osobných údajov), a koho údaje (údaje klienta, údaje zamestnancov atď.) sa spracúvajú; (f) vyhlásenie klienta, že poskytovateľ cloudových služieb bol vybraný na základe jeho odbornej, technickej, organizačnej a personálnej spôsobilosti, a jeho schopnosti zaručiť bezpečnosť spracovania údajov; g) v prípade, že poskytovateľ bude využívať služby subdodávateľa, je potrebný súhlas klienta; (h) dobu, na ktorú sa zmluva uzatvára.

30 Napríklad informácia o predmete a dobe spracúvania, účele spracúvania, type osobných údajov, kategórie dotknutých osôb a práv a povinností prevádzkovateľa.

náklady. Pôvodný návrh systému one-stop-shop menil tento komplexný systém v tom zmysle, že v rámci EÚ budú tieto spoločnosti podliehať kompetencii jedného dozorného orgánu v EÚ.

Tento návrh, aj keď bol pre nadnárodné spoločnosti zaujímavý, sa nakoniec nedostal do finálneho znenia GDPR. Európsky parlament kritizoval jeho prílišnú simplicitu a národné dozorné orgány, najmä v menších krajinách, sa obávali straty akéhokoľvek vplyvu na tieto spoločnosti. Rovnako boli obavy, či by dozorné orgány, napríklad v menších krajinách, boli schopné efektívne regulovať veľké nadnárodné koncerny.

Možno len ťažko tvrdiť, že súčasné znenie princípu one-stop-shop obsahuje očividné zjednodušenie pre spoločnosti usídlené vo viacerých krajinách EÚ, respektíve či skutočne posilní práva jednotlivcov. Namiesto pôvodne plánovaného konceptu, že jeden dozorný orgán preberie zodpovednosť nad všetkými spracovateľskými operáciami, vo všetkých štátoch EÚ, kde nadnárodná spoločnosť pôsobí, súčasné znenie GDPR ustanovuje len:

a. **Vedúci dozorný orgán** (lead supervisory authority), ktorý bude riešiť zásadné otázky a má koordinačnú úlohu (napríklad pri vyšetrovaní, ktoré zahŕňa viacero jurisdikcií), a
b. **Dotknuté dozorné orgány** (supervisory authorities concerned), ktoré budú riešiť zvyšné otázky[31].

Určenie, ktorý orgán je v rámci spoločnosti pôsobiacej vo viac ako v jednom štáte v EÚ[32] vedúcim dozorným orgánom, vôbec nie je podľa GDPR jednoduché. GDPR obsahuje komplexný a relatívne zložitý právnický matrix určenia tohto orgánu, založený na posúdení, kde má spoločnosť **miesto centrálnej správy v EÚ** (teda ktoré je miesto, kde sa prijímajú rozhodnutia[33]).

Je zrejme nemožné predpokladať, že systém one-stop-shop podľa GDPR nepovedie k „forum shopping". Spoločnosti sa zrejme budú snažiť svoju argumentáciu viesť smerom, aby sa vyhli dozorným orgánom v členských štátoch EÚ, ktoré sú tradične známe svojím anti-business friendly prístupom ako ich vedúcim dozorným orgánom. Aj keď spoločnosť si svoj vedúci dozorný orgán zvolí sama, táto determinácia nesmie byť svojvoľná podľa toho, v ktorom štáte by chcela dozorný orgán, ale musí takúto voľbu náležite preukázať, a to podľa kritérií stanovených pre hlavnú prevádzkareň. Možnosti voľby sú však pomerne obmedzené umiestnením hlavnej prevádzky danej spoločnosti.

Koncept one-stop-shop budú môcť využiť aj sprostredkovatelia. V prípade, že sa vyšetrovanie týka tak sprostredkovateľa, ako aj jeho klienta (prevádzkovateľa[34]), vedúcim dozorným orgánom bude vedúci dozorný orgán prevádzkovateľa, a vedúci dozorný orgán sprostredkovateľa bude už „len" dotknutým dozorným orgánom.[35]

31 Napríklad ak bola sťažnosť podaná na dotknutom dozornom orgáne, vyšetrí ju tento dozorný orgán, na ktorom bola sťažnosť podaná, resp. ak sa spracúvanie týka len vybraného jedného štátu (napríklad marketingová kampaň sa týka len zákazníkov v jednej určitej krajine EÚ), rovnako sa ňou bude zaoberať tento orgán.

32 Resp. pre spoločnosti, ktoré majú síce prevádzkareň v jednom štáte v EÚ, avšak spracúvanie podstatne ovplyvní jednotlivcov vo viac ako jednom štáte.

33 Často ňou bude materská spoločnosť, resp. operačné ústredie skupiny. Prítomnosť technických prostriedkov (napríklad serverovne) nie je relevantným kritériom pre určenie hlavnej prevádzkarne.

34 Ak je usadený v EÚ.

35 Pracovná skupina 29, usmernenie k určovaniu vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa z 13.12.2016, str. 11. Slovenský preklad usmernenia bol publikovaný Úradom na ochranu osobných údajov SR a je dostupný: https://dataprotection.gov.sk/uoou/sites/default/files/urcenie_veduceho_dozorneho_organu_podla_nariadenia_gdpr_-_sumar_0.pdf (str. 8)

9.2 Odporúčania

Spoločnosti, ktoré spracúvajú osobné údaje vo viacerých krajinách, by si mali určiť, ktorý dozorný orgán je ich vedúcim dozorným orgánom. Treba však myslieť na to, že ich možnosti sú obmedzené umiestnením hlavnej prevádzky danej spoločnosti.

