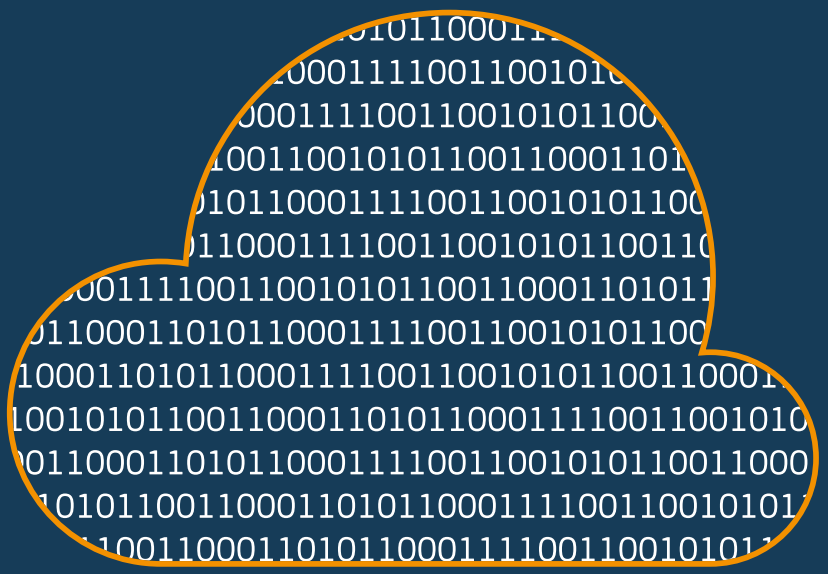
Európska komisia

GDPR: nové príležitosti, nové povinnosti



Čo musí každý podnik vedieť o všeobecnom nariadení EÚ o ochrane údajov

Spravodlivosť a spotrebitelia

Printed by Bietlot in Belgium

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2018

Print	ISBN 978-92-79-79448-3	doi:10.2838/444729	DS-01-18-082-SK-C
PDF	ISBN 978-92-79-79419-3	doi:10.2838/205905	DS-01-18-082-SK-N

OBSAH

1. KAPITOLA

PODNIKATEĽSKÉ PRÍLEŽITOSTI

Všeobecným nariadením o ochrane údajov (GDPR) sa reguluje spôsob, akým podniky spracúvajú a spravujú osobné údaje. Platí od 25. mája 2018 a vzťahuje sa na všetky podniky a organizácie (napr. nemocnice, orgány verejnej správy atď.). Predstavuje najväčšiu zmenu pravidiel EÚ v oblasti ochrany údajov za uplynulých 20 rokov.

GDPR udeľuje občanom väčšiu kontrolu nad tým, ako sa používajú ich osobné údaje, a zároveň výrazne zjednodušuje regulačné prostredie pre podniky. Dosahuje to zavedením jednotného rámca pre právne predpisy o ochrane údajov v celej EÚ. Inými slovami, namiesto toho, aby mala každá krajina vlastné právne predpisy o ochrane údajov, sa teraz celá EÚ riadi jedným nariadením. Spoločnosť, ktorá pôsobí vo viacerých krajinách, teda viac nemusí dodržiavať množstvo predpisov, ktoré sa často rôznia. Stačí, aby dodržiavala GDPR, a môže ponúkať svoje služby kdekoľvek v EÚ.

Aký prínos môže mať GDPR pre vašu spoločnosť

- **Jedna Únia, jedno právo:** vďaka jednému súboru pravidiel je pre spoločnosti jednoduchšie a lacnejšie podnikať v EÚ.
- **Jednotné kontaktné miesto:** vo väčšine prípadov spoločnosti musia komunikovať len s jedným úradom na ochranu údajov (DPA).
- **Európske pravidlá na európskej pôde:** spoločnosti so sídlom mimo EÚ musia uplatňovať rovnaké pravidlá ako európske spoločnosti, keď ponúkajú svoj tovar alebo služby jednotlivcom v EÚ.
- **Prístup založený na riziku:** GDPR predchádza ťažkopádnej univerzálnej povinnosti a namiesto toho prispôsobuje povinnosti príslušným rizikám.
- **Pravidlá priaznivé pre inováciu:** GDPR je technologicky neutrálne.

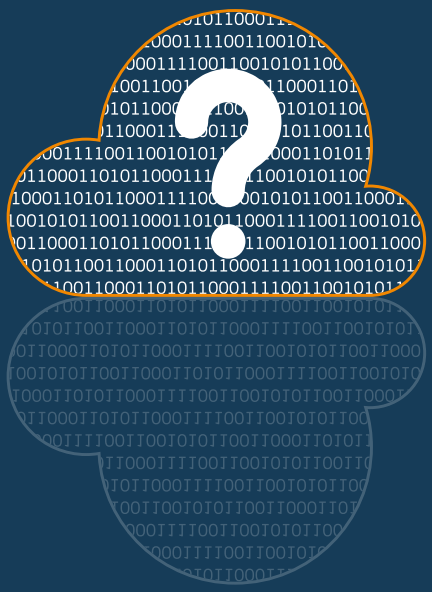
Všetko je to o dôvere

Ochrana osobných údajov je pre jednotlivcov zdrojom veľkých obáv. Preto majú aj naďalej malú dôveru voči digitálnym prostrediam. Podľa prieskumu Eurobarometra:

- osem z desiatich osôb sa domnieva, že nemá úplnú kontrolu nad svojimi osobnými údajmi;
- šesť z desiatich osôb uvádza, že nedôveruje online podnikom;
- viac ako 90 % Európanov uvádza, že si želá rovnaké práva ochrany údajov vo všetkých krajinách EÚ.

GDPR predstavuje novú príležitosť pre podniky na zlepšenie dôvery spotrebiteľov prostredníctvom správy osobných údajov založenej na riziku.

„Podnikom, ktoré nebudú primerane chrániť osobné údaje jednotlivcov, hrozí, že prídu o dôveru spotrebiteľov, ktorá je zásadná pre povzbudzovanie ľudí, aby používali nové výrobky a služby.“



2. KAPITOLA

AKO CHÁPAŤ GDPR

Uplatňuje sa na mňa GDPR?

GDPR sa uplatňuje na ***všetky*** podniky, ktoré:

spracúvajú osobné údaje prostredníctvom **automatizovaného** alebo **manuálneho** spracúvania (pokiaľ sú údaje zorganizované podľa kritérií).

Tieto pravidlá musíte dodržiavať dokonca aj v prípade, že váš podnik spracúva údaje len v mene iných spoločností.

GDPR sa uplatňuje, ak:

- vaša spoločnosť spracúva osobné údaje a má sídlo v EÚ, bez ohľadu na to, kde dochádza k samotnému spracúvaniu údajov; alebo
- je vaša spoločnosť zriadená mimo EÚ, ale ponúka tovar či služby alebo monitoruje správanie jednotlivcov v rámci EÚ.

Čo sú osobné údaje?

Osobné údaje sú všetky informácie, ktoré sa týkajú identifikovanej alebo identifikovateľnej živej osoby. Ich súčasťou môže byť:

- meno;
- adresa a telefónne číslo;
- miesto;
- zdravotné záznamy;
- príjem a bankové údaje;
- kultúrne preferencie
- ...a ďalšie údaje.

Osobné údaje, ktoré boli odidentifikované alebo pseudonymizované, ale možno ich naďalej použiť na opätovnú identifikáciu osoby, takisto patria do rozsahu pôsobnosti GDPR. Osobné údaje, ktoré boli nezvratne anonymizované takým spôsobom, že jednotlivec už nie je identifikovateľný, sa nepovažujú za osobné údaje, a teda sa neriadia GDPR.

GDPR je zároveň technologicky neutrálne, čiže chráni osobné údaje bez ohľadu na použitú technológiu alebo spôsob uchovávania osobných údajov. Či už váš podnik spracúva a uchováva osobné údaje pomocou komplexného systému IT alebo v papierových súboroch, budete sa riadiť GDPR.

„Či už váš podnik spracúva a uchováva osobné údaje pomocou komplexného systému IT alebo v papierových súboroch, budete sa riadiť GDPR.“

S osobitnými (citlivými) kategóriami osobných údajov zaobchádzajte mimoriadne opatrne

Ak osobné údaje, ktoré zbierate, zahŕňajú informácie o jednotlivcovi, ktoré sa týkajú jeho zdravia, rasového pôvodu, sexuálnej orientácie, náboženstva, politického presvedčenia alebo členstva v odboroch, považujú sa za citlivé. Vaša spoločnosť môže spracúvať tieto údaje len za konkrétnych podmienok a možno budete musieť zaviesť dodatočné ochranné opatrenia, ako je šifrovanie.

Čo predstavuje spracúvanie osobných údajov?

Podľa GDPR patria do definície spracúvania osobných údajov úkony, ako sú zber, používanie a vymazanie osobných údajov.

Monitorujete svoje priestory cez kamerový systém? Konzultujete na podnikateľské účely databázu, ktorá obsahuje osobné údaje? Posielate propagačné e-mailové správy? Vymazávate (digitálne) súbory o zamestnancoch alebo skartujete dokumenty? Prípadne publikujete fotografiu osoby na vašej webovej lokalite alebo kanáloch sociálnych médií?

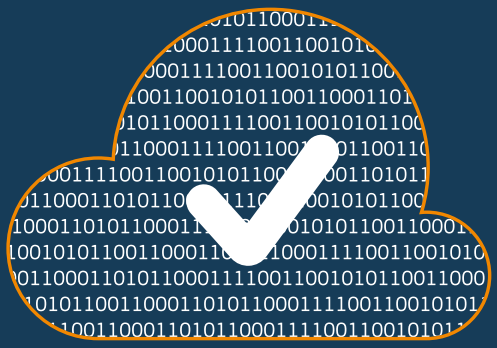
Ak ste odpovedali „áno“ na ktorúkoľvek z týchto otázok, potom vaša spoločnosť rozhodne spracúva osobné údaje.

Ako GDPR pomáha znižovať náklady?

GDPR prihliada na potreby podnikov. Napríklad, cieľom nariadenia je odstrániť administratívne požiadavky, aby sa znížili náklady a čo najviac sa zmenšila administratívna záťaž:

- **Ruší sa predchádzajúce oznamovanie**: reformou sa ruší väčšina predchádzajúcich oznamovaní orgánom dohľadu spolu s ich súvisiacimi nákladmi.
- **Úradníci pre ochranu údajov:** spoločnosti musia vymenovať DPO hlavne vtedy, keď ich hlavné činnosti zahŕňajú spracúvanie citlivých údajov vo veľkom rozsahu alebo keď zahŕňajú rozsiahle, pravidelné a systematické monitorovanie jednotlivcov. Orgány verejnej správy sú povinné vymenovať DPO.
- **Posúdenia vplyvu na ochranu údajov**: spoločnosti sú povinné vykonávať posúdenia vplyvu na ochranu údajov len vtedy, keď navrhovaná činnosť spracovania údajov zahŕňa veľké riziko pre práva a slobody jednotlivcov.
- **Vedenie záznamov**: spoločnosti s menej ako 250 zamestnancami nemusia viesť záznamy, pokiaľ je spracúvanie údajov príležitostné alebo nezahŕňa citlivé údaje.

„Cieľom nariadenia je odstrániť administratívne požiadavky, aby sa znížili náklady a čo najviac sa zmenšila administratívna záťaž.“



3. KAPITOLA

VAŠE POVINNOSTI PODĽA GDPR

GDPR ukladá priame povinnosti pri spracúvaní údajov spoločnostiam na úrovni celej EÚ. Podľa GDPR spoločnosť môže spracúvať osobné údaje len za určitých podmienok. Napríklad, spracúvanie by malo byť spravodlivé a transparentné, na konkrétny a legitímny účel a obmedzovať sa na údaje potrebné na naplnenie daného účelu. Musí sa tiež zakladať na niektorom z uvedených právnych dôvodov.

- **Súhlas** dotknutého jednotlivca.
- **Zmluvný záväzok** medzi vami a jednotlivcom.
- Na splnenie **právneho záväzku**.
- Na ochranu **životne dôležitých záujmov** jednotlivca.
- Na vykonávanie **úlohy**, **ktorá je vo verejnom záujme**.
- V rámci **oprávnených záujmov** vašej spoločnosti, ale len ak najskôr overíte, či nie sú závažne ovplyvnené základné práva a slobody jednotlivca, ktorého údaje sa spracúvajú. Ak záujmy danej osoby prevažujú vaše záujmy, nemôžete údaje spracúvať.

Pod lupou: ako získať súhlas s používaním osobných údajov

GDPR uplatňuje prísne pravidlá spracúvania údajov na základe súhlasu. Cieľom týchto pravidiel je zabezpečiť, aby jednotlivec rozumel, s čím súhlasí. Znamená to, že súhlas by mal byť **poskytnutý slobodne, konkrétny, podložený** a **jednoznačný** a získaný na základe žiadosti predloženej v jasnom a jednoduchom jazyku. Súhlas by mal navyše byť poskytnutý **pozitívnym úkonom**, ako je zaškrtnutie políčka online alebo podpísanie formulára.

Ak spracúvate osobné údaje týkajúce sa **dieťaťa** na základe súhlasu, vyžaduje sa súhlas rodiča. Keďže veková hranica v jednotlivých krajinách sa rôzni od 13 do 16 rokov, odporúčame vám konzultovať vnútroštátne právne predpisy.

Pripomienka! Keď niekto súhlasí so spracúvaním osobných údajov, môžete spracúvať údaje iba na účely, na ktoré bol poskytnutý súhlas. Okrem toho mu musíte dať možnosť zrušiť súhlas.

Určite, akú máte úlohu a zodpovednosť

Keď určíte, že GDPR sa uplatňuje na váš podnik a že dochádza k spracúvaniu osobných údajov, ďalším krokom je určiť, akú máte úlohu.

V pravidlách ochrany údajov sa rozlišuje medzi prevádzkovateľom údajov a spracovateľom údajov, pričom na každého z nich sa vzťahujú iné povinnosti. Zatiaľ čo prevádzkovateľ určuje účel a prostriedky spracúvania osobných údajov, spracovateľ iba spracúva osobné údaje v mene prevádzkovateľa. Neznamená to však, že spracovateľ údajov sa môže jednoducho skrývať za prevádzkovateľom.

V GDPR sa vyžaduje, aby prevádzkovateľ najal len takého spracovateľa údajov, ktorý ponúka dostatočné záruky. Tieto záruky by mali byť zahrnuté do písomnej zmluvy medzi prevádzkovateľom a spracovateľom. Zmluva musí tiež obsahovať niekoľko povinných doložiek, napr. doložku, v ktorej sa ustanovuje, že spracovateľ bude spracúvať osobné údaje len podľa zdokumentovaných pokynov prevádzkovateľa.

Povinnosti na ochranu práv jednotlivca

GDPR zahŕňa niekoľko povinností, ktorých cieľom je chrániť právo jednotlivca na kontrolu nad jeho osobnými údajmi.

Vaša povinnosť: poskytovať transparentné informácie

Spoločnosti musia poskytovať jednotlivcom informácie o tom, kto spracúva čo a prečo. V týchto informáciách sa musí jasne uvádzať najmenej:

- kto ste;
- prečo spracúvate údaje;
- aký je právny základ;
- kto získa údaje (ak sa to uplatňuje).

V niektorých prípadoch sa v informáciách musia tiež uvádzať:

- kontaktné údaje úradníka pre ochranu údajov; oprávnený záujem (keď je oprávnený záujem právnym základom spracúvania);
- základ prenosu údajov do krajiny mimo EÚ;
- ako dlho sa údaje budú uchovávať;
- práva jednotlivca týkajúce sa ochrany údajov (t. j. právo na prístup, opravu, vymazanie, obmedzenie, námietku, prenosnosť atď.);
- ako môže byť súhlas zrušený (keď je súhlas právnym základom spracúvania);
- či existuje zákonná alebo zmluvná povinnosť na poskytovanie údajov;
- v prípade automatizovaného rozhodovania, informácie o logike, význame a dôsledkoch rozhodnutia.

„Spoločnosti musia poskytovať jednotlivcom informácie o tom, kto spracúva čo a prečo.“

Vaša povinnosť: právo na prístup a právo na prenosnosť údajov

Jednotlivci majú právo požiadať o bezplatný prístup k svojim osobným údajom v prístupnom formáte. Ak dostanete takúto žiadosť, musíte:

- povedať jednotlivcovi, prečo spracúvate jeho osobné údaje;
- informovať ho o spracúvaní (napr. o účeloch spracúvania, kategóriách dotknutých osobných údajov, príjemcoch ich údajov atď.);
- poskytnúť kópiu osobných údajov, ktoré sa spracúvajú.

Keď je spracúvanie založené na súhlase alebo zmluve, jednotlivec okrem toho môže požiadať, aby mu boli jeho osobné údaje vrátené alebo prevedené inej spoločnosti. Nazýva sa to právo na prenosnosť údajov. Údaje by sa mali poskytnúť v bežne používanom a strojovo čitateľnom formáte.

Napriek tomu, že tieto dve práva úzko súvisia, ide o dve rozdielne práva. Preto sa musíte ubezpečiť, že tieto dve práva sa nezamieňajú a príslušne informovať jednotlivca.

Vaša povinnosť: právo na vymazanie (právo byť zabudnutý)

Za určitých okolností jednotlivec môže požiadať prevádzkovateľa, aby vymazal jeho osobné údaje, napr. keď údaje viac nie sú potrebné na naplnenie účelu spracúvania. Vaša spoločnosť však nie je povinná vyhovieť žiadosti jednotlivca, ak:

- je spracúvanie nutné na dodržiavanie slobody prejavu a informácií;
- musíte uchovávať osobné údaje, aby ste si splnili zákonnú povinnosť;
- existujú iné dôvody vo verejnom záujme na uchovávanie týchto osobných údajov, ako je verejné zdravie alebo vedecké účely či účely historického výskumu;
- musíte uchovávať osobné údaje na preukázanie právneho nároku.

Vaša povinnosť: právo na opravu a právo namietať

Ak sa jednotlivec domnieva, že jeho osobné údaje sú nesprávne, neúplné alebo nepresné, má právo opraviť ich alebo doplniť bez zbytočného odkladu.

Jednotlivec tiež môže kedykoľvek namietať proti spracúvaniu svojich osobných údajov na konkrétne použitie, keď ich vaša spoločnosť spracúva na základe vášho oprávneného záujmu alebo na výkon úlohy vo verejnom záujme. Pokiaľ nemáte oprávnený záujem, ktorý prevažuje záujem jednotlivca, musíte prestať spracúvať dané osobné údaje. Jednotlivec môže podobne požiadať, aby bolo spracúvanie jeho osobných údajov obmedzené, pričom sa musí určiť, či váš oprávnený záujem prevažuje alebo neprevažuje jeho záujem. V prípade priameho marketingu ste však vždy povinní prestať spracúvať osobné údaje na žiadosť jednotlivca.

Upozornenie o automatizovanom rozhodovaní a profilovaní

Jednotlivci majú právo nepodliehať rozhodnutiu, ktoré je založené výlučne na automatizovanom spracúvaní. Sú však určité výnimky z tohto pravidla, napr. keď jednotlivec výslovne súhlasil s automatizovaným rozhodovaním. Okrem prípadov, keď je automatizované rozhodnutie založené na právnom predpise, vaša spoločnosť musí:

- informovať jednotlivca o automatizovanom rozhodovaní;
- priznať jednotlivcovi právo na preskúmanie automatizovaného rozhodnutia človekom;
- umožniť jednotlivcovi napadnúť automatizované rozhodnutie.

Napríklad ak banka automatizuje svoje rozhodnutie o tom, či určitému jednotlivcovi udelí alebo neudelí úver, daný jednotlivec by mal byť informovaný o automatizovanom rozhodnutí a malo by mu byť umožnené napadnúť rozhodnutie a žiadať ľudský zásah.

Povinnosti založené na riziku

GDPR obsahuje okrem povinností zameraných na ochranu práv jednotlivca aj niekoľko povinností, ktorých uplatňovanie závisí od rizika.

Vaša povinnosť: vymenovať úradníka pre ochranu údajov (DPO)

DPO je zodpovedný za monitorovanie vášho súladu s GDPR. Jednou z hlavných úloh DPO je informovať zamestnancov a radiť zamestnancom, ktorí vykonávajú samotné spracúvanie osobných údajov, o ich povinnostiach. DPO tiež spolupracuje s úradom na ochranu údajov (DPA), pričom slúži ako kontaktné miesto medzi DPA a jednotlivcami.

Vaša spoločnosť má povinnosť vymenovať DPO, keď:

- pravidelne alebo systematicky monitorujete jednotlivcov alebo spracúvate osobitné kategórie údajov;
- spracúvanie predstavuje hlavnú podnikateľskú činnosť; a
- robíte to vo veľkom rozsahu.

Napríklad ak spracúvate osobné údaje s cieľom zameriavať reklamu prostredníctvom vyhľadávačov na základe online správania ľudí, v tom prípade sa v GDPR vyžaduje, aby ste mali DPO. Ak však svojim klientom posielate propagačné materiály len raz ročne, nebudete potrebovať DPO. Podobne, ak ste lekár, ktorý zbiera údaje o zdraví pacientov, pravdepodobne nebudete potrebovať DPO. Ak však spracúvate osobné údaje o genetike a zdraví pre nemocnicu, v tom prípade sa DPO vyžaduje.

Vaša povinnosť: špecificky navrhnutá a štandardná ochrana údajov

V GDPR sa zavádzajú dve nové zásady – špecificky navrhnutá a štandardná ochrana údajov.

Špecificky navrhnutá ochrana údajov pomáha zabezpečiť, aby spoločnosť zohľadňovala ochranu údajov v skorých fázach plánovania nového spôsobu spracúvania osobných údajov. Podľa tejto zásady musí prevádzkovateľ vykonať všetky potrebné technické a organizačné kroky, aby sa uplatňovali zásady ochrany údajov a chránili sa práva jednotlivcov. Tieto kroky môžu zahŕňať napríklad použitie pseudonymizácie.

Špecificky navrhnutou ochranou údajov sa zmenšujú riziká narušenia súkromia a zvyšuje sa dôvera. Ak sa ochrana údajov posunie do popredia pri vývoji nového tovaru alebo služieb, je možné predchádzať už v skorej fáze akýmkoľvek možným problémom v oblasti ochrany údajov. Navyše tento postup pomáha zvyšovať povedomie o ochrane údajov vo všetkých oddeleniach a na všetkých úrovniach spoločnosti.

Štandardná ochrana údajov znamená, že musíte zabezpečiť, aby štandardné nastavenie vo vašej spoločnosti bolo vždy prostredie, ktoré je čo najpriaznivejšie naklonené ochrane súkromia. Napríklad ak sú možné dve nastavenia ochrany súkromia a v jednom z týchto nastavení sa predchádza prístupu k osobným údajom inými osobami, toto nastavenie by malo byť použité ako štandardné nastavenie.

„Špecificky navrhnutou ochranou údajov sa zmenšujú riziká narušenia súkromia a zvyšuje sa dôvera.“

„Štandardná ochrana údajov znamená, že musíte zabezpečiť, aby štandardné nastavenie vo vašej spoločnosti bolo vždy prostredie, ktoré je čo najpriaznivejšie naklonené ochrane súkromia.“

Vaša povinnosť: poskytnúť vhodné oznámenie v prípade porušenia ochrany údajov

K porušeniu ochrany údajov dochádza vtedy, keď osobné údaje, za ktoré ste zodpovední, sú zverejnené buď náhodne alebo nezákonne neoprávneným príjemcom alebo sú dočasne nedostupné alebo pozmenené.

Pre podniky je zásadne dôležité, aby boli zavedené primerané technické a organizačné opatrenia s cieľom vyhnúť sa porušeniu ochrany údajov. Ak však dôjde k porušeniu ochrany údajov a toto porušenie predstavuje ohrozenie práv a slobôd jednotlivca, mali by ste to oznámiť úradu na ochranu údajov do 72 hodín odvtedy, ako ste sa dozvedeli o porušení.

V závislosti od toho, či porušenie ochrany údajov predstavuje alebo nepredstavuje *veľké* riziko pre zasiahnuté osoby, podnik môže byť tiež povinný informovať všetkých jednotlivcov, ktorých zasiahlo porušenie ochrany údajov.

Prenášate osobné údaje mimo EÚ?

GDPR sa uplatňuje na Európsky hospodársky priestor (EHP), do ktorého patria všetky krajiny EÚ plus Island, Lichtenštajnsko a Nórsko. Keď sa osobné údaje prenášajú mimo EHP, ochrana zabezpečená GDPR by mala cestovať spolu s údajmi. Znamená to, že pri vývoze údajov do zahraničia musia spoločnosti zabezpečiť, aby boli zavedené určité ochranné opatrenia.

GDPR ponúka rozmanitý súbor mechanizmov na prenos údajov do tretích krajín. Podľa GDPR sú takéto prenosy povolené, keď:

1. EÚ považuje ochranné opatrenia krajiny za vhodné; alebo
2. vaša spoločnosť napríklad prijme potrebné opatrenia na zabezpečenie primeraných ochranných opatrení, ako je zahrnutie osobitných doložiek do zmluvy uzatvorenej s mimoeurópskym dovozcom osobných údajov; alebo
3. vaša spoločnosť sa napríklad opiera o osobitný základ na prenos (tzv. výnimky), ako je súhlas jednotlivca.

Ďalšie informácie o pravidlách, ktoré sa uplatňujú na medzinárodný prenos údajov, nájdete v oznámení Európskej komisie o výmene a ochrane osobných údajov v globalizovanom svete: http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52017DC0007&from=SK

Kedy musíte vykonať posúdenie vplyvu na ochranu údajov (DPIA)?

Vykonanie posúdenia vplyvu je povinné vždy, keby plánované spracúvanie predstavovalo veľké riziko pre práva a slobody jednotlivcov. Môže to byť napríklad v prípade, keď sa používajú nové technológie.

Podľa GDPR sa vyskytuje najmenej také veľké riziko, keď:

- sú použité mechanizmy automatizovaného spracúvania a profilovania na systematické a rozsiahle hodnotenie jednotlivcov;
- sa veľkom rozsahu systematicky monitoruje verejne dostupné priestranstvo (napr. kamerový systém);
- sa vo veľkom rozsahu spracúvajú citlivé údaje (napr. zdravotné údaje).

Cieľom DPIA je identifikovať možné riziká pre práva a slobody jednotlivcov pred tým, ako sa začne spracúvanie osobných údajov a pred vznikom rizika. Ak sa riziko zmierni vopred, možno zabrániť škodám a znížiť náklady.

Ak sa opatreniami uvedenými v DPIA neodstránia všetky identifikované veľké riziká, musí sa to konzultovať s DPA pred vykonávaním spracúvania údajov.

„Vykonanie posúdenia vplyvu je povinné vždy, keby plánované spracúvanie predstavovalo veľké riziko pre práva a slobody jednotlivcov.“

Čo musíte robiť

Odpovedať na žiadosti

Ak je vašej spoločnosti doručená žiadosť jednotlivca, ktorý si želá uplatniť svoje práva, mali by ste odpovedať na túto žiadosť bez zbytočného odkladu a v každom prípade do jedného mesiaca od doručenia žiadosti. Tento čas odozvy sa však môže predĺžiť o dva mesiace v prípade komplexných alebo viacnásobných žiadostí, pokiaľ bol jednotlivec informovaný o predĺžení. Okrem toho by sa žiadosti mali vybavovať **bezplatne**. Ak je žiadosť zamietnutá, musíte jednotlivca informovať o dôvodoch zamietnutia a o tom, že má právo predložiť sťažnosť na úrade na ochranu údajov.

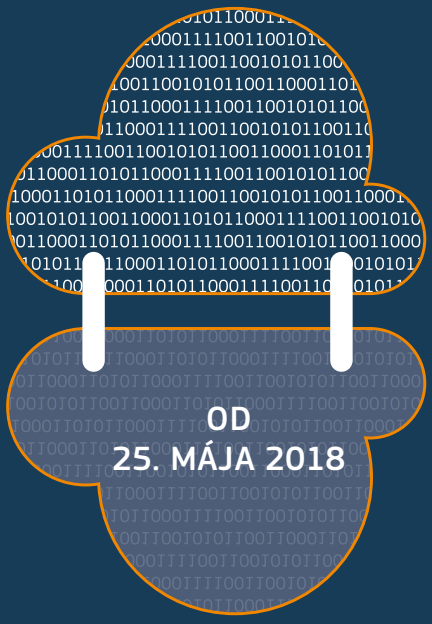
Preukazovať súlad s predpismi a viesť záznamy!

Jednou z hlavných zásad, na ktorých stojí GDPR je zabezpečiť, aby spoločnosti vedeli preukázať súlad s predpismi. Znamená to, že musíte byť schopní dosvedčiť, že vaša spoločnosť koná v súlade s GDPR a plní si všetky platné povinnosti, a to najmä na žiadosť alebo pri inšpekcii DPA.

Jeden zo spôsobov, ako to uskutočniť, je viesť podrobné záznamy o týchto záležitostiach:

- názov a kontaktné údaje vášho podniku, ktorý sa venuje spracúvaniu údajov;
- dôvod(-y) spracúvania osobných údajov;
- opis kategórií jednotlivcov, ktorí poskytujú osobné údaje;
- kategórie organizácií, ktoré dostávajú osobné údaje;
- prenos osobných údajov do inej krajiny alebo organizácie;
- doba uchovávania osobných údajov;
- opis bezpečnostných opatrení použitých pri spracovaní osobných údajov.

Okrem toho by vaša spoločnosť mala viesť a pravidelne aktualizovať aj písomné postupy a usmernenia a predstavovať ich vašim zamestnancom.



4. KAPITOLA

STE PRIPRAVENÍ NA DODRŽIAVANIE PREDPISOV?

V otázke spracúvania osobných údajov vám GDPR dáva do rúk opraty. Prvým krokom je zmapovať vaše aktuálne činnosti spracúvania údajov a prehodnotiť vaše vnútropodnikové postupy. Predovšetkým musíte:

- identifikovať, aké údaje uchovávate, a na aký účel a na akom právnom základe ich uchovávate;
- posúdiť všetky platné zmluvy, a najmä zmluvy medzi prevádzkovateľmi a spracovateľmi;
- zhodnotiť všetky dostupné metódy medzinárodných prenosov; a
- preskúmať celkovú správu vo vašej spoločnosti (t. j. aké IT a organizačné opatrenia máte zavedené) vrátane toho, či musíte alebo nemusíte vymenovať úradníka pre ochranu údajov.

Zásadným prvkom tohto postupu je zabezpečiť, aby najvyššia úroveň vedenia vašej spoločnosti bola zapojená do týchto preskúmaní, poskytovala podnety a pravidelne dostávala aktuálne informácie a bola konzultovaná o zmenách politiky ochrany údajov.

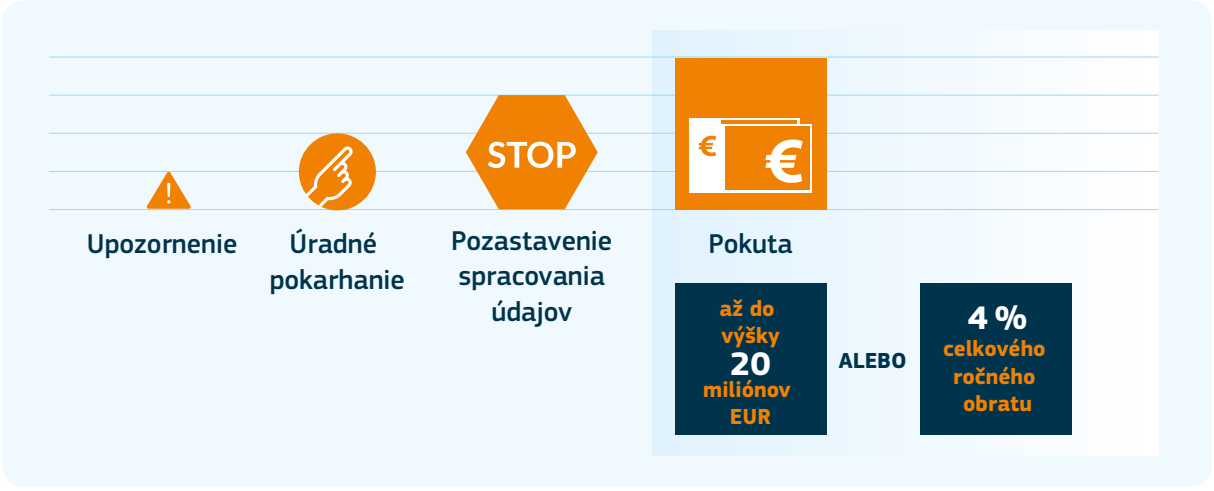
Spracúvate údaje vo viac ako jednej krajine?

V prípade cezhraničného spracúvania môže byť príslušným úradom dozorný úrad inej krajiny, a nie váš vnútroštátny DPA. Zvyčajne ide o DPA v krajine, ktorá je hostiteľkou hlavného sídla vašej spoločnosti (kde sa prijímajú rozhodnutia o prostriedkoch a účeloch spracúvania) v rámci EÚ.

Riziká nedodržiavania predpisov

Nedodržiavanie GDPR môže viesť k veľkým pokutám – až do výšky 20 miliónov EUR alebo 4 % celosvetového obratu vašej spoločnosti v prípade niektorých porušení. DPA môže uvaliť dodatočné nápravné opatrenia, ako je nariadenie ukončenia spracúvania osobných údajov. Takisto by ste mali pamätať na poškodenie dobrého mena, ktoré môže spôsobiť nedodržiavanie predpisov.

Náklady na nedodržiavanie GDPR sú jednoznačne oveľa väčšie ako akékoľvek investície vynaložené na zabezpečenie súladu s nariadením.



Máte otázky? Máte obavy? Obráťte sa na svoj vnútroštátny úrad na ochranu údajov.

Nájdite svoj úrad na ochranu údajov online

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

DÔLEŽITÉ OZNÁMENIE

Informácie a usmernenia v tejto brožúre majú prispieť k lepšiemu pochopeniu pravidiel EÚ o ochrane údajov.

Slúžia len ako usmerňujúci nástroj – iba znenie všeobecného nariadenia o ochrane údajov (GDPR) má právnu váhu. Znamená to, že iba nariadenie o ochrane údajov môže vytvárať práva a povinnosti jednotlivcov. Tieto usmernenia nevytvárajú žiadne vymožiteľné právo ani očakávanie.

Záväzný výklad právnych predpisov EÚ je vo výlučnej právomoci Súdneho dvora Európskej únie. Názormi vyjadrenými v týchto usmerneniach nie je dotknuté stanovisko, ktoré môže prijať Komisia pred Súdnym dvorom.

Európska komisia ani žiadna osoba konajúca v mene Európskej komisie nenesie zodpovednosť za možné použitie informácií v tejto brožúre.

Táto brožúra odráža stav vecí v čase jej zostavovania a mala by sa považovať za „živý dokument“, ktorý je otvorený pre zlepšenie, a jej obsah môže podliehať zmene bez oznámenia.

Obráťte sa na EÚ

Osobne

V rámci celej EÚ existujú stovky informačných centier Europe Direct. Adresu centra najbližšieho k vám nájdete na tejto webovej stránke: https://europa.eu/european-union/contact_sk

Telefonicky alebo e-mailom

Europe Direct je služba, ktorá odpovedá na vaše otázky o Európskej únii. Túto službu môžete kontaktovať:
– prostredníctvom bezplatného telefónneho čísla: 00 800 6 7 8 9 10 11 (niektorí operátori môžu tieto hovory spoplatňovať),
– prostredníctvom štandardného telefónneho čísla: +32 22999696, alebo
– e-mailom na tejto webovej stránke: https://europa.eu/european-union/contact_sk

Vyhľadávanie informácií o EÚ

Online

Informácie o Európskej únii sú dostupné vo všetkých úradných jazykoch Európskej únie na webovej stránke Europa: https://europa.eu/european-union/index_sk

Publikácie EÚ

Publikácie EÚ, bezplatné alebo platené, si môžete stiahnuť alebo objednať z kníhkupectva EU Bookshop na webovej stránke: https://publications.europa.eu/bookshop. Ak chcete získať viac než jeden výtlačok bezplatných publikácií, obráťte sa na službu Europe Direct alebo vaše miestne informačné centrum (pozri https://europa.eu/european-union/contact_sk).

Právo EÚ a súvisiace dokumenty

Prístup k právnym informáciám EÚ vrátane všetkých právnych predpisov EÚ od roku 1952 vo všetkých úradných jazykoch nájdete na webovej stránke EUR-Lex: http://eur-lex.europa.eu

Otvorený prístup k údajom z EÚ

Portál otvorených dát EÚ (http://data.europa.eu/euodp/sk) poskytuje prístup k súborom dát z EÚ. Dáta možno stiahnuť a opätovne použiť bezplatne na komerčné aj nekomerčné účely.

DS-01-18-082-SK-C

Všeobecným nariadením o ochrane údajov (GDPR) sa reguluje spôsob, akým podniky spracúvajú a spravujú osobné údaje. Vďaka jednotnému európskemu právnemu predpisu o ochrane osobných údajov musí odteraz vaša spoločnosť dodržiavať prevažne jeden právny predpis o ochrane údajov, pričom môže poskytovať tovar a služby kdekoľvek v EÚ.

Zjednodušením regulačného prostredia pre podniky GDPR prináša podnikom novú príležitosť na zlepšenie správy osobných údajov a následné zvýšenie dôvery spotrebiteľov v podnik.

Táto brožúra poukazuje na povinnosti vašej spoločnosti podľa GDPR.

europa.eu/dataprotection/sk

Úrad pre publikácie

ISBN 978-92-79-79448-3