

TaylorWessing

**Vybrané aspekty
poskytovania služieb
cloud computingu vo
svetle GDPR**

JUDr. Zoltán Nagy

Bratislava, 26. septembra 2017



Cloud Computing

- > Poskytovanie IT služieb prevádzkovaných na virtuálnej infraštruktúre poskytovateľa prostredníctvom internetu a internetového prehliadača.
- > Smernica NIS pod službou v oblasti cloud computingu rozumie „*digitálnu službu, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať*“.



Cloud Computing - kategórie

- > IaaS – **Infraštruktúra ako služba**
 - hardvérová a softvérová infraštruktúra do úrovne operačného systému a v požadovanej špecifikácii. Služba poskytuje klientovi pomerne veľký rozsah kontroly nad spracúvanými údajmi (napr. Amazon Web Services).
- > PaaS – **Platforma ako služba**
 - poskytovaná komplexná platforma (hardvér, vývojová platforma, operačný systém), na ktorej zákazník ďalej vyvíja a používa vlastné aplikácie (napr. Microsoft Azure).
- > SaaS – **Softvér ako služba**
 - jeden z najpoužívanějších typov cloudových služieb- poskytovateľ poskytuje a sprístupňuje svoje služby prostredníctvom webových aplikácií (napr. Google Apps, Dropbox).



Cloud Computing & Data Protection

> Riziká:

- Strata výlučnej kontroly zákazníka nad spracúvanými osobnými údajmi;
- Nedostatok informácií, ktoré má zákazník k dispozícii o tom, ako je s jeho údajmi zaobchádzané a kde sa tieto údaje aktuálne nachádzajú;
- Existencia hrozby poskytnutia týchto údajov z cudzím zahraničným orgánom.



Klient, poskytovateľ služby & GDPR - I

- > Spracúvanie osobných údajov
 - GDPR je **technologicky** a **sektorovo neutrálne**:
 - operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, **napríklad** získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Klient, poskytovateľ služby & GDPR - II

- > Prevádzkovateľ
 - Kto sám alebo spoločne s inými určí účel a prostriedky spracúvania osobných údajov;
 - Primárna zodpovednosť za proaktívne plnenie všetkých povinností spojených so spracúvaním osobných údajov podľa GDPR a za zdokumentovanie súladu s ustanoveniami GDPR.



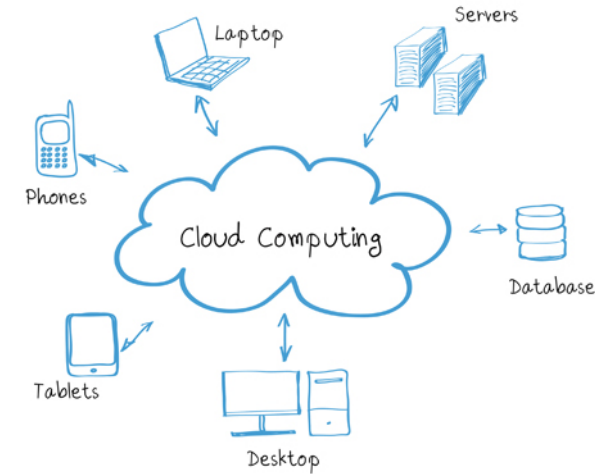
Klient, poskytovateľ služby & GDPR - III

> Sprostredkovateľ

- Kto spracúva osobné údaje v mene a podľa pokynov prevádzkovateľa, t.j. v podriadenom postavení voči prevádzkovateľovi;
- GDPR: **priame povinnosti a priama zodpovednosť**;
- Zodpovedá za ujmu spôsobenú dotknutej osobe, ak
 - i. poruší povinnosť, ktorú mu ukladá nariadenie alebo
 - ii. koná nad rámec pokynov prevádzkovateľa alebo v rozpore s nimi;
- Sankcia zo strany dozorného úradu, až do výšky 20 000 000 EUR, alebo v prípade podniku až do výšky 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok.

Klient, poskytovateľ služby & GDPR - IV

- > Klient = Prevádzkovateľ
- > Poskytovateľ cloudu = Sprostredkovateľ
- > Potrebné posudzovať vždy od prípadu k prípadu –
Princíp: zvyšovanie vplyvu poskytovateľa cloudovej služby na účel a prostriedky spracúvania posúva poskytovateľa z pozície sprostredkovateľa k pozícii prevádzkovateľa.
- > Spoločný prevádzkovatelia (joint controllership)
účel (zámer) a prostriedky spracúvania budú určené spoločne (nadmárodná podniková skupina)
- > Poskytovateľ cloudu = samostatný prevádzkovateľ
spracúva údaje na vlastné účely / účely, ktoré neboli určené a dohodnuté s klientom (služby poskytované „zadarmo“ – t.j. za osobné údaje)





Predzmluvné povinnosti (klient)

- > Štandardné zmluvné podmienky poskytovateľov vs. Výhradné právo klienta **rozhodnúť o výbere** konkrétneho poskytovateľa
- > GDPR: Zodpovednosť za voľbu **vhodného sprostredkovateľa**
„dostatočné záruky na to, že má implementované primerané **technické a organizačné opatrenia** tak, aby spracúvanie spĺňalo požiadavky GDPR a aby sa zabezpečila ochrana práv dotknutej osoby“
- > Povinnosť prevádzkovateľa pred poverením sprostredkovateľa dôkladne posúdiť otázku, či sprostredkovateľ implementoval dostatočné technické a bezpečnostné opatrenia.

Kódex správania & Certifikácia

- > Jedným z prvkov preukazujúcich splnenie primeraných záruk je dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu (čl. 28 ods. 5 GDPR)
 - **Kódex správania**
súbor noriem, ktoré upresňujú podmienky spracúvania osobných údajov s ohľadom na špecifiká odvetvia, v ktorom tieto kódexy boli prijaté;
 - **Certifikačné mechanizmy**
nástroj samoregulácie, ktorý pomáha subjektom preukazovať súlad s podmienkami GDPR (nie je naviazaná na odvetvia);
 - Pre cloud napríklad CCSL a CCSM – Cloud Computing Certification prijatý Agentúrou EÚ pre sieťovú a informačnú bezpečnosť (ENISA).
 - Dobrovoľný princíp, pomoc pri preukazovaní súladu s podmienkami GDPR, ale nenahrádza audit;

Zmluva (Data Processing Agreement) - I

- > GDPR: Písomná zmluva musí obsahovať nevyhnutné náležitosti:
 - predmet a doba spracúvania,
 - povaha a účel spracúvania,
 - typ osobných údajov kategórie dotknutých osôb a
 - povinnosti a práva prevádzkovateľa,
 - katalóg povinností sprostredkovateľa.



Zmluva (Data Processing Agreement) - II

- > **Viazanosť** zdokumentovanými **pokynmi** prevádzkovateľa
Úprava spôsobu a formy udeľovania pokynov (e-mailom, intranetovým prostredím sprostredkovateľa a pod.);
- > **Zabezpečiť mlčanlivosť** osôb, ktoré spracúvajú osobné údaje v mene sprostredkovateľa
Vrátane zamestnancov, freelancerov, a pod.;
- > **Implementácia primeraných technických a organizačných opatrení** s cieľom zaistiť úroveň bezpečnosti zodpovedajúcej danému riziku spracúvania
- > Konkrétne opatrenia vychádzajú najmä z medzinárodných bezpečnostných štandardov – ISO 27018 týkajúce sa spracúvania osobných údajov vo verejnom cloude; ISO 27001 pri spôsobe zavádzania týchto opatrení;



Zmluva (Data Processing Agreement) - III

- > Bezpečnostné opatrenia podľa GDPR (len demonštratívny výpočet):
 - **Pseudonymizácia** a šifrovanie osobných údajov (anonymizácia?);
 - Schopnosť zabezpečiť **trvalú dôvernosť, integritu, dostupnosť a odolnosť** systémov spracúvania a služieb;
 - Schopnosť **včas obnoviť dostupnosť osobných údajov** a prístup k nim v prípade fyzického alebo technického incidentu;
 - Proces pravidelného **testovania, posudzovania a hodnotenia** účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Zmluva (Data Processing Agreement) - IV

- > Záväzok **súčinnosti** pomáhať prevádzkovateľovi pri plnení jeho povinnosti reagovať na žiadosti o **výkon práv dotknutej osoby**. Podľa kontextu spracúvania, je žiaduce upraviť súčinnosť v nasledovných oblastiach:
 - pri implementovaní **bezpečnostných opatrení** (čl. 32),
 - pri povinnosti **oznamovať porušenia ochrany osobných údajov** dozornému orgánu a dotknutej osobe (čl. 33 a 34),
 - pri povinnosti vykonať **posúdenie vplyvu** na ochranu osobných údajov (čl. 35),
 - pri povinnosti uskutočniť s dozorným orgánom **predchádzajúcu konzultáciu**, ak spracúvanie môže viesť k vysokému riziku (čl. 36)



Zmluva (Data Processing Agreement) - V

- > Poskytnutie všetkých informácií potrebných na preukázanie splnenia povinností podľa GDPR a umožniť **audit**
 - Audity vykonávané prevádzkovateľom alebo nezávislým audítorom, povinnosť logovania spracovateľských operácií, a pod.
- > Po ukončení poskytovania služieb **zabezpečiť výmaz** alebo vrátenie všetkých údajov prevádzkovateľovi, vrátane back-up
 - Neplatí, ak uloženie kópií vyžaduje právny poriadok.
- > GDPR = len **minimálny a nevyhnutný štandard zmluvnej úpravy**, odporúča sa upraviť ďalšie otázky - zodpovednosť, spôsob a forma odškodnenia a regresné nároky, a pod.



Subdodávateľ

- > Základné pravidlo – udelenie predchádzajúceho **písomného** súhlasu prevádzkovateľa;
- > **Konkrétny** alebo **všeobecný** súhlas;
- > **Notifikačná** povinnosť o zapojení každého nového subdodávateľa, resp. o jeho zmene;
- > Právo prevádzkovateľa **namietat'** zapojenie nového subdodávateľa;
- > **Zmluva** sprostredkovateľ – subdodávateľ: rovnaká úroveň ochrany spracúvaných údajov;
- > Výmaz alebo vrátenie všetkých údajov prevádzkovateľovi;
- > **Zodpovednostné** bremeno a regresné nároky.





Sprostredkovateľ – vybrané otázky - I

> **Záznamy o spracovateľských činnostiach**

- Život osobných údajov v organizácii; písomné preukazovanie súladu s GDPR, skrátenie reakčného času pri bezpečnostných incidentoch.

> **Povinnosť určiť zodpovednú osobu**

- Povinnosť:
 - i. hlavnými činnosťami sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu,
 - ii. hlavnými činnosťami sprostredkovateľa je spracúvanie osobitných kategórií údajov vo veľkom rozsahu.



Sprostredkovateľ – vybrané otázky - II

> Práva dotknutých osôb

- Novokoncipované práva dotknutých osôb:
 - i. právo byť zabudnutý (t.j. právo na výmaz) a
 - ii. právo na portabilitu údajov (t.j. právo na prenosnosť údajov, t. j. prevod osobných údajov z IT prostredia prevádzkovateľa A do IT prostredia prevádzkovateľa B, v štruktúrovanej, bežnej, strojovo čitateľnej podobe, t.j. vo formáte, ktorý môže byť použitý u prevádzkovateľa B) – interoperabilita medzi rôznymi IT prostrediami?

> Obmedzenie prenosu osobných údajov do tretích krajín

- Možnosti prenosu osobných údajov do tretích krajín naďalej pomerne prísne regulované. Základným kritériom je určenie toho, **či cieľová krajina zaručuje alebo nezaručuje primeranú úroveň ochrany.**

Praktické odporúčania pre poskytovateľov cloudu - I

- > Spracúvanie osobných údajov **len dohodnutý účel**, inak potreba právneho základu (napr. súhlas osoby);
- > **Zmapovanie** procesov a dátových tokov & Zabezpečenie príslušnej dokumentácie, vrátane **revízie** všeobecných obchodných podmienok, zmlúv, apod.;
- > **Implementácia** vhodných technických a organizačných opatrení & Poskytnutie dostatočných **záruk** (certifikácia);
- > **Interné politiky** pre splnenie práv dotknutých osôb;
- > Zohľadnenie zásad ochrany osobných údajov **už pri vývoji** a programovaní IT riešení;



