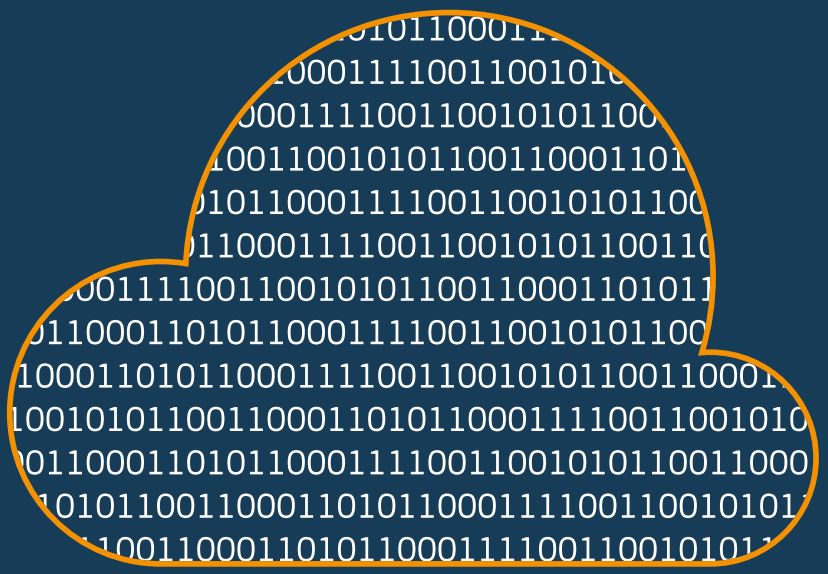
Evropská komise

GDPR: nové příležitosti, nové povinnosti



Co musí každý podnik vědět o obecném nařízení EU o ochraně osobních údajů

Spravedlnost a spotřebitelé

Printed by Bietlot in Belgium

Lucemburk: Úřad pro publikace Evropské unie, 2018

Print	ISBN 978-92-79-79427-8	doi:10.2838/50718	DS-01-18-082-CS-C
PDF	ISBN 978-92-79-79437-7	doi:10.2838/246812	DS-01-18-082-CS-N

OBSAH

KAPITOLA 1

OBCHODNÍ PŘÍLEŽITOST

Nařízení GDPR upravuje způsob, jakým podniky zpracovávají a spravují osobní údaje. Bude účinné od 25. května 2018, vztahuje se na všechny podniky a organizace (např. nemocnice, veřejné správní orgány apod.) a představuje největší změnu pravidel ochrany údajů v EU za posledních dvacet let.

Nařízení GDPR dává občanům nejen větší kontrolu nad tím, jak jsou jejich osobní údaje využívány, ale také významnou měrou zefektivňuje regulační prostředí pro podniky. Provádí to tím, že zakládá jednotný rámec pro právní předpisy o ochraně údajů napříč EU. Jinými slovy, místo toho, aby každá země měla své vlastní právní předpisy o ochraně údajů, je nyní celá EU řízena jedním jediným nařízením. Společnost působící v různých zemích tak již nemusí dodržovat mnoho – často odlišných – předpisů. Místo toho musí při nabízení svých služeb kdekoli v EU dodržovat pouze nařízení GDPR.

Jaký prospěch může mít z nařízení GDPR vaše společnost

- **Jedna Unie, jedno právo:** jednotný soubor pravidel usnadňuje a zlevňuje podnikání v EU.
- **Jediné kontaktní místo:** ve většině případů musí společnosti jednat pouze s jedním úřadem pro ochranu údajů.
- **Evropská pravidla na evropské půdě:** když společnosti se sídlem mimo území EU nabízejí své zboží nebo služby fyzickým osobám v EU, musejí dodržovat stejná pravidla jako evropské společnosti.
- **Přístup založený na riziku:** nařízení GDPR ruší obtížnou univerzální povinnost a místo toho upravuje povinnosti podle příslušných rizik.
- **Pravidla vyhovující inovacím:** nařízení GDPR je technologicky neutrální.

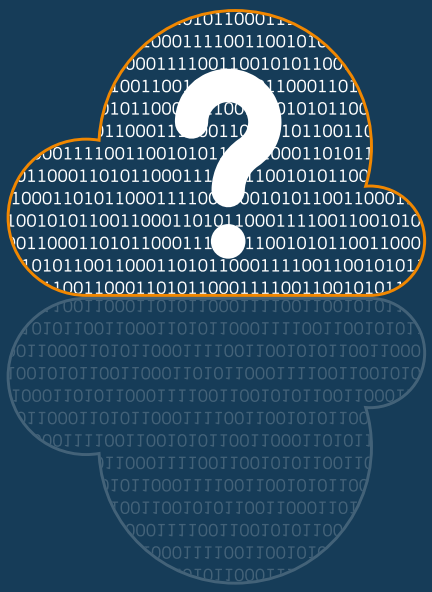
Jde o důvěru

Ochrana osobních údajů vyvolává ve fyzických osobách značné obavy. Z tohoto důvodu zůstává jejich důvěra v digitální prostředí nízká. Podle průzkumu Eurobarometr:

- osm z deseti lidí má pocit, že své osobní údaje nemá zcela pod kontrolou,
- šest z deseti lidí uvádí, že nedůvěřují internetovým podnikům,
- více než 90 % Evropanů si podle vlastního vyjádření přeje, aby ve všech zemích EU platila stejná práva na ochranu údajů.

Nařízení GDPR představuje novou příležitost pro váš podnik, jak zvýšit důvěru spotřebitelů na základě správy osobních údajů založené na riziku.

„Podniky, které nechrání osobní údaje fyzických osob dostatečně, riskují, že přijdou o důvěru spotřebitelů, která je zásadní pro přesvědčování lidí k používání nových výrobků a služeb.“



KAPITOLA 2

POCHOPENÍ NAŘÍZENÍ GDPR

Týká se GDPR i mě?

Stručně řečeno, GDPR se týká ***každého*** podniku, který:

zpracovává osobní údaje automatickým nebo **manuálním** způsobem (pokud jsou údaje uspořádány podle kritérií).

I když váš podnik zpracovává údaje pouze jménem jiných společností, musíte se těmito pravidly řídit.

Nařízení GDPR platí, pokud:

- vaše společnost zpracovává osobní údaje a má sídlo v EU bez ohledu na to, kde vlastní zpracování údajů probíhá, nebo
- vaše společnost je usazena mimo EU, ale nabízí zboží či služby fyzickým osobám v EU nebo monitoruje jejich chování.

Co jsou to osobní údaje?

Osobní údaje označují jakékoli informace, které se týkají identifikované nebo identifikovatelné žijící osoby. Může mezi ně patřit:

- jméno
- adresa a telefonní číslo
- poloha
- zdravotní záznamy
- příjem a bankovní údaje
- kulturní preference
- ... a další.

Nařízení GDPR se vztahuje i na osobní údaje, které sice byly zbaveny informací umožňujících identifikaci nebo byly pseudonymizovány, ale lze je použít ke zpětné identifikaci osoby. Avšak osobní údaje, které byly anonymizovány takovým nezvratným způsobem, že příslušná osoba již není identifikovatelná, za osobní údaje považovány nejsou, a nařízení GDPR se na ně tudíž nevztahuje.

Nařízení GDPR je též technologicky neutrální, což znamená, že chrání osobní údaje bez ohledu na použitou technologii nebo způsob uložení osobních údajů. Nehledě na to, zda váš podnik osobní údaje zpracovává nebo uchovává pomocí složitého IT systému nebo papírových složek, bude se na vás nařízení GDPR vztahovat.

„Nehledě na to, zda váš podnik osobní údaje zpracovává nebo uchovává pomocí složitého IT systému nebo papírových složek, bude se na vás nařízení GDPR vztahovat.“

Dávejte zvláštní pozor na speciální (citlivé) kategorie osobních údajů

Pokud osobní údaje, které shromažďujete, zahrnují informace o zdraví fyzické osoby, její rase, sexuální orientaci, náboženském a politickém přesvědčení nebo členství v odborech, jsou pokládány za citlivé. Vaše společnost může tyto údaje zpracovávat pouze za specifických podmínek a vy možná budete muset provést další bezpečnostní opatření, jako je šifrování.

Co je to zpracování osobních údajů?

Podle nařízení GDPR spadají do definice zpracování osobních údajů taková opatření, jako je shromažďování, používání a odstraňování osobních údajů.

Monitorujete své prostory pomocí kamerového systému? Nahlížíte pro účely podnikání do databáze obsahující osobní údaje? Zasíláte propagační e-maily? Mažete (digitální) složky o zaměstnancích nebo skartujete dokumenty? Nebo zveřejňujete fotografii nějaké osoby na své internetové stránce nebo kanálech sociálních médií?

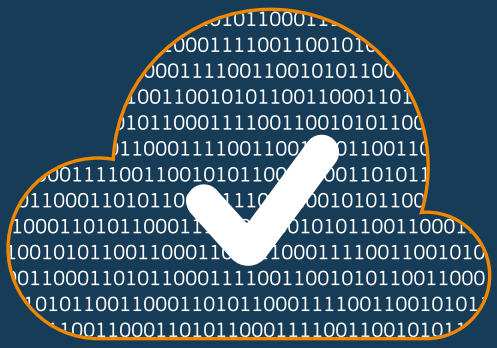
Pokud jste na některou z těchto odpověděli „ano“, pak vaše společnost zcela jistě zpracovává osobní údaje.

Jak nařízení GDPR pomáhá snižovat náklady?

Nařízení GDPR zohledňuje potřeby podniků. Jeho cílem je například odstranit administrativní požadavky za účelem snížení nákladů a minimalizace administrativní zátěže:

- **Již žádná oznámení předem**: ve většině případů ruší reforma povinnost informovat dozorové úřady předem, a to i se souvisejícími náklady.
- **Pověřenci pro ochranu osobních údajů**: společnosti musí především jmenovat pověřence pro ochranu osobních údajů, pokud mezi jejich hlavní činnosti patří rozsáhlé zpracování citlivých osobních údajů nebo pravidelné a systematické monitorování fyzických osob. Orgány veřejné správy mají vždy povinnost jmenovat pověřence pro ochranu osobních údajů.
- **Posouzení vlivu na ochranu osobních údajů**: společnosti jsou povinny provádět posouzení vlivu na ochranu osobních údajů pouze v případě, že navrhovaná činnost v rámci zpracování údajů představuje vysoké riziko pro práva a svobody fyzických osob.
- **Uchovávání záznamů**: společnosti s méně než 250 zaměstnanci nejsou povinny uchovávat záznamy, pokud zpracování údajů je náhodné nebo nezahrnuje citlivé údaje.

„Cílem je například odstranit administrativní požadavky za účelem snížení nákladů a minimalizace administrativní zátěže.“



KAPITOLA 3

VAŠE POVINNOSTI PODLE NAŘÍZENÍ GDPR

Nařízení GDPR ukládá společnostem na úrovni EU přímé povinnosti týkající se zpracování údajů. Podle něj může společnost zpracovávat osobní údaje pouze za určitých podmínek. Například zpracování by mělo být spravedlivé a transparentní, mělo by probíhat pro upřesněný a oprávněný účel a mělo by se omezovat na údaje nutné ke splnění tohoto účelu. Musí se opírat o jeden z následujících právních důvodů.

- **Souhlas** dotčené fyzické osoby.
- **Smluvní závazek** mezi vámi a danou fyzickou osobou.
- Splnění **právního závazku**.
- Ochrana životně důležitých zájmů fyzické osoby.
- Splnění úkolu prováděného ve veřejném zájmu.
- Pro **oprávněné zájmy** vaší společnosti, ale pouze po ujištění se, že nejsou závažně dotčena základní práva a svobody fyzické osoby, jejíž osobní údaje zpracováváte. Pokud práva dotyčné fyzické osoby převažují nad vašimi zájmy, pak zpracování údajů není možné.

Hlavní bod: získání souhlasu s používáním osobních údajů

Nařízení GDPR uplatňuje přísná pravidla pro zpracování údajů na základě souhlasu. Účelem těchto pravidel je zajistit, aby fyzická osoba chápala, s čím souhlasí. To znamená, že souhlas by měl být **dobrovolný, konkrétní, informovaný** a **jednoznačný** na základě žádosti formulované jasným a jednoduchým jazykem. Kromě toho by měl být souhlas vyjádřen formou **potvrzení**, jako je zaškrtnutí okénka na internetu nebo podepsání formuláře.

Zpracováváte-li osobní údaje týkající se **dítěte** na základě souhlasu, je vyžadován souhlas rodiče. Ale vzhledem k tomu, že se věková hranice pohybuje v jednotlivých zemích od 13 do 16 let, doporučujeme vám, abyste si to ověřili ve vnitrostátním právu.

Nezapomeňte! Pokud někdo souhlasí se zpracováním osobních údajů, můžete tyto údaje zpracovat pouze pro účely, pro něž byl dán souhlas. Musíte též dát fyzickým osobám příležitost ke zrušení jejich souhlasu.

Určení vaší role a odpovědnosti

Jakmile jste určili, že se nařízení GDPR vztahuje na váš podnik a že dochází ke zpracování osobních údajů, je dalším krokem určení vaší role.

Pravidla ochrany údajů rozlišují mezi správcem osobních údajů a zpracovatelem osobních údajů, přičemž každý z nich má jiné povinnosti. Zatímco správce osobních údajů určuje účel a prostředky zpracování osobních údajů, zpracovatel osobních údajů osobní údaje pouze zpracovává jménem správce údajů. To však neznamená, že se zpracovatel může jednoduše skrýt za správce.

Nařízení GDPR vyžaduje, aby správce osobních údajů zapojil pouze zpracovatele osobních údajů, který nabízí dostatečné záruky. Tyto záruky by měly být obsaženy v písemné smlouvě, kterou správce a zpracovatel spolu uzavřou. Smlouva musí zahrnovat řadu povinných ustanovení, například včetně ustanovení, že zpracovatel bude osobní údaje zpracovávat pouze na základě zdokumentovaných pokynů správce.

Povinnosti, které chrání práva fyzických osob

Nařízení GDPR zahrnuje řadu povinností, jejichž cílem je ochrana práva fyzické osoby mít kontrolu nad svými osobními údaji.

Vaše povinnost: poskytování transparentních informací

Společnosti musí fyzickým osobám poskytovat informace o tom, kdo co zpracovává a proč. Minimálně musí tyto informace jasně uvádět:

- kdo jste,
- proč údaje zpracováváte,
- co je právním základem,
- kdo údaje obdrží (je-li to relevantní).

V některých případech musí informace též uvádět:

- kontaktní údaje pověřence pro ochranu osobních údajů,
- oprávněný zájem (je-li oprávněný zájem právním základem zpracování),
- základ pro přenos údajů do země mimo EU,
- jak dlouho budou údaje uchovávány,
- práva fyzické osoby na ochranu údajů (např. právo na přístup k údajům, jejich opravu, výmaz, omezení, námitku, přenositelnost apod.),
- jak lze souhlas zrušit (když je souhlas právním základem zpracování),
- zda existuje zákonná nebo smluvní povinnost poskytovat údaje,
- v případě automatizovaného rozhodování, informace o příslušné logice, významu a důsledcích daného rozhodnutí.

„Společnosti musí fyzickým osobám poskytovat informace o tom, kdo co zpracovává a proč.“

Vaše povinnost: právo na přístup k údajům a právo na přenositelnost údajů

Fyzické osoby mají právo požádat o bezplatný přístup k osobním údajům a v přístupném formátu. Pokud takovou žádost obdržíte, musíte:

- sdělit fyzické osobě, zda její osobní údaje zpracováváte,
- informovat ji o zpracování (například o účelech zpracování, kategoriích dotčených osobních údajů, příjemcích jejich údajů atd.),
- poskytnout kopii osobních údajů, které zpracováváte.

Navíc, když se zpracování opírá o souhlas nebo smlouvu, může fyzická osoba požádat o vrácení jejích osobních údajů nebo o jejich převedení na jinou společnost. Tomu se říká právo na přenositelnost údajů. Údaje by měly být poskytovány v běžně používaném a strojově čitelném formátu.

Ačkoli tato dvě práva spolu úzce souvisí, jedná se o dvě odlišná práva. Musíte se tak ujistit, že mezi těmito dvěma právy nedochází k záměně, a musíte fyzickou osobu podle toho informovat.

Vaše povinnost: právo na výmaz (právo být zapomenut)

Za určitých okolností může fyzická osoba požádat správce osobních údajů o výmaz svých osobních údajů, například když její údaje již nejsou nutné k účelu zpracování. Vaše společnost však není povinna této žádosti vyhovět, pokud:

- zpracování je zapotřebí k respektování svobody projevu a informací člověka,
- musíte si osobní údaje ponechat ze zákonných důvodů,
- existují pro zachování osobních údajů jiné důvody ve veřejném zájmu, např. veřejné zdraví nebo účely vědeckého či historického výzkumu,
- osobní údaje si musíte ponechat pro určení právního nároku.

Vaše povinnost: právo na opravu údajů a právo vznést námitku

Domnívá-li se fyzická osoba, že její osobní údaje nejsou správné, úplné nebo přesné, má právo na jejich neprodlenou opravu nebo doplnění.

Fyzická osoba může též kdykoli vznést námitku proti zpracování svých osobních údajů pro konkrétní účel, když je vaše společnost zpracovává na základě vašeho oprávněného zájmu nebo pro účely plnění úkolu ve veřejném zájmu. Nemáte-li oprávněný zájem, který převažuje nad zájmy fyzické osoby, musíte od zpracování osobních údajů upustit. Podobně může fyzická osoba požádat o omezení zpracování osobních údajů, zatímco je určováno, zda váš oprávněný zájem převažuje nad jejími zájmy či nikoli. Avšak v případě přímého marketingu jste na žádost fyzické osoby vždy povinni zpracování osobních údajů ukončit.

Upozornění na automatizované rozhodování a profilování

Fyzické osoby mají právo nebýt předmětem rozhodnutí založeného na automatizovaném zpracování. Existuje však několik výjimek z tohoto pravidla, například když fyzická osoba s automatizovaným rozhodnutím výslovně souhlasila. S výjimkou situace, kdy je automatizované rozhodování založeno na právním předpisu, musí vaše společnost:

- informovat fyzickou osobu o automatizovaném rozhodování,
- poskytnout fyzické osobě právo na přezkum automatizovaného rozhodnutí nějakým člověkem,
- poskytnout fyzické osobě příležitost k napadení automatizovaného rozhodnutí.

Pokud například banka automatizuje své rozhodnutí o tom, zda určité fyzické osobě poskytne půjčku či nikoli, měla by být tato osoba o automatizovaném rozhodnutí informována a měla by dostat příležitost toto rozhodnutí napadnout a požádat o lidský zásah.

Povinnosti založené na riziku

Kromě povinností zaměřených na ochranu práv fyzických osob obsahuje nařízení GDPR i řadu povinností, jejichž uplatňování závisí na riziku.

Vaše povinnost: jmenování pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů nese odpovědnost za monitorování toho, jak dodržujete nařízení GDPR. Jedním z jeho hlavních úkolů je informovat zaměstnance, kteří provádějí vlastní zpracování osobních údajů, o jejich povinnostech a radit jim. Pověřenec též spolupracuje s úřadem pro ochranu údajů a slouží jako kontaktní místo pro tento úřad a fyzické osoby.

Vaše společnost musí jmenovat pověřence pro ochranu osobních údajů, když:

- pravidelně a systematicky monitorujete fyzické osoby nebo zpracováváte zvláštní kategorie údajů,
- toto zpracování je hlavní činností vašeho podnikání a
- zpracováváte údaje ve velkém rozsahu.

Například pokud zpracováváte osobní údaje pro účely cílené reklamy pomocí vyhledávačů na základě chování lidí na internetu, pak nařízení GDPR vyžaduje, abyste měli pověřence pro ochranu osobních údajů. Pokud však svým klientům posíláte propagační materiály pouze jednou ročně, pověřence potřebovat nebudete. Podobně platí, že pokud jste lékař, který shromažďuje údaje o zdraví pacientů, pověřenec pravděpodobně nebude nutný. Ale pokud zpracováváte osobní údaje genetického a zdravotního charakteru pro nemocnici, bude pověřenec vyžadován.

Vaše povinnost: záměrná a standardní ochrana osobních údajů

Nařízení GDPR zavádí dvě nové zásady: záměrnou a standardní ochranu osobních údajů.

Záměrná ochrana osobních údajů pomáhá zajistit, aby společnost brala ochranu údajů v úvahu v raných stadiích plánování nového způsobu zpracování osobních údajů. V souladu s touto zásadu musí správce údajů podniknout všechny nezbytné technické a organizační kroky, aby zavedl zásady ochrany údajů a chránil práva fyzických osob. Tyto kroky by měly například zahrnovat využívání pseudonymizace.

Záměrná ochrana osobních údajů minimalizuje rizika pro soukromí a zvyšuje důvěru. Tím, že se ochrana údajů dostává do popředí vývoje nového zboží či služeb, lze se veškerých problémů při ochraně údajů vyvarovat již na samém začátku. Tato praxe též pomáhá zvyšovat povědomí o ochraně údajů napříč všemi odděleními a úrovněmi společnosti.

Součástí **standardní ochrany osobních údajů** je zajištění, že vaše společnost má jako standard co možná nejvstřícnější nastavení k ochraně soukromí. Například pokud jsou možná dvě nastavení ochrany soukromí a jedno z nich brání jiným osobám v přístupu k osobním údajům, mělo by být právě toto nastavení použito jako standardní.

„Záměrná ochrana osobních údajů minimalizuje rizika pro soukromí a zvyšuje důvěru.“

„Součástí standardní ochrany osobních údajů je zajištění, že vaše společnost má jako standard co možná nejvstřícnější nastavení k ochraně soukromí.“

Vaše povinnost: řádné oznámení v případě porušení zabezpečení osobních údajů

K porušení zabezpečení osobních údajů dochází, když jsou osobní údaje, za které odpovídáte, sděleny, náhodně nebo protiprávně, neoprávněným příjemcům nebo pokud jsou tyto osobní údaje dočasně nedostupné nebo jsou pozměněny.

Pro podnik je životně důležité zavést vhodná technická a organizační opatření, aby k porušení zabezpečení osobních údajů nedocházelo. Pokud k tomu však dojde a porušení představuje riziko pro práva a svobody dotčené fyzické osoby, měli byste do 72 hodin po zjištění tohoto porušení informovat svůj úřad pro ochranu údajů.

V závislosti na tom, zda porušení zabezpečení osobních údajů představuje vysoké riziko pro dotčené osoby, může být podnik povinen informovat všechny fyzické osoby, jichž se porušení zabezpečení osobních údajů dotklo.

Předávání osobních údajů mimo EU?

Nařízení GDPR se vztahuje na Evropský hospodářský prostor (EHP), kam patří všechny země EU, Island, Lichtenštejnsko a Norsko. Při předávání osobních údajů mimo EHP by měla ochrana, kterou poskytuje nařízení GDPR, cestovat společně s údaji. To znamená, že pro účely vývozu údajů do zahraničí musí společnosti zajistit, aby byla zavedena určitá bezpečnostní opatření.

Nařízení GDPR nabízí diverzifikovaný soubor mechanismů k předávání údajů do třetích zemí. Podle nařízení GDPR je takové předávání povoleno, když:

1. ochrana dané země je považována Evropskou unií za dostatečnou nebo
2. vaše společnost přijme nezbytná opatření pro poskytnutí vhodných bezpečnostních opatření, například zahrnutím specifických ustanovení do smlouvy, která byla uzavřena s mimoevropským dovozcem osobních údajů, nebo
3. vaše společnost se spoléhá na specifické důvody pro předávání (nazývané „výjimky“), například souhlas fyzické osoby.

Více informací o pravidlech týkajících se mezinárodního předávání údajů obsahuje sdělení Evropské komise Výměna a ochrana osobních údajů v globalizovaném světě: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017DC0007&from=CS

Musíte provést posouzení vlivu na ochranu osobních údajů?

Posouzení vlivu na ochranu osobních údajů je povinné vždy, když by zpracování představovalo vysoké riziko pro práva a svobody fyzických osob. K tomu může dojít například při používání nových technologií.

Podle nařízení GDPR nastává takové vysoké riziko, minimálně když:

- se mechanismy automatizovaného zpracování a profilování používají k systematickému a rozsáhlému hodnocení fyzických osob,
- veřejný prostor je systematicky velkokapacitně monitorován (např. kamerovým systémem),
- jsou ve velkém měřítku zpracovávány citlivé osobní údaje (např. zdravotní údaje).

Účelem posouzení vlivu na ochranu osobních údajů je určit potenciální rizika pro práva a svobody fyzických osob předtím, než začne zpracování osobních údajů a než se zhmotní riziko. Zmírněním rizika hned na začátku lze předejít škodám a minimalizovat náklady.

Pokud opatření uvedená v posouzení vlivu na ochranu osobních údajů neodstraní všechna identifikovaná vysoká rizika, je nutné před zamýšleným zpracováním údajů konzultovat úřad pro zpracování údajů.

„Posouzení vlivu na ochranu osobních údajů je povinné vždy, když by zpracování představovalo vysoké riziko pro práva a svobody fyzických osob.“

Co musíte udělat

Reakce na žádosti

Dostane-li vaše společnost žádost fyzické osoby, která chce uplatnit svá práva, měli byste na tuto žádost odpovědět bez zbytečného odkladu a v každém případě do jednoho měsíce od jejího přijetí. Tato lhůta na odpověď však může být u složitých nebo mnohočetných žádostí prodloužena o dva měsíce za předpokladu, že daná fyzická osoba je o prodloužení informována. Žádosti by měly být vyřizovány **bezplatně**. Je-li žádost zamítnuta, musíte danou fyzickou osobu informovat o důvodech a o jejím právu podat stížnost u úřadu pro ochranu údajů.

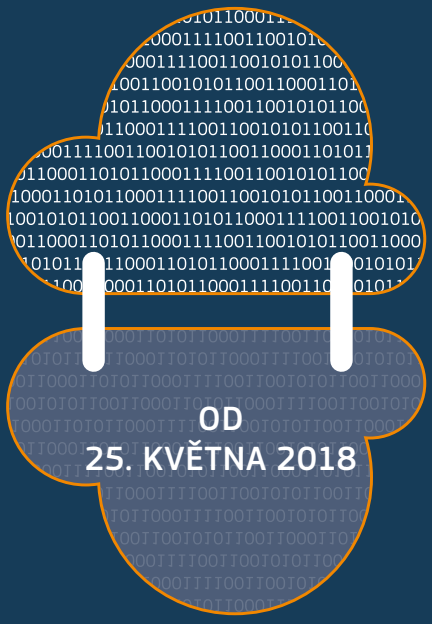
Prokazujte plnění předpisů a uchovávejte záznamy!

Jednou z klíčových zásad nařízení GDPR je zajistit, aby společnosti mohly prokázat, že nařízení dodržují. To znamená, že musíte být schopni doložit, že vaše společnost jedná v souladu s nařízením GDPR a plní všechny příslušné povinnosti – zejména na žádost nebo na základě kontroly ze strany úřadu pro ochranu údajů.

Jedním ze způsobů, jak to udělat, je vést podrobné záznamy o takových věcech, jako je:

- název a kontaktní údaje vašeho podniku zapojeného do zpracování údajů,
- důvod(y) pro zpracování osobních údajů,
- popis kategorií fyzických osob poskytujících osobní údaje,
- kategorie organizací, které osobní údaje dostávají,
- přenos osobních údajů do jiné země či organizace,
- doba uložení osobních údajů,
- popis bezpečnostních opatření uplatňovaných při zpracovávání osobních údajů.

Vaše společnost by měla navíc vést – a pravidelně aktualizovat – písemné postupy a směrnice a seznamovat s nimi vaše zaměstnance.



KAPITOLA 4

JSTE PŘIPRAVENI JE PLNIT?

Pokud jde o zpracování osobních údajů, stanovuje nařízení GDPR, že musíte konat vy. Prvním krokem je zmapovat vaše aktuální činnosti v oblasti zpracování údajů a přehodnotit vaše interní podnikové procesy. Zejména musíte:

- určit, které údaje máte a za jakým účelem a na jakém právním základě,
- posoudit všechny své smlouvy, zejména ty mezi správcem a zpracovateli údajů,
- zhodnotit všechny dostupné cesty mezinárodního předávání údajů a
- provést přezkum celkového řízení ve vaší společnosti (tj. jaká máte zavedena IT a organizační opatření), včetně toho, zda musíte nebo chcete jmenovat pověřence pro ochranu osobních údajů.

Zásadní součástí tohoto procesu je zajistit, aby vaše společnost uplatňovala při takových přezkumech nejvyšší úroveň řízení, které bude poskytovat vstupní údaje a bude pravidelně aktualizováno a konzultováno ohledně změn politiky v oblasti údajů.

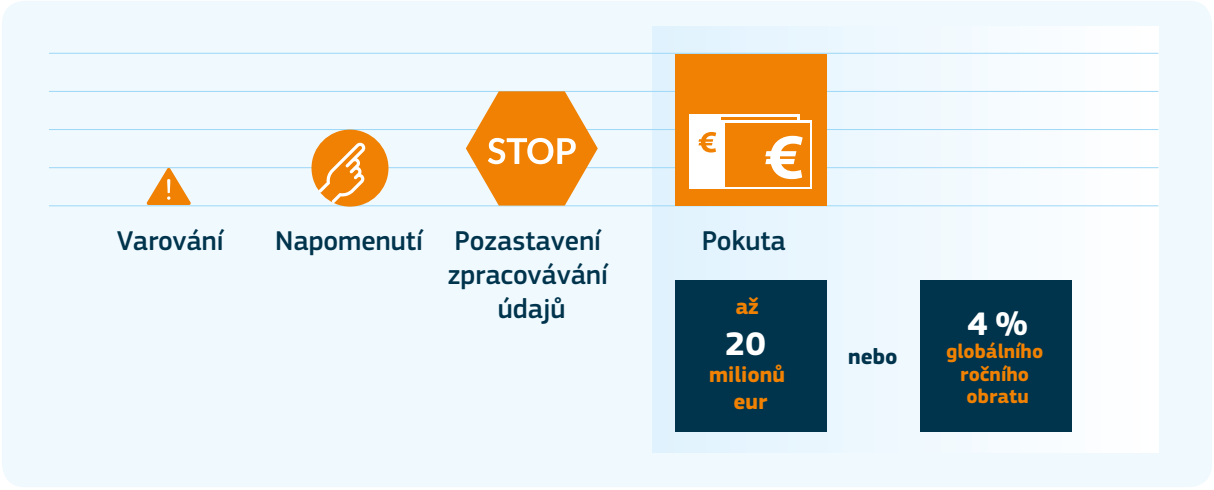
Zpracování údajů ve více než jedné zemi?

V případě přeshraničního zpracování údajů může být příslušným orgánem dozorový orgán v jiné zemi, a nikoli orgán pro ochranu údajů ve vaší zemi. Zpravidla se jedná o orgán pro ochranu údajů v zemi, kde má vaše společnost hlavní sídlo (kde jsou přijímána rozhodnutí o prostředcích a účelech zpracování) v EU.

Rizika v případě nedodržení pravidel

V důsledku nedodržování nařízení GDPR mohou být uloženy výrazné pokuty – za některá porušení až do výše 20 milionů EUR nebo 4 % celkového obratu vaší společnosti. Orgán pro ochranu údajů může uložit další opravná opatření, například může nařídit ukončení zpracování osobních údajů. Měli byste též vzít v úvahu poškození pověsti, které by nedodržování pravidel mohlo přinést.

Náklady spojené s nedodržením nařízení GDPR jsou očividně mnohem vyšší než jakékoli investice vynaložené na jeho plnění.



Máte otázky? Něco vás znepokojuje? Obraťte se prosím na svůj vnitrostátní orgán pro ochranu údajů.

Najděte si vnitrostátní úřad pro ochranu osobních údajů online.

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

DŮLEŽITÉ UPOZORNĚNÍ

Informace a pokyny v této brožuře mají přispět k lepšímu pochopení pravidel pro ochranu údajů v EU.

Mají sloužit čistě jako orientační nástroj – právní závaznost má pouze text obecného nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR). Proto pouze GDPR může fyzickým osobám uložit práva a povinnosti. Tyto pokyny nestanoví žádné vymahatelné právo ani očekávání.

Závazná interpretace právních předpisů EU je výlučnou pravomocí Soudního dvora Evropské unie. Názory vyjádřené v těchto pokynech nemají vliv na to, jaké postavení zaujme Komise před Soudním dvorem.

Evropská komise ani žádná osoba, která jedná jejím jménem, nenese odpovědnost za možné použití informací uvedených v této brožuře.

Tato brožura odráží aktuální stav v době jejího koncipování, je třeba na ni pohlížet jako na „živý dokument“, který lze vylepšovat a jehož obsah může být bez předchozího oznámení upraven.

Obraťte se na EU

Osobně

Po celé Evropské unii se nachází stovky informačních středisek Europe Direct.
Adresu nejbližšího střediska naleznete na internetové stránce: https://europa.eu/european-union/contact_cs.

Telefonicky nebo e-mailem

Europe Direct je služba, která odpoví na vaše dotazy o Evropské unii. Můžete se na ni obrátit:
– prostřednictvím bezplatné telefonní linky: 00 800 6 7 8 9 10 11 (někteří operátoři mohou tento hovor účtovat),
– na standardním telefonním čísle: +32 22999696 nebo
– e-mailem prostřednictvím internetové stránky: https://europa.eu/european-union/contact_cs.

Vyhledávání informací o EU

On-line

Informace o Evropské unii ve všech úředních jazycích EU jsou dostupné na internetových stránkách Europa na adrese: https://europa.eu/european-union/index_cs.

Publikace EU

Publikace EU, ať už bezplatné, nebo placené, si můžete stáhnout nebo objednat prostřednictvím internetových stránek EU Bookshop na adrese: https://publications.europa.eu/bookshop. Chcete-li obdržet více než jeden výtisk bezplatných publikací, obraťte se na službu Europe Direct nebo na místní informační střediska (viz https://europa.eu/european-union/contact_cs).

Právo EU a související dokumenty

Právní informace EU včetně všech právních předpisů EU od roku 1952 ve všech úředních jazykových verzích jsou dostupné na stránkách EUR-Lex na adrese: http://eur-lex.europa.eu.

Veřejně přístupná data od EU

Portál veřejně přístupných dat EU (http://data.europa.eu/euodp/cs) umožňuje přístup k datovým souborům z EU. Data lze bezplatně stahovat a opakovaně použít pro komerční i nekomerční účely.

DS-01-18-082-CS-C

Obecné nařízení o ochraně osobních údajů (GDPR) upravuje způsob, jakým podniky zpracovávají a spravují osobní údaje. Vzhledem k existenci jediného evropského právního předpisu pro ochranu osobních údajů musí teď vaše společnost dodržovat při nabízení zboží a služeb kdekoli v EU primárně jeden právní předpis o ochraně osobních údajů.

Zjednodušením regulačního prostředí pro podniky představuje nařízení GDPR novou příležitost pro váš podnik, jak zlepšit správu osobních údajů a následně zvýšit důvěru spotřebitelů ve váš podnik.

Tato brožura zdůrazňuje povinnosti, které váš podnik má podle nařízení GDPR.

europa.eu/dataprotection/cs

Úřad pro publikace

ISBN 978-92-79-79427-8