

# ALLEN & OVERY

## *Nariadenie o ochrane osobných údajov (GDPR)*



**Mgr. Katarína Matulníková**

## Čo je GDPR?

– **Nariadenie (EÚ) 2016/679** Európskeho parlamentu a Rady 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 osobných údajov**)

## Prečo sa o tom rozprávame?

– GDPR nepredstavuje novelu v oblasti ochrany osobných údajov, ale „minirevolúciu“. Bude sa aplikovať na **každého**, kto spracúva osobné údaje

## Kedy sa začne uplatňovať?

– Nariadenie nadobudne platnosť **25. mája 2018** a nahradí náš zákon č. 122/2013 Z.z o ochrane osobných údajov, ktorý bude zrušený. **Avšak...**

# Definícia osobného údaju

## Článok 4 Nariadenia

Na účely tohto nariadenia:

1. „osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby

# Najdôležitejšie zmeny

One-stop-shop



# Povinnosť oznamovať incidenty

## Dozornému orgánu

- bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa prevádzkovateľ o tejto skutočnosti dozvedel (sprostredkovateľ – podá prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel)
- minimálny štandard oznámenia

incident

## Dotknutej osobe

- v prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe
- minimálny štandard oznámenia
- výnimky

**porušenie ochrany osobných údajov** je 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

# Pokuty

suma	delikt
do <b>20 miliónov Eur</b> alebo v prípade podniku do <b>4% celosvetového ročného obratu</b> v predchádzajúcom finančnom roku, podľa toho, ktorá suma je vyššia.	<ul style="list-style-type: none"> <li>▪ porušenie zásad spracúvania vrátane podmienok súhlasu</li> <li>▪ porušenie práv dotknutých osôb</li> <li>▪ porušené zásady prenosu dát mimo územia EÚ</li> <li>▪ nesplnenie príkazu alebo nedodržanie dočasného alebo definitívneho obmedzenia spracúvania alebo pozastavenia tokov údajov nariadeného dozorným orgánom alebo neposkytnutie prístupu.</li> </ul>
do <b>10 miliónov Eur</b> alebo alebo v prípade podniku do <b>2% celosvetového ročného obratu</b> v predchádzajúcom finančnom roku, podľa toho, ktorá suma je vyššia.	<ul style="list-style-type: none"> <li>▪ porušenie povinnosti prevádzkovateľa alebo sprostredkovateľa (zmluva so sprostredkovateľom, ktorá nespĺňa podmienky podľa GDPR, nezabezpečenie dostatočnej bezpečnosti spracúvaných osobných údajov (okrem iného napríklad aj šifrovaním), neoznámenie incidentu, nenominovanie zodpovednej osoby)</li> </ul>

# Pokuty

druh	obsah
<b>vyšetrovacie</b> právomoci ÚOOÚ	<ul style="list-style-type: none"> <li>nariadiť poskytnutie potrebných informácií</li> <li>viest' vyšetrovania vo forme auditov</li> <li>vykonávať preskúmania certifikácií</li> <li>oznamovať údajné porušenie tohto nariadenia</li> <li>získať prístup ku všetkým osobným údajom a všetkým informáciám potrebným na plnenie svojich úloh</li> <li>získať prístup do všetkých priestorov a zariadeniu a prostriedkom na spracúvanie údajov</li> </ul>
<b>nápravné</b> právomoci ÚOOÚ	<ul style="list-style-type: none"> <li>upozorniť, že plánované operácie pravdepodobne porušia GDPR</li> <li>napomenúť, ak operácie porušili ustanovenia GDPR</li> <li>nariadiť vyhovieť žiadostiam dotknutej osoby o uplatnenie jej práv</li> <li>nariadiť zosúladienie operácií (určeným spôsobom a v rámci určenej lehoty) s GDPR</li> <li>nariadiť oznámenie incidentu</li> <li>nariadiť dočasné alebo trvalé obmedzenie vrátane zákazu spracúvania;</li> <li>nariadiť opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania</li> <li><b>uložiť v závislosti od okolností každého jednotlivého prípadu pokutu (popri opatreniach alebo namiesto nich)</b></li> <li>nariadiť pozastavenie toku údajov</li> </ul>

# Súhlas

**Súhlas dotknutej osoby** je akýkoľvek 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 týka.



Ak dá dotknutá osoba súhlas v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola **jasne odlíšiteľná** od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho. Akákoľvek časť takéhoto vyhlásenia, ktorá predstavuje porušenie tohto nariadenia, nie je záväzná.



Dotknutá osoba má právo **kedykoľvek odvolať svoj súhlas**. Pred poskytnutím súhlasu musí byť dotknutá osoba **o tejto skutočnosti informovaná**. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie.



**Prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.**





# Súhlas - ďalšie striktnejšie požiadavky

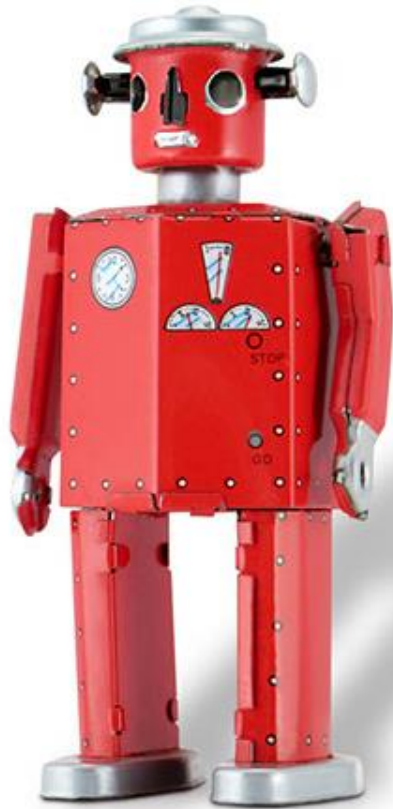
**Mlčanie ani pre-ticked boxes  
nebudú považované za súhlas.**

**Súhlas môže byť vyjadrený napr.  
písomným vyhlásením, ústnym  
vyhlásením, označením (zakliknutím  
políčka) alebo iným zrozumiteľným  
úkonom, z ktorého je jasné, že  
dotknutá osoba súhlasí.**

**Pri spracúvaní osobných  
citlivých údajov ostáva  
povinnosť samostatného  
výslovného súhlasu dotknutej  
osoby.**

**GDPR obsahuje špecifické  
podmienky pre súhlas  
udelený dieťaťom.**

# Nominácia zodpovednej osoby (ZO)



**GDPR ukladá povinnosť ustanoviť zodpovednú osobu (prevádzkovateľ aj sprostredkovateľ) v nasledujúcich prípadoch:**

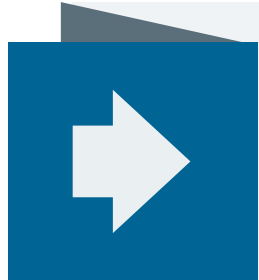
- Spracúvanie vykonáva orgán verejnej moci / verejnoprávny subjekt (okrem súdov) alebo spoločnosti vykonávajúce úlohy vo verejnom záujme;
- Hlavnou činnosťou prevádzkovateľa alebo sprostredkovateľa je monitorovanie jednotlivcov vo veľkom rozsahu;
- Hlavnou činnosťou prevádzkovateľa alebo sprostredkovateľa je spracúvanie citlivých údajov jednotlivcov vo veľkom rozsahu.

# Právo byť zabudnutý (Právo na výmaz)

- **Právo na výmaz** podľa GDPR je koncipované širšie a taktiež je detailnejšie upravené ako právo na výmaz podľa zákona o ochrane osobných údajov
- Ak sú dáta spracúvané **protizákonne** alebo keď je **odvolaný súhlas**
- Špecifický režim pre zabudnutie už zverejnených dát (informovať aj iných prevádzkovateľov, plus linky a kópie)

- **Nie je to** absolútne právo jednotlivca (musí byť posúdené so slobodou prejavu a právom na informácie)
- Ak by právo byť zabudnutý vyúsťovalo do cenzúry tlače, tejto žiadosti sa nebude musieť vyhovieť.

# “Privacy by Design and by Default“



Ochrana osobných údajov musí byť zakomponovaná do projektov od ich ranného štádia:



Pseudonymizácia údajov



Minimalizácia údajov



Vypracovanie **posúdenia vplyvu na ochranu osobných údajov** (*impact assessment*)



# Sprostredkovateľ

**zmluva** (písomná, aj v elektronickej podobe), musí obsahovať:

predmet, doba, povaha a účel spracúvania, typ osobných údajov, kategórie dotknutých osôb, povinnosti a práva

spostredkovateľ spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa

spostredkovateľ zabezpečí zachovanie dôvernosti informácií

záväzok pomáhať prevádzkovateľovi pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby

zapojenie ďalšieho sprostredkovateľa len na základe osobitného alebo všeobecného povolenia a za tých istých podmienok

spostredkovateľ vykoná všetky požadované opatrenia na zaistenie bezpečnosti

- pomáhať prevádzkovateľovi pri oznamovaní incidentov a zaistení bezpečnosti spracúvania
- po ukončení spracúvania všetky osobné údaje vymazať alebo vrátiť (a vymazať kópie)
- poskytnúť prevádzkovateľovi informácie a umožniť audity a kontroly

