Ochrana osobních údajů a GDPR

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Obsah

Seznam zkratek

DPA: Data Protection Authority (Úřad pro ochranu údajů)

DPO: Data Protection Officer (Úředník pro ochranu údajů)

DSG: Austrian data protection act Datenschutzgesetz (Rakouský zákon o ochraně údajů)

DSVGO: German Datenschutz-Grundverordung

EEA: European Economic Area (Evropský hospodářský prostor)

ePR: ePrivacy Regulation (Regulace elektronického soukromí)

EU: European Union (Evropská unie)

GDPR: General Data Protection Regulation (Obecné nařízení o ochraně údajů)

Obrázky

Tabulky

1. Úvod

V dnešní době je svět stále více závislý na datech, jelikož právě data mohou významně zvýšit hodnotu mnoha ekonomických subjektů. V Evropské unii (EU) existují předpisy týkající se osobních údajů: nařízení (EU) 2016/679 (obecné nařízení o ochraně údajů) a nařízení o elektronickém soukromí – ePrivacy (ePR), které je návrhem směrnice o soukromí a elektronických komunikacích z roku 2002 (ePrivacy Směrnice 2002/58 / ES).

Cílem nařízení (EU) 2018/1807 je odstranit překážky týkající se volného pohybu neosobních údajů napříč členskými státy EU a informačních technologií v Evropě. Spolu s obecným nařízením o ochraně údajů (GDPR) zajišťuje toto nařízení komplexní a soudržný přístup k volnému pohybu všech údajů v Evropě. Předmětem ePR je posílit důvěru a bezpečnost na jednotném digitálním trhu aktualizací právního rámce pro ePrivacy (ePR).

Tato tři nařízení se vztahují na každou evropskou zemi, i když existují určitá úvodní ustanovení, která ponechávají vnitrostátním zákonodárcům určitou volnost.

V této zprávě naleznete nejdůležitější informace týkající se těchto právních předpisů. Dokument dále přináší informace, jak byla evropská legislativa o ochraně osobních údajů upravena v Rakousku, Španělsku, Portugalsku a České republice.

2. GDPR

GDPR (Nařízení (EU) 2016/679) je zákon EU o ochraně údajů a soukromí pro všechny jednotlivé občany EU a Evropského hospodářského prostoru (EHP). Zabývá se také exportem osobních údajů mimo výše uvedené zeměpisné oblasti. GDPR je v platnosti od května 2018 a má tři hlavní cíle:

a) Harmonizovat zákony o ochraně osobních údajů v celé Evropě;

b) Chránit a posilovat soukromí všech občanů EU;

c) Změnit způsob, jakým organizace v celém regionu přistupují k ochraně osobních údajů.

Obrázek 1 - GDPR

Zdroj: Business2Community (2019)

S GDPR Evropa signalizuje svůj pevný postoj k ochraně osobních údajů a bezpečnosti a GDPR mění způsob, jakým společnosti / organizace spravují data. GDPR se vztahuje na:

a) **společnost nebo subjekt, který zpracovává osobní údaje v rámci činnosti jedné z jejích poboček působících v EU**, bez ohledu na to, kde jsou údaje zpracovávány; nebo,

b) **společnost nebo subjekt působící mimo EU, který nabízí zboží / služby** (placené nebo bezplatné) nebo které monitorují chování jednotlivců v EU.

2.1. Principy GDPR

GDPR má některé obecné zásady týkající se procesu osobních údajů. Jeden z těchto principů vyžaduje transparentní zpracování dat, což znamená, že tento proces musí být jasný a legitimní. Také množství zpracovaných dat musí být udržováno na minimu, v závislosti na účelu, musí být data přesná, a doba skladování musí být omezena na dobu, která je vázána pro tento účel. Kromě toho musí být chráněna integrita a důvěrnost údajů. Hlavní principy GDPR jsou uvedeny na následujícím obrázku.

Obrázek 2 - Principy GDPR

Zdroj: I-scoop (2019)

Obecně je hlavním kontaktním místem pro otázky týkající se ochrany údajů Zákon o ochraně údajů (DPA) dostupný v každém členském státě EU, ve kterém má společnost / organizace sídlo. Pokud však vaše společnost / organizace zpracovává údaje v různých členských státech EU nebo je součástí skupiny společností se sídlem v různých členských státech EU, může být hlavním kontaktním místem DPA v jiném členském státě EU.

Národní úřad pro ochranu údajů najdete na adrese:
https://edpb.europa.eu/about-edpb/board/members_en

2.2. Používání, zpracování, ukládání a přenos údajů v EU

Jako jednotlivec, společnost nebo organizace máte právo používat, shromažďovat, ukládat, přenášet nebo spravovat osobní údaje a používat datová centra nebo cloudové služby kdekoli v EU. Pravidla pro nakládání s osobními údaji se liší od pravidel pro neosobní údaje. Osobní a jiné, než osobní údaje se však často shromažďují a ukládají společně, což se nazývá smíšené údaje. Při zpracování osobních údajů, které jsou na následujícím obrázku, musí společnosti / organizace splnit určitá témata.

Obrázek 3 - Zpracování osobních údajů

Zdroj: European Commission (2019)

Během zpracování mohou osobní data procházet různými společnostmi nebo

organizacemi a v rámci tohoto cyklu existují dva hlavní profily, které se zabývají zpracováním osobních údajů: správce údajů a zpracovatel údajů.

Obrázek 4 – Kontrolor dat a procesor dat

Kontrolor dat: určuje účel a způsob zpracování osobních údajů

Procesor dat: uchovává a zpracovává data jménem správce dat

Zdroj: vlastní zpracování

Společnosti / organizace zpracovávající údaje jsou povinny vést záznamy o zpracovatelských činnostech, pokud nemají méně než 250 zaměstnanců. Společnosti / organizace musí také jmenovat inspektora ochrany údajů (DPO), pokud platí jeden z následujících aspektů:

- Je-li zpracování prováděno veřejným orgánem (s výjimkou soudů);
- Pokud se hlavní činnosti zpracovatele „skládají ze zpracování, které vzhledem ke své povaze, rozsahu a / nebo účelu vyžadují pravidelné a systematické monitorování údajů ve velkém měřítku";
- Při zpracování zvláštních kategorií údajů nebo „údajů týkajících se odsouzení za trestný čin".

DPO někdo, koho mohla určit společnost a odpovídá za sledování zpracování osobních

údajů a za informování zaměstnanců, kteří zpracovávají osobní údaje a informují o nich. DPO může být zaměstnancem vaší organizace nebo může být navázán externě na základě servisního kontaktu. DPO rovněž spolupracuje s Úřadem pro ochranu údajů (DPA), který slouží jako kontaktní místo vůči DPA a občanům.

2.3. Souhlas se zpracováním údajů

Odpovědnost za dodržení GDPR závisí na společnostech / organizacích, které zpracovávají osobní údaje. S přihlédnutím k povaze, rozsahu, kontextu a účelu zpracování a závažnosti pro práva a svobody občanů zavede správce vhodná technická a organizační opatření, aby zajistil a mohl prokázat, že zpracování je prováděno v souladu s tímto nařízení. Tato opatření se v případě potřeby přezkoumají a aktualizují. Příkladem těchto opatření je například šifrování.

GDPR uplatňuje přísná pravidla pro zpracování dat na základě souhlasu. Účelem těchto pravidel je zajistit, aby jednotlivec rozuměl tomu, s čím souhlasí. To znamená, že souhlas by měl být požadován kladným aktem, jako je zaškrtnutí políčka online nebo podepsání formuláře. Pokud někdo souhlasí se zpracováním svých osobních údajů, můžete je zpracovat pouze pro účely, pro které byl souhlas udělen. Je také důležité říci, že musíte jednotlivcům jasně poskytnout informace o tom, kdo o nich zpracovává osobní údaje, a o důvodech. Například by měl být uveden minimálně následující údaj:

Obrázek 5 - Zpracování osobních údajů

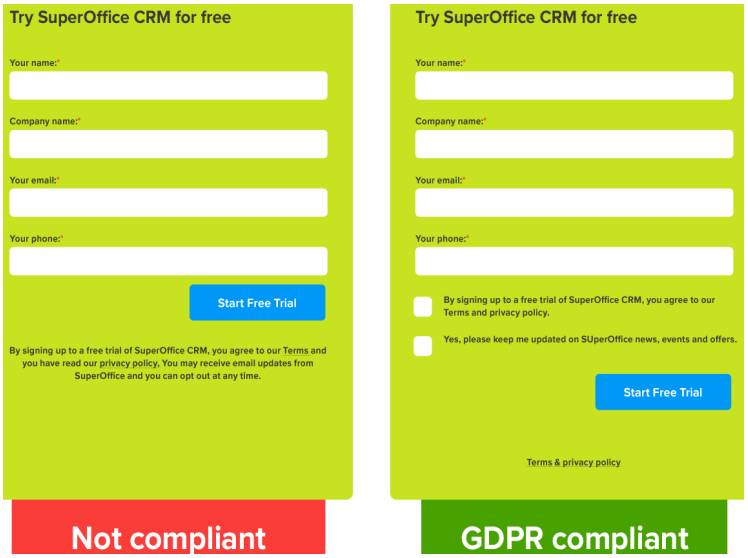
Zdroj: European Commission (2019)

V některých situacích musí poskytnuté informace také zahrnovat:
- Kontaktní informace člověka, který dohlíží na ochranu osobních údajů (pokud existuje);
- Co je záměrem společnosti, kvůli kterému souhlasíte se zpracováním;
- Opatření použitá pro přenos údajů do země mimo EU;
- Jak dlouho budou data uložena;
- Práva jednotlivce na ochranu údajů;
- Jakým způsobem lze souhlas odvolat (pokud je souhlas právním důvodem pro zpracování);
- Zda existuje zákonná nebo smluvní povinnost poskytnout údaje;
- V případě automatizovaného rozhodování informace o logice, významu a důsledcích rozhodnutí.

Je důležité si uvědomit, že tyto informace by měly být jasné, musíte tedy použít jednoduchou a srozumitelnou formu jazyka.

Podmínky pro souhlas byly posíleny a společnosti / organizace již nemohou používat dlouho nečitelné podmínky plné právních pojmů. Žádost o souhlas musí být podána srozumitelnou a snadno přístupnou formou za účelem zpracování údajů. Souhlas musí být jasný a odlišitelný od ostatních záležitostí a musí být poskytnut srozumitelnou a snadno přístupnou formou.
Následující obrázek ukazuje příklad toho, jakým způsobem by se mělo postupovat. Na dalším obrázku můžete vidět, že GDPR změnil mnoho věcí pro společnosti / organizace. Proto musí společnosti přezkoumat své obchodní procesy, aplikace a formuláře, aby byly v souladu s e-mailovým marketingem. Chcete-li komunikovat, budou potenciální zákazníci muset vyplnit formulář nebo zaškrtnout políčko a poté potvrdit, že to byly jejich akce v dalším e-mailu.

Obrázek 6 – Příklad souhlasu



Zdroj: SuperOffice (2019)

2.4. Právo na přístup a právo na přenositelnost dat

Společnosti a organizace musí zajistit, aby jednotlivci měli právo na bezplatný přístup ke svým osobním údajům. Pokud obdržíte takový požadavek:

- Řekněte jim, zda zpracováváte jejich osobní údaje;
- Sdělte jim informace o zpracování (účel zpracování, kategorie dotčených osobních údajů atd.);
- Poskytněte jim kopii zpracovávaných osobních údajů (v přístupném formátu).

S novým GDPR se stává důležitější informovat zákazníka nebo osobu, jejíž data zpracováváte, o tom, co se s jejich údaji děje. Práva, která musíte znát, jsou shrnuta na následujícím obrázku.

Obrázek 7 – Práva podle GDPR

Zdroj: Serveit (2019)

Tato práva jsou udělena jednotlivcům za účelem ochrany jejich soukromého života a kontroly digitálních stop, které zanechávají při používání internetových aplikací a služeb. Účelem těchto práv je vytvořit otevřenost, kontrolu a důvěru mezi všemi stranami.

2.5. Porušení ochrany dat

Porušení ochrany dat nastává, když jsou osobní údaje, ať už náhodně nebo nezákonně, poskytnuty neoprávněným příjemcům, jsou dočasně nedostupné nebo změněny.
Pokud dojde k porušení údajů a toto porušení představuje riziko pro individuální práva a svobody, měli byste informovat svého DPA do 72 hodin poté, co se o narušení dozvěděli.

2.6. Pokuty

Pokuty se stále zvyšují a časové limity se zkracují. V rámci GDPR jsou nyní oznámení o narušení povinná u všech členů, u nichž je pravděpodobné, že narušení údajů „povede k ohrožení práv a svobod jednotlivců". To musí být provedeno do 72 hodin od prvního zjištění porušení. Od zpracovatelů dat se rovněž požaduje, aby bez zbytečného odkladu

informovali své zákazníky, řadiče poté, co se poprvé dozvěděli o narušení dat.

Proto GDPR zavádí přísnější režim vymáhání a vystavuje subjekty zvýšenému finančnímu závazku. V některých případech závažného porušení by mohlo dojít k pokutám až do 4 % ročně. Maximální pokuta je 20 milionů EUR nebo 4 % celosvětového příjmu, podle toho, co je vyšší. Úřady pro ochranu údajů mohou také ukládat sankce, jako jsou zákazy zpracování údajů nebo veřejné pokárání.

V rámci GDPR jsou pokuty spravovány regulátorem ochrany údajů v každé zemi EU. Bude stanovena konečná částka pokut a v jaké výši: záměr; zmírnění; preventivní opatření; historie; spolupráce; kategorie dat; oznámení; osvědčení; přitěžující / zmírňující faktory. Pokud kontroloři určí, že organizace má více porušení GDPR, bude potrestána pouze za nejzávažnější porušení, pokud jsou všechna porušení součástí stejné operace zpracování.

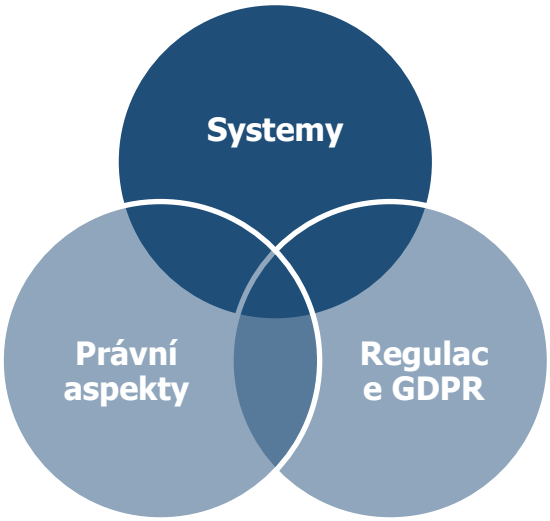
2.7. Příprava na plnění GDPR

Použití GDPR klade přísné požadavky na způsob, jakým společnosti / organizace shromažďují, ukládají a spravují osobní údaje. S ohledem na to poskytuje GDPR občanům EU větší kontrolu nad jejich osobními údaji a zajišťuje, že jejich informace jsou bezpečně chráněny v celé Evropě, bez ohledu na to, zda se zpracování údajů v EU provádí či nikoli.

GDPR zahrnuje tři hlavní oblasti, které musí každý podnik zvážit (viz obrázek 8):

1. Samotné nařízení GDPR;
2. Systémy, které používáte k ukládání všech vašich zákaznických dat;
3. Právní aspekty nařízení a jak to ovlivní způsob nakládání s osobními údaji.

Obrázek 8 – dodržování GDPR



Zdroj: vlastní zpracování

Kromě toho klíčovou součástí právních předpisů GDPR je ochrana soukromí již od samotného návrhu. Ochrana soukromí již od počátku vyžaduje, aby všechna oddělení ve společnosti / organizaci pečlivě sledovala svá data a jak s nimi nakládají. Existuje mnoho témat, které musí společnost udělat, aby byla v souladu s GDPR. Najděte několik kroků, které mohou pomoci zahájit tento proces. Zmapujte údaje o vaší společnosti:

1. **Mějte přehled**, odkud pocházejí všechna osobní data v celé vaší firmě, a dokumentujte je. Určete, kde jsou data uložena, kdo k nim má přístup a zda jsou s daty spojena rizika.

2. **Určete, jaká data je třeba uchovávat:** GDPR podporuje disciplinovanější zacházení s osobními údaji. Z tohoto důvodu je důležité uchovávat pouze ty informace, které jsou nezbytné, a odstranit veškerá data, která nepoužíváte. Pokud vaše společnost / organizace shromáždila mnoho údajů bez jakéhokoli skutečného prospěchu / využití, je čas zvážit, která data jsou pro vaši společnost / organizaci důležitá. V procesu čištění můžete sledovat výše uvedené otázky:
   - Proč přesně tato data archivujeme, namísto abychom je pouze vymazali?
   - Proč ukládáme všechna tato data?
   - Čeho se snažíme dosáhnout shromažďováním všech těchto kategorií

osobních údajů?

- Je finanční zisk z vymazání těchto informací větší než jejich šifrování?

3. **Zavádějte bezpečnostní opatření:** vytvořte a implementujte bezpečnostní opatření v celé infrastruktuře, která vám pomohou omezit případné narušení dat. To znamená zavést opatření proti porušování údajů a podniknout rychlé kroky k informování jednotlivců a orgánů v případě, že k porušení dojde.

4. **Zkontrolujte vaši dokumentaci:** v rámci GDPR musí jednotlivci výslovně souhlasit se získáním a zpracováním svých údajů. Předběžně zaškrtnutá políčka a předpokládaný souhlas již nebudou přijatelné.

2.8. Povědomí o GDPR – jeden rok po implementaci

Po jednom roce provádění GDPR, nejdůležitější a nejvýznamnější změny v právním rámci ochrany údajů si evropští občané začínají více uvědomovat práva a povinnosti, které při uplatňování právních předpisů o ochraně osobních údajů mají.

Podle výsledků zveřejněných v červnu 2019 zprávy „Obecné nařízení o ochraně údajů" provedené Evropskou komisí ukázalo, že většina (více než dvě třetiny) Evropanů slyšela o GDPR a také slyšeli o zaručených právech podle GDPR, s výjimkou práva na slovo při automatizaci rozhodnutí (41 %). Kromě toho země, které znají více GDPR, jsou: Švédsko (90 %), Nizozemsko (87 %) a Polsko (86 %). Kromě toho respondenti ve věku 25–54 let (75 %) mají o GDPR největší přehled, respondenti ve věku 15–54 let jsou si více vědomi svých práv na osobní údaje, než lidé ve věku 55 let a starší. Dále u mužů je více pravděpodobné, že si budou více vědomi těchto práv ve srovnání se ženami. Čím má respondent vyšší vzdělání, tím je pravděpodobnější, že se o této legislativě dozví.

Kromě toho má Irsko, Slovensko a Polsko některé z nejvyšších podílů respondentů, kteří slyšeli o GDPR, a vědí a také nejvyšší podíl respondentů, kteří slyšeli o všech právech, o nichž se v průzkumu, který byl proveden, mluvilo.

Pokud jde o povědomí vnitrostátních veřejných orgánů odpovědných za ochranu údajů, většina (6 z 10) uvedla, že slyšeli o existenci veřejné moci ve své zemi, která je odpovědná za ochranu svých práv na jejich osobní údaje.

Od roku 2018 jsou vnitrostátní orgány pro ochranu údajů pověřeny prosazováním nových pravidel a lépe koordinují své činnosti. Pokud však jde o problémy s dodržováním předpisů, je třeba ještě udělat nějakou práci, protože se jedná o dynamický proces.

Podle zprávy společnosti Deloitte „GDPR: Šest měsíců po implementaci: Perspektivy odborníka" je ještě třeba udělat mnoho věcí ohledně implementace GDPR. Nejdůležitější závěry této zprávy naznačují, že je důležité:

- První věc, kterou je třeba učinit, pokud jde o dodržování GDPR, je seznámit se s podrobnostmi o zpracování osobních údajů, protože stále není dostatečné povědomí o základních pravidlech;
- Zlepšit transparentnost zpracování osobních údajů subjektům údajů, jak je požadováno v rámci GDPR;
- Zlepšit pokyny, doporučení nebo oficiální stanoviska dozorčí rady v oblasti ochrany údajů;
- Realizovat školení a zvyšovat povědomí zaměstnanců a zapojení všech lidí s nejrelevantnějšími požadavky GDPR, protože každý musí pochopit, jak uplatňovat a implementovat do své každodenní práce;
- Zavést bezpečnostních opatření, která jdou nad rámec požadovaných minimálních standardů (například šifrování všech dokumentů připojených k e-mailu);
- Vytvořit nekomerční platformu pro sdílení odborných právních znalostí, osvědčených postupů a praktických a tvůrčích řešení mezi odborníky na ochranu osobních údajů;
- Vytvořit pokyny pro malé a střední podniky s cílem pomoci jim v praxi uplatňovat novou právní úpravu ochrany osobních údajů;
- Vytvořit několik šablon pro řešení několika otázek souvisejících s GDPR (shromažďování, implementace a přenos ochrany osobních údajů a vyžádání

povolení k přenosu osobních údajů;

- Vypracovat některé iniciativy zaměřené na školy a školicí materiály od raných fází.

3. Elektronické soukromí - ePrivacy

Cílem strategie jednotného digitálního trhu je zvýšit důvěru a bezpečnost digitálních služeb. Klíčovým krokem v této oblasti byla reforma rámce ochrany údajů, zejména přijetí GDPR. Strategie jednotného digitálního trhu rovněž oznámila přezkum směrnice 2002/58 / ES (směrnice o soukromí a elektronických komunikacích) s cílem poskytnout uživatelům elektronických komunikačních služeb vysokou úroveň ochrany soukromí.

Směrnice o soukromí a elektronických komunikacích stanoví některá pravidla zaručující ochranu soukromí v odvětví elektronických komunikací. Elektronická komunikace zahrnuje e-mail; aplikace; telefon; rychlé zasílání zpráv; spam; přímý marketing; telekomunikační firmy; vývojáři mobilních aplikací; online reklamní sítě mimo jiné. Tato směrnice rovněž poskytuje ochranu uživatelům a účastníkům elektronických komunikačních služeb před nevyžádanou komunikací.

Směrnice o elektronickém soukromí vyžaduje, aby poskytovatelé elektronických komunikačních služeb, jako je přístup k internetu a pevný a mobilní telefon, aby:

a) přijmout vhodná opatření zajišťující bezpečnost elektronických komunikačních služeb;

b) Zajištění důvěrnosti komunikací a souvisejících provozních údajů ve veřejných sítích.

Tři hlavní cíle směrnice o soukromí a elektronických komunikacích jsou tyto:

- Zajistit rovnocennou úroveň ochrany základního práva na soukromí a důvěrnost, pokud jde o zpracování osobních údajů v odvětví elektronických komunikací v celé EU. Tato ochrana je poskytována také účastníkům, kteří jsou právnickými osobami;
- Zajistit rovnocennou úroveň ochrany, pokud jde o zpracování osobních údajů v odvětví elektronických komunikací, aby byla chráněna základní práva na ochranu údajů;
- Zajistit volný pohyb osobních údajů zpracovávaných v odvětví elektronických

komunikací a volný pohyb koncových zařízení a služeb elektronických komunikací v EU.

ePR nahradí stávající směrnici EU o elektronickém soukromí a směrnici o elektronických komunikacích z roku 2002. Toto nařízení je důležité, protože to znamená, že bude právním aktem a bude v celém rozsahu vymahatelné ve všech členských státech, jako je GDPR. Tento návrh musí navíc zajistit soulad s GDPR.

