Ta nejlepší GDPR příručka pro markeťáky a podnikatele

**General Data Protection Regulation** neboli **Obecné nařízení na Ochranu osobních údajů** bylo poprvé navrženo v roce 2012, poté následovaly čtyři roky diskuzí, debat a úprav. Konečná podoba nařízení byla Evropským parlamentem přijata v roce 2016. Členské země, firmy a organizace poté měly dva roky na to, aby se na toto nařízení připravily, a to do 25. května 2018. V té době se to zdálo jako dostačující doba na to, aby se každý připravil.
Ale tento čas rychle utekl a GDPR už je doslova za dveřmi.

Na veřejnosti o tomto nařízení už toho bylo mnoho řečeno a napsáno, přesto však spousta majitelů podniků zcela nechápe, co všechno GDPR vlastně znamená, a zda budou tímto nařízením ovlivněny, či nikoliv. S touto GDPR příručkou chceme vnést trochu světla na to, co General Data Protection Regulation vlastně znamená a zároveň zodpovědět nejčastěji se objevující dotazy ohledně GDPR, ale také představit pár kroků, které vedou k jeho implementování.

Níže najdete obsah, který vám pomůže najít přesně to, co potřebujete vědět.

[**Srozumitelnou češtinou: Vše, co potřebujete vědět o GDPR** 3](#_Toc511460166)

[**Největší otázky Obecného Nařízení o Ochraně osobních údajů (GDPR)** 6](#_Toc511460167)

[Bude se mne GDPR týkat? 6](#_Toc511460168)

[Bude GDPR platit po Brexitu? 6](#_Toc511460169)

[Nahradí GDPR zákon DPA? 6](#_Toc511460170)

[Ovlivní GDPR studené kontakty? 7](#_Toc511460171)

[Bude GDPR zpožděno? 8](#_Toc511460172)

[Vstoupí GDPR v účinnost? 8](#_Toc511460173)

[Ovlivní GDPR tzv. B2B? 8](#_Toc511460174)

[Kdy vchází GDPR v účinnost? 8](#_Toc511460175)

[Co znamená GDPR pro marketing? 9](#_Toc511460176)

[Co znamená GDPR pro firmy? 9](#_Toc511460177)

[Co znamená GDPR pro HR? 10](#_Toc511460178)

[Na koho se GDPR vztahuje? 11](#_Toc511460179)

[Je možné se pojistit proti GDPR pokutám? 11](#_Toc511460180)

[Jak ovlivní GDPR podniky z USA? 11](#_Toc511460181)

[Jakým způsobem mění GDPR podmínky pro výzkum dat? 12](#_Toc511460182)

[Jakým způsobem ovlivní GDPR školy? 13](#_Toc511460183)

[Jak GDPR ovlivní Google nebo Facebook? 14](#_Toc511460184)

[Ovlivní GDPR nábory? 14](#_Toc511460185)

[Jaký bude mít GDPR dopad na charitativní organizace? 15](#_Toc511460186)

[Proč je GDPR takový strašák? 15](#_Toc511460187)

[Čím je GDPR dobré pro podnikání? 16](#_Toc511460188)

[**Jak snížit dopad GDPR na vaše podnikání** 16](#_Toc511460189)

[Seznámení 16](#_Toc511460190)

[Odpovědnost 16](#_Toc511460191)

[Komunikace se zákazníky, zaměstnanci a uživateli 17](#_Toc511460192)

[Osobní ochrana osobních údajů 18](#_Toc511460193)

[Bude žádost o přístup změněna? 19](#_Toc511460194)

[Co je míněno Zákonným důvodem pro Zpracování? 19](#_Toc511460195)

[Používání Souhlasu Zákazníka jako Zákonného důvodu pro Zpracování 20](#_Toc511460196)

[Zpracovávání osobních údajů dětí 20](#_Toc511460197)

[Oznámení Porušení zabezpečení 20](#_Toc511460198)

[Posouzení vlivu na ochranu osobních údajů (DPIA) a Výchozí ochrana osobních údajů 21](#_Toc511460199)

[Pověřenec na ochranu osobních údajů 21](#_Toc511460200)

[Mezinárodní organizace a GDPR 21](#_Toc511460201)

# **Srozumitelnou češtinou: Vše, co potřebujete vědět o GDPR**

Nyní již moc dobře víme, jak technologie zasahují do nového i starého průmyslu: Služby Uber a Lyft narušují dopravní průmysl, Netflix narušuje tradiční způsob výroby filmů a seriálů, AI poté narušuje prakticky veškeré možné průmyslové odvětví způsobem, jaký pro nás byl před pár lety nepředstavitelný. Technologie poté zasahují také do oblastí práv a regulací implementovaných v zemích samotných. GDPR je však navrženo tak, aby nahradilo současnou direktivu, která již není efektivní: Direktiva **95/46/EC** (direktiva na ochranu údajů).

Již z názvu General Data Protection Regulation plyne, že je toto nařízení zaměřeno na data, ne však na všechna, hlavním záměrem tohoto nařízení jsou osobní údaje o jednotlivcích, zejména jednotlivcích ze všech členských zemí EU. Toto nařízení tedy aktualizuje již existující, a přidává nové, regulace se zaměřením ne sběr a zacházení s osobními údaji. Toto nařízení se však nevztahuje pouze na podniky se sídlem v EU. Mnohé firmy a organizace po celém světe se budou muset tomuto nařízení přizpůsobit, pokud chtějí zpracovávat osobní údaje lidí, kteří žijí na území EU.

Účelem této regulace není zhoršit podmínky pro podnikání nebo prodej, či omezit normální funkce podniku. Účelem je dát jedincům více kontroly nad jejich vlastními osobními údaji, zejména nad tím kdo tyto údaje sbírá a zpracovává, na co jsou využívány a jak jsou chráněny.

Tohoto je docíleno zejména rozlišením dvou pojmů **osobní údaj** a **citlivý osobní údaj**. Osobním údajem se rozumí takový údaj, který nám dovolí identifikovat, přímou nebo nepřímou cestou, daného jedince. Jedná se o takové identifikátory jako jsou jména, rodná čísla, údaje o poloze, nebo online identifikátory. Také citlivé osobní údaje dovolují identifikovat jedince, avšak v mnohem širším rozhraní informací a specifických faktorů – zejména fyzický vzhled, fyziologické, psychologické a genetické údaje, ale také údaje
o psychickém stavu či ekonomické, kulturní nebo sociální identity. Sbírání a zpracovávání citlivých osobních údajů je dovoleno pouze za velmi specifických podmínek s dalším zaměřením na jejich ochranu.

Dále GDPR upravuje způsoby a podmínky pro získávání souhlasů:

• Jasný souhlas jedince

• Zákaz automatického souhlasu, například jako součástí obchodních podmínek nebo jako podmínku pro nákup služby/zboží

• Musí existovat jednoduchá možnost, jak souhlas odvolat

V rámci GDPR existuje několik příležitostí, kdy souhlas není nutností. Tyto příležitosti však vždy mají svůj základ v legislativě, která může sběr osobních údajů vyžadovat.

GDPR dále specifikuje práva jedinců s ohledem na jejich osobní údaje. Jedná se o následující práva:

* **Právo být informován**
Zakotveno v dokumentu na ochranu osobních údajů. Detailní informace o tom, kdo sbírá a zpracovává osobní údaje, jak budou využity a jejich volná přístupnost pro jedince. Tento dokument musí být sepsán jasným a srozumitelným jazykem.
* **Právo na přístup**
Jedinci mohou vyžádat potvrzující formulář, který definuje, jak jsou data spravována. Mohou si dále vyžádat formulář o tom, jaká data jsou v podniku o jedinci uložena, spolu s dalšími informacemi. Toto vyžádání by nemělo být zpoplatněno a musí být vyřízeno do jednoho měsíce od obdržení žádosti jedince.
* **Právo na opravu**
Jedinci vás mohou zažádat o opravu jakýchkoliv neúplných nebo nepřesných informací, které o jedinci spravujete. Při takové změně je poté vaší povinností tuto změnu předat jakékoliv propojené třetí straně.
* **Právo na výmaz**
Toto není absolutním právem na to být zapomenut, ale spíše zpřístupnění možnosti zažádat o výmaz osobních údajů v případech, kdy již neexistuje legitimní důvod na jejich uchovávání a zpracovávání, nebo možnost jedince zrušit svůj souhlas s jejich zpracováním.
* **Právo na omezené zpracovávání**
Za některých podmínek mohou jednotlivci zažádat o omezené zpracovávání jejich osobních údajů. Toto se liší od práva na výmaz. Data budou dále uchovávána, avšak nebudou dále předávána nebo zpracovávána.
* **Právo na přenos dat**
Toto právo dovoluje jednotlivcům přenést veškerá data z vaší služby ke službě jiné. Nicméně, toto právo lze aplikovat pouze v případech, kdy to dovoluje druh služby
a kdy je firma správcem těchto dat. Jedná se zejména o případy zabývající se převodem smluv k jinému poskytovateli.
* **Právo na námitku**
Pokud nemáte přesně daný a jasný souhlas jednotlivce, má majitel osobních údajů právo vznést námitku, a to z mnoha důvodů spojených se správou nebo zpracováváním osobních údajů.
* **Práva spojená s automatickým rozhodováním a profilováním**
V případě, že je pro služby využíváno automatických rozhodnutí (např. na základě algoritmu), vyžaduje GDPR přesné bezpečnostní podmínky, které zamezí riziku škodlivého rozhodování, které mohou ovlivnit rozhodnutí bez lidského faktoru. Jedinec má právo být informován či vyžádat odůvodnění rozhodnutí.

GDPR se velmi podrobně věnuje odpovědnosti a správě dat uvnitř firem a organizací.
A to v oblastech:

• Implementace změn a jejich jasné prokázání. Do toho může spadat politika interní ochrany osobních údajů, jako je školení zaměstnanců, interní audity zpracovatelských aktivit
a kontrola interní HR politiky.

• Zajištění relevantní dokumentace veškerých zpracovatelských aktivit

• Identifikování vaší organizace z pohledu správce, zpracovatele, nebo z obou pohledů. Tento krok je důležitý pro správné pochopení požadavků GDPR, v některých případech bude nutné najmout zodpovědného pracovníka.

• Implementační změny, které jsou dostačující pro zásady plynoucí z ochrany osobních údajů, jako jsou:

 - minimalizace dat
 - pseudonymizace a anonymizace dat
 - možnost jedinců monitorovat průběh zpracování jejich údajů
 - neustálé vylepšování bezpečnostních možností

Nakonec musíme zmínit, že GDPR představuje nové požadavky pro způsob, jakým jsou osobní údaje zpracovávány, a to pro zajištění jejich bezpečnosti. Zároveň toto nařízení udává podmínky pro podniky a organizace ohledně oznamovacích povinností v případě narušení zabezpečení a ohrožení osobních údajů.

Je důležité si uvědomit, že se GDPR nedotkne úplně všech podniků a organizací, ale pouze těch, které sbírají nebo zpracovávají osobní údaje svých klientů nebo klientů jiné organizace. Pokud nesbíráte a nezpracováváte žádná osobní data jedinců, poté se nemusíte ničeho bát. Pokud je vaše odpověď ano, poté je důležité se zabývat vaší připraveností na požadavky GDPR. GDPR by v žádném případě nemělo omezit vaše podnikání, ačkoliv vás možná přinutí učinit několik změn v otázce zpracovávání dat, což se může zkomplikovat, avšak nemělo by to být nemožné.

Vysoké pokuty, které GDPR doprovází nemají za úkol ničit podniky, ale spíše varovat před ignorováním regulací, což může vystavit osobní údaje jedinců nebezpečí.

Nicméně, jako se všemi nařízeními a regulacemi, i zde budeme muset počkat na den platnosti tohoto nařízení a první legislativní případ, který ovlivní veškeré další. Ale také na dopad, který nařízení bude mít na podniky i jedince, což může přimět budoucí změnu samotného nařízení.

# **Největší otázky Obecného Nařízení o Ochraně osobních údajů (GDPR)**

## **Bude se mne GDPR týkat?**

Krátká odpověď je ano. Pro jednotlivce GDPR stanovuje, kdy a jak organizace a firmy zpracovávají nebo kontrolují jakékoliv osobní údaje, které se vás mohou týkat. Pokud jste součástí nějaké společnosti, která sbírá a upravuje data o občanech EU, poté GDPR ukládá, kdy může k takovému spravování dojít a jak by mělo být provedeno. To tedy znamená, že GDPR se netýká pouze firem se sídlem v EU, ale také firem, které nabízejí své zboží nebo služby občanům jakéhokoliv členského státu EU, i když se zde podnik nenachází.

## **Bude GDPR platit po Brexitu?**

GDPR bude neustále platit i po Brexitu, jelikož je toto nařízení nastaveno tak, že firma nebo organizace nemusí mít sídlo vně EU. Jakmile jsou zpracovávány údaje o občanech EU, nařízení platí bez závislosti na tom, kde je samotné sídlo společnosti. Dodáme, že Zákon na Ochranu Osobních údajů byl ve Velké Británii představen ve Sněmovně lordů 13. září 2017. Tento zákon nahrazuje předešlou legislativu a je nejen kompatibilní s GDPR, dodává také specifické úpravy platné pro Velkou Británii. Do toho spadají úpravy týkající se například akademického výzkumu, finančních služeb nebo ochrany dětí.

## **Nahradí GDPR zákon DPA?**

Ano i ne. Krátce můžeme říct, že GDPR nahrazuje zákon Data Protection Act (britský zákon na ochranu osobních údajů) z roku 1998 (DPA). Nicméně, Británie se zároveň připravuje také na Brexit, a zatímco GDPR reguluje ochranu osobních údajů pro občany EU, po Brexitu bude Británie potřebovat chránit vlastní občany. Tento zákon byl představen v roce 2017 a bude platný od května 2018. Výše zmíněný zákon zastává stejné standardy jako GDPR, avšak dále vyjasňuje kontext mezi GDPR a Velkou Británií.

## **Ovlivní GDPR studené kontakty?**

Obecné nařízení na ochranu osobních údajů (GDPR) rozhodně ovlivní všechny formy studených kontaktů, včetně spojeného e-mailového marketingu. GDPR nastavuje vysoký standard pro souhlasy, zejména na možnost jeho zrušení (firmy/jednotlivce) a tím ovlivňuje vybudování důvěry.

Správný souhlas pod GDPR znamená následující:

* Souhlas musí být jasný skrze pozitivní přihlášení. To znamená, že předem označené kolonky jsou zakázány, zakázán je také souhlas jako podmínka pro nákup nebo poskytnutí služby.
* Souhlas nesmí být vágní. Jednotlivec musí udělit specifický souhlas ze kterého plyne, že jednotlivec rozumí s čím souhlasí. Pokud tento souhlas nějakým způsobem souvisí se třetími stranami, musí to být jasně napsáno v souhlase.
* Souhlas by měl být oddělen od jakýchkoliv dalších pravidel a podmínek
* Databáze souhlasů musí být zpravována a vedena. Včetně informací kdo, kdy, jak
a co.
* Pro jednotlivce musí být jednoduché svůj souhlas odvolat, a musí být dále informováni o tom, jak v případě odvolání souhlasu postupovat.
Vaše záznamy souhlasů by měly být pravidelně kontrolovány, zejména s ohledem na případné změny důvodů nebo způsobů zpracování osobních údajů. V případě změn musí být souhlasy obnoveny.

## **Bude GDPR zpožděno?**

Jakékoliv zpoždění ohledně vstoupení GDPR v účinnost je vysoce nepravděpodobné. GDPR bylo EU Parlamentem schváleno v roce 2016 a veškeré členské státy měly dva roky na přípravu.

## **Vstoupí GDPR v účinnost?**

GDPR bylo schváleno EU Parlamentem v roce 2016 a vstoupí v účinnosti 25. května 2018. Jakékoliv posunutí tohoto data je vysoce nepravděpodobné, toto datum neovlivní ani situace kolem Brexitu.

## **Ovlivní GDPR tzv. B2B?**

GDPR se specificky zaměřuje na jednotlivce, takže v kontextu vašich B2B vztahů by nemělo dojít ke změně – zde však záleží na tom, jaké kontakty k této komunikaci využíváte. Pokud tyto kontakty obsahují jakékoliv osobní údaje, poté je již nutné implementovat dané regulace, včetně souhlasů.
To dále znamená implementování Obecného nařízení.

Pokud však vaše záznamy obsahují pouze všeobecné kontaktní informace (číslo smlouvy nebo e-mailovou adresu beze jména) není nutné zajišťovat souhlas, avšak společnost musí mít možnost kdykoliv souhlas odvolat, toto musí být zaevidováno.

## **Kdy vchází GDPR v účinnost?**

GDPR bylo Evropským parlamentem schváleno v roce 2016, v účinnost vejde 25. května 2018. Jakýkoliv podnik, který nebude mít nové regulace implementovány může čelit vysokým pokutám.

## **Co znamená GDPR pro marketing?**

GDPR není popravou pro marketing, je to pouze způsobem regulování některých aspektů marketingu. Nejde o vraždu přímého marketingu, ale spíše o způsob předání části kontroly jednotlivcům. To znamená, že se markeťáci nyní musí ujistit, že mají jasný souhlas od jednotlivců, kterým je přímý marketing poskytován (ať již telefonem, e-mailem, nebo poštou).

Znamená to, že marketingoví pracovníci musí informovat jednotlivce o:

* Kdo marketing poskytuje (firma nebo organizace). Vyjmenování všech třetích stran, kterým mohou být data předávána.
* Jak budou osobní údaje jednotlivců využívány a pro jaké účely
* Možnost odhlášení, včetně vysvětlení postupu.

Je však také velmi důležité pochopit, že celkový souhlas pro marketingovou skupinu již není povolen. Pod GDPR je zavedeno následující: jeden souhlas na jeden druh marketingové kampaně. Pokud se důvod kampaně změní je nutné vyžádat si nový souhlas. Pokud tedy váš zákazník dá souhlas se zasíláním informací ohledně zahradního nábytku, nesmíte mu na
e-mail zasílat informace o nábytku do koupelny.

## **Co znamená GDPR pro firmy?**

Firmy a organizace, které spravují a zpracovávají osobní údaje o občanech Evropské Unie, bez závislosti na tom, kde se nachází sídlo společnosti, si musí být vědomi následujícího:

* GDPR jasně definuje jiné role pro správce a zpracovatele. Zpracovatelé provádějí konkrétní zpracovávání dat, zatímco správci definují, proč a jak jsou data zpracovávána. Správci dat jsou také zodpovědní za to, že zpracovatelé splňují nařízení GDPR.
* Některé organizace jsou povinny zajistit DPO (Pověřenec pro ochranu osobních údajů). Pracovní skupina WP29 publikuje konkrétní pravidla pro DPO, ale také užitečné FAQ odpovědi.
* Firmy a organizace jsou povinny zajistit a evidovat souhlasy jednotlivců pro osobní data, která jsou spravována (zpracovávána). Souhlas musí vysvětlovat, jak jsou osobní údaje využívány.
* Narušení bezpečnosti, které může vést k ohrožení práv svobod jednotlivců, musí být nahlášeno příslušným úřadům během 72- hodin (v ČR se jedná o Úřad na ochranu osobních údajů). Pokud narušení bezpečnosti spadá do vysokého rizika ohrožení práv svobod jednotlivce, musí být nahlášeno okamžitě.
* Jednotlivci mají právo na vyžádání kopií jejich osobních údajů a dalších informací, zejména se zaměřením na způsob zpracovávání. Díky tomu mohou jednotlivci slevovat správnost právních postupů a postupů zpracovávání osobních údajů
* GDPR poskytuje jednotlivcům práva na výmaz, které je občas označováno jako „Právo být zapomenut“. Toto právo dovoluje občanům požádat o vymazání osobních údajů, které již nejsou potřebné nebo nejsou zákonem vyžadovány. Toto právo není absolutní a společnost může tuto žádost zamítnout za předem jasně stanovených podmínek.
* Přenos dat dává jednotlivcům právo získat své osobní údaje a znovu je využít u jiných poskytovatelů služeb. Díky tomuto právu mohou jednotlivci přesunout, kopírovat nebo převádět jejich osobní údaje z jednoho prostředí do druhého, a to z mnoha důvodů.
* Soukromí se vždy vázalo na ochranu osobních údajů, GDPR však tyto podmínky ukládá jako povinné. Zejména s ohledem na zpracovávání osobních údajů a další příbuzné aktivity.

## **Co znamená GDPR pro HR?**

Články 6 (1) c) a e) Obecného nařízení dovolují členským státům implementovat specifické podmínky, které budou založeny na legislativních podmínkách dané země, s ohledem na ochranu osobních údajů. Musí být splněna alespoň jedna z šesti podmínek, z nichž dvě konkrétní jsou:

• c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

• e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

Toto naznačuje, že zpracovávání osobních údajů zaměstnanců pro některé legitimní operace HR nevyžaduje jasný souhlas. Nicméně, také zde platí veškeré další aspekty GDPR ohledně podmínek pro osobní údaje, včetně:

* Jak a pro co jsou osobní údaje používány
* Ochrana osobních údajů
* Přenos dat a právo na výmaz
* Použití osobních údajů třetími stranami

## **Na koho se GDPR vztahuje?**

GDPR se vztahuje na veškeré společnosti a organizace, které spravují a zpracovávají osobní údaje o jednotlivcích žijících na území Evropské unie, bez závislosti na umístění sídla firmy. To znamená, že GDPR platí i pro ty podniky, které se fyzicky nenacházejí v žádném z členských států EU.

## **Je možné se pojistit proti GDPR pokutám?**

Na tuto otázku zatím neexistuje přesná odpověď, nicméně, současný pohled na tuto problematiku nepředpokládá, že by bylo nějaké pojištění možné. S pokutami až do výše 4 % z ročního obratu se může nedodržování podmínek tohoto nařízení prodražit jakékoliv firmě. Přesný postup v této otázce bude moci být nastaven až poté, co vejde nové nařízení v platnost a do doby, než bude proveden první soudní spor. Nicméně, specifické podmínky pro cyber pojištění by mohly chránit podniky proti pokutám spojeným s únikem dat a s nimi spojené soudní výhrady, ale také reputaci firmy.

## **Jak ovlivní GDPR podniky z USA?**

GDPR platí pro všechny společnosti a organizace, které sbírají a spravují osobní údaje o jedincích z Evropské unie, bez ohledu na to, kde je sídlo dané organizace. To znamená, že jak na organizace z USA, tak na organizace ze zbytku světa se toto nařízení opravdu vztahuje. Toto nařízení pravděpodobně neovlivní květinářství ve státě Wyoming, ale jakmile společnost zpracovává údaje o občanech EU, již se musí připravit na tuto implementaci.
Součástí této implementace je:

* Jasný a zaevidovaný souhlas se sběrem a zpracováním osobních údajů jedinců
* Jasné vysvětlení o tom jak a jaká data jsou sbírána, a na co budou využita
* Zpracování ochrany osobních údajů a příprava na možné ohrožení dat
* Podpora pro přenos dat a právo na jejich výmaz
* Dodržování pravidel obecného nařízení GDPR třetími stranami

Mnoho podniků spoléhá na úvodní stránky a newslettery k přihlášení odběrů a vybudování úspěšného podniku. Tato praxe již pod GDPR nebude možná, tedy alespoň z pohledu občanů EU, celkový souhlas je nyní zakázán. GDPR schvaluje pouze ty souhlasy, které jsou specifické, což musí ze souhlasu jasně vyplívat. Pokud se občas EU přihlásí k odběru novinek jednou za týden, poté to je ten jediný druh e-mailu, který takovému jedinci můžete zaslat. Pokud zašlete jiný e-mail, například s novou nabídkou, poté již GDPR porušujete. Pokud se důvod souhlasu změní, musí být vyžádán souhlas nový.

## **Jakým způsobem mění GDPR podmínky pro výzkum dat?**

Mezi klíčové oblasti výzkumu, které budou ovlivněny obecným nařízením GDPR patří:

* **MOŽNOST SBÍRAT DATA.**
Souhlas – být informován o tom proč jsou data sbírána a za jakým účelem budou zpracována je nejdůležitějším faktorem. Ustanovení právního základu pro zpracovávání dat má specifické nároky, které nejsou aplikovatelné na veškeré situace nebo organizace.
* **MOŽNOST UŽÍVAT DATA**
Pokud byl udělen souhlas, je důležité si pamatovat, že tento souhlas byl jedincem udělen ke zpracování osobních údajů. Pokud se předmět souhlasu změní, musí být získán nový a specifický souhlas jedince. Zároveň mají jedinci právo kdykoliv blokovat udělený souhlas ke zpracování, vznést proti zpracování námitku nebo uplatnit právo na výmaz osobních údajů, což může zásadně ovlivnit nebo limitovat výsledek výzkumu, který je s těmito daty spojen.
* **MOŽNOST PŘESNÁŠET DATA PRO/OD TŘETÍ STRANY**
GDPR ukládá přísné omezení na to jak a kdy jsou data přenášena do zemí mimo EU
a do rukou mezinárodních organizací. Tato část nařízení značně ovlivní možnosti vědeckých výzkumů dat a jejich sdílení.
* **AUTOMATIZACE**
Automatické profilování a rozhodování má nově vbudované zásady pro jedince, které jim dovolují, v některých případech, vyžádat zásah lidského faktoru, a to zejména v podobě vysvětlení automatického rozhodnutí.
* **POŽADAVKY NA SKLADOVÁNÍ DAT**
Ochrana osobních údajů je základem GDPR, tato ochrana je značně jednoduší v případech, kdy jsou data anonymizována a identifikace jedinců je nemožná. Je však důležité v organizaci zajistit, že anonymizace dat je věrohodná a kompletní.

## **Jakým způsobem ovlivní GDPR školy?**

Školy a školní administrátoři si musí být vědomi následujícího:

* Souhlas rodičů je nutností pro sběr dat o dětech mladších 16 let. Tato věková hranice je v Britském zákoně na ochranu osobních údajů snížena na 13 let.
* GDRP definuje rozdíl mezi osobním údajem a citlivým osobním údajem, a to následujícím způsobem:
* Zpracovávání osobních dat jejichž obsah definuje rasový nebo etnický původ, politické zaměření, náboženské nebo filosofické myšlení, členství v odborech a zpracovávání genetických a biometrických dat za účelem identifikování jedince, údaje o zdravotním stavu nebo sexuálním životě a orientaci jedince jsou zakázány.
* Sbírání těchto dat je možností za přesně stanovených podmínek. Školy se v tomto případě mohou obrátit na Článek 9 obecného nařízení.
* Údaje, které vedou k identifikaci jedince musí být vedeny pouze po dobu, po kterou byla data původně vyžádána. Výjimkami jsou dokumenty, které musí být archivovány dle zákonů české (nebo jiné) legislativy.
* Marketing je možný pouze v případech, kdy k němu byl předán jasný a přesný souhlas. V případě marketingu musí být volba odhlášení jednoduchá a jasně vysvětlená.
* Také u škol stále platí ostatní GDPR pravidla.

## **Jak GDPR ovlivní Google nebo Facebook?**

Jak Google, tak Facebook se silně spoléhají na sběr a zpracovávání osobních údajů svých uživatelů. Některá tato data jsou poskytnuta dobrovolně během registrace ke Google nebo Facebook službám, ale některé údaje jsou sbírány způsobem sledování skrze připojené platformy a služby. Tyto funkce jsou poté využity nejen ke zlepšování služeb, ale hlavně k personalizaci pro poskytování reklam. Toto je v GDPR problematickou kapitolou. Prvním důvodem je právní důvod, který je pro sběr osobních údajů zapotřebí, a to včetně jasně specifikovaného souhlasu. Druhým problémem je kompletní souhlas, který již není povolen. Vše musí mít specifický souhlas.

To znamená, že jak Google a Facebook, tak další podobné služby, budou muset připravit pro uživatele hned několik dialogových oken, každé navázané na specifickou službu, s jasným popisem záměru daného souhlasu. Tato volba jedince nesmí být předem označena nebo schválena, zároveň musí být volitelná pro následné poskytování služeb. A nakonec musí mít jedinci možnost svou volbu stáhnout, a to kdykoliv.

Není pochyb o tom, že organizace velikosti Google nebo Facebooku budou schopni plnit požadavky tohoto nařízení s co nejmenším možným dopadem na jedince. To však neznamená, že nebude značně ovlivněn podnikatelský model těchto společností. Obě platformy využívají enormní množství osobních údajů k vybudování detailních profilů pro přesné a účinné reklamy (například zaměřením dle demografie apod.), nyní však tento model může být ovlivněn specifickými požadavky GDPR.

Konkrétní dopad obecného nařízení na společnosti typu Google a Facebook nám budou známy až poté, co vejde GDPR v účinnost.

## **Ovlivní GDPR nábory?**

Tak jako s marketingem, ani v případě pracovních agentur se nejedná o GDPR popravu, zejména pokud do současné doby fungovaly v souladu se Zákonem na ochranu osobních údajů. GDPR bylo sepsáno tak, aby v mnoha oblastech fungoval stejným způsobem, jak to předepisují předešlé legislativy, a to v mnoha oborových oblastech. Pracovní agentury si musí dávat pozor na následující:

* Souhlas jedince musí být poskytnut pro veškeré aktivity spojené se zpracováním osobních údajů. Kompletní nebo vágní souhlasy nejsou povoleny.
* Pokud bude uchazeč odpovídat požadavkům jiné pracovní pozice nežli té, o kterou usiluje, musí být nejdříve kontaktován s bližšími informacemi o pozici a dále předat souhlas se zpracováním osobních údajů pro novou pozici.
* Musí existovat zabezpečení v případě automatického rozhodování a profilování. Toto zabezpečení musí jedince chránit před vykonáním rizikového automatického rozhodnutí.

## **Jaký bude mít GDPR dopad na charitativní organizace?**

GDPR klade nejvyšší nároky na definování souhlasů. Tím vrací více kontroly nad osobními údaji zpět vlastníkům/zákazníkům/dárcům, díky tomu bude vybudována větší úroveň důvěry.

Platný souhlas dle GDPR znamená následující:

* Souhlas musí být výslovný a označený jedincem. Souhlasy tedy nesmí být předem zaškrtnuty jako platné nebo podmínkou poskytnutí prodeje či služby.
* Souhlas nesmí být vágní. Jedinec musí předat jasný souhlas a musí dobře rozumět tomu s čím souhlasí a komu souhlas poskytují. Pokud jsou údaje předávány třetím stranám, tato informace musí být v souhlasu zahrnuta.
* Souhlas by měl být oddělen od všech ostatních pravidel a podmínek (např. obchodních podmínek).
* Souhlas musí být evidován a archivován. A to včetně informací: kdo, kdy, jak, proč.
* Pro jedince musí být jednoduché takový souhlas odvolat. Zároveň musí být informováni o tom, jak svůj souhlas odvolat.
* Evidence souhlasů by měla být pravidelně kontrolována, zejména pro případné změny v obsahu souhlasu. Pokud ke změnám došlo, musí být souhlas obnoven za nových podmínek.

Charity a další organizace, které do současné doby spoléhaly na předem označené souhlasy nebo kompletní souhlasy budou muset aktualizovat svou databázi dárců/zákazníků, a to odesláním nových žádostí o souhlas, který musí posléze být zaevidován. Tyto souhlasy se týkají občanů EU. Mnoho charit se dále spoléhá na práci dobrovolníků, tito pracovníci musí být informováni a proškoleni v oblasti těchto změn.

## **Proč je GDPR takový strašák?**

Toto obecné nařízení sebou přináší mnoho změn, které mohou podnikání finančně zatížit,
a to zejména v oblasti pokut. Ve výsledku se však jedná o poměrně dobré změny, které přinášejí více kontroly jedincům, a to pro potřeby ochrany a kontroly nad jejich vlastními osobními údaji. Spolu s tím je zde možnost vybudovat vztah založený na důvěře mezi zákazníky a organizací. GDPR je v mnoha ohledech také mnohem jasnější a zjednodušenější oproti dříve platným legislativám. Pokud byly tyto legislativy dodržovány do současné doby, čeká na firmy pouhých pár změn. Aby mohlo být porozuměno pravému dopadu na organizace budeme muset počkat na dobu, kdy bude obecné nařízení účinné a poté zejména na první soudní rozhodnutí, které určí další postup.

## **Čím je GDPR dobré pro podnikání?**

GDPR přináší možnost vybudovat silnější a důvěrnější vztah mezi zákazníky a organizacemi, což je vždy pozitivní. Pro mnoho organizací je to také možností, jak pročistit své marketingové a prodejní databáze. Díky tomu firmy nejen aktualizují osobní údaje, ale mohou zároveň vyčlenit neaktivní uživatele, ale také uživatele, kteří obnoví svůj zájem o služby nebo produkty firem. Dále se jedná o příležitost firem zaměřit se na způsob, jakým s tímto druhem dat nakládají a odhalit tak slabá místa nebo nový potenciál pro změnu, která může naopak přinést marketingový a prodejní růst. Ale jak to s nařízeními bývá, je nutné počkat na první soudní rozhodnutí, které přijde spolu s účinností tohoto nařízení.

# **Jak snížit dopad GDPR na vaše podnikání**

Existuje africké pořekadlo, které se k GDPR perfektně hodí:

 „Nejlepší způsob, jak sníst slona stojícího v cestě je rozkrájet jej na malé kousky.“

A nejlepší způsob, jak minimalizovat dopad Obecného nařízení na ochranu osobních údajů na vaše podnikání je rozdělit jeho požadavky na několik menších úkolů.

Úřad na ochranu osobních údajů ve Velké Británii (ICO) připravil obsáhlou GDPR příručku, která mimo jiné, obsahuje také online formulář pro správce i zpracovatele údajů. Dále ICO představuje 12 kroků, které by měla firma podniknout již nyní, aby se na GDPR připravila.

## **Seznámení**

První krok je poměrně očividný. Základem je seznámit všechny zaměstnance s blížícími se změnami, ale také se změnami postupů, které budou uvnitř podnikání nově zavedeny.

## **Odpovědnost**

Odpovědnost začíná s kompletním informačním auditem, důležitý je také rozsah vašeho podniku a množství osobních údajů, které vlastníte. Informační audit je jedním z největších úkolů, které na vás v rámci tohoto nařízení čekají. Je také jedním z těch vůbec nejdůležitějších.

Informační audit odhalí přesné informace o veškerých osobních údajích, které nyní spravujete a zodpoví vám následující otázky:

* Jak byly osobní údaje sbírány? Byly vám předány jedincem, a pokud ano, jak?
Nebo byla data získána zcela jiným způsobem?
* Jaký byl původní záměr pro sběr těchto dat? Jaký byl původní důvod? Bylo to přihlášením k odběru novinek, žádostí o doplnění informací o produktu/službě, nebo vytvořením profilu (například v případě e-shopů)?
* Budete pokračovat ve spravování/zpracovávání těchto údajů, a na jak dlouho? Pokud již neexistuje právní důvod pro uchovávání těchto údajů, musí být zlikvidovány.
* Jsou údaje zabezpečeny? A to jak z pohledu šifrování, tak z pohledu omezení přístupů k osobním údajům.
* Byly údaje někdy sdíleny s třetí stranou. Pokud ano, existuje záznam o tomto sdílení pro potřeby GDPR. Jsou si majitelé osobních údajů vědomi, s kým jsou data sdílena a za jakým účelem?

Nejenže GDPR požaduje po firmách schopnost prokázat způsob jakým odpovídají obecnému nařízení, v mnoha ohledech je nutné tyto postupy dobře zdokumentovat. Opět můžeme doporučit webovou stránku britského ICO, která obsahuje krátký formulář, který může podnikům pomoci identifikovat slabá místa ohledně záznamů evidencí a spravování souhlasů.

## **Komunikace se zákazníky, zaměstnanci a uživateli**

Dodržování GDPR je také silně odvozeno od toho, že váš podnik aktualizuje veškeré dokumenty vztahující se k ochraně osobních údajů, nebo je vytvoří. Předtím, než tento dokument budete opravovat je zcela zásadní si uvědomit, jakým způsobem jsou údaje sbírány, a to nejen v tradičním slova smyslu. Sbírání osobních údajů se může vztahovat také na následující:

* SLEDOVÁNÍ, a to využitím technologií pro sledování uživatelů internetu skrze chytrá zařízení;
* ODVOZENÍ na základě dalších sbíraných údajů
* ALGORITMY pro potřeby analýzy údajů získaných z takových platforem jako jsou sociální média, údaje o lokalitě nebo záznamy o nákupech, a to s cílem profilování uživatelů, jejich solventnosti, zdraví, nebo vhodnosti pro pracovní pozici.

Dokument o ochraně osobních údajů musí být stručný, sepsaný prostým jazykem a jednoduše přístupný. GDPR dále nařizuje konkrétní informace, které musí být v těchto dokumentech obsaženy, s menšími rozdíly v případech, zda jsou údaje získávány přímo od jedinců, či nikoliv. Pomůže vám obrázek níže:

|  |  |  |
| --- | --- | --- |
| **Jaké informace musí být zmíněny?**  | **Údaje získány přímou cestou** | **Údaje získány nepřímou cestou**  |
| Identifikace a kontaktní údaje správce (a jeho zástupce – pokud je) a kontakt na Pověřence osobních údajů | Znak zaškrtnutí | Znak zaškrtnutí |
| Účel a zákonný důvod pro zpracování osobních údajů | Znak zaškrtnutí | Znak zaškrtnutí |
| Zákonný důvod třetích stran (pokud existuje) | Znak zaškrtnutí | Znak zaškrtnutí |
| Kategorie osobních údajů |  | Znak zaškrtnutí |
| Příjemce nebo kategorie příjemců osobních údajů | Znak zaškrtnutí | Znak zaškrtnutí |
| Informace o přenosu dat do třetích zemí a jejich zabezpečení  | Znak zaškrtnutí | Znak zaškrtnutí |
| Kritéria pro určení délky uchování osobních údajů | Znak zaškrtnutí | Znak zaškrtnutí |
| Existující práva majitelů osobních údajů | Znak zaškrtnutí | Znak zaškrtnutí |
| Právo na odvolání souhlasu (kdykoliv) | Znak zaškrtnutí | Znak zaškrtnutí |
| Právo na vznesení námitky u příslušného úřadu | Znak zaškrtnutí | Znak zaškrtnutí |
| Původ osobních údajů (včetně informace o veřejném zdroji) |  | Znak zaškrtnutí |
| Informace, zda je poskytnutí osobních údajů povinné v návaznosti na naplnění služby a důsledek v případě neposkytnutí těchto údajů  | Znak zaškrtnutí | Znak zaškrtnutí |
| Existence automatického rozhodování a profilování a jeho důsledky. | Znak zaškrtnutí | Znak zaškrtnutí |
| Kdy jsou tyto informace poskytnuty? | V momentě jejich sběru  | * V přiměřené lhůtě (do měsíce)
* V případě, kdy jsou údaje použity za účelem komunikace
* Pokud jsou údaje předávány dál
 |

## **Osobní ochrana osobních údajů**

Je nutné se zaměřit na veškeré procesy, kterých vaše firma využívá pro sbírání a zpracovávání osobních údajů. Důvodem je začlenění veškerých práv jedinců, které jsou v GDPR zahrnuty.

Zohlednit musíte následující:

* Jaký zaměstnanec bude pověřen rozhodováním o výmazu osobních údajů? Právo na výmaz není absolutním právem a podléhá ostatním legislativám, podniky tedy mohou tuto žádost zamítnout.
* Jak dlouho bude podniku trvat vydat kopii s informacemi ohledně osobních údajů, které firma o jedinci uchovává a jak dlouho bude trvat případná oprava/výmaz?
* Jakým způsobem bude kontrolována správnost osobních údajů nebo nutnost jejich likvidace, a to včetně údajů uchovávaných třetími stranami?
* Bude váš podnik schopen dodržovat pravidla přístupu k osobním údajům pro jedince (na základě žádosti)? A to zejména s možností poskytnout údaje v elektronické podobě a v nejčastěji využívaných formátech?

## **Bude žádost o přístup změněna?**

GDPR vyžaduje, aby byly žádosti o přístup vyřizovány bez zbytečného odkladu, a to nejpozději do měsíce od jejího podání. Tyto žádosti mohou být podány nejen z pohledu poskytnutí kopií uchovávaných údajů jedince, ale také z pohledu potvrzení o zpracovávání dat a dalších informací o zpracovávání, které by měly být součástí dokumentu o ochraně osobních údajů: jak jsou data zpracovávána, za jakým účelem, nebo zda jsou s někým sdílena apod. Dále vám mohou přijít žádosti o výmaz osobních údajů nebo žádost o opravu osobních údajů. Je proto důležité zkontrolovat veškeré postupy a ujistit se, že jako podnik budete schopni na tyto žádosti reagovat.

## **Co je míněno Zákonným důvodem pro Zpracování?**

Ačkoliv GDPR klade velký důraz na souhlas jedince, existují případy, kdy souhlasu není pro zpracování osobních údajů zapotřebí. Zkontrolujte veškeré způsoby zpracovávání osobních údajů ve vaší firmě za účelem určení zákonného zpracování. Tento krok je důležitý jak pro doplnění podmínek na ochranu osobních údajů, tak pro definování potřebnosti souhlasu.

## **Používání Souhlasu Zákazníka jako Zákonného důvodu pro Zpracování**

GDPR očekává, že veškeré souhlasy budou „dobrovolné, specifické, informativní a jednoznačné“. Jedinci musí vědět s čím přesně souhlasí. Souhlas nesmí být podmínkou k poskytnutí prodeje nebo služby. Zkontrolujte proto veškeré způsoby, jakými jsou data sbírána a požadována. Zaměřte se na následující:

* Jakákoliv žádost o souhlas by měla být oddělena od Obchodních podmínek. Je důležité změnit Obchodní podmínky dle tohoto nařízení.
* Pokud je souhlas udělován zaškrtávacím políčkem, ať již v elektronické nebo papírové formě, ujistěte se, že tato políčka nejsou předem označena.
* Ujistěte se, že vaše CRM a databáze jsou vybaveny záznamem o souhlasech. Tyto záznamy by měly obsahovat zejména datum a čas udělení souhlasu, jak byl souhlas udělen a jaké bylo jeho znění.
* Pokud sbíráte údaje za pomocí online formulářů doporučujeme služby typu MailChimp, které mají možnost dvojího potvrzení a zaznamenání času i data každého podání.
* Ujistěte se, že váš systém dovoluje jednoduché odvolání souhlasu přímo jedincem.

Zároveň je důležité zkontrolovat veškeré souhlasy, které již vlastníte, a to nejlépe před spuštěním GDPR.

## **Zpracovávání osobních údajů dětí**

Pokud sbíráte osobní údaje o dětech mladších 16 let, je velmi důležité prověřit váš systém z pohledu bezpečnosti nebo potvrzení věku jedince, včetně získávání souhlasu rodičů či zákonných zástupců.

## **Oznámení Porušení zabezpečení**

Podnik musí zajistit dostatečné procesy pro detekování, vyšetření a oznamování porušení zabezpečení. Dle obecného nařízení GDPR jsou podniky povinny nahlásit nebezpečné narušení ochrany osobních údajů příslušnému úřadu na ochranu osobních údajů, a to do 72 hodin od zjištění takového narušení. V některých případech je důležité informovat také majitele osobních údajů. Nesplnění těchto požadavků může mít za výsledek velmi vysokou pokutu.

## **Posouzení vlivu na ochranu osobních údajů (DPIA) a Výchozí ochrana osobních údajů**

Ačkoliv ochrana osobních údajů vždy byla zakořeněna v legislativě, GDPR nyní přináší kombinaci posouzení vlivu na ochranu osobních údajů (DPIA) a výchozí ochranu osobních údajů v případech, kdy se jedná o rizikové zpracovávání osobních údajů. Kromě podmínek na ochranu osobních údajů doporučujeme se zaměřit na následující:

* Využití šifrování osobních údajů a pseudonymizace a/nebo anonymizace dat.
* Sdílení údajů. Jaká data jsou sdílena a za jakým účelem. Jsou data sdílena bezpečně a splňuje organizace, které jsou údaje poskytovány, podmínky obecného nařízení GDPR?

## **Pověřenec na ochranu osobních údajů**

Povinnost zavedení pozice Pověřence ochrany osobních údajů není povinností pro veškeré podniky. Je však důležité se seznámit s podmínkami této pozice a částečně se jimi inspirovat pro správné plnění obecného nařízení.

## **Mezinárodní organizace a GDPR**

Toto obecné nařízení se zaměřuje na všechny organizace a firmy, které sbírají osobní údaje
o jedincích pocházejících z členských států Evropské unie, a to bez ohledu na to, kde je se nachází sídlo samotné firmy. Každý členský stát má svou vlastní autoritu (pro ČR Úřad na ochranu osobních údajů), nicméně, mezinárodní organizace mohou spolupracovat s Vedoucím orgánem pro dohled (LSA).