

Písomné vyjadrenie panelistov na nezodpovedané otázky z panelu počas konferencie IT právo

1. ak prevádzkujem informacny web a pouzivam google analytics, mozem sa spolať, že neporusujem gdpr?

Berthoty Jakub: Podľa dostupných informácií sa Google pripravuje na GDPR a e-Privacy nariadenie rovnako ako jeho zákazníci a dá sa očakávať, že do mája 2018 by mal byť Google pripravený na tieto predpisy.

Zimen Ondrej: V každom prípade ak umožníte Google cez Analytics na Vašom webe spracúvať osobné údaje návštevníkov už teraz Vám odporúčam túto skutočnosť transparentne uviesť v príslušnej časti toho webu. Ideálne je to vysvetliť v Privacy Policy zverejnej na webe.

.....

2. Kto a akým spôsobom prípadne v ktorých prípadoch bude kontrolovať súlad firmy s gdpr?

Berthoty Jakub: Súlad firmy s GDPR môže kontrolovať Úrad na ochranu osobných údajov, akýkoľvek súd v rámci civilného konania a zároveň zahraničný dozorný úrad z iného členského štátu (v spolupráci s Úradom) ak daná firma má tzv. hlavnú prevádzku v inom členskom štáte EÚ.

Zimen Ondrej: Doplním Jakuba, že v budúcnosti ak sa prevádzkovatelia či sprostredkovatelia rozhodnú dobrovoľne podstúpiť samoregulačný challenge v rámci GDPR certifikácie od akreditovaného certifikačného subjektu alebo pristúpiť k schválenému kódexu správania môžu byť kontrolovaní aj iným subjektom ako verejnoprávnymi regulátormi (DPA - Data Protection Authority). V podstate pôjde o 1) dozorným orgánom schválenú osobu, ktorá bude mať postavenie subjektu monitorujúceho dodržiavanie konkrétného kódexu správania, 2) samotný akreditovaný certifikačný subjekt, ktorý udelí certifikáciu. Okrem toho nemožno vylúčiť audity, ktoré sú prevádzkovatelia oprávnení vykonávať voči sprostredkovateľom, aj prostredníctvom splnomocnencov (napr. advokátov) ak sa to zmluvne dohodne.

Tatiana Valentová: V prípade, že sa na prevádzkovateľa bude vzťahovať pôsobnosť zákona o ochrane osobných údajov (nový zákon v legislatívnom procese), bude podliehať dozornej činnosti Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“). Jedným z mechanizmov dozornej činnosti je kontrola spracúvania osobných údajov (riadna alebo mimoriadna kontrola na základe podozrenia z porušenia povinností pri spracúvaní osobných údajov alebo v konaní o ochrane osobných údajov), kontrola dodržiavania schváleného kódexu správania (predpokladá členstvo v kódexe správania), kontrola súladu spracúvania osobných údajov s vydaným certifikátom a kontrola dodržiavania vydaného osvedčenia o udelení

akreditácie. Kontrolu vykoná úrad prostredníctvom kontrolného orgánu zloženého zo zamestnancov úradu. Kontroly sa môže zúčastniť aj prizvaná osoba z iného dozorného orgánu za podmienok stanovených zákonom a GDPR. Pri výkone kontroly je kontrolný orgán povinný postupovať v súlade so zákonom a GDPR.

.....

3. Aplikuje sa právo na prenosnosť údajov plosne alebo len keď je to u prevádzkovateľa technicky možné? Ako dozorný orgán skúma túto technickú možnosť/nemožnosť?

NAGY Zoltán: Právo na prenosnosť údajov si dotknutá osoba môže uplatniť len za určitých predpokladov, a to ak spracúvanie jej údajov (i) je založené na súhlase alebo (ii) je nevyhnutné na plnenie zmluvy a súčasne sa toto spracúvanie vykonáva automatizovanými prostriedkami. V zmysle Nariadenia má dotknutá osoba právo na prenosnosť údajov, len ak je to technicky možné. Hoci Nariadenie neukladá prevádzkovateľom priamu povinnosť používať interoperabilné formáty na účely plnenia práva na portabilitu, na viacerých miestach však apeluje na používanie takých formátov, ktoré túto interoperabilitu umožnia. V každom prípade, technická možnosť/nemožnosť splnenia daného práva bude potrebné posudzovať od prípadu k prípadu.