Zatímco GDPR zajišťuje ochranu osobních údajů, cílem ePR je zajistit důvěrnost komunikací, které mohou také obsahovat jiné než osobní údaje a údaje týkající se právnické osoby.

EPR měl vstoupit v platnost dne 25. května 2018 spolu s GDPR, nicméně pokračující jednání a lobbování některých z nich zpožďovalo uplatňování tohoto nařízení.

3.1. Klíčové body návrhu Evropské komise

Návrh nařízení o vysokých pravidlech ochrany soukromí pro všechny elektronické komunikace zahrnuje:

Obrázek 9 – Pravidla elektronického soukromí

Simples rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users, will be stramlined. The new rule will be more user-friendly as browser setting and other identifiers. The proposal also clarifies that no consent is needed for non-privacy instrusive cookies improving internet experience or cookies used by a website to count the number of visitors.

Protection agains spam: this proposal bans unsolicited eletronic communications by emails, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.

More effective enforcement: the enforcement of the confidentiality rules in the regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.

Zdroj: European Commission (2019)

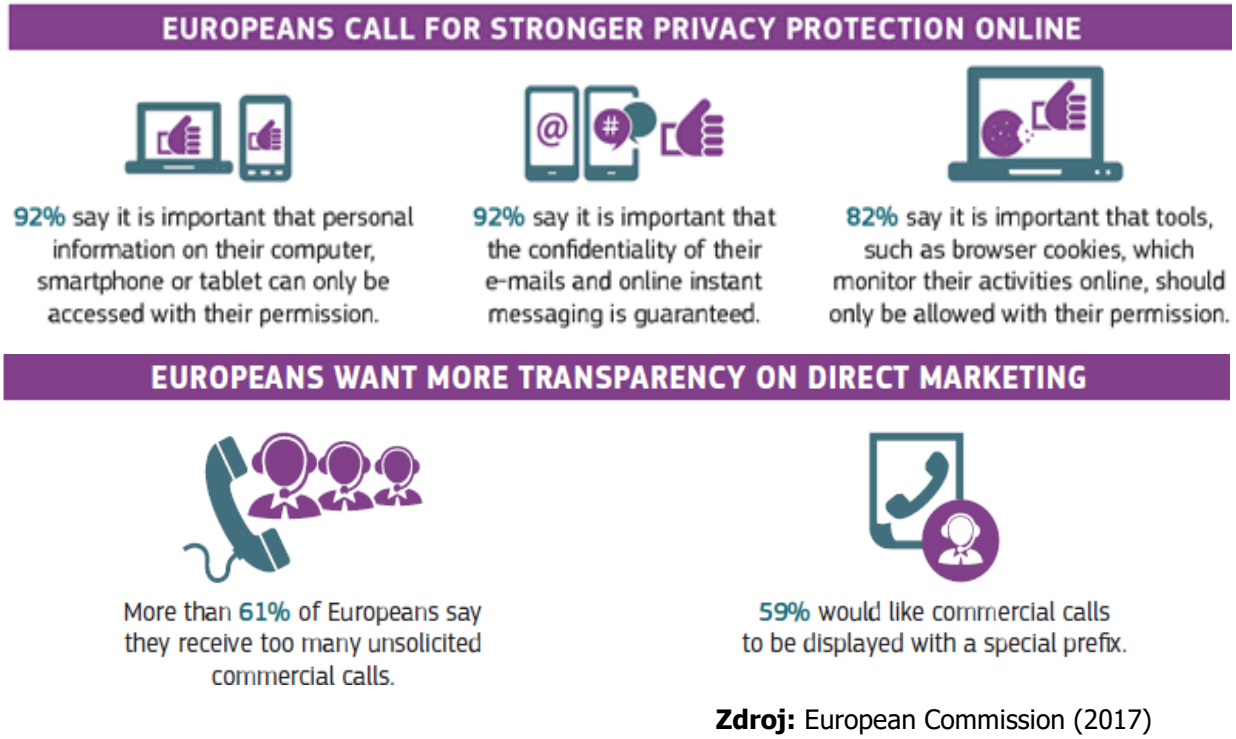
3.2. Přísnější pravidla ochrany osobních údajů pro elektronickou komunikaci

Jak je již známo, stále více Evropanů používá online komunikační služby as elektronickou komunikací ePR Evropané jsou důvěrní bez ohledu na použitou technologii, navrhovaná pravidla se budou vztahovat také na hlasové služby a internetové zasílání zpráv na internetu.

Na dalším obrázku můžeme pozorovat, že Evropané potřebují silnější ochranu soukromí online zejména na svých mobilních zařízeních (počítač, chytrý telefon nebo tablet).

Evropané navíc chtějí větší transparentnost v oblasti přímého marketingu. Z tohoto důvodu se lidé budou muset tímto nařízením dohodnout dříve, než jim budou zaslány marketingové zprávy automatizovanými volacími stroji, například SMS nebo e-mailem. Budou také muset souhlasit s přijímáním marketingových volání, ledaže jim vnitrostátní právo dává právo vznést námitku proti přijetí takových hovorů. Kromě toho budou muset marketingoví volající uvést své telefonní číslo nebo použít speciální předběžnou opravu, která označuje marketingový hovor.

Obrázek 10 – Online ochrana soukromí



Zdroj: European Commission (2017)

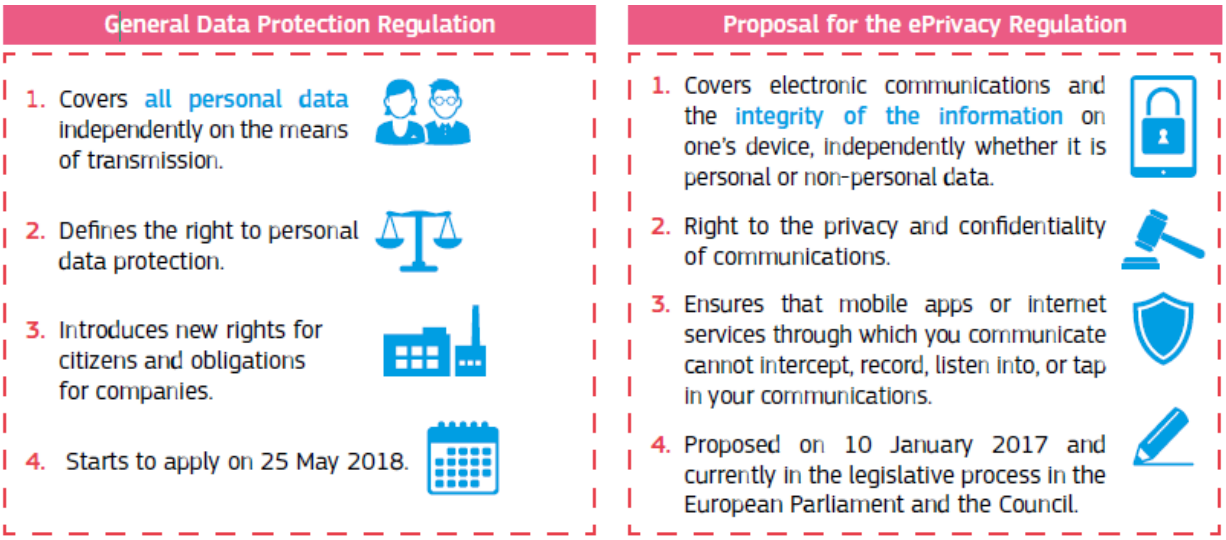
3.3. Právo a přeshraniční situace

Směrnice o soukromí a elektronických komunikacích neobsahuje výslovné ustanovení, pokud jde o použitelné vnitrostátní právo. To může vést k právní nejistotě ohledně toho, které právo by se mělo použít v přeshraničním kontextu. Nejasná situace vyplývá z neexistence zvláštního pravidla použitelného práva, které brání účinnému uplatňování pravidel v přeshraniční situaci.