# Medzinárodné prenosy dát

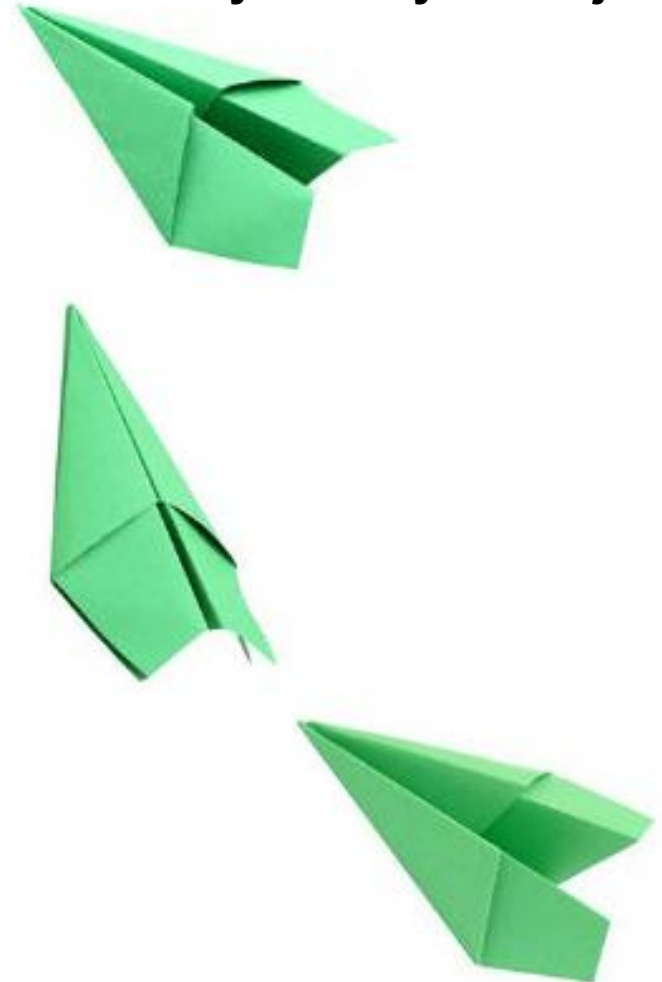
- Podmienka uzatvárať mnohostrannové zmluvy pred každým prenosom dát mimo územia EÚ **ostáva**
- „Prenos“ osobných údajov = široká škála situácií
- Pri prenášaní osobných údajov záleží, či cieľová krajina zaručuje **primeranú úroveň ochrany**



# Medzinárodné prenosy dát

Bude potrebné prijať „**dodatočné záruky**“ v prípade, že príjemca údajov sa nachádza v krajine, ktorá podľa EK **nezaručuje primeranú úroveň ochrany osobných údajov**. Týmto sú najmä:

	Štandardné zmluvné doložky
	Záväzné vnútropodnikové pravidlá (Binding Corporate Rules/BCRs)
	Výslovný súhlas (kde dotknutej osobe boli vysvetlené riziká prenosu)
	Legitímny záujem prevádzkovateľa (nie pre masové prenosy a je potrebné informovať regulátora)
	Verejný záujem pri prenose údajov



# 99 článkov a 173 odôvodnení GDPR nestačí... Úrad pripravil nový zákon na ochranu osobných údajov

- September/október: 1. a 2. čítanie
- Účinnosť máj 2018 (spolu s GDPR)
- Zákon „preklápa“ nariadenie
- Dôvod prijatia zákona: GDPR nepokrýva každého (??)





# Ďakujem za pozornosť

## Otázky?



**Katarína Matulníková**

Allen & Overy Bratislava, s.r.o.

Tel: +421 (2) 5920 2407

Fax: +421 (2) 5920 2424

[katarina.matulnikova@allenoververy.com](mailto:katarina.matulnikova@allenoververy.com)



**Tento dokument je všeobecný informačný dokument a nepredstavuje konkrétne poradenstvo (nie je poskytnutím právnej služby).**

**V tomto dokumente pojem Allen & Overy znamená Allen & Overy LLP a/alebo jej spriaznené osoby. Slovo partner sa používa na označenie člena Allen & Overy LLP, zamestnanca alebo konzultanta s obdobným postavením a kvalifikáciou, prípadne osoby s obdobným štatútom v jednej zo spriaznených osôb Allen & Overy LLP.**