Praktické odporúčania pre poskytovateľov cloudu - II

- > **Subdodávateľov** zapojiť len na základe predchádzajúceho **súhlasu** klienta & dôkladná zmluvná úprava ochrany osobných údajov so svojim subdodávateľom;
- > Kontrolu nad tým, kde sa **nachádzajú** osobné údaje a kto má k nim prístup (vhodné záruky pri cezhraničnom prenose);
- > **Transparentnosť** a spolupráca pri plnení požiadaviek GDPR so zákazníkom;
- > **Zodpovednosť** za súlad s GDPR a súvisiace riziko leží na pleciach oboch.



www.taylorwessing.com/globaldatahub

TaylorWessing

Global
DataHub

Topical Issues

Global DP guide

Our Services

Latest News & Events

Contact us

Global Data Hub

Global Data Hub draws on Taylor Wessing's international expertise to provide you with insight and guidance on data protection issues. Our in-depth analysis, news updates and events will help you navigate the minefield of global data protection law.

Latest News

We summarise the latest key developments in data protection

[More](#)

<>



LATEST NEWS [ECB to require t_](#)



GDPR Checklists (part II)

We have more checklists for you this month to help prepare the groundwork for GDPR-compliant policies. This month we look at privacy policies, SARs, DPIAs and data retention. Again, these are intended as starting points and we are happy to advise in more detail.

[More](#)



GDPR checklists

As organisations are beginning to get to grips with GDPR requirements, we set out the key obligations on data controllers and processors, provide a checklist to help kick off the audit process and checklists to help with data security and breach reporting policies.

[More](#)



HR data – challenges ahead for UK and EU employers

The new General Data Protection Regulation will apply from 25 May 2018. Bringing enhanced rights for individuals and an increased compliance burden for most employers, businesses need to get ready for compliance. At the same time, concerns around data exports outside the EU and Brexit will create new challenges, particularly for UK businesses. Planning ahead is essential and this month, we look at key issues for employers

[More](#)

GDPR checklists

As organisations are beginning to get to grips with GDPR requirements, we set out the key obligations on data controllers and processors, provide a checklist to help kick off the audit process and checklists to help with data security and breach reporting policies.



Data controller obligations under the GDPR

A high level summary of GDPR requirements on data controllers.

[More](#)



Data processor obligations under the GDPR

A high level summary of GDPR requirements on data processors.

[More](#)



GDPR audit checklist

We provide a checklist of key questions data controllers and data processors need to ask themselves at the start of a data audit process to prepare for GDPR compliance.

[More](#)



Cybersecurity checklist

Past Glass and Chris Wheatley set out a checklist of key cybersecurity issues a business should consider to help limit the risk and impact of a data breach and to be GDPR-compliant.

[More](#)



Breach response checklist

Past Glass and Chris Wheatley provide a checklist which sets out the key issues which a business should consider in preparing for a data breach.

[More](#)



TW-Cyber Response

TW Cyber Response is a mobile app developed by Taylor Wessing to assist clients in preparing for, and responding to, data breaches. It includes pre-breach issues, a roadmap for the first 48 hours of responding to a data breach, encrypted external directories and external contact directories as well as regular updates on relevant issues.

[More](#)

TaylorWessing

Global
DataHub

Topical Issues

Global DP guide

Our Services

Latest News & Events

Contact us

[Back](#)

GDPR Checklists (part II)

We have more checklists for you this month to help prepare the groundwork for GDPR-compliant policies. This month we look at privacy policies, SARs, DPIAs and data retention. Again, these are intended as starting points and we are happy to advise in more detail.



Privacy Policy Checklist

This checklist is designed to help you gather the information you will need to put a GDPR-compliant privacy policy on your website or in-app.

[More](#)



Data Protection Impact Assessments Checklist

This checklist helps you assess whether a DPIA is required and provides a spreadsheet for some of the issues you will need to consider in more detail if you do need or choose to carry out a DPIA.

[More](#)



Subject Access Requests Checklist

What you need to consider to enable you to handle SARs efficiently and in compliance with the GDPR.

[More](#)



Data Retention Policy Checklist

How much data is too much and how long can you hold onto it? This checklist should help you focus on issues around data retention.

[More](#)

Ďakujeme za pozornosť!



JUDr. Zoltán Nagy
Associate, Bratislava
Taylor Wessing CEE
z.nagy@taylorwessing.com
www.taylorwessing.com

