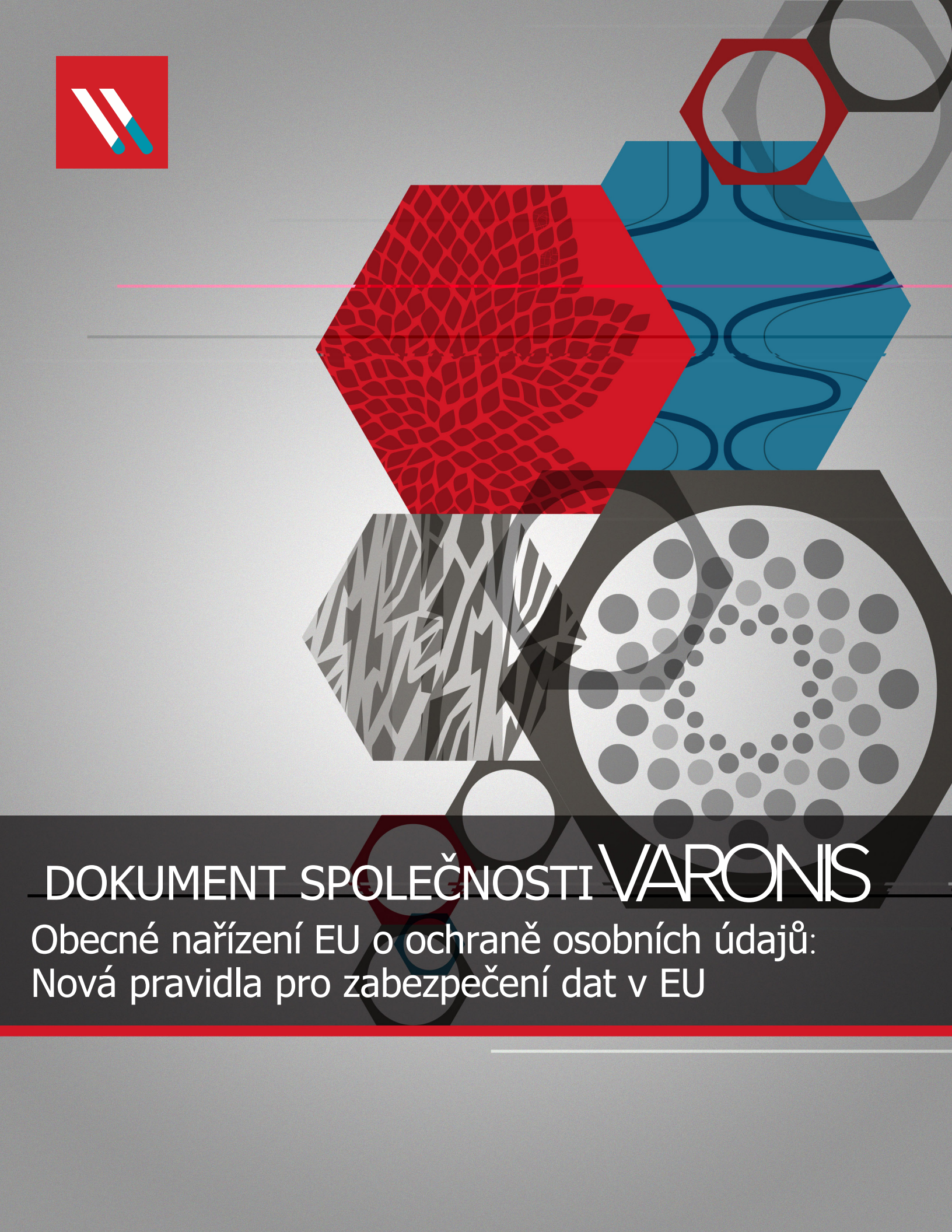

DOKUMENT SPOLEČNOSTI VARONIS

# Obecné nařízení EU o ochraně osobních údajů: Nová pravidla pro zabezpečení dat v EU

# OBSAH

# OBECNÉ NAŘÍZENÍ EU O OCHRANĚ OSOBNÍCH ÚDAJŮ: NOVÁ PRAVIDLA PRO ZABEZPEČENÍ DAT V EU

## PŘEHLED:

Když v roce 1995 přijala Evropská unie směrnici o ochraně osobních údajů (OOÚ), znamenalo to přijetí ambiciózních pravidel pro zabezpečení dat a ochranu soukromí. Směrnice vyžadovala získání souhlasu spotřebitele, stanovovala omezení počtu uchovávaných údajů a možnost opravy a odstranění osobních údajů na vyžádání a požadovala po organizacích mazání těch údajů, které již nepotřebují.

Evropská unie byla jedním z prvních, kdo mnohé principy ochrany soukromí – které dnes známe spíše pod názvem záměrná ochrana osobních údajů – zakotvil v reálných zákonech a pravidlech pro zabezpečení dat. Evropská směrnice pro ochranu osobních údajů (OOÚ) byla daleko před ostatními i z hlediska definice identifikovatelných údajů, které jsou označovány za osobní údaje a o jejichž ochranu se zákon snaží. Směrnice pro tyto údaje stanovila robustní definici, která se vztahuje jak na standardní identifikátory, tak na označení z internetové éry.