Okrem toho sa právo na portabilitu neuplatní v prípade, ak je spracúvanie vykonávané prevádzkovateľom pri výkone verejnej moci (napr. štátnym orgánom) alebo pri plnení úlohy vo verejnom záujme.

Tatiana Valentová: Prevádzkovateľ by mal vždy postupovať tak, aby vyhovel požiadavke na prenosnosť údajov, ak sa na neho táto povinnosť vzťahuje. Technické možnosti a podmienky bude úrad skúmať individuálne, vždy vo vzťahu k mechanizmom a podmienkam spracúvania, ktoré prevádzkovateľ nastavil. Môžem prevádzkovateľom odporučiť, aby v súlade so zásadou zodpovednosti, riadne definovali všetky okolnosti, vykonali posúdenie možnosti/nemožnosti prenosnosti vo svojich podmienkach a uchovali túto analýzu pre možné budúce preukazovanie súladu so zákonom/GDPR.

.....

4. Ukladanie PII mimo územia EU upravuje už dostatočne dlho Data Protection Directive, takže nič sa nemení. Alebo je tam niečo nové?

Berthoty Jakub: Bez zachádzania do detailov suhlasim, že podstatne zmeny v cezhraničnom prenose nenastali.

ZIMEN Ondrej: Koncepcia zostala zachovaná. Všeobecný právny základ + vedomosť dotknutej osoby + osobitná právna záruka vo forme BCR schválených príslušným dozorným orgánom, štandardných zmluvných doložiek schválených Európskou Komisiou atď. Osobitná právna záruka pre prenos do tretej krajiny sa bude dať tiež preukázať certifikáciou alebo schváleným kódexom správania. Namiesto podmienok certifikačnej schémy Safe Harbour pre US podniky máme vylepšený Privacy Shield a vznikla nová úprava, ktorá stanovuje podmienky pre Komisiu na vydávanie tzv.

adequacy decision, ktorými sa určuje status tretej krajiny s primeranou úrovne ochrany osobných údajov, kam nie je potrebné riešiť osobitné záruky.

.....

5. Zaznelo tu, že osobné údaje dokážu identifikovať iba dátoví analytici po detailnej analýze. Ako ich teda posúdi kontrolný orgán?

ZIMEN Ondrej: Vždy v kontexte konkrétnej individuálnej právnej veci, ktorá bude predmetom príslušného právneho konania. Aktuálne v slovenskej praxi prebieha drvivá väčšina kontrol vykonávaných dozorným orgánom v kontexte úzko vymedzeného predmetu a účelu kontroly zameraného na časť procesov nie úplne na všetko. Riziko, že v rôznom kontexte, variabilite rôznych spracovateľských operácii a interakcii rôznych datasetov vzniknú nové osobné údaje nie je možné nikdy úplne vylúčiť. Ak dozorné orgány kontrolujú bežných prevádzkovateľov a nie Big data analytiku sústreďujú sa na dáta, ktoré sú bežne konvenčne chápané ako osobné údaje. Primárne na personalizované a personalizovateľné klientske dáta a zamestnanecké dáta - i.e. to čo do podnikov tečie cez zmluvnú agendu, registračné formuláre, kamery, RFID terminály apod. Na tieto dve základné skupiny dát je potrebné primárne zamerať pozornosť a compliance úsilie.

Ivan Makatura: Budme k sebe úpriní: Úrad v tejto chvíli nemá dostatočnú kvalifikáciu na podobný typ analýzy. Okem toho - nejestvuje žiadna formálna metrika na stanovenie úrovne rizík. Preto otázka, ako riziká posúdi kontrolný orgán, by mala byť smerovaná na predstaviteľov Úradu na ochranu osobných údajov. Ja si v súčasnej situácii neviem predstaviť ,ako bude Úrad vykonávať kontrolné činnosti na dostatočne odbornej úrovni.

Tatiana Valentová: Úrad sa už dlhšie pripravuje aj na takéto špecifické podmienky výkonu kontroly. Buduje odborne zdatný a kvalifikovaný personál a tiež dopĺňa materiálne a technické vybavenie. Už dnes vykonávame kontroly, ktoré rozhodne nie sú len o kontrolách ľahko dostupných dát na úrovni jednoduchých základných identifikátorov dotknutých osôb. Podmienky výkonu kontroly striktne zodpovedajú a budú zodpovedať zákonným požiadavkám. Dávam do pozornosti povinnosť prevádzkovateľa poskytnúť súčinnosť pri výkone kontroly.

.....

