VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

TECHNICKÉ POŽADAVKY NA ZABEZPEČENÍ DLE GDPR

THESIS TITLE

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE — **DANIEL OLEARČIN**
AUTHOR

VEDOUCÍ PRÁCE — **PAVEL OČENÁŠEK, Mgr. Ing. Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Cieľom práce bolo zistiť technické požiadavky na zabezpečenie poďla GDPR, konkrétne sa venujem v tejto práci na mobilné technológie.

Abstract

The aim of the work was to find out the technical requirements for securing the GDPR, specifically I am dealing with mobile technologies.

Klíčová slova

GDPR, zabezpečení, mobilní technologie

Keywords

GDPR, security, mobile technologies

Citace

OLEARČIN, Daniel. *Technické požadavky na zabezpečení dle GDPR.* Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Pavel Očenášek, Mgr. Ing. Ph.D.

Technické požadavky na zabezpečení dle GDPR

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Daniel Olearčin

30. dubna 2021

Obsah

Kapitola 1

Úvod

1.1 Čo je to GDPR

Všeobecné nariadenie o ochrane údajov (anglicky General Data Protection Regulation, skrátene GDPR), plným názvom 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 zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), je nariadenie Európskej únie, ktorého cieľom je výrazné zvýšenie ochrany osobných údajov občanov. V Úradnom vestníku Európskej únie bolo vyhlásené 27. apríla 2016. Nariadenia, v schválenom znení, sú priamo účinné pre každý členský štát EÚ. V slovenskom právnom poriadku je nariadenie premietnuté aj do zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov z 29. novembra 2017. Zákon 18/2018 Z. z. je účinný na Slovensku rovnako ako GDPR od 25. mája 2018. Viac viz [3].

1.2 Prečo vzniklo GDPR

Nariadenie chráni základné práva a slobody fyzických osôb so zameraním na právo ochrany osobných údajov. Stanovuje pravidlá ochrany fyzických osôb a pravidlá pre voľný pohyb (ktorý sa nesmie obmedziť ani zakázať) osobných údajov v Európskej únii. Táto konzistentná úroveň ochrany fyzických osôb v celej Únii má zabrániť rozdielom, ktoré sú prekážkou voľného pohybu osobných údajov v rámci vnútorného trhu (preambula, ods.13). Viac viz [3].

1.3 Na čo všetko sa vzťahuje GDPR

Nariadenie spresňuje a rozširuje okruh a definíciu osobných údajov takto: akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Osobným údajom je teda aj emailová adresa, dokonca podľa nariadenia GDPR osobné údaje (online identifikátory) sú aj cookies,IP adresy, či iné virtuálne identifikátory.

Osobné údaje sú informácie o osobe, preto osobným údajom nie sú napr. údaje o právnickej osobe (o jej zamestnancoch už ale áno), údaje o osobách zomretých, nie sú to údaje, ktoré konkrétnu osobu nestotožňujú (napr. Obyčajné bežné meno a priezvisko) a medzi osobné údaje nepatria údaje anonymizované, teda také, ktoré pôvodne možnosť identifikácie osoby obsahovali, ale taký identifikátor z nich bol odstránený. Viac viz [3].

Kapitola 2

Všeobecné technické požiadavky na zabezpečenie podľa GDPR

2.1 Všeobecné nariadenie o ochrane údajov

Všeobecné nariadenie o ochrane údajov sa uplatňuje, keď:

- vaša spoločnosť spracúva osobné údaje a má sídlo v EÚ bez ohľadu na to, kde sa skutočné spracúvanie údajov uskutočňuje,
- vaša spoločnosť je usadená mimo EÚ, ale spracúva osobné údaje v súvislosti s ponukou tovaru alebo služieb jednotlivcom v EÚ alebo monitoruje správanie jednotlivcov v rámci EÚ.

Podniky, ktoré nemajú sídlo v EÚ a spracúvajú údaje občanov EÚ, musia vymenovať zástupcu v EÚ.

Všeobecné nariadenie o ochrane údajov sa neuplatňuje, keď:

- dotknutá osoba je mŕtva,
- dotknutá osoba je právnickou osobou, jednotlivcov v rámci EÚ.
- spracúvanie sa vykonáva osobou konajúcou na účely, ktoré nesúvisia s jej obchodnou činnosťou, podnikaním alebo povolaním.

Viac viz [2].

2.2 Spracovávanie osobných údajov v rámci firmy

Monitorovaním spracúvania osobných údajov a poskytovaním informácií a poradenstva zamestnancom, ktorí spracúvajú osobné údaje, v súvislosti s ich povinnosťami je poverená zodpovedná osoba, ktorá môže byť určená spoločnosťou. Zodpovedná osoba takisto spolupracuje s orgánom pre ochranu osobných údajov, pričom slúži ako kontaktné miesto pre orgán pre ochranu osobných údajov a jednotlivcov.

Vaša spoločnosť je povinná vymenovať zodpovednú osobu, ak:

- pravidelne alebo systematicky monitoruje jednotlivcov alebo spracúva osobitné kategórie údajov,
- toto spracúvanie je hlavnou podnikateľskou činnosťou,
- spracúva údaje vo veľkom rozsahu.

Napríklad, ak spracúvate osobné údaje s cieľom zacieliť reklamu prostredníctvom vyhľadávačov na základe správania ľudí na internete, vyžaduje sa, aby ste určili zodpovednú osobu. Ak však iba raz ročne posielate klientom propagačné materiály, nepotrebujete mať zodpovednú osobu. Podobne, ak ste lekár a získavate údaje o zdraví pacientov, pravdepodobne nepotrebujete mať zodpovednú osobu. Ak však spracúvate osobné údaje týkajúce sa genetiky alebo zdravia pre nemocnicu, potom sa vyžaduje mať zodpovednú osobu.

Zodpovedná osoba môže byť pracovníkom vašej organizácie alebo ňou môže byť externá osoba na základe zmluvy o poskytovaní služieb. Zodpovedná osoba môže byť jednotlivcom alebo súčasťou organizácie. Viac viz [2].

2.3 Kedy sa môžu spracovávať osobne údaje

Na základe pravidiel EÚ o ochrane údajov by ste mali údaje spracúvať spravodlivo a zákonným spôsobom na určené a legitímne účely a spracúvať len údaje, ktoré sú potrebné na splnenie tohto účelu. Na spracúvanie osobných údajov sa vyžaduje, aby ste spĺňali jednu z týchto podmienok:

- máte súhlas dotknutej osoby,
- osobné údaje potrebujete na plnenie zmluvných záväzkov voči dotknutej osobe,
- osobné údaje potrebujete na splnenie právnej povinnosti,
- osobné údaje potrebujete na ochranu životne dôležitých záujmov dotknutej osoby,
- osobné údaje spracúvate na účely plnenia úlohy vo verejnom záujme,
- konáte v oprávnených záujmoch svojej spoločnosti, pokiaľ sa tým závažným spôsobom neovplyvňujú základné práva a slobody osoby, ktorej údaje sa spracúvajú. Ak práva dotknutej osoby prevažujú nad záujmami vašej spoločnosti, dané osobné údaje nemôžete spracúvať.

Viac viz [2].

2.4 Poskytovanie transparentných informácií

Jednotlivcom musíte poskytnúť jasné informácie o tom, kto osobné údaje o nich spracúva a prečo. Informácie musia zahŕňať minimálne toto:

- kto ste,
- prečo spracúvate osobné údaje,
- aký je právny základ,
- (prípadne) kto získa tieto údaje.

V niektorých prípadoch musia poskytované informácie obsahovať aj:

- kontaktné údaje prípadnej zodpovednej osoby,
- aký oprávnený záujem spoločnosť sleduje, ak je to právnym dôvodom na spracovanie údajov,
- opatrenia uplatňované na prenos údajov do krajiny mimo EÚ,
- práva na ochranu údajov jednotlivca (t. j. právo na prístup, opravu, vymazanie, obmedzenie, námietku, prenosnosť atď.)
- a mnoho ďalších.

Viac viz [2].

Kapitola 3

GDPR v rámci mobilných tenchológií.

3.1 GDPR proti ponukám cez telefón

S nariadením o ochrane osobných údajov sú firmy opatrnejšie pri ponúkaní produktov cez telefón alebo SMS. GDPR sa snaží pri tomto procese zaistiť väčšiu ochranu nad osobnými údajmi. Kto vám môže ponúkať takéto služby a ako sa vyhnúť nepríjemným telefonátom? Ak už nechcete, aby vám niečo ponúkali, jednoducho ich na to upozornite. Viac viz [1].