V průběhu let regulační orgány tuto směrnici různě interpretovaly a Evropský soudní dvůr k ní vydával různá rozhodnutí. Původní směrnice tak byla rozšířena, aby se vztahovala i na poskytovatele cloudových služeb, mazání údajů na internetu a přinejmenším pro USA zahrnovala i další rámec – Bezpečný přístav EU-US 1 – který se zabýval vývozem údajů mimo Evropskou unii.

Brzy se však ukázalo, že směrnice začíná zastarávat. Jedním z důvodů byl fakt, že umožňovala státům EU vytvářet na jejím základě vlastní zákony a poté je interpretovat. V důsledku toho se začaly objevovat rozdíly. Ačkoliv směrnice OOÚ představovala pevný základ, nebyla připravena na prudký nárůst objemu shromažďovaných a uchovávaných údajů a výslovně se nevěnovala jejich cloudovému zpracování, které se tak z hlediska předpisů stalo šedou zónou.

V prosinci 2015 bylo dokončeno nové obecné nařízení EU o ochraně osobních údajů (GDPR), které směrnici OOÚ nahradí. Toto nařízení vytváří jednotné právo platné v celé Evropské unii a řeší mnoho nedostatků směrnice OOÚ. GDPR vstoupí v platnost na počátku roku 2018.

GDPR stanoví požadavky na dokumentování procesů IT, vyhodnocování rizik za určitých podmínek, určí povinnost vyrozumět spotřebitele a úřady o narušení bezpečnosti a posílí pravidla nařizující uchovávat jen minimum údajů. Vzhledem k principu extrateritoriality, který GDPR uplatňuje, se nařízení bude vztahovat i na společnosti, které údaje o občanech EU shromažďují pouze na internetu, aniž by ve státě byly formálně přítomny.

A konečně, GDPR bude obsahovat značné finanční postihy za nedodržování pravidel. Maximální výše pokut je odstupňovaná, přičemž u některých porušení jde o 2 % světových příjmů firmy, zatímco u vážnějších o 4 %.

Celkově nové nařízení firmám, které pod jeho působnost spadají, vysílá poselství, že nyní bude ještě nezbytnější mít o shromažďovaných údajích dobrý přehled – o tom, kde se nacházejí, kdo k nim přistupuje a kdo by k nim přistupovat měl.

Abychom vaší společnosti pomohli splnit požadavky GDPR, uvádíme v příloze tabulku, která přiřazuje jednotlivé požadavky k produktům Varonis.

# STRUČNÝ POHLED NA SMĚRNICI EU O OCHRANĚ OSOBNÍCH ÚDAJŮ

Počátky směrnice EU o ochraně osobních údajů lze vystopovat v osmdesátých letech dvacátého století. Tehdy se Evropská komise rozhodla formalizovat principy ochrany soukromí – jako základního práva – formou sady pravidel pro zabezpečení dat, která měla nahradit tehdejší nesourodé národní předpisy [2].

Výsledkem byla směrnice OOÚ přijatá v roce 1995. Ačkoli se jí nepodařilo dosáhnout zamýšleného sjednocení pravidel pro ochranu údajů – k tomu se ještě vrátíme – znamenala začátek cesty k jednotnému přístupu Evropské unie k nim. Protože GDPR výrazně vychází z OOÚ – z hlediska terminologie i principů – podívejme se stručně na nejdůležitější aspekty této směrnice.

Směrnice OOÚ zavádí tři významné myšlenky související se spotřebiteli a údaji o nich, se shromažďováním těchto údajů a s jejich zpracováním.

Ve smyslu směrnice OOÚ znamenají osobní údaje informace „o identifikované nebo identifikovatelné fyzické osobě", která je označována jako subjekt údajů. Identifikovatelnou osobou se rozumí každý, koho „lze přímo či nepřímo identifikovat, zejména s odkazem na určité identifikační číslo nebo na jeden či více faktorů".

Zahrnuje to zjevné identifikační údaje, jako jsou telefonní čísla, adresy a čísla účtů, definice je však dostatečně flexibilní – cokoli vztahující se k dotyčné osobě – aby se vztahovala i na údaje, jejichž existenci autoři směrnice OOÚ nepředpokládali, například na e-mailové a IP adresy, biometrické údaje a dokonce i fotografie obličeje. Namísto statického seznamu jednotlivých identifikačních údajů – což bylo tehdy běžné – přišla směrnice OOÚ s definicí, která obstojí i v budoucnosti.

Kromě definování osobních údajů zavádí OOÚ i významné pojmy správce údajů a zpracovatel údajů, které pak hojně používá.

Správce údajů je každý, kdo určuje „účely a prostředky zpracování osobních údajů". To jinými slovy znamená, že správcem je společnost nebo organizace, která rozhoduje o prvotním přijetí údajů od subjektu údajů.

Zpracovatelem údajů je pak každý, kdo údaje pro správce zpracovává. Směrnice OOÚ jako formu zpracování výslovně uvádí i uchovávání, takže bere v úvahu centralizované databáze vlastněné třetími stranami.

Shrneme-li to, stanoví směrnice OOÚ pravidla pro ochranu osobních údajů během jejich shromažďování správci údajů a předávání zpracovatelům. Požadavky směrnice OOÚ byly napsány výslovně tak, aby se vztahovaly na správce. Zpracovatelé údajů jsou však vázáni povinností chránit osobní údaje na základě smluv se správci – to je uvedeno v článku 17.

Z toho především plyne, že směrnice OOÚ tyto dvě funkce připouští a že organizace mohou využívat služeb externích zpracovatelů. Směrnice předpokládala vzestup externích databází a v jistém smyslu i samotného cloudu – ačkoli tomu se daleko lépe věnuje až nové nařízení GDPR.

## ŘÍZENÍ PŘÍSTUPU K DŮVĚRNÝM INFORMACÍM

Se znalostí uvedených informací bude snazší pochopit konkrétnější požadavky této směrnice. Směrnice je založena na sedmi základních principech (viz schéma), které jsou stanoveny v jejím článku 6.

| | |
|---|---|
| 1. Korektnost | |
| | „Zákonné a korektní" zpracování údajů |
| 2. Specifický účel | Je nutno zajistit, aby údaje byly uchovávány a zpracovávány „s jasně uvedeným, jednoznačným a legitimním účelem a nebyly dále zpracovávány způsobem, který není s tímto účelem v souladu". |
| 3. Omezení | Je nutno zajistit, aby údaje byly „adekvátní a relevantní a nebyly nepřiměřené ve vztahu" k účelům, s nimiž jsou shromažďovány. |
| 4. Přesnost | Je nutno zajistit, aby údaje byly „přesné, a v případě potřeby je aktualizovat", takže jsou prováděny „všechny přiměřené kroky k zajištění nápravy či odstranění" chyb. |
| 5. Likvidace zastaralých údajů | Neuchovávat osobní údaje „déle, než je nezbytné" pro účely, pro které byly shromážděny a zpracovány. |
| 6. Bezpečnost | Údaje musí být zpracovány s adekvátním „zabezpečením" („Správce musí mimo to přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti ... zničení nebo ... ztrátě, úpravám a neoprávněnému sdělování nebo přístupu..."). |
| 7. Automatické zpracování | „Rozhodnutí" o zpracovávání údajů nesmí „vycházet výlučně z automatizovaného zpracování údajů," které „hodnotí osobní aspekty". |

To by pro vás nemělo být novinkou, protože to souvisí s principem záměrné ochrany osobních údajů (PbD). Obojí přitom vychází ze starších principů, zakotvených v pokynu Organizace pro hospodářskou spolupráci a rozvoj (OECD) o ochraně soukromí 3. V každém případě i GDPR tyto principy obsahuje – viz článek 5 – a dále je rozšiřuje a posiluje.

Tyto principy se staly základem jednotlivých článků směrnice OOÚ. Podívejme se na tři nejdůležitější.

Článek 12 (právo na přístup) „stanoví právo subjektu údajů požadovat po správci, aby ... v přiměřené míře opravil, vymazal nebo zablokoval údaje, jejichž zpracování není v souladu s touto směrnicí, zejména kvůli neúplnosti nebo nepřesnosti těchto údajů".

Podle směrnice OOÚ tedy spotřebitelé skutečně mají právo požadovat vymazání (a opravu) údajů – ačkoli se toto pravidlo vztahuje jen na správce. V průběhu let různé soudní rozsudky rozšířily pravidlo o výmazu i na zpracovatele a konkrétně i na cloudové vyhledávací služby. Bylo by samozřejmě přehlednější, kdyby správce i zpracovatele přímo zmiňovala již původní směrnice OOÚ v článku 12.

Směrnice OOÚ stanoví správcům i další povinnosti. Její článek 6 po nich požaduje, aby osobní údaje byly „přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány," a poté vymazány, nejsou-li již dále potřeba.

Tyto dva články v podstatě zajišťují uplatňování zásad minimalizace uchovávaných údajů, zakotvených v principech 2 a 5 směrnice OOÚ.

Článek 17 (bezpečnost zpracování) říká, že správce „musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení ... neoprávněnému sdělování nebo přístupu".

Ačkoli zabezpečení údajů by mělo být základní součástí zákona, který začíná slovy „ochrana údajů", byla směrnice OOÚ v tomto ohledu ještě poněkud vágní.

Směrnice OOÚ funguje jako jakási šablona a od států EU se čeká, že pravidla „přenesou" do konkrétních zákonů. Ty pak vymáhá úřad pro ochranu osobních údajů (DPA) příslušného státu. To ovšem vedlo k problémům, protože se objevily různé interpretace a systémy vymáhání podle toho, v jaké zemi správce údajů sídlil.

# TECHNOLOGICKÝ VÝVOJ: SNAHA PŘIZPŮSOBIT SMĚRNICI O OCHRANĚ OSOBNÍCH ÚDAJŮ

Až donedávna se předpisy o zabezpečení dat netěšily pozornosti sdělovacích prostředků. Jistě, po svém přijetí na konci 90. let se směrnice OOÚ týkala převážně advokátů, pracovníků zodpovědných za dodržování předpisů a v omezené míře i vedoucích pracovníků IT. Jenže pak přišel internet, revoluce v ukládání dat a všudypřítomná spotřebitelská zařízení.

Výsledek? Exponenciální meziroční nárůst množství informací, které jsou ukládány a přístupné ze spotřebitelských zařízení.

Prvním problémem, který se objevil v souvislosti se strukturou směrnice OOÚ a těmito změnami, bylo, že každý stát měl určitou svobodu ve způsobu interpretace základních pravidel.

V internetové éře se například zrodil zcela nový zdroj elektronických identifikátorů: e-mailové a IP adresy, internetové identifikátory a biometrické údaje. Jsou to ale osobní údaje? V mnoha státech Evropské unie byly tyto základní elektronické identifikátory chráněny, některé úřady pro ochranu osobních údajů je však za osobní údaje nepovažovaly. [4]

Objevily se ovšem i další rozdíly týkající se přenosů dat. Některé státy se tak staly daleko zajímavější než jiné, pokud jde o umístění sídla firmy a datových center. [5]

Mnohonárodní společnosti se brzy naučily pečlivě si vybírat, kam umístí své sídlo. Tím v podstatě podrývaly záměr směrnice OOÚ zajistit v oblasti ochrany údajů jednotné právo.

Spolu se vzestupem cloudu a vzhledem k obrovskému objemu zpracování a úložišť dostupných na vyžádání se objevily i otázky ohledně právního postavení takových služeb. Vzpomeňte si, že směrnice OOÚ je zaměřena na správce údajů.

Je ale cloud správcem údajů nebo jejich zpracovatelem?

V roce 2012 pracovní skupina EU pro článek 29, jejímž úkolem je radit ve věcech OOÚ, vydala doporučení: Společnosti, které využívají cloud, jsou správci, protože řídí, jak by měl provozovatel cloudu s daty nakládat [6]. Samotný cloud je tedy zpracovatelem.

Na své místo pak zapadlo i všechno ostatní. Jako zpracovatel musí mít provozovatel cloudu podle směrnice OOÚ uzavřenou platnou smlouvu.

Pracovní skupina dodala, že zákazníci cloudu by od provozovatele cloudu neměli akceptovat standardizované a plošně používané smlouvy. Namísto toho by smlouvy mezi těmito stranami měly zajišťovat určité minimální zabezpečení údajů podle směrnice OOÚ a právo na přístup k nim – provozovatel cloudu musí například vyhovět žádosti o smazání údajů o zákazníkovi.

Nicméně i v tomto případě měly jednotlivé úřady na ochranu osobních údajů interpretační volnost a mohly určovat vlastní podmínky těchto smluv. [7]

Další problémy se týkaly provozovatelů vyhledávacích strojů, kteří by, jakožto zpracovatelé údajů v cloudu, taktéž museli na vyžádání vymazat údaje – v jejich případě výsledky vyhledávání. Tato záležitost byla teprve nedávno po dlouhém soudním sporu vyřešena [8].

Podle Evropského soudního dvora aktuální směrnice OOÚ v podstatě stanoví „právo být zapomenut". Je zajímavé, že toto právo má extrateritoriální povahu – osobní údaje občanů EU lze vymazat i v případě, že zpracovatel údajů nesídlí v žádném ze států EU [9].

Daleko přímočařejší by samozřejmě bylo, kdyby směrnice OOÚ jednoznačněji definovala zpracovatele dat a právo na vymazání údajů a členské státy by tedy měly v interpretaci těchto pravidel méně volnosti. To vše se brzy změní.

# NOVÉ OBECNÉ NAŘÍZENÍ EU O OCHRANĚ OSOBNÍCH ÚDAJŮ

Evropská komise si uvědomovala nutnost zastaralou směrnici o ochraně osobních údajů přepracovat a v roce 2012 zahájila práci na novém právním předpisu. Jejím hlavním cílem bylo vytvořit jediný zákon vztahující se na všechny státy EU a zavést jednotný přístup k jeho vymáhání prostřednictvím jediného úřadu pro ochranu osobních údajů. Výsledkem je obecné nařízení o ochraně osobních údajů (GDPR), které vstoupí v platnost na počátku roku 2018.

GDPR není úplným přepracováním směrnice OOÚ. Stávající směrnici spíše vylepšuje. Stanoví však i nové požadavky, zejména na oznamování narušení bezpečnosti a vedení rozsáhlejší dokumentace.

## ČÁST JE STARÁ A PŘEPRACOVANÁ

Podívejme se nejprve, co GDPR zpřesňuje a přepracovává.

Za prvé, GDPR zdokonaluje definici osobních údajů tak, aby bylo ještě jasnější, že zahrnuje více než jen zjevné identifikační údaje. Říká, že osobním údajem je cokoli, pomocí čeho lze subjekt identifikovat „přímo nebo nepřímo pomocí všech prostředků, o nichž lze rozumně předpokládat, že budou (někým) použity". Tato formulace je jednoznačnější v tom, že zahrnuje takzvané poloidentifikátory, tedy samostatné informace či skupiny informací – například geolokační údaje – které s pomocí odkazů na další externí údaje lze nepřímo využít k určení osoby.

GDPR stanoví konkrétnější povinnosti pro zpracovatele údajů, a tedy i pro cloud. Ty jsou popsány v článcích 26 (zpracovatel) a 30 (bezpečnost zpracování) – jsou obdobou článku 17 směrnice OOÚ – a v podstatě říkají, že poskytovatel cloudu musí chránit bezpečnost údajů, které mu byly jejich správcem svěřeny. Nařízení GDPR přidává možnost, aby spotřebitel přímo zažaloval zpracovatele o náhradu škod – ve směrnici OOÚ mohl nést odpovědnost pouze správce [10].

Článek 5 (principy týkající se zpracování osobních údajů) v podstatě odráží požadavky na minimalizaci údajů stanovené v článku 6 směrnice OOÚ: osobní údaje musí být „přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány...“ Dále však říká, že za bezpečnost a zpracování údajů nese konečnou odpovědnost jejich správce.

Myšlenky záměrné ochrany údajů dále rozvádí článek 23 (záměrná a standardní ochrana osobních údajů). Ten explicitněji stanoví omezení pro uchovávání dat a pravidla pro jejich minimalizaci. Určuje, že je standardně nutno stanovit pro údaje určité limity (doba uchovávání, přístup), a dává Komisi pravomoc později přijmout konkrétnější technické předpisy.

## A ČÁST JE NOVÁ

Článek 28 (dokumentace) přidává správcům a zpracovatelům nové požadavky na dokumentování jejich činnosti. Nejdůležitějším z nich je zavedení pravidel pro kategorizaci údajů shromažďovaných správci, zaznamenávání příjemců, jimž jsou údaje sděleny, a uvedení časových limitů pro dobu uchovávání osobních údajů před jejich smazáním.

Článek 33 požaduje, aby správce před spuštěním nových služeb nebo produktů pracujících s údaji o zdraví, ekonomické situaci, poloze a osobních preferencích subjektu – konkrétně i údajů týkajících se rasy, pohlavního života a infekčních chorob – prováděl analýzy vlivu ochrany osobních údajů (DPIA). Účelem DPIA je chránit soukromí subjektu dat tím, že mimo jiné požaduje, aby správce popsal použité způsoby zabezpečení.

Největší mediální pozornost si zřejmě získalo nové pravidlo o oznamování narušení bezpečnosti. Před přijetím GDPR musely narušení bezpečnosti do 24 hodin oznámit pouze telekomunikační a internetoví operátoři, kterým to ukládá směrnice o ochraně soukromí v elektronické komunikaci [11].

Článek 31 GDPR byl vytvořen po vzoru starší směrnice a stanoví, že správci musí dozorčímu úřadu sdělit povahu narušení bezpečnosti, kategorie údajů a počet dotčených subjektů údajů a dále opatření, která provedli s cílem dopad bezpečnostního průlomu omezit.

Pokud narušení bezpečnosti osobních údajů ohrožuje spotřebitele, musí jej správci příslušnému dozorčímu úřadu oznámit (nejpozději) do 72 hodin od okamžiku, kdy se o něm dozví. Ale i v případě méně vážných ohrožení si firma musí vést alespoň interní záznamy.

Podle GDPR je za narušení bezpečnosti považováno nezákonné zničení, ztráta, úpravy, neoprávněné sdělování osobních údajů nebo přístup k nim.

Článek 32 dále stanoví, že o narušení bezpečnosti musí být informovány i subjekty dat, ovšem až poté, co je informován dozorčí úřad. Pokud firma údaje uchovává zašifrované nebo podnikla jiná bezpečnostní opatření, díky nimž jsou údaje nečitelné, nemusí subjekty informovat.

Článek 17 (právo na vymazání a právo být zapomenut) posílilo stávající pravidla ve směrnice OOÚ týkající se mazání údajů. Dále doplnil kontroverzní právo na zapomenutí. Nové nařízení tedy přímo vyžaduje, aby správci podnikli přiměřené kroky k informování třetích stran o požadavku na výmaz informací. To znamená, že v případě sociálních sítí, které na webu zveřejňují osobní údaje svých členů, budou tyto firmy muset nejenom odstranit původní informace, ale také kontaktovat jiné weby, které mohly dotyčné informace převzít. To ovšem nebude jednoduchý proces.

A konečně, jedním z méně mediálně probíraných požadavků, který však bude mít významné dopady, je nový princip extrateritoriality popsaný v článku 3. Ten říká, že pokud firma shromažďuje údaje o subjektech údajů z EU – například na webových stránkách – tak pro ni platí všechny požadavky GDPR i v případě, že není v EU fyzicky přítomna.

Jde o značně kontroverzní myšlenku zejména z hlediska toho, jak by ji bylo možno vymáhat. Jak jsme již poukázali, tato myšlenka už byla v menší míře aplikována ve stávající směrnice OOÚ, a to v případě vyhledávačů.

# ZÁVĚRY: CO JE TŘEBA KE SPLNĚNÍ POŽADAVKŮ GDPR

Během jednání Evropského parlamentu, Rady a Komise byl konečný návrh GDPR vytvořen na základě různých verzí předkládaných účastníky jednání.

Mezi hlavní rozdíly, které byly v prosinci 2015 vyřešeny, patří struktura pokut stanovená GDPR, pracovníci pro ochranu údajů (DPO) a oznamování narušení bezpečnosti. O oznamovací povinnosti jsme již mluvili, zmíníme se tedy o zbylých dvou oblastech.

GDPR definuje odstupňovanou strukturu pokut. Společnost může dostat pokutu až do výše 2 % svého celosvětového příjmu, pokud nebude mít v pořádku záznamy (článek 28), neoznámí dozorčímu úřadu a subjektu údajů, že došlo k narušení bezpečnosti (články 31 a 32), nebo neprovede posouzení vlivu (článek 33).

Za vážnější porušení lze dostat až 4% pokutu. Patří mezi ně porušení základních principů zabezpečení údajů (článek 5) a podmínek týkajících se souhlasu spotřebitele (článek 7) – jde v podstatě o porušení základních myšlenek záměrné ochrany osobních údajů obsažených v tomto právním předpisu.

Pravidla směrnice GDPR EU se vztahují na správce i zpracovatele dat, tedy na „cloud". Vymáhání GDPR se tedy bude týkat i obřích poskytovatelů cloudových služeb.

V průběhu jednání se objevily rozdílné názory na to, zda mají mít firmy povinnost jmenovat pracovníka pro ochranu údajů, který by byl zodpovědný za dohled nad dodržováním GDPR a související poradenství a zároveň by firmu zastupoval při jednáních s dozorčím úřadem. Vzhledem ke konečné podobě GDPR bude takového pracovníka pro ochranu údajů, neboli DPO, zřejmě potřebovat celá řada firem (článek 35).

Pokud hlavní činnost vaší společnosti zahrnuje „systematické monitorování subjektů údajů ve velkém rozsahu" nebo rozsáhlé zpracování „zvláštních kategorií" údajů – o rasovém či etnickém původu, politických názorech, náboženských nebo filosofických názorech, zdravotním stavu, pohlavním životě nebo sexuální orientaci, případně jde o biometrické údaje – pak musíte DPO jmenovat.

Byly však stanoveny výjimky pro malé a střední podniky, na něž se nevztahuje požadavek jmenování DPO ani oznamovací povinnost vůči dozorčím úřadům. A nebudou muset ani provádět výše zmíněné analýzy vlivu ochrany údajů.

V případě společností z EU a jejich amerických či jiných zahraničních poboček, na něž se již vztahuje současná směrnice OOÚ, bude nové nařízení GDPR považováno za evoluci stávajících předpisů. Kvůli oznamovací povinnosti narušení bezpečnosti a novým požadavkům na dokumentaci nicméně budou muset věnovat dodržování předpisů větší úsilí.

Pro společnosti, zejména ty americké, které spadnou do sítě extrateritoriality, bude GDPR tak trochu šokem. Platí to zvláště pro webové služby, které nepodléhají regulaci podle stávajících amerických zákonů o zabezpečení finančních a lékařských údajů.

Společnosti, které již uplatňují standardy zabezpečení dat v IT – SANS 20, PCI DSS, ISO 27001 nebo NIST 800-53 – by neměly mít s dodržením evropského GDPR problémy.

Naše obecné doporučení pro všechny společnosti, jichž se nový zákon týká, je zaměřit se na níže uvedené body:

- **Klasifikace údajů** – Mějte přehled o tom, kde ve vašem systému jsou uloženy osobní údaje, zejména v případě nestrukturovaných formátů dokumentů, prezentací a tabulek. Má to zásadní význam jak pro ochranu údajů, tak pro možnost vyhovět žádostem na opravu nebo vymazání osobních údajů.
- **Metadata** – Vzhledem k požadavku na omezení doby uchovávání údajů budete potřebovat základní informace o tom, kdy byly údaje získány, proč a k jakému účelu. Osobní údaje v systémech IT by měly být periodicky kontrolovány a mělo by být ověřováno, zda je ještě třeba je dál ukládat.
- **Řízení dat** – Vzhledem k uzákonění záměrné a standardní ochrany osobních údajů by se společnosti měly zaměřit na základy řízení dat. U nestrukturovaných údajů by to mělo zahrnovat informace o tom, kdo k osobním údajům ve firemním systému přistupuje a kdo by oprávnění k přístupu mít měl, a dále omezení souborových oprávnění na základě skutečných rolí zaměstnanců – tedy řízení přístupu podle rolí.
- **Monitorování** – Povinnost oznamovat narušení bezpečnosti je pro správce údajů novým břemenem. Podle GDPR by mantra zabezpečení IT měla znít „nikdy nepřestávejte monitorovat". Budete muset být schopni rozpoznat nezvyklé vzorce přístupu k souborům s osobními údaji a rychle o zjištěném ohrožení informovat místní úřad pro ochranu osobních údajů. Nedodržením této povinnosti se můžete vystavit obrovským pokutám, zejména v případě mnohonárodních společností s vysokými celosvětovými příjmy.

# PŘÍLOHA

## Přiřazení relevantních článků GDPR EU k produktům a řešením společnosti Varonis

| **Požadavek EU** | | **Řešení Varonis** |
|---|---|---|
| Kapitola III: Práva subjektu údajů | | |
| Oddíl 2: Oprava a výmaz<br>Článek 17: Právo na výmaz a „právo být zapomenut“ | …subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají... | **Uchovávání, archivace a likvidace osobních údajů**<br><br>Varonis Data Transport Engine spolu se systémem Varonis Data-Classification Framework umožňují flexibilně nastavit úplná pravidla migrace: definovat podmínky zdroje podle cesty a obsahu, klasifikační pravidla, vlastnictví a sledování v systému Varonis (značka/štítek), určit cílovou cestu, složku a převod oprávnění i čas provedení migrace.<br><br>Díky možnosti nastavení těchto pravidel lze rychle a bezpečně provést i složité datové migrace a snadno zavést a uplatňovat zásady pro uchovávání a odstraňování údajů. |
| Kapitola IV: Správce a zpracovatel | | |
| Oddíl 1: Obecné povinnosti<br>Článek 23: Záměrná a standardní ochrana osobních údajů | …aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob. | **Systém řízení přístupu**<br><br>Systém Varonis DatAdvantage monitoruje každý kontakt uživatele a souboru a ve formátu s možností prohledávání ukládá všechny aspekty využívání údajů týkající se informací uložených na souborových serverech a na zařízeních NAS (Network Attached Storage).<br><br>Protože DatAdvantage zjišťuje, kdo má k údajům přístup, a sleduje každý kontakt uživatele se souborem, dokáže doporučit odebrání přístupového oprávnění k datům u těch uživatelů, kteří nemají pracovní důvod příslušné údaje znát – díky tomu je přístup uživatelů k údajům vždy odůvodněný a je založen na principu nejnižšího možného oprávnění.<br><br>DatAdvantage poskytuje správcům údajů podrobné sestavy včetně informací o každém kontaktu uživatelů dat se souborem, o uživatelských aktivitách souvisejících s citlivými údaji a o změnách oprávnění týkajících se přístupu k určenému souboru nebo složce. Vede i podrobné záznamy o rušení oprávnění včetně uživatelů a údajů, pro něž byla oprávnění odebrána.<br><br>Varonis DataPrivilege je webová aplikace, která řídí, monitoruje a spravuje žádosti uživatelů o nestrukturovaná data (soubory, e-maily, SharePoint atd.).<br><br>Další informace o záměrné ochraně osobních údajů naleznete v příspěvku „PbD Cheat Sheet“ na našem blogu. |

| Požadavek EU | | Řešení Varonis |
|---|---|---|
| Oddíl 1: Obecné povinnosti<br><br>Článek 28: Záznamy o kategoriích činností při zpracování osobních údajů | Každý správce (...) a jeho případný zástupce vede záznamy o činnostech zpracování všech kategorií osobních údajů, za něž odpovídá. | 64 % organizací tvrdí, že neví, kde se u nich citlivý obsah nachází nebo kdo k němu má přístup. Najít citlivý obsah je však teprve začátek. Jakmile víte, kde citlivý obsah uchováváte, přichází ty skutečně obtížné otázky:<br>• Kdo k němu má přístup?<br>• Kdo jej využívá?<br>• Kdo jej vlastní?<br>• Byla narušena jeho bezpečnost?<br>• Mohu jej vymazat nebo archivovat?<br>• Kde jsem nejvíce ohrožen?<br>• Koho se dotkne, pokud něco změním?<br><br>Díky systému Varonis DatAdvantage mohou organizace kdykoli provádět kontroly zabezpečení dat (atestace) a jediným kliknutím myši sestavovat přehledy přístupu. Tyto informace mohou být úzce zaměřeny na údaje určitého typu či na přístupy prováděné určitou skupinou, nebo široce na trendy přístupu v celé organizaci (tedy přehledy aktivních a neaktivních uživatelů, aktivních a zastaralých data, vlastnictví dat v organizaci atd.). Auditorům umožňují zjistit, zda existují a jsou uplatňovány vhodné bezpečnostní zásady. |
| Oddíl 2: Zabezpečení údajů<br><br>Článek 30: Zabezpečení zpracování | ... aby zajistili úroveň zabezpečení odpovídající danému riziku. | **Snížení rizika a řízení přístupu**<br><br>Pomocí systému Varonis DatAdvantage můžete vytvářet přehledy, které umožní odhalovat nadbytečné přístupy k citlivým údajům s velkým rizikem, stanovovat pro ně priority a následně je řešit.<br><br>Varonis DataPrivilege pomáhá definovat zásady a postupy, podle nichž se řídí to, kdo má přístup k nestrukturovaným údajům a kdo může přístup k nim udělovat. Slouží však také k uplatňování pracovních postupů a provádění požadovaných akcí (tedy například povolit, odmítnout, povolit na určitý čas). To má dvojí vliv na konzistentní a dobrou informovanost o přístupových zásadách:<br>• poskytuje všem zodpovědným stranám včetně vlastníků dat, auditorů, uživatelů dat a pracovníků IT stejnou sadu informací,<br>• a umožňuje organizacím průběžně monitorovat systém přístupových oprávnění a pomocí jeho změn a optimalizací zajišťovat, aby byla oprávnění vždy odůvodněná.<br><br>Díky systémům DatAdvantage a DataPrivilege mohou pracovníci dohlížející na dodržování předpisů a auditoři pravidelně dostávat zprávy o využívání dat a přístupových aktivitách k privilegovaným a chráněným informacím. To jim pomůže zajistit jejich bezpečnost a využívání v souladu s předpisy. |

| Požadavek EU | | Řešení Varonis |
|---|---|---|
| Oddíl 2: Zabezpečení údajů<br><br>Článek 31: Oznamování případů porušení | Jakékoli porušení zabezpečení osobních údajů ... musí správce ohlásit dozorčímu úřadu bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl... | **Analýza chování uživatelů**<br><br>Technologie UBA vyhledává vzorce využívání, které naznačují neobvyklé či anomální chování – bez ohledu na to, zda má dotyčnou aktivitu na svědomí hacker, vlastní zaměstnanec firmy nebo třeba škodlivý software či jiné procesy.<br><br>Díky systému DatAlert a jeho upozorněním v reálném čase bude vaše organizace schopna dodržet limit 72 hodin. Nechte si zasílat upozornění:<br><br>• kdykoli budou mazány tisíce citlivých souborů,<br>• když uživatel (nebo útočník) získá kořenový přístup,<br>• když dojde ke změně důležitých bezpečnostních skupin nebo skupinových zásad,<br>• jsou porušena oprávnění k citlivým složkám,<br>• dojde k riskantním změnám mimo časové období vyhrazené pro změny,<br>• škodlivý software šifruje soubory na vašich serverech.<br><br>Upozornění můžete dostávat e-mailem, formou protokolu událostí, v syslogu nebo si je nechat posílat na vaše SIEM či do nástrojů pro správu sítě. |
| Oddíl 2: Zabezpečení údajů<br><br>AČlánek 33: Posouzení vlivu na ochranu osobních údajů | ... správce před zpracováním provede posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. (...) | DatAdvantage vám může s posouzením rizik. Po kliknutí sem budete moci provést bezplatné vyhodnocení rizik pomocí systému Varonis:<br><br>Ochrana proti hrozbám zvenku i zevnitř, ať už zlovolným nebo neúmyslným, je nesmírně náročná. O to náročnější, že 71 % zaměstnanců tvrdí, že má přístup k informacím, které vůbec nemají vidět!<br><br>Pomůžeme vám:<br><br>• znepřístupnit nadměrně přístupný citlivý obsah,<br>• omezit účty s nadbytečnými oprávněními,<br>• analyzovat účty vykazující podezřelou aktivitu,<br>• upozorňovat na rozšiřování oprávnění,<br>• odhalovat útoky typu CryptoLocker a další škodlivé programy,<br>• vyhledávat zastaralé účty a skupiny,<br>• …a mnoho dalšího! |

## REFERENCE


[1] http://www.export.gov/safeharbor/eu/eg_main_018476.asp

[2] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

[3] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[4] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/IP%20addresses%20subject%20to%20Personal%20Data%20Regulation.pdf

[5] http://techcrunch.com/2013/07/25/ireland-prism/

[6] http://idpc.gov.mt/dbfile.aspx/WP196.pdf

[7] http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework

[8] http://searchengineland.com/library/legal/legal-right-to-be-forgotten

[9] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[10] http://blogs.lexisnexis.co.uk/wipit/open-season-on-service-providers-the-general-data-protection-regulation-cometh/

[11] http://www.insideprivacy.com/data-security/data-breaches/data-breach-notification-within-24-hours-in-the-electronic-communication-sector-an-example-to-foll/


## ZÁKONY EU TÝKAJÍCÍ SE ÚDAJŮ

*Směrnice o ochraně osobních údajů:*
http://eur-lex.europa.eu/LexUriServ/LexUriServdo?uri=CELEX:31995L004:en:HTML

*Obecné nařízení EU o ochraně osobních údajů (parlamentní verze)*
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:en:PDF

*Obecné nařízení EU o ochraně osobních údajů (verze Rady):*
http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

# O SPOLEČNOSTI VARONIS

Varonis je předním dodavatelem softwarových řešení, která chrání data před kybernetickými útoky i hrozbami od vlastních zaměstnanců. Prostřednictvím inovativní softwarové platformy Varonis organizacím umožňuje analyzovat, zabezpečovat a migrovat velká množství nestrukturovaných údajů. Varonis se specializuje na souborové a e-mailové systémy, v nichž jsou ukládány cenné tabulky, textové dokumenty, prezentace, zvukové a video soubory, e-maily a texty. Tyto rychle se zvětšující data často obsahují finanční informace o firmě, její produktové plány, strategické iniciativy, duševní vlastnictví a důvěrné záznamy o zaměstnancích, zákaznících nebo pacientech. Firmy i pracovníci IT využívají software od společnosti Varonis k mnoha různým účelům, například k zabezpečení nebo řízení dat, k zajištění souladu s předpisy, k analýze chování uživatelů, k archivaci, k vyhledávání a k synchronizaci a sdílení souborů.

## Vyzkoušejte si zdarma náš software po dobu 30 dní:

### BĚHEM NĚKOLIKA HODIN PO INSTALACI

Budete moci okamžitě provést kontrolu oprávnění: Zjistíte oprávnění k přístupu k souborům a složkám a jejich přiřazení ke konkrétním uživatelům a skupinám. Budete dokonce moci vytvářet přehledy.

### BĚHEM JEDNOHO DNE PO INSTALACI

Varonis DatAdvantage začne zobrazovat, kteří uživatelé k datům přistupují a jakým způsobem.

### DO TŘÍ TÝDNŮ PO INSTALACI

Varonis DatAdvantage vám začne předkládat velmi užitečná doporučení o tom, jak by bylo možno omezit přístup k souborům a složkám pouze na ty uživatele, kteří je ke své práci potřebují.

STÁHNOUT BEZPLATNOU ZKUŠEBNÍ VERZI