6. Spoločnosti, ktoré svoj biznis riadia podľa správania sa jej klientov a účel spracovania OÚ je pre nich kľúčový a trvá, musia sa OÚ zbaviť ihneď po spracovaní?

Berthoty Jakub: Urcite mate viac ucelov spracovania, nie len jeden. Pri kazdom ucele je potrebne skumat, ci osobitne predpisy nevyzaduju uchovavanie udajov po urcitu dobu (napr. uchovavanie uctovnej dokumentacie). Je vhodne sa zamysliet aj nad zakonom o archivoch a registraturach, ci vam neumožnuje osobne udaje spracovat este dlhsie za ucelom spravy registratury alebo archivacie.

Tatiana Valentová: Nerozumiem celkom otázke. Budem predpokladať, že spracúvanie osobných údajov klientov – sledovanie ich správania – je zákonné, teda prebieha na

základe jasne a zrozumiteľne definovaného účelu spracúvania osobných údajov, na relevantnom právnom základe (napr. súhlas alebo oprávnený záujem prevádzkovateľa). Na také spracúvanie bude naviazané splnenie informačnej povinnosti voči osobám, o ktorých sú osobné údaje spracúvané a nastavenie mechanizmov na zaručenie práv dotknutých osôb a bezpečnosti spracovaných údajov. Lehota spracúvania a následného uchovávanía musí zodpovedať stanovenému účelu – musí byť primeraná. Po skončení účelu spracúvania, je prevádzkovateľ povinný osobné údaje likvidovať, samozrejme ak neexistuje iný relevantný účel na ich následné uchovávanie (napr. uchovávanie účtovných dokladov, existencia možnosti následného uplatnenia práv fyzickej osoby a pod.).

.....

7. Aký bude vzťah spracovaného už existujúceho bezpečnostného projektu a zavedenia GDPR? Zostáva bezpečnostný projekt naďalej v platnosti?

Berthoty Jakub: GDPR nepozná bezpečnostný projekt - takže nejde o vyslovnu povinnosť. Niektoré časti bezpečnostných projektov (riziková analýza) však môžu byť relevantné pre tzv. posúdenie vplyvu alebo posudzovanie rizika pri bezp. incidentoch. Navrhujem počkať si na vzorové situácie, ktoré budú spadať pod posudzovanie vplyvu, ktoré by mal zverejniť Úrad.

ZIMEN Ondrej: Bezpečnostný projekt možno do značnej miery vnímať ako internú politiku pôsobiacu na ochranu osobných údajov. Ak nejde vyslovene o formálny low budget draft, ale ide o dokument rešpektujúci relevantné ISO normy a reálne aplikovateľné procesy vo firme, tak viacero jeho častí sa dá racionálne použiť pri compliance práci na GDPR konverzii právno-bezpečnostnej dokumentácie (napr. bezpečnostné smernice, popis okolia informačných systémov, analýza bezpečnosti, klasifikácia informácií a informačných aktív apod.)

Ivan Makatura: Napriek snahe zamestnávateľských zväzov, podľa vyjadrenia ÚOOÚ nebude v novom zákone žiadnym spôsobom upravené, akým spôsobom budú vnímané doterajšie bezpečnostné projekty spracované v zmysle zákona 122/2013. Preto by som odporúčal zabudnúť na pôvodné bezpečnostné projekty.

Kedy sa však pýtate na to, či bude potrebná akákoľvek bezpečnostná dokumentácia, dovoľte niekoľko citácií z GDPR:

Na to, aby mohol prevádzkovateľ preukázať súlad s Nariadením, by mal prijať interné pravidlá a prijať opatrenia, ktoré budú predovšetkým spĺňať zásady špecificky navrhutej ochrany údajov a štandardnej ochrany údajov.

Prevádzkovateľ mal pred spracúvaním vykonať posúdenie vplyvu na ochranu údajov, aby posúdil osobitnú pravdepodobnosť a závažnosť vysokého rizika, pričom zohľadní povahu, rozsah, kontext a účely spracúvania a zdroje rizika. Uvedené posúdenie vplyvu by malo zahŕňať najmä plánované opatrenia, záruky a mechanizmy na zmiernenie daného rizika, na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením.

Prevádzkovateľ pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie.