3.2 Kto vám môže ponúkať svoje služby a produkty po telefóne

GDPR dopadá na telefonické ponuky a ponuky cez SMS podobne ako na emailové reklamné oznámenia. Ako vaše telefónne číslo, tak aj emailová adresa sú osobným údajom. Spoločnosti môžu svoje produkty či služby po telefóne, cez SMS alebo emailom ponúkať len na základe vášho súhlasu. Ak si tak kúpite nový mobilný telefón, je predajca oprávnený vám zaslať napríklad ponuku príslušenstva k vybranému prístroju. Ďalej sa môže stať, že vás osloví marketingová agentúra, s ktorou má správca údajov uzatvorenú zmluvu, aby vám služby či produkty daného správcu ponúkala. Pokiaľ vás ale osloví niekto s ponukou bez toho, aby ste s danou spoločnosťou mali nejaký vzťah, môže ísť o porušenie predpisov o ochrane osobných údajov. Viac viz [1].

3.3 Ako je to so spoločnosťami, ktoré si dáta o zákazníkoch kupujú

Spoločnosti, ktoré prevádzkujú telemarketing, zvyčajne pracujú s telefónnymi číslami, ktoré nezískavajú priamo od ľudí, ale z databáz s údajmi. S databázami údajov tohto druhu sa často obchoduje a dáta sa do nich získavajú tak, že zákazníci e-shopov, užívatelia rôznych webov a ďalších služieb zadajú svoje telefónne čísla a odsúhlasia podmienky spracovania osobných údajov, v ktorých je ukrytý súhlas s takýmto využitím ich mobilného čísla. Viac viz [1].

3.4 Je dôležitý jasný súhlas

GDPR zavádza pre súhlas so spracovaním osobných údajov niektoré nové podmienky – v tomto prípade je najmä dôležitý dôraz na odlišnosť súhlasu od ostatných skutočností.

Subjekt musí jasne vedieť, že udeľuje súhlas so spracovaním údajov a súhlasom nesmie byť podmienené napríklad plnenie zmluvy. Vzhľadom k tomu, že súhlasy ukryté v obchodných podmienkach tieto kritériá nespĺňajú, nemožno údaje získané takouto formou naďalej využívať. Aby to bolo možné, musel by byť súhlas udelený znovu podľa podmienok, ktoré požaduje GDPR. Viac viz [1].

3.5 Ako sa nechať vymazať?

Platí, že zákazník musí mať možnosť jednoducho (napr. prostredníctvom odkazu) bezplatne sa odhlásiť, resp. odmietnuť ďalšie zasielanie marketingových oznámení. Jedná sa typicky o akékoľvek obchodné oznámenia a ponuky zasielané na email alebo telefónne číslo zákazníka. GDPR nestanovuje jednotný postup pre uplatnenie práva na to nebyť ďalej oslovovaný s reklamnými ponukami. Jeho uplatnenie by ale malo byť rovnako jednoduché, ako udelenie súhlasu. Uplatnenie tohto práva sa tak líši spoločnosť od spoločnosti.

Všeobecne je možné podať takúto žiadosť napr. listom, emailom, cez web. V prípade telefonického oslovovania bude najskôr rovnako možné volajúcemu oznámiť žiadosť o výmaz. Ľudia by si však mali byť vedomí, že uplatnením práva na vymazanie nemusí dôjsť k vymazaniu všetkých ich osobných údajov. Keď napríklad odoberú operátorovi súhlas pre marketingové akcie, ten bude aj naďalej spravovať ich údaje k zmluve napríklad o tarife. Pravdepodobne dôjde k vymazaniu údajov používaných pre marketingové oslovovanie, ale nemusí dôjsť k vymazaniu údajov, ktoré spoločnosť potrebuje na plnenie zákonných povinností či plnenie uzatvorenej zmluvy. Viac viz [1].

3.6 Je s GDPR vymazanie z marketingových databáz jednoduchšie?

Takúto možnosť poznala aj doterajšiu právna úprava, GDPR však celkovo zvyšuje dôraz na dodržiavanie pravidiel ochrany osobných údajov, takže možno očakávať, že k právam dotknutých osôb budú mať spoločnosti väčší rešpekt. Všeobecne je GDPR ústretové k elektronickej forme komunikácie, takže možno komunikovať emailom, ale je na mieste si všetku komunikáciu uchovávať. Viac viz [1].

Literatura

[1] GDPR proti ponukám cez telefón. [online], [upravené: 2019-01-23]. Dostupné z: https://www.osobnyudaj.sk/novinka/38-gdpr-proti-ponukam-cez-telefon

[2] Ochrana údajov na základe všeobecného nariadenia o ochrane údajov. [online], [upravené: 2019-04-26]. Dostupné z: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_sk.htm#shortcut-4

[3] Všeobecné nariadenie o ochrane údajov. [online], [upravené: 2020-08-14]. Dostupné z: https://sk.wikipedia.org/wiki/V%C5%A1eobecn%C3%A9_nariadenie_o_ochrane_%C3%BAdajov