3.4. Vztah mezi GDPR a ePR

Pokud jde o GDPR a ePR, existuje jen několik rozdílů a podobností. Zatímco ePR chrání důvěrnost elektronických komunikací, GDPR chrání osobní údaje. To znamená, že ePR doplňuje GDPR v odvětví elektronických komunikací. Na následujícím obrázku je srovnání GDPR a ePR.

Obrázek 11 - GDPR vs ePR

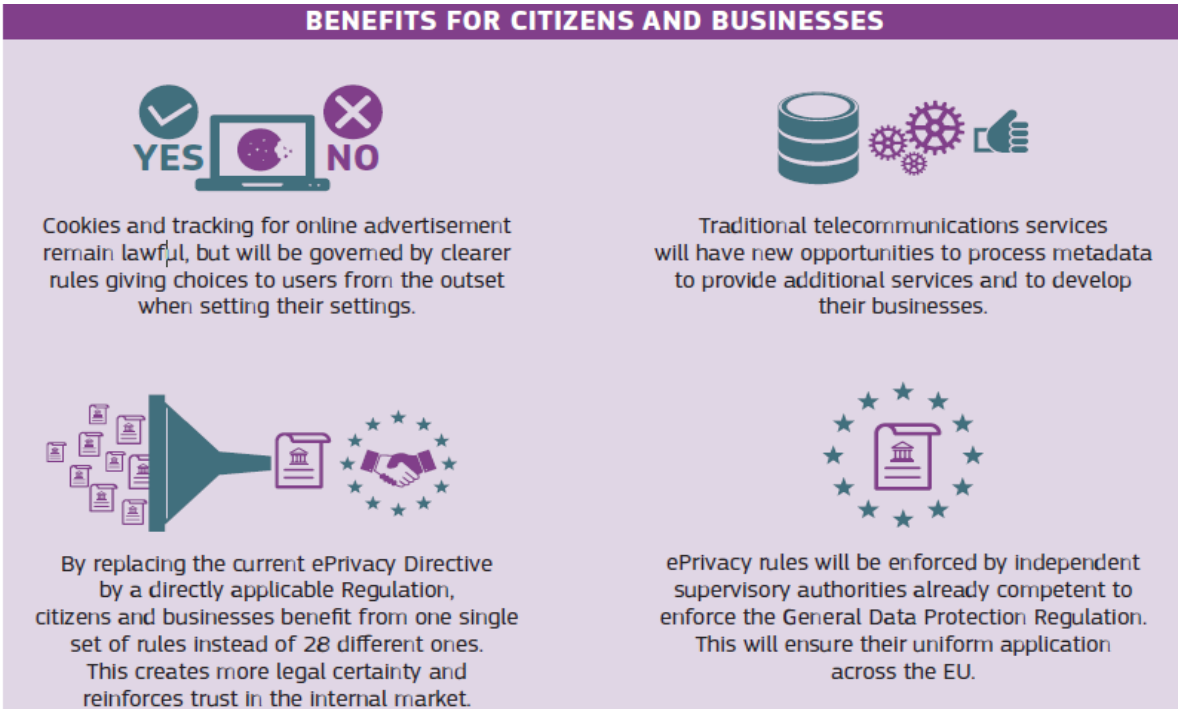


Zdroj: European Commission (2016)

3.5. Výhody pro společnost a podniky

Podle Evropské komise má toto nařízení pro občany a podniky určité výhody. Hlavní přínosy pro občany a podniky jsou vidět na následujícím obrázku.

Obrázek 12 – Výhody pro společnost a podniky



Zdroj: European Commission (2017)

4. Ochrana osobních údajů

Podle Evropské komise jsou osobní údaje jakékoli informace, které se vztahují k identifikovanému nebo identifikovatelnému žijícímu jedinci. Jinými slovy, osobní údaje jsou jakékoli informace, které lze použít k identifikaci osoby.

Rámec EU pro ochranu soukromí a údajů má dvě hlavní předpisy: GDPR a ePR.

GDPR 2016/679 je nařízení EU o ochraně údajů a soukromí pro všechny občany EU a také EHP.

GDPR vstoupil v platnost 25. května 2018 v každé evropské zemi. Účelem GDPR je uložit jednotný zákon o bezpečnosti údajů všem členům EU, aby každý členský stát již nemusel psát své vlastní zákony na ochranu údajů, a v důsledku toho jsou zákony jednotné v celé EU. Cílem požadavků GDPR je vytvořit důslednější ochranu spotřebitelských a osobních údajů ve všech zemích EU.

Kromě toho se GDPR zaměřuje na zajištění toho, aby uživatelé věděli, chápali a souhlasili se shromažďovanými údaji o nich. GDPR chrání osobní údaje bez ohledu na technologii (automatizované nebo ruční zpracování) použité pro zpracování těchto údajů v souladu s předem definovanými kritérii. Nezáleží také na tom, jak jsou data ukládána (například video, papír atd.), Na osobní údaje se ve všech případech vztahují požadavky na ochranu stanovené GDPR a ePR.

Cílem ePR je poskytovat uživatelům elektronických komunikačních služeb vysokou úroveň ochrany soukromí a byla navržena Evropskou komisí v lednu 2017 jako součást strategie jednotného digitálního trhu a nahradí směrnici o elektronickém soukromí z roku 2002.

Ačkoli základní nařízení o ochraně údajů je přímo použitelné jako nařízení EU v každém členském státě EU, obsahuje některé úvodní doložky a ponechává vnitrostátnímu zákonodárci určitou volnost, jak uvidíme v následující části.

4.1. Jaká nařízení doplňují evropská nařízení

4.1.1. Rakousko

Platí předpisy týkající se ochrany osobních údajů:

- GDPR – v německém Datenschutz-Grundverordung (DSVGO);

- ePR;

- Rakouský zákon o ochraně údajů Datenschutzgesetz (DSG), který doplňuje GDPR;

- **K provedení těchto úvodních ustanovení a marží byly přijaty Zákon o přizpůsobení ochrany údajů 2018 a Zákon o ochraně údajů z roku 2018** (dvě změny zákona o ochraně údajů). Zákon o přizpůsobení ochrany údajů 2018 byl zveřejněn v BGBl I č. 120/2017 a zákon o ochraně údajů z roku 2018 v BGBl I č. 24/2018 vstoupil v platnost 25. května 2018;

- Směrnice o ochraně údajů je směrnice pro oblast spravedlnosti a vnitřních věcí založená na této směrnici je založena na směrnici Evropského parlamentu a Rady EU (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob s ohledem na zpracování osobních údajů příslušnými orgány pro tyto účely: předcházení, vyšetřování, odhalování nebo stíhání trestných činů, výkon trestů, volný pohyb údajů a zrušení rámcového rozhodnutí Rady 2008/977 / SVV (Österreichische Datenschutzbehörde, 2019).