Riadit' sa súčasnou právnou úpravou podľa zákona 122/2013 bude možné ešte niekoľko mesiacov. Potom bude platiť vyššie uvedené. A netreba si mýliť názvoslovie. Bezpečnostný projekt tak, ako ho poznal zákon 122/2013 podľa GDPR skutočne nie je požadovaný. Ale interné pravidlá, dokumentácia opatrení, plánované opatrenia – to sú všetko určité typy dokumentácií, ktoré sú v konečnom dôsledku komplexnejšie, než bol Bezpečnostný projekt podľa Zákona 122/2013.

.....

8. Ako by asi vyzeralo posúdenie costs/benefits GDPR legislatívy pre európske firmy a ich konkurencieschopnosť voči US, Ázii a zvyšku sveta?

Berthoty Jakub: Ak chcú US a Ázijské firmy pracovať s Európou, musia tiež riešiť GDPR. Ak by sme sa pozreli na idealisticky príklad firmy, ktorá má zabezpečený úplný súlad s GDPR, jej konkurenčná výhoda je, že má 'poriadok v dátach', čo je koniec-koncov lepší predpoklad pre ďalšiu dátovú analýzu. Da sa najst' aj iný business zmysel GDPR - orientácia na zákazníka alebo PR konkurenčná výhoda.

.....

9. Právo na zabudnutie: je definované, ako rýchlo musia byť údaje zmazané? Može to byť v priebehu niekoľkých dní?

ZIMEN Ondrej: Checknite si článok 12 ods. 3 GDPR - i.e. bez zbytočného odkladu a v každom prípade najneskôr do 1 mesiaca od doručenia žiadosti dotknutej osoby

Ivan Makatura: GDPR prichádza z požiadavkou minimalizácie spracúvania OÚ. Pokiaľ zanikne účel na spracúvanie OÚ, osobné údaje je potrebné odstrániť, bez zbytočného odkladu.

.....

10. V bežnej situácii, kedy je prevádzka informacného systému outsourcovaná do IT firmy, aké je postavenie takejto IT firmy vo vzťahu k "vlastníkovi" IS?

Berthoty Jakub: pravdepodobne pôjde o sprostredkovateľa (data processor) - ak bude táto firma spracovávať nejaké osobné údaje v mene vlastníka. Vždy je vhodné zamyslieť sa aj nad tým, či táto firma neplánuje využívať osobné údaje aj na svoje vlastné účely - potom by bola v postavení prevádzkovateľa.

ZIMEN Ondrej: Ak IT support nevykonáva žiadne spracovateľské dáta v mene klienta - prevádzkovateľa (controller) napr. záloha, testovanie, uchovávanie na vlastnom serveri, ale iba napr. cez remote access poskytuje technický support a aktualizácie za účelom funkčnosti a spoľahlivosti systému pôjde o tretiu stranu a nie sprostredkovateľa (data processor). Podľa môjho názoru je potom ok bežná NDA/SLA a nie je potrebné riešiť osobitné regulačné požiadavky na obsah kontraktu v zmysle článku 28 ods. 3 GDPR.

NAGY Zoltán: Len doplním, že v prípade, ak IT firma vykonáva pre zákazníka určité spracovateľské operácie s osobnými údajmi (napr. už spomenuté uchovávanie údajov na vlastnom serveri), a teda je v postavení sprostredkovateľa, musí byť medzi zákazníkom (prevádzkovateľom) a IT firmou (sprostredkovateľom) uzatvorená okrem SLA aj písomná zmluva (prípustná je aj elektronická forma) s presne vymedzenými náležitosťami podľa čl. 28 GDPR.

.....

11. Ak bude firma v sulade s novym zakonom o ochrane osobnych udajov (novym) bude aj v sulade s gdpr?

NAGY Zoltán: Na organizácie v EÚ sa primárne aplikujú ustanovenia GDPR, ktoré majú aplikačnú prednosť pred vnútroštátnymi zákonmi. Vo všeobecnosti je tak potrebné zabezpečiť súlad priamo s ustanoveniami GDPR a ďalej s ustanoveniami pripravovaného zákona, ktoré upravujú osobitné situácie spracúvanie (ide o štvrtú časť pripravovaného zákona).

.....

12. posunutie terminu GDPR nie je o nepripravenosti subjektov, ale o nepripravenosti statu. Preto nie je schvaleny zakon a predpisy?

Irena Hudecová: Zákon predstavuje vo vzťahu k GDPR len doplnkovú úpravu v oblastiach, v ktorých Nariadenie členské štáty oprávňuje na jej prijatie. Snahou Úradu na ochranu osobