# Working Paper

**Podklad k diskusi na workshopu 24. února 2016**

##

## **Aktuální vývoj**

Osobní údaje uživatelů jsou v současnosti pravděpodobně nejcennější komoditou digitální ekonomiky. Na rostoucí zájem o data reaguje i dlouhá léta připravovaná regulace Evropské unie. Na konci roku 2015 bylo úspěšně uzavřeno vyjednávání mezi Evropskou komisí, Parlamentem a Radou o podobě nového Obecného nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation). Tento předpis, který by měl nabýt účinnosti během dvou let, nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a, vzhledem k jeho přímé aplikovatelnosti, rovněž zákon č. 101/2000 Sb.

V tomto přehledovém dokumentu je vybráno několik zásadních novinek, které budou mít významný vliv na praktické fungování celého systému ochrany osobních údajů. Dále jsou seřazeny do tří skupin dle jejich povahy.

## **Zpracování osobních údajů**

### **a) Přísnější pravidla pro souhlas se zpracováním**

Souhlas se zpracováním osobních údajů zůstává jedním ze způsobů, kterým může jejich správce legitimizovat plánované zpracování osobních údajů (čl. 6 GDPR). A to včetně zvláštních kategorií údajů[[1]](#footnote-1) (čl. 9 GDPR).

GDPR přináší jako novinku konkrétní úpravu bližší specifikace požadavků na souhlas se zpracováním (čl. 7). Požadavky v tomto článku uvedené nejsou zcela nové, protože se interpretačně daly dovodit již ze současné směrnice 95/46/ES, případně z výkladových materiálů Úřadu pro ochranu osobních údajů (ÚOOÚ) a Pracovní skupiny zřízené dle článku 29 (WP29).[[2]](#footnote-2) GDPR klade na správce údajů vyšší nároky požadavkem na větší vstřícnost vůči subjektům údajů během procesu získání jejich souhlasu. Konkrétně pak následujících podmínek:

* Pokud je souhlas se zpracováním součástí jiného dokumentu (smlouvy), musí být zřetelně oddělen, aby nevznikl pocit, že smlouvu není možné uzavřít bez udělení souhlasu;[[3]](#footnote-3)
* Při popisu zpracování za účelem získání souhlasu musí být použit prostý a srozumitelný jazyk;
* Subjekt údajů má možnost souhlas kdykoli odejmout (a to stejně snadno, jako jej udělí) a musí být o této možnosti informován;
* Souhlas je platný jedině, pokud je udělen svobodně, tedy bez rizika neposkytnutí služby, nebo zhoršení situace subjektu údajů;.[[4]](#footnote-4)

Povinnost správce údajů být schopen prokázat existenci souhlasu po celou dobu probíhajícího zpracování zůstává zachována.

Novinkou je specifické pravidlo, které stanoví, že souhlas se zpracováním osobních údajů subjektu mladšího 16 nebo 13 let[[5]](#footnote-5) může být udělen jen jeho zákonným zástupcem. Osobní údaje zpracované tímto způsobem pak bez dalšího spadají do režimu údajů, jejichž výmaz je možné požadovat na základě práva na výmaz (na zapomnění) dle čl. 17.[[6]](#footnote-6)

### **b) Únikové klauzule**

Únikové klauzule z povinností, kde není možné jejich plnění je novinkou GDPR, která nepřidává správcům údajů žádné nové povinnosti. Je zmíněna jako příklad toho, že se nová právní úprava snaží reflektovat nedostatky současné směrnice 95/46/ES, která již v mnoha oblastech nestačí na rychle se rozvíjející technologie a vyžaduje plnění povinností tam, kde to není v reálné praxi možné.[[7]](#footnote-7)

Čl. 10 GDPR zavádí výjimku, podle které pokud pro účel zpracování osobních údajů není nutná další identifikace subjektu údajů, správce tuto identifikaci nemusí získat aby splnil povinnosti z GDPR. Druhým takovým příkladem je čl. 14a odst. 4 písm. b), který zavádí výjimky z obecné povinnosti informovat subjekt údajů pro případy, kdy by poskytnutí informace o zpracování bylo nemožné, nebo představovalo nepřiměřené úsilí.

### **c) Právo na výmaz (zapomnění)**

Nově formulované právo, (často diskutované po rozhodnutí Soudního dvora EU ve věci Google Spain), které vychází ze současného práva subjektu údajů požadovat zanechání zpracování údajů, které nejsou odpovídající účelu jejich zpracování. Čl. 17 a 17a GDPR vymezují následující situace, kdy subjekt údajů může požadovat zanechání zpracování jeho osobních údajů a jejich výmaz:

* Údaje nejsou nezbytné vzhledem k účelu zpracování, pro které byly sesbírány, nebo zpracovávány;
* Subjekt odejme souhlas se zpracováním a správce nemá žádný jiný zákonný důvod pro zpracování údajů;
* Subjekt údajů namítá zpracování osobních údajů dle čl. 19 GDPR;[[8]](#footnote-8)
* Údaje byly zpracovávány protiprávně;
* Údaje mají být vymazány za účelem splnění právní povinnosti;
* Údaje byly sbírány a zpracovávány na základě souhlasu zákonného zástupce;

Pokud dojde na základě některého z výše uvedených důvodů k vymazání údajů, které správce[[9]](#footnote-9) uveřejnil, má rovněž povinnost podniknout přiměřeně nezbytné kroky k tomu, aby o požadavku subjektu údajů informoval další osoby, které tato data zpracovávají. Článek 17 odst. 3 pak uvádí několik výjimek, kdy se právo na výmaz neaplikuje (např. pokud by tím mělo být zasaženo do práva svobody projevu).

Toto právo je jedno z řady nově výslovně vyjádřených práv subjektu údajů, které správci budou nuceni vzít v potaz a vyhradit zdroje pro jejich naplňování.

## **Nové povinnosti správce související s bezpečností údajů**

V této části je vybráno několik zásadních nových povinností, které bude muset správce údajů plnit v souvislosti se zajištěním zabezpečení zpracování osobních údajů. Oproti směrnici 95/46/ES ubyla povinnost registrace správce údajů u národního orgánu ochrany osobních údajů. Na druhou stranu ale zase přibyla povinnost provádět v určitých případech hodnocení dopadů plánovaného zpracování osobních údajů a zřízení pozice tzv. inspektora osobních údajů.

### **a) Ochrana By Design & By Default**

„Data protection by design“ úzce souvisí se zásadou tzv. minimalizace údajů. Na pozadí tohoto principu, který budou mít správci nově povinnost dodržovat, stojí myšlenka, že je mnohem efektivnější (jak funkčně, tak ekonomicky), pokud je s ochranou osobních údajů počítáno již od počátku návrhu praktického řešení jejich zpracování.[[10]](#footnote-10) Může se jednat jak o technická řešení typu anonymizace, pseudonymizace a rozdělení (ať už fyzické, nebo logické) oblastí s uloženými daty. Nebo personální a organizační opatření (kdo ze zaměstnanců správce údajů má přístup k jakým údajům, jaké jsou toky dat v rámci společnosti atd.).

Princip „data protection by default“ pak má zajistit, aby v základním nastavení služby byly zpracovávány jen osobní údaje, které jsou zcela nezbytné pro její poskytování. Tento princip pak zřejmě míří primárně na zpracování osobních údajů při nabízení služeb online.

### **b) Bezpečnost zpracování a ohlašování případů narušení bezpečnosti (Data Breach)**

GDPR klade na správce požadavek zajistit za pomoci technických a organizačních prostředků bezpečnost zpracování osobních údajů. Čl. 30 GDPR výslovně uvádí, že při poměřování nezbytné míry zabezpečení je třeba brát v potaz na jedné straně náklady nezbytné pro zajištění takových prostředků a na straně druhé povahu zpracovávaných osobních údajů a riziko možných dopadů jejich případného zničení, úniku, nebo nezákonného zpracování. V tomto smyslu GDPR navazuje na směrnici 95/46/ES.

Novinkou je ohlašovací povinnost v případě narušení bezpečnosti zpracování osobních údajů („data breach“). Správce má povinnost bez odkladu, nejpozději však do 72 hodin, incident ohlásit DPA[[11]](#footnote-11), do jejíž jurisdikce náleží. Čl. 31 GDPR pak stanoví, že v případě, že by důsledkem data breach bylo vysoké riziko zásahu do základních lidských práv a svobod subjektu údajů, má správce povinnost informovat jej o incidentu, a to bez zbytečného odkladu. Při hlášení má správce údajů povinnost popsat například charakter incidentu, možná rizika a kroky, které byly podniknuty pro jeho odvrácení.

### **c) Posuzování dopadu na ochranu údajů**

Článek 33 GDPR zavádí povinnost vypracovat posouzení dopadů plánovaného zpracování osobních údajů. A to v případech, kdy vzhledem k povaze jejich zpracování[[12]](#footnote-12) hrozí vysoké riziko zásahu do základních práv a svobod subjektů údajů,. Jako příkladný výčet zpracování, k nimž by mělo být posouzení dopadů vypracováno, odst. 2 uvádí:

* Profilování;
* Zpracování velkého množství citlivých údajů;
* Systematické monitorování veřejného prostoru.

DPA může stanovit seznam druhů zpracování osobních údajů, pro které je vypracování posouzení dopadů povinné.

Čl. 34 GDPR dále stanoví, že správce údajů má v případech, kdy z posouzení dopadů vyplyne vysoké riziko zásahu do základních práv a svobod subjektů údajů, povinnost před zahájením zpracování konzultovat následný postup s DPA, do jejíž jurisdikce spadá. DPA pak v kooperaci se správcem údajů zajistí, aby nedošlo k nezákonnému zpracování osobních údajů.

### **d) Jmenování inspektora ochrany údajů**

Správce údajů má povinnost jmenovat inspektora osobních údajů (formou zaměstnaneckého poměru, nebo dohody o externí spolupráci).[[13]](#footnote-13) To platí v případech kdy:

* Zpracování je prováděno orgánem veřejné moci;
* Hlavní činnost správce spočívá ve zpracování údajů v podobě pravidelného systematického monitorování velkého množství subjektů údajů;
* Hlavní činnost správce spočívá ve zpracování velkého množství citlivých údajů;
* Další případy, kdy je jmenování inspektora nezbytné pak může určit národní právo.

Více správců se pak může domluvit, že budou společně využívat služeb jednoho inspektora. Ten má být vybrán a jmenován na základě svých profesních kvalit a zkušeností a má mít poměrně silnou a nezávislou pozici v rámci struktury správce údajů. Čl. 36 GDPR stanoví, že inspektor přímo odpovídá nejvyššímu vedení správce údajů, má mu být umožněno vykonávání jeho povinností vyplývajících z GDPR a nesmí být propuštěn, nebo penalizován za to, že tyto povinnosti plní. Inspektor pak má fungovat jako prostředník mezi správcem údajů a DPA a mohou se na něj přímo obracet subjekty údajů.

## **Předávání údajů do zahraničí**

Zejména v souvislosti s rozhodnutím Soudního dvora Evropské unie ve věci Schrems je v poslední době hojně diskutovaný problém předávání osobních údajů do zahraničí. Úprava GDPR navazuje na současnou úpravu dle směrnice 95/46/ES. Předpokládá následující právní důvody pro předávání osobních údajů do zemí mimo EU:

* Rozhodnutí Komise o adekvátní úrovni ochrany (čl. 41);
* Předávání při existenci potřebných opatření pro zajištění úrovně ochrany (čl. 42);
* Binding corporate rules (čl. 43);
* Specifické případy předávání údajů uvedené v čl. 44 jako jsou například:
	+ Výslovný souhlas subjektu údajů s předáním do třetí země;
	+ Předání je nezbytné pro splnění smlouvy mezi správcem a subjektem údajů;
	+ Předání je nezbytné pro důležitý veřejný zájem;
	+ Ve velmi omezeném a přísném režimu, předání je nezbytné pro naplnění oprávněného zájmu správce údajů.
1. Dnes známé jako „citlivé údaje“. [↑](#footnote-ref-1)
2. Poradní orgán Komise pro oblast ochrany osobních údajů sestávající se ze zástupců národních úřadů pro ochranu osobních údajů. [↑](#footnote-ref-2)
3. Zpracování údajů za účelem plnění smlouvy je v GDPR, stejně jako dnes, zvláštní legitimizační důvod. [↑](#footnote-ref-3)
4. Tento požadavek je platný již nyní, byť není tak jasně formulovaný. [↑](#footnote-ref-4)
5. Bude záviset na národní legislativě. [↑](#footnote-ref-5)
6. Viz dále. [↑](#footnote-ref-6)
7. Jako příklad může sloužit povinnost informovat subjekt údajů o probíhajícím zpracování, která v případě správce, jako je internetový vyhledávač ve smyslu rozhodnutí Google Spain, není naplnitelná. [↑](#footnote-ref-7)
8. Namítat zpracování je možné v případech, kdy je zpracování prováděno na legitimizačním základě veřejného zájmu a oprávněného zájmu správce dle čl. 6/ odst. 1 písm. e, f. [↑](#footnote-ref-8)
9. Obecně se povinnosti zde uváděné týkají jak správce, tak zpracovatele osobních údajů. [↑](#footnote-ref-9)
10. Ve zkratce můžeme říci, že je snadnější technické a další prostředky ochrany soukromí a osobních údajů vložit do systému při jeho vzniku, než je později „přišívat“ k již hotovému. [↑](#footnote-ref-10)
11. Data Protection Authority, v českém případě jde o Úřad pro ochranu osobních údajů. [↑](#footnote-ref-11)
12. Zejména v souvislosti s užitím nových technologií. [↑](#footnote-ref-12)
13. Čl. 35. [↑](#footnote-ref-13)