10. MEDZINÁRODNÉ PRENOSY DÁT

Tí, ktorí dúfali v to, že GDPR odstráni podmienku uzatvárať mnohostranové zmluvy pred každým prenosom dát mimo územia EÚ len s nevôľou zistia, že GDPR zásadne túto byrokraciu nemení. Rovnako stále platí, že pod prenosom osobných údajov treba chápať relatívne širokú škálu situácií. Treba k nim zaradiť nielen situácie, keď zamestnanec z EÚ zašle pdf dokument obsahujúci osobné údaje kolegovi do Ázie, ale aj ak osoba z USA dostane prístup (napríklad prostredníctvom hesla) k údajom zamestnancov alebo klientom z EÚ (napríklad prostredníctvom webového portálu).

Stále platí, že osobné údaje môžu byť prenesené aj k príjemcom do tretích krajín mimo EÚ/EHP. Podmienky prenosu sa odlišujú podľa toho, či cieľová krajina, do ktorej budú osobné údaje prenesené, zaručuje alebo nezaručuje primeranú úroveň ochrany.

a. Pokiaľ je príjemca údajov v jednej z tretích krajín, ktoré **zabezpečujú primeranú úroveň ochrany osobných údajov**, ktorými sú:

- **I.** krajiny EÚ a EHP, a
- **II.** niektoré ďalšie krajiny, o ktorých bolo rozhodnuté, že ich úroveň ochrany osobných údajov je dostatočná[36] (napríklad Izrael, Kanada, Monako, Argentína, Švajčiarsko, USA – spoločnosti, ktoré sa prihlásili k „Privacy Shield"[37]), ten, kto prenáša (vyváža) osobné údaje musí dotknutým osobám poskytnúť základné informácie o spracovaní (ako napríklad, ktoré osobné údaje budú prenesené do ktorej krajiny, za akým účelom atď.), avšak zmluva o prenose osobných údajov nebude potrebná. Na tieto krajiny sa teda hľadí ako na krajiny, ktorých právny systém dostatočne chráni súkromie dotknutých osôb, a teda dáta môžu byť prenesené.

b. Pokiaľ sa príjemca údajov nachádza v krajine, ktorá podľa rozhodnutia Európskej komisie **nezaručuje primeranú úroveň ochrany osobných údajov**, bude potrebné prijať „dodatočné záruky", ktorými sú najmä:

- **I.** „**Štandardné zmluvné doložky**" (**Doložky**) prijaté Európskou komisiou alebo národným dozorným orgánom. Ak boli medzi vývozcom a dovozcom údajov Doložky prijaté, prenos sa môže uskutočniť bez potreby ďalšieho schvaľovania dozorným orgánom.[38]
- **II.** **Záväzné vnútropodnikové pravidlá** (Binding Corporate Rules/BCRs), ktoré však musia prejsť schvaľovacím procesom dozornými orgánmi v EÚ predtým, ako bude možné ich použiť.
- **III.** Na základe **výslovného súhlasu** dotknutej osoby, avšak len v prípade, že dotknutej osobe boli vysvetlené riziká takéhoto prenosu, a napriek tomu s prenosom udelila súhlas.

36 Zoznam krajín je na nasledujúcej stránke: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

37 Privacy Shield nahradil systém „Safe Harbor", ktorý bol rozhodnutím Súdneho Dvora EÚ Schrems (prípad ref. C-362/14) zrušený. Momentálne je v štádiu diskusií, či systém Privacy Shield stále bude možné použiť po tom, ako prezident Trump vydal Executive Order on „Enhancing Public Safety in the Interior of the United States".

38 Takéto schvaľovanie nebolo potrebné ani podľa zákona o ochrane osobných údajov ak Doložky boli inkorporované bez zmien. Ak použité Doložky vykazovali nesúlad oproti verzii Doložiek, ktoré prijala Európska komisia, bude potrebné ešte pred prenosom osobných údajov požiadať Úrad na ochranu osobných údajov o súhlas s prenosom.

IV. Na základe **legitímnych záujmov prevádzkovateľa** (kde súhlas dotknutej osoby nebude potrebný), avšak len za predpokladu, že prenos bude len jednorazový a bude sa týkať iba niektorých jednotlivcov (teda nebude sa jednať o masívny prenos). V tomto prípade však vývozca údajov o prenose musí informovať dozorný orgán ako aj jednotlivcov.

V. Prenos údajov je možné uskutočniť aj na základe **verejného záujmu**.

10.2 Odporúčania

Pre slovenských vývozcov údajov sa systém prenosov dát mimo územia EHS príliš nezmení. GDPR teda neprináša zmiernenie pravidiel medzinárodných prenosov, ktoré zostane relatívne náročné, najmä čo sa týka zmluvnej dokumentácie. Spoločnosti, ktoré dáta prenášali na základe súhlasu, by sa mali zamyslieť nad alternatívnymi formami prenosov. Spoločnosti, ktoré prenášajú pravidelne veľké množstvo dát, by mali zvážiť prijatie BCRs.

Právne závery obsiahnuté v tejto publikácii boli spracované advokátskou kanceláriou Allen & Overy Bratislava, s.r.o.

Zuzana Hečko
Advokátka
Allen & Overy Bratislava, s.r.o.
Zuzana.Hecko@allenovery.com

ESET, spol. s r.o
Obchodné oddelenie
Tel.: +421 (2) 322 44 250
obchod@eset.sk

GDPR READY

SIFROVANIE.ESET.SK

ESET

ENDPOINT ENCRYPTION

Vaša najlepšia voľba pre šifrovanie dát

Jednoducho použiteľná ochrana dát v súlade s GDPR, vhodná pre firmu akejkoľvek veľkosti.

BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE