CESTA K DODRŽIAVANIU GDPR

(GDPR - VŠEOBECNÉ NARIADENIE O OCHRANE ÚDAJOV)

Pracovný dokument 1/2017

Pracovná skupina združenia IAB Europe pre implementáciu všeobecného nariadenia o ochrane údajov

22 Máj 2017

O združení IAB Europe

IAB Europe je popredným európskym združením v oblasti digitálneho podnikania. Jeho poslaním je presadzovať rozvoj európskeho reklamného ekosystému vytváraním regulačného prostredia, investovaním do výskumu a vzdelávania, prípravou a zavádzaním štandardov v digitálnej ekonomike.

O skupine pre implementáciu všeobecného nariadenia o ochrane údajov (GDPR)

Pracovná skupina združenia IAB Europe pre implementáciu všeobecného nariadenia o ochrane údajov (GDPR) spája popredných expertov z celého odvetvia digitálnej reklamy. Jej cieľom je prediskutovať nový právny predpis Európskej únie o ochrane údajov, zdieľať navzájom najnovšie postupy a poznatky a dohodnúť sa na spoločnom postoji digital odvetvia k najdôležitejším otázkam vyplývajúcich z nariadenia, ktoré sa týkajú sektora digitálnej reklamy. Pracovná skupina je fórum založené na členskej báze, ktoré prispieva dôležitou mierou ku spoločnému úsiliu o dodržiavanie GDPR nariadenia zo strany digitálneho odvetvia, čo je možné len vďaka spolupráci všetkých jej členov.

Poďakovanie

Úvodný dokument o všeobecnom nariadení o ochrane údajov pripravili členovia pracovnej skupiny združenia IAB Europe pre implementáciu GDPR pod vedením spoločnosti **Improve Digital.**

Kontakty

Matthias Matthiesen (matthiesen@iabeurope.eu)

Senior Manager – Ochrana súkromia a verejná politika, IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)

Riadiaci pracovník pre verejnú politiku, IAB Europe

Obsah

1. Prehľad

Európska únia prijala 27. apríla 2016 všeobecné nariadenie o ochrane údajov („GDPR“)*1 GDPR sa stane priamo uplatniteľným právnym predpisom v Európskej únii (ďalej len „EÚ) a v Európskom hospodárskom priestore (ďalej len „EHP“) **25. mája 2018** a nahradí tak vnútroštátne právne predpisy o ochrane osobných údajov, ktoré sú v súčasnosti v platnosti.

GDPR sa nebude vzťahovať len na spoločnosti so sídlom v EÚ, ale aj na spoločnosti na celom svete, ktoré ponúkajú tovar a služby ľuďom na území Únie alebo monitorujú správanie jednotlivcov, ktorí sa na ňom nachádzajú. Týmto právnym predpisom sa upravuje spracúvanie osobných údajov, ktoré sú ním široko definované ako akékoľvek informácie, ktoré sa týkajú identifikovanej alebo identifikovateľnej fyzickej osoby, ktoré môžu okrem iného zahŕňať online identifikátory a identifikátory zariadení, a ktoré môžu byť použité na zber údajov o jednotlivých užívateľoch, napríklad na účely digitálnej reklamy.

GDPR udeľuje orgánom pre ochranu osobných údajov právomoc vyberať značné administratívne pokuty od firiem, u ktorých bolo zistené porušenie zákona. **V závislosti od závažnosti porušenia môžu pokuty dosiahnuť výšku až 20 000 000 EUR alebo 4 percentá ročného globálneho obratu spoločnosti, podľa toho, čo je vyššie.**

Tento dokument pripravili členovia pracovnej skupiny združenia IAB Europe pre implementáciu GDPR s cieľom poskytnúť spoločnostiam na celom svete možnosť lepšie porozumieť tomu, čo takto postavená definícia osobných údajov pre ne znamená.

1 1 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), k dispozícii na http://eur-lex.europa.eu/eli/reg/2016/679/oj/.

2. Cesta k dodržiavaniu GDPR - všeobecného nariadenia o ochrane údajov

2.1. Prehodnoďte a zdokumentujte činnosti a bezpečnostné opatrenia týkajúce sa spracovávania údajov

Ústrednou témou prítomnou v celom všeobecnom nariadení o ochrane údajov (GDPR) je zodpovednosť. Preskúmanie a zdokumentovanie všetkých vašich činností týkajúcich sa bezpečnosti a spracovania údajov je prvým krokom na ceste k dosiahnutiu zodpovednosti vo vzťahu k osobným údajom vo vašej spoločnosti.

Ako súčasť tohto procesu by ste mali identifikovať prečo a ako spracúvate osobné údaje, ktoré uchovávate. Základné pochopenie činností týkajúcich sa spracovania údajov si môže vyžadovať, aby ste venovali pozornosť osobitným úvahám – najmä tomu, či spracúvate citlivé osobné údaje. Okrem toho môže tento proces odhaliť, že vaše spracovateľské činnosti si vyžadujú osobitné podmienky ochrany, takže v závislosti od povahy vykonávaného spracovania údajov si bezpečnostné procesy zavedené vo vašej spoločnosti môžu tiež vyžadovať opätovné posúdenie. To je dôležitý krok vzhľadom na oveľa vyššie pokuty, ktoré budú môcť byť spoločnostiam uložené v prípade porušenia nariadenia.

Do tohto procesu by bolo dobré zapojiť rôzne oddelenia vašej spoločnosti. Implementácia nariadenia GDPR by nemala byť ponechaná len na právne oddelenia, úradníka pre ochranu údajov alebo IT. Dotazníky a rozhovory so zamestnancami zo všetkých oddelení – prípadne s kľúčovými dodávateľmi a partnermi – vám umožnia identifikovať, aký typ spracovania údajov sa deje v každej oblasti práce vašej spoločnosti. Pochopenie všetkých týchto procesov je kľúčové. To vám ako spoločnosti umožní zaznamenať každý typ spracovania dát na základe jeho účelu, čo poskytuje neuveriteľne cenný prehľad Vytvorte zoznam vecí, ktoré sa majú zdokumentovať potrebný pre zabezpečenie súladu interných predpisov a smerníc s GDPR.

2.2. Vytvorte zoznam vecí, ktoré sa majú zdokumentovať

Pri zdokumentovávaní vašich činností týkajúcich sa spracovania údajov by ste mali každú zvážiť na základe kritérií „čo, kde, kedy, prečo“, ako aj očakávaných dôsledkov procesu spracovania a pre každý takýto proces vykonať analýzu rizík. To zahŕňa aj údaje o každom zamestnancovi, ktoré spracúvate. V tomto procese vám môžu pomôcť tieto otázky:

- Aké informácie sú poskytnuté pred zberom a spracovaním údajov?
- Koho údaje spracúvate, o aké údaje ide, kde sú spracúvané, kedy sú spracúvané a prečo sú spracúvané? (Máte právoplatné podklady? Spracúvate v súlade so zásadami spracovania údajov?)
- Aké údaje sú anonymizované, aké údaje sú pseudonymizované?
- Na ako dlho uchovávate takéto údaje?
- S kým zdieľate takéto údaje?

- Aká je úroveň rizika na každom stupni procesu spracovania?
- V ktorých prípadoch je váš podnik prevádzkovateľom, sprostredkovateľom alebo spoločným prevádzkovateľom?*2
- Spracúvate niečo, čo by AKÝKOĽVEK členský štát považoval za osobné údaje (napríklad IP adresa, cookies, akýkoľvek online identifikátor)?
- Slúži váš proces na bezpečnostné účely? Ak áno, zdokumentujte podrobnosti týkajúce sa tohto procesu.
- Majte na pamäti, že „osobné" údaje, ktoré sú ukladané alebo zasielané mimo EÚ, musia dodržiavať pravidlá cezhraničného prenosu (kapitola 13 GDPR).
- Dostávate súhlas so spracovaním dát a posielate ho vašim sprostredkovateľom a iným tretím stranám? Je prijatý súhlas určený len vám alebo aj vašim tretím stranám?
- Preskúmajte a zdokumentujte procesy týkajúce sa bezpečnosti spracovania údajov.
- Ako vy a akákoľvek spoločnosť, ktorá pôsobí ako sprostredkovateľ, subsprostredkovateľ alebo spoločný prevádzkovateľ zaisťujete bezpečnosť vašich údajov? Podľa GDPR musí byť porušenie týkajúce sa ochrany údajov nahlásené orgánu pre ochranu osobných údajov do 72 hodín od porušenia.*3 Ak ešte nemáte pre tento prípad plán, mali by ste ho vytvoriť. Zamyslite sa nad vytvorením vzoru na zasielanie takýchto informácií.

2.3. Vytvorte a uplatňujte plán dodržiavania GDPR

Vyššie uvedené postupy by vám mali pomôcť identifikovať činnosti, ktoré by mohli sčasti alebo úplne viesť k nesúladu s nariadením GDPR, a preto si vyžadujú zmenu. Počas tohto procesu by ste mali pouvažovať nad nasledujúcimi otázkami:

- Akým spôsobom sú vaše súčasné interné procesy v rozpore s GDPR a existujú zmeny, ktoré by ste mohli zaviesť na vyriešenie tohto rozporu?
- Ako dlho bude vykonanie potrebných zmien trvať?
- Spracúvate údaje na základe súhlasu používateľov? Používate štandardizovanú metódu na prijímanie súhlasu a jeho posielanie tretím stranám a sprostredkovateľom?
- Potrebujete vybudovať dodatočné logy? Napríklad, ak sú údaje spracúvané na základe súhlasu používateľov, zaznamenať pomocou časovej pečiatky, kedy bol súhlas poskytnutý, kedy nebol poskytnutý alebo kedy bol odvolaný (v súvislosti s IP adresou, cookies a/alebo iným identifikátorom).
- Ako budete uplatňovať právo používateľa na prístup ku údajom a iné práva dotknutej osoby (kapitola III GDPR, články 12 až 22) a uchovávať váš dôkaz o jeho dodržiavaní?
- Spolupracujte s vašimi sprostredkovateľmi a subsprostredkovateľmi na vytvorení a zdokumentovaní pokynov týkajúcich sa nakladania s údajmi (dohody so sprostredkovateľmi údajov).

[2] GDPR definuje tieto termíny v článku 4 ods. 7 a ods. 8.
[3] GDPR, článok 33, odôvodnenia 73 a 85 až 88.

2.4. Analyzujte vplyv ochrany údajov pri nových činnostiach*4

GDPR vyžaduje, aby prevádzkovatelia vykonali pred každou novou činnosťou týkajúcou sa spracovania údajov posúdenie jej vplyvu na ich ochranu v týchto prípadoch:

- Keď je použitá nová technológia;
- Keď je pravdepodobné, že spracovanie bude predstavovať vysoké riziko pre dotknuté osoby. Môžete použiť jediné posúdenie vplyvu pre viaceré spracovateľské operácie, ak predstavujú podobné riziká;
- Keď zahŕňa systematické a rozsiahle hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracovaní vrátane profilovania a na základe ktorého sa prijímajú rozhodnutia, ktoré majú právne účinky týkajúce sa fyzickej osoby alebo majú vplyv na fyzickú osobu podobne dôležitým spôsobom;
- Keď spracúvate širokú škálu citlivých osobných údajov *5;
- Keď systematicky monitorujete verejne dostupnú oblasť vo veľkom rozsahu.

Venujte mimoriadnu pozornosť práci dozorných orgánov – ich úlohou je zriadiť verejný zoznam spracovateľských činností, ktoré si vyžadujú posúdenie ich vplyvu na ochranu údajov. Môžu sa tiež rozhodnúť uverejniť „white list“ – zoznam spracovateľských činností, ktoré si nevyžadujú posúdenie vplyvu na ochranu údajov.

2.5. Preskúmajte a pozmeňte existujúce zmluvné podmienky a zásady ochrany osobných údajov

Preskúmanie, prípadne zmena vašich interných procesov, je len jednou časťou cesty smerom k ich zosúladeniu so smernicou GDPR. Ďalším dôležitým aspektom je zabezpečiť, aby sa tieto zmeny odzrkadlili v zmluvách, ktoré máte so svojimi partnermi. V určitých prípadoch GDPR vyžaduje, aby ste mali vo vašej spoločnosti uzavreté dohody so spoločnosťami, s ktorými spolupracujete, napríklad v prípade, keď sa vaša spoločnosť a iná spoločnosť považujú za „spoločných prevádzkovateľov“. Je potrebné pripomenúť, že prevádzkovateľom údajov je ten, kto určí účel aj spôsob spracovania osobných údajov.

Napokon, spoločnosti musia preskúmať a aktualizovať aj už existujúce predajné zmluvy a svoje vlastné zásady ochrany súkromia.

Odporúčame vám:

- Preskúmajte všetky predajné zmluvy a podľa potreby ich zmeňte.

[4] Návrh usmernení pracovnej skupiny podľa článku 29 týkajúcich sa posúdení vplyvu na ochranu údajov (pracovný dokument 248), k dispozícii na: : http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.
[5] GDPR, článok 9, odôvodnenia 51 až 56.

- V prípade viacerých sprostredkovateľov údajov sa musí vytvoriť „dohoda“ medzi spoločnými sprostredkovateľmi s cieľom rozdeliť si medzi sebou zodpovednosť za dodržiavanie ochrany údajov. *6

- Preskúmajte vaše obchodné podmienky.
- Preskúmajte vaše oznámenia o ochrane súkromia (externé zverejnené) a zásady ochrany údajov (interné pravidlá).

  Mali by ste mať tiež zavedené pravidlá a postupy pre zamestnancov, ktorí pracujú s osobnými údajmi, a mali by ste ich zadefinovať v zásadách ochrany súkromia.

  Dotknuté osoby musia byť informované o zbere a ďalšom spracovaní ich osobných údajov.

  Tieto informácie musia byť poskytnuté „v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho […]“ – zvyčajne vo forme oznámenia o ochrane súkromia. *7

  Zhrnutie dohody medzi spoločnými poskytovateľmi musí byť sprístupnené dotknutým osobám.

Mohli by ste pouvažovať nad používaním nástrojov alebo softvéru na monitorovanie toho, či tretie strany konajú v súlade s tým, čo bolo dohodnuté v zmluve a v podmienkach ochrany súkromia. Existuje široká škála trhových riešení v súvislosti s únikom údajov vrátane riešení týkajúcich sa tag manažmentu, nástrojov na ochranu súkromia, nástrojov na predchádzanie strate údajov atď.

2.6. Vymenujte úradníka pre ochranu údajov *8

GDPR vyžaduje od spoločností, aby určili úradníka pre ochranu údajov:

- Ak si to vyžaduje právo členského štátu;
- Ak kľúčové činnosti spoločnosti pozostávajú zo spracúvania, ktoré si vyžaduje pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu;
- Ak je spracovanie údajov kľúčovou činnosťou a zahŕňa pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo sú spracúvané údaje citlivými informáciami odhaľujúcimi rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenia, členstvo v odborových organizáciách, genetické údaje alebo biometrické údaje a údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie fyzickej osoby.

Úradník pre ochranu údajov je formálne poverený zabezpečiť, aby si bola organizácia vedomá povinností týkajúcich sa ochrany údajov a aby si ich plnila. Úradníci pre ochranu údajov by mali mať odborné znalosti o právnych predpisoch v oblasti ochrany údajov a prax a mali by byť schopní vykonávať tieto funkcie:

- Informovať príslušného poskytovateľa alebo sprostredkovateľa (a všetkých zamestnancov, ktorí spracúvajú osobné údaje) o ich povinnostiach podľa GDPR a poskytnúť im v tejto súvislosti poradenstvo;

[6] GDPR, článok 4 ods. 7, článok 26 ods. 1, odôvodnenie 79.

[7] GDPR, článok 5 ods. 1 písm. a), články 12 až 14, odôvodnenia 39, 58, 60.

[8] Usmernenia pracovnej skupiny podľa článku 29 týkajúce sa úradníkov pre ochranu údajov (pracovný dokument 243 rev. 1 k dispozícii na http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

- Monitorovať dodržiavanie GDPR zo strany poskytovateľa alebo sprostredkovateľa;
- Poskytovať poradenstvo v oblasti posúdenia vplyvu činnosti na ochranu údajov a zapájať sa do predbežných konzultácií s orgánmi pre ochranu osobných údajov;
- Spolupracovať s orgánmi pre ochranu osobných údajov a pôsobiť ako kontaktné miesto;
- Zaoberať sa všetkými záležitosťami v oblasti ochrany údajov, ktoré sa týkajú prevádzkovateľa, náležite a včas. Prevádzkovateľ alebo sprostredkovateľ musí poskytnúť úradníkovi pre ochranu údajov na to potrebné zdroje a podporu.

Úradníkom pre ochranu údajov môže byť zamestnanec alebo externý konzultant. V GDPR sa stanovuje, že skupiny spoločností môžu vymenovať jedného úradníka pre ochranu údajov, ak tento úradník môže plniť svoju funkciu pre každú z týchto spoločností. Úradník pre ochranu údajov je viazaný povinnosťou mlčanlivosti vo vzťahu k svojej práci a má tiež špeciálnu ochranu zo strany svojho zamestnávateľa. Organizácia nemôže inštruovať úradníka pre ochranu údajov pri výkone jeho povinností a nemôže ukončiť jeho pracovný pomer ani prijať žiadne disciplinárne opatrenie vyplývajúce z výkonu jeho povinností.

2.7. Zriaďte jednotné kontaktné miesto s vaším orgánom pre ochranu osobných údajov *9

Jedným z možných prínosov, ktoré môže GDPR poskytnúť spoločnostiach, je koncepcia jednotného kontaktného miesta. To platí pre organizácie s viacerými miestami podnikateľskej činnosti v EÚ, keďže im umožňuje určiť „vedúci dozorný orgán“. Z toho dôvodu organizácie pôsobiace vo viacerých členských štátoch musia starostlivo zvážiť svoje možnosti v súvislosti so zriadením jednotného kontaktného miesta.

Podľa GDPR orgán pre ochranu osobných údajov v krajine EÚ, kde má organizácia svoje „hlavné miesto podnikateľskej činnosti“ bude jej „vedúcim orgánom“. Aby bola organizácia oprávnená na jednotné kontaktné miesto, potrebuje „hlavné miesto podnikateľskej činnosti“ v rámci EÚ. Hlavným miestom podnikateľskej činnosti je spravidla európska centrála spoločnosti, ale podľa práva EÚ týkajúceho sa spoločností by to mohlo byť v určitých situáciách inak.

Mať jednotné kontaktné miesto a jedného vedúceho úradníka pre ochranu údajov (namiesto orgánov pre ochranu osobných údajov vo viacerých členských štátoch) umožní jednotnejšie uplatňovanie a dodržiavanie GDPR na trhoch EÚ*10.

2.8. Informujte, buďte informovaní a uplatňujte v praxi

Mali by ste informovať a školiť svojich zamestnancov o dôsledkoch vyplývajúcich z GDPR a z vašich nových zásad na ochranu súkromia, ktoré sa týkajú ich práce, a uistiť sa, že dodržiavanie vašich zásad ochrany súkromia sa v prípade potreby presadzuje prostredníctvom primeraných disciplinárnych opatrení.

[9] Usmernenia pracovnej skupiny podľa článku 29 o vedúcom dozornom orgáne (pracovný dokument 244 rev. 1), k dispozícii na: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[10] Celý zoznam orgánov pre ochranu osobných údajov v Európe možno nájsť tu: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

Majte prehľad o nových iniciatívach a normách digital odvetvia pripojením sa k združeniu IAB Europe a k regionálnym kanceláriám IAB v krajinách, v ktorých pôsobíte. Spolupracujte s nimi a sledujte prácu pracovnej skupiny podľa článku 29 (budúceho Európskeho výboru pre ochranu údajov) a orgánov pre ochranu osobných údajov na trhoch, na ktorých pôsobíte.

Je tiež dôležité, aby ste včas informovali vašich obchodných partnerov o akýchkoľvek zmenách vo vašich produktoch alebo službách vyplývajúcich z vašej snahy dosiahnuť súlad s nariadením GDPR. V prípade, že je vaša organizácia spotrebiteľsky orientovaná, je potrebné informovať taktiež spotrebiteľov o vašich aktualizovaných zásadách ochrany súkromia. Najmä pokiaľ ide o používanie súhlasu ako právneho základu na spracovanie osobných údajov, je mimoriadne dôležité, aby boli novozavedené procesy oznámené všetkým zainteresovaným stranám.

- Informujte zamestnancov, sprostredkovateľov, užívateľov a klientov (ešte pred 25. májom 2018) o zmenách vašich obchodných podmienok a zásad ochrany súkromia.
- Informujte predajcov, sprostredkovateľov, subsprostredkovateľov a spoločných poskytovateľov o potrebných zmenách v zmluvách.

O pracovnej skupine združenia IAB Europe

Pracovná skupina združenia IAB Europe pre implementáciu všeobecného nariadenia o ochrane údajov spája vedúcich expertov z celého odvetvia digitálnej reklamy s cieľom prediskutovať nový právny predpis Európskej únie o ochrane údajov, vymieňať si najlepšie postupy a dohodnúť sa na spoločnom výklade a postoji odvetvia k najdôležitejším otázkam týkajúcim sa sektora digitálnej reklamy.

Pracovná skupina pre implementáciu všeobecného nariadenia o ochrane osobných údajov je fórum na členskej báze, ktoré na základe diskusií a výmeny názorov prispieva k informovanosti svojich členov pôsobiacich v oblasti digitálnej reklamy ohľadne implementácie novej legislatívy do ich procesov tak, aby bolo v súlade s nariadením GDPR.

Tento dokument ako aj jeho odporúčania by nemohli vzniknúť bez práce a vedenia zúčastnených členov tejto pracovnej skupiny.

Pre viac informácií prosím kontaktujte:

MMatthias MMatthiesen (matthiesen@iabeurope.eu)
Senior manažér, Ochrana súkromia a verejná politika, IAB Europe
Chris Hartsuiker (hartsuiker@iabeurope.eu)
Riadiaci pracovník pre verejnú politiku, IAB Europe

Združenie pre internetovú reklamu IAB Slovakia aktívne komunikuje s IAB Europe ohľadne problematiky GDPR a zabezpečilo pre svojich členov ako i ostatné digitálne subjekty preklad dokumentu do slovenského jazyka. IAB Slovakia je členom IAB Europe.

združenie pre internetovú reklamu iab.SK

iab.europe