4.1.2. Česká republika

V případě České republiky jsou použitelné následující právní předpisy:

- GDPR;

- ePR;

- Usnesení č. 205 (15. března 2010) se zabývá otázkami kybernetické bezpečnosti a zřídilo Ministerstvo vnitra České republiky jako koordinátora otázek kybernetické bezpečnosti a vnitrostátní orgán pro danou oblast;

- Usnesením č. 380 (24. května 2010) byla zřízena Meziresortní koordinační rada pro

oblast kybernetické bezpečnosti;

- **Usnesení č. 564** (20. července 2011) souvisí s českou strategií pro kybernetickou bezpečnost na období 2011–2015;
- **Usnesením č. 781** (19. října 2011) byl úřad zřízen jako koordinátor pro záležitosti kybernetické bezpečnosti a vnitrostátní orgán pro oblast kybernetické bezpečnosti;
- **Zákon o kybernetické bezpečnosti** (1. ledna 2015) přímo souvisí s otázkami kybernetické bezpečnosti;
- **Vyhláška č. 437/2017** (8. prosince 2017) provádí příslušné právní předpisy EU a upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a specifikace pro určení významu dopadu přerušení základní služby na bezpečnost sociálních a hospodářských činností;
- **Zákon č. 181/2014 Sb.** (19. prosince 2014) o kybernetické bezpečnosti a změně souvisejících zákonů byl zveřejněn ve Sbírce zákonů: vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, incidentech s kybernetickou bezpečností a reaktivních opatřeních („nařízení o kybernetické bezpečnosti"); Vyhláška č. 317/2014 Sb. o důležitých informačních systémech a jejich kritériích pro určování; a nařízení vlády č. 315/2014 Sb. , kterým se mění nařízení vlády č. 315/2014 Sb. , kterou se mění nařízení vlády č. 432/2010 Sb. o kritériích pro identifikaci prvku kritické infrastruktury;
- **Vyhláška č. 82/2018 Sb.** (21. května 2018) je spojena s bezpečnostními opatřeními, incidenty s kybernetickou bezpečností, reaktivními opatřeními, požadavky na podávání zpráv o kybernetické bezpečnosti a likvidací dat (nařízení o kybernetické bezpečnosti).

4.1.3. Portugal

V Portugalsku je rámec ochrany osobních údajů regulován:

- GDPR;

- ePR;

- Zákon o soukromí a elektronických komunikacích (29. srpna 2012), který by se měl použít na zpracování osobních údajů v souvislosti s poskytováním veřejně dostupných elektronických komunikačních služeb ve veřejných komunikačních sítích, včetně veřejných komunikačních sítí podporujících zařízení pro sběr a identifikaci údajů,

upřesňující a doplňující ustanovení zákona č. 67/98 ze dne 26. října. Společnosti poskytující veřejné dostupné elektronické komunikační služby by měly stanovit vnitřní postupy pro reakce na žádosti o přístup k osobním údajům uživatele předložené příslušnými soudními orgány v souladu s uvedenými zvláštními právními předpisy. Podle zákona o soukromí a elektronických komunikacích podléhá doručení nevyžádané komunikace pro přímý marketing předchozímu souhlasu účastníka, který je jednotlivec nebo uživatel;

- **Ústava Portugalské republiky** (článek 35), která stanoví, že všichni občané mají právo na přístup k jakýmkoli počítačovým údajům, které se jich týkají, a právo být informováni o použití, pro které jsou údaje určeny. Podle tohoto zákona jsou tedy oprávněni požadovat, aby byl obsah spisů a záznamů opraven a aktuální. Tento zákon stanoví, jaké osobní údaje jsou, jakož i podmínky vztahující se na automatické zpracování, připojení, přenos a použití a měl by zaručit jejich ochranu prostřednictvím nezávislého správního orgánu;

- **Zákon o ochraně údajů – zákon č. 67/98** - (26. října 1998), což je právní rámec, který se obecně vztahuje jak na soukromý a veřejný sektor, tak na jakoukoli činnost v tomto odvětví. Cílem zákona o ochraně údajů je chránit právo jednotlivce na soukromý život při zpracování osobních údajů stanovujících práva a související postupy fyzických osob (subjektů údajů) a práva, povinnosti a povinnosti právnických a fyzických osob při zpracování osobních údajů. Zákon o ochraně údajů rovněž stanoví zásady a povinnosti, které musí zpracovatelé údajů při zpracování osobních údajů dodržovat. Obecná zásada tohoto zákona stanoví, že zpracování osobních údajů musí být prováděno transparentně a přísně, pokud jde o soukromí a další základní práva, svobody a záruky;

- **Zákon č. 32/2008** (ze dne 18. července 2008), který stanoví povinnosti uchovávání údajů uložené poskytovatelům veřejně dostupných služeb elektronických komunikací. Tento zákon se týká uchovávání dat vytvořených nebo zpracovaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí;

- Zákony o elektronické komunikaci – zákon č. 5/2014 - (10. února 2004) a zákon o elektronickém soukromí. Podle těchto zákonů by v případě narušení bezpečnosti

nebo integrity měli tito poskytovatelé informovat regulátor (Národní komunikační úřad nebo ANACOM), Comissão Nacional de Proteção de Dados a za určitých okolností účastníky a uživatele služeb;

- **Směrnice EU 2016/1148 o kybernetické bezpečnosti.** Podle této směrnice existují v červenci 2016 opatření pro vysokou společnou úroveň bezpečnosti síťových a informačních systémů v celé EU. Tato směrnice umožňuje rozšíření povinnosti provádět bezpečnostní opatření a oznamovat narušení bezpečnosti na jiné subjekty.

4.1.4. Spain

Ve Španělsku jsou uplatňovány následující právní předpisy o ochraně osobních údajů:

- **GDPR;**
- **ePR;**
- **Lisabonská smlouva (charta základních práv EU) a španělská ústava z roku 1978,** které se týkají ochrany údajů a soukromí a jsou oběma základními právy;
- **Několik kodexů chování v oblasti ochrany údajů,** které byly schváleny podle dřívějších španělských nařízení o ochraně údajů pro různá odvětví;
- **Nařízení týkající se jednotlivých odvětví**, která rovněž zahrnují ustanovení o ochraně údajů, protože určité kategorie osobních údajů a určité činnosti zpracování mohou vyžadovat zvláštní ochranu, jako je zpracování osobních údajů v odvětví finanční, elektronické komunikace nebo zdravotnictví;
- **Nový španělský zákon o ochraně údajů** (25. května 2018) stanoví zvláštní nařízení o ochraně údajů v různých oblastech, které nejsou výslovně zahrnuty do GDPR nebo jsou zahrnuty do GDPR, ale v rozsahu, který umožnil zavedení podrobnějších předpisů členem státy. Tento zákon navíc španělský právní systém zahrnuje seznam nových práv občanů v souvislosti s novými technologiemi známými jako „digitální práva". Tento zákon rovněž zahrnuje změnu španělského obecného volebního zákona, který politickým stranám umožňuje zpracovávat osobní údaje pro konkrétní volební propagační činnosti;
- Ustanovení o ochraně údajů mohou obsahovat také **Zákon o elektronickém obchodu 34/2002 (LSSI)** a **Obecný telekomunikační zákon 9/2014 (GTL),** které se vztahují k odvětvovým předpisům;

- **Směrnice Evropského parlamentu a Rady EU 2016/680** (27. dubna 2016) ze dne 27. dubna 2016 o ochraně fyzických osob s ohledem na zpracování osobních údajů příslušnými orgány pro účely předcházení, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů a volného pohybu těchto údajů a zrušení rámcového rozhodnutí Rady 2008/977 / SVV;
- **Kód kybernetické bezpečnosti**, který sdružuje všechna aktualizovaná pravidla, která přímo ovlivňují kybernetickou bezpečnost. Předpisy o kybernetické bezpečnosti však stále potřebují další rozvoj.

V následující tabulce naleznete stručné shrnutí zákonů o ochraně osobních údajů, které se uplatňují v Portugalsku, České republice, Portugalsku a Španělsku.

Tabulka 1 – Zákon o ochraně osobních údajů

		Osobní údaje		Neosobní údaje	Další právní předpisy v oblasti osobních údajů	Stručné vysvětlení
		GDPR	ePR	Regulace (EU 2018/1807)		
Rakousko		✓	✓	✓	**Zákon o ochraně údajů v Rakousku Datenschutzgesetz**	Rakouský zákon o ochraně údajů (DSG) doplňuje GDPR
					Zákon o přizpůsobení ochrany údajů 2018 (BGBI I č. 120/2017)	Tyto dva zákony byly přijaty k provedení úvodních ustanovení a marží (kromě změn četných věcných zákonů) zákona o ochraně údajů. Tyto zákony také doplňují GDPR
					Zákon o deregulaci ochrany údajů 2018 (BGBI I č. 24/2018)	
					Směrnice o ochraně údajů	Tato směrnice je založena na směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů za volný pohyb údajů
Česká republika		✓	✓	✓	**Usnesení č. 205**	Zaměřit se na otázky kybernetické bezpečnosti a zřídit Ministerstvo vnitra České republiky jako koordinátor otázek kybernetické bezpečnosti a vnitrostátní orgán pro oblast
					Usnesení č. 380	Byla zřízena Meziresortní koordinační rada pro oblast kybernetické bezpečnosti
					Usnesení č. 564	Česká strategie kybernetické bezpečnosti 2011–2015
					Usnesení č. 781	Úřad jako koordinátor pro záležitosti kybernetické bezpečnosti i vnitrostátní
					Zákon o kybernetické	Tento zákon upravuje kybernetickou bezpečnost v České republice a je účinný od 1. ledna 2015

					bezpečnosti	
					Vyhláška č. 437/2017	Tato vyhláška provádí příslušné právní předpisy EU a upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a specifikace pro určení významu dopadu narušení základní služby na bezpečnost sociálních a hospodářských činností.
					Usnesení č.181/2014 Coll	Souvisí s kybernetickou bezpečností a změnou souvisejících aktů na toto téma
					Vyhláška č. 82/2018 Sb	Souvisí s bezpečnostními opatřeními, incidenty s kybernetickou bezpečností, reaktivními opatřeními, požadavky na podávání zpráv o kybernetické bezpečnosti a likvidací dat (vyhláška o kybernetické bezpečnosti)
Portugalsko		✓	✓	✓	**Zákon o ochraně osobních údajů**	Zpracování osobních údajů v souvislosti s poskytováním veřejně dostupných elektronických komunikačních služeb ve veřejných komunikačních sítích, včetně veřejných komunikačních sítí podporujících zařízení pro sběr a identifikaci dat
					Ústava Portugalské republiky (článek 35)	Stanovit, že všichni občané mají právo na přístup k jakýmkoli počítačovým datům, která se jich týkají, a právo na informace o použití, pro které jsou údaje určeny, a proto jsou podle tohoto zákona oprávněni požadovat, aby obsah spisů a záznamy opraveny a aktuální. Tento zákon stanoví, jaké osobní údaje jsou, jakož i podmínky vztahující se na automatické zpracování, připojení, přenos a použití a měl by zaručit jejich ochranu prostřednictvím nezávislého správního orgánu
					Zákon č. 67/98 ze dne 26. října	Právní rámec týkající se zákona o ochraně údajů, který se obecně vztahuje jak na soukromý a veřejný sektor, tak na jakoukoli činnost v tomto odvětví
					Zákon č. 32/2008 ze dne 18. července	Stanovuje povinnosti uchovávání údajů uložené poskytovatelům veřejně dostupných služeb elektronických komunikací
					Zákon č. 5/2014 ze dne 10. února a zákon o elektronickém soukromí	Podle těchto zákonů by v případě narušení bezpečnosti nebo integrity měli tito poskytovatelé informovat regulátor (Národní komunikační úřad nebo ANACOM), Comissão Nacional de Proteção de Dados a za určitých okolností účastníky a uživatele služeb
					Směrnice EU 2016/1148	Umožňuje rozšíření povinnosti provádět bezpečnostní opatření a oznamovat narušení bezpečnosti na další subjekty
Španělsko		✓	✓	✓	**Lisabonská smlouva**	Souvisí s ochranou údajů a soukromí a jsou základními právy

					Španělská ústava of 1978	
					Nový španělský zákon o ochraně údajů č. 3/2018 ze dne 7. prosince	Poskytnout zvláštní nařízení o ochraně údajů v různých oblastech, které nejsou výslovně zahrnuty do GDPR nebo které jsou zahrnuty do GDPR, ale v rozsahu, který umožnil členským státům zavést podrobnější předpisy.
					Zákon o elektronickém obchodování 34/2002 (LSSI) Obecné telekomunikační právo 9/2014 (GTL)	Souvisí s odvětvovými předpisy
					Směrnice Evropského parlamentu a Rady EU 2016/680 ze dne 27. dubna 2016	Ochrana fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestních sankcí a volného pohybu těchto údajů a zrušení rámcového rozhodnutí Rady 2008/977 / SVV
					Kód kybernetické bezpečnosti	Uvádí hlavní pravidla, která je třeba brát v úvahu při ochraně kybernetického prostoru a zajištění výše uvedené kybernetické bezpečnosti

Zdroj: vlastní zpracování

5. Neosobní údaje

Volný tok neosobních údajů znamená neomezený pohyb údajů přes hranice a systémy informačních technologií v EU.

Nařízení o volném toku neosobních údajů v EU již platí. Přesný název tohoto nařízení je nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v EU.

Cílem tohoto nařízení je zajistit volný tok údajů jiných než osobní údaje v rámci EU stanovením pravidel týkajících se požadavků na lokalizaci údajů, dostupnosti údajů příslušným orgánům a přenosu dat pro profesionální uživatele.

Toto nařízení se rovněž vztahuje na zpracování jiných než osobních údajů v EU, které jsou:

- Poskytována jako služba uživatelům, kteří mají bydliště nebo provozovnu v Unii, bez ohledu na to, zda je poskytovatel služeb usazen v Unii;
- Prováděna z údajů nebo právnických osob, které mají bydliště nebo sídlo v Unii pro vlastní potřebu;

Toto nařízení se nevztahuje na činnost, která nespadá do oblasti působnosti práva Unie.

Obrázek 13 – Neosobní údaje

Zdroj: Business2Community (2019)

Plynulý tok neosobních údajů má v celé EU tyto zásady:

- Zásada volného toku neosobních údajů odstraňuje neodůvodněná omezení lokalizace údajů uložená orgány veřejné moci, zvyšuje právní jistotu a zvyšuje důvěru;
- Zásada dostupnosti údajů pro příslušné orgány zajišťuje, že údaje zůstávají přístupné pro regulační a dohledovou kontrolu také při přeshraničním skladování nebo zpracování v EU;
- Opatření na podporu poskytovatelů cloudových služeb ve vývoji samoregulačních kodexů chování pro snadnější přepínání poskytovatele a přenos dat zpět na interní servery, které musí být provedeny do poloviny roku 2020;
- Bezpečnostní požadavky na ukládání a zpracování dat zůstávají použitelné, i když podniky ukládají nebo zpracovávají data v jiném členském státě. Totéž platí, když zadávají zpracování dat poskytovatelům cloudových služeb;
- Jednotná kontaktní místa v každém členském státě pro styk s kontaktními místy ostatních členských států a komisí pro zajištění účinného uplatňování nových pravidel pro volný tok neosobních údajů.

GDPR a nařízení o volném toku neosobních údajů budou fungovat společně, aby umožnily volný tok jakýchkoli údajů a vytvořily společný evropský prostor pro získané údaje. Tato dvě nařízení společně vytvářejí právní jistotu pro společnosti a zaručují, že osobní a jiné osobní údaje se mohou volně pohybovat v rámci EU.

5.1. Volný pohyb údajů v rámci EU

Požadavky na lokalizaci údajů jsou zakázány, pokud nejsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality. Členské státy proto neprodleně sdělí Komisi jakýkoli návrh aktu, který zavádí nový požadavek na lokalizaci údajů nebo provádí změny stávajícího požadavku na lokalizaci údajů v souladu s postupy uvedenými v článcích 5, 6 a 7 směrnice (EU) 2015/1535.

Kromě toho **nařízení vztahující se na neosobní údaje** zajišťuje:

- **Volný pohyb neosobních údajů přes hranice**: každá organizace by měla mít možnost ukládat a zpracovávat údaje kdekoli v EU;
- **Dostupnost údajů pro regulační kontrolu:** veřejné orgány si zachovají přístup k údajům, i když jsou umístěny v jiném členském státě nebo pokud jsou uloženy nebo zpracovány v cloudu;
- Snadnější přepínání poskytovatelů cloudových služeb pro profesionální uživatele. Komise začala v této oblasti usnadňovat samoregulaci a vybízet poskytovatele, aby vypracovali kodexy chování týkající se podmínek, za nichž mohou uživatelé přenášet data mezi poskytovateli cloudových služeb a zpět do svého vlastního IT prostředí;
- Plná konzistence a synergie s balíčkem kybernetické bezpečnosti a vyjasnění, že veškeré bezpečnostní požadavky, které již platí pro podniky, které ukládají a zpracovávají údaje, budou tak činit i nadále, když ukládají nebo zpracovávají data přes hranice v EU nebo v cloudu.

Spolu s tímto nařízením, již GDPR stanoví volný pohyb osobních údajů. Do 30. května 2021 mají členské státy některá pravidla týkající se požadavků na lokalizaci údajů stanovená na základě stávajících právních předpisů Unie.

5.2. Přenos dat

Evropská komise podporuje a usnadňuje vývoj samoregulačních kodexů chování na úrovni Unie s cílem přispět ke konkurenceschopné ekonomice údajů založených na zásadách transparentnosti a usnadnit vývoj samoregulačních kodexů s cílem přispět k konkurenční ekonomika dat.

5.3. Postup pro spolupráci mezi orgány

Podle článku 7 určí každý členský stát jedno kontaktní místo, které bude v souvislosti s uplatňováním tohoto nařízení jednat s jednotnými kontaktními místy s ostatními členskými státy a Komisí. To znamená, že členské státy oznámí Komisi určená jednotná kontaktní místa a jakékoli následné změny.

5.4. Dostupnost dat pro kompetentní orgány

Pokud jde o článek 5, tímto nařízením nejsou dotčeny pravomoci příslušných orgánů požadovat nebo získat přístup k údajům za účelem plnění svých úředních povinností v souladu s právem Unie nebo vnitrostátním právem. Po vyžádání přístupu k údajům uživatele příslušný orgán nezíská přístup a pokud podle práva Unie nebo mezinárodních dohod neexistuje žádný zvláštní mechanismus spolupráce pro výměnu údajů mezi příslušnými orgány různých členských států, může tento příslušný orgán požádat příslušný orgán o pomoc jiný členský stát podle článku 7.

5.5. Sankce za porušení

Toto nařízení stanoví sankce za porušení, které stanoví různé sankce za různá porušení (stejné sankce, které se uplatňují v rámci GDPR, se vztahují také na ePR). To znamená, že pokuty se mohou pohybovat od 10 milionů EUR do 2 % celosvětového ročního obratu za vážnější porušení, podle toho, co je v každém případě vyšší.

Případné pokuty jsou silně závislé na řadě polehčujících faktorů, jako je rozsah incidentu, zda došlo k porušení předpisů v důsledku úmyslného jednání a jak usilovná byla společnost, pokud jde o prevenci takových incidentů.

6. Katalog pojmů

Kybernetická bezpečnost: je praxe ochrany systémů, sítí a programů před digitálními útoky. Cílem těchto kybernetických útoků je obvykle přístup, změna nebo zničení citlivých informací, vydírání peněz od uživatelů nebo přerušení běžných obchodních procesů.

Zákon o ochraně údajů: nezávislé veřejné orgány, které dohlížejí na uplatňování zákona o ochraně údajů. Poskytují odborné poradenství v otázkách ochrany údajů a řeší stížnosti na porušení GDPR a příslušných vnitrostátních právních předpisů.

Úředník pro ochranu údajů: osoba odpovědná za sledování a uplatňování pravidel ochrany údajů v Evropské komisi. DPO je zaměstnancem ve vaší organizaci, který odpovídá za pochopení a zajištění souladu vaší organizace. DPO zajišťuje vnitřní uplatňování pravidel ochrany údajů ve spolupráci s evropským inspektorem ochrany údajů.

Nařízení o elektronickém soukromí: návrh Evropské komise, jehož cílem je posílit ochranu soukromého života občanů Evropské unie a vytvořit nové příležitosti pro podnikání.

GDPR: regulace v právu EU o ochraně údajů a soukromí pro všechny jednotlivé občany Evropské unie a Evropského hospodářského prostoru. Zabývá se také převodem osobních údajů mimo Evropskou unii a Evropský hospodářský prostor.

Neosobní údaje: elektronické informace, které nelze vysledovat zpět k identifikované nebo identifikovatelné fyzické osobě (nebo byly jako takové anonymizovány).

Osobní údaje: jakékoli informace, které se vztahují k jednotlivci, který lze přímo nebo nepřímo identifikovat. Jména, fotografie, geografické informace, webové cookies, e-mailová adresa jsou příklady osobních údajů.

7. Závěr

Ochrana údajů a kybernetická bezpečnost se stávají základními hodnotami pro společnost, a proto tyto dvě oblasti nedávno prošly významným právním vývojem a jsou v EU konsolidovány více.

Nařízení o nakládání s osobními údaji se liší od nařízení o jiných než osobních údajích v členských státech EU. Předpisy týkající se jiných než osobních údajů a osobních údajů jsou však pro všechny členské státy stejné. V této souvislosti se nařízení (EU) 2018/1807 vztahuje na volný tok neosobních osob, zatímco pokud jde o ochranu údajů, hlavním pravidlem je GDPR. Spolu s GDPR bude regulace spojená s volným tokem jiných než osobních údajů fungovat společně, aby umožnila volný tok jakýchkoli údajů, jejichž výsledkem bude společný evropský prostor pro údaje.

GDPR navíc stanoví některá pravidla týkající se ochrany soukromí v odvětví elektronických komunikací. Toto nařízení se vztahuje zejména na poskytovatele elektronických komunikačních sítí a služeb a mělo vstoupit v platnost dne 25. května 2018, ale spolu s GDPR však pokračující jednání a lobování některých jeho jemnějších zpoždění uplatňování tohoto nařízení zpozdilo. EPR neobsahuje výslovné ustanovení, pokud jde o použitelné vnitrostátní právo, které vytváří právní nejistotu ohledně toho, které právo by se mělo použít v přeshraničním kontextu.

Přestože je základní nařízení o ochraně údajů přímo použitelné jako nařízení EU v každém členském státě EU, obsahuje řadu ustanovení o zahájení a ponechává vnitrostátnímu zákonodárci určitou volnost.

8. Zdroje

Business2Community (2019). Why User Data is the Next Big Deal in Digital? Retrieved from https://www.business2community.com/mobile-apps/why-user-data-is-the-next-big-deal-in-digital-02179282.

Deloitte (2019). The GDPR: Six Months after Implementation. Retrieved from https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html.

EU GDPR.ORG (2019). The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. Retrieved from https://eugdpr.org/.

European Commission (2019). Complete guide to GDPR compliance. Retrieved from https://gdpr.eu/.

European Commission (2019). Data protection under GDPR. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company.

European Commission (2019). Eurobarometer on ePrivacy. Retrieved from https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy.

European Commission (2019). Free flow of non-personal data. Retrieved from https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data.

European Commission (2019). General Data Protection Regulation: one year on. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610.

European Commission (2019). Proposal for a regulation on privacy and electronic communications. Retrieved from https://ec.europa.eu/digital-single-

market/en/news/proposal-regulation-privacy-and-electronic-communications.

i-Scoop (2019). Data processing principles: the 9 GDPR principles relating to processing personal data. Retrieved from https://www.i-scoop.eu/gdpr/gdpr-personal-data-processing-principles/.

ITPRO (2019). ePrivacy Regulation: What is it and how does it affect me? Retrieved from https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me.

Serve IT (2017). GDPR for developers - data subject rights. Retrieved from https://www.serveit.com/gdpr-for-developers-data-subject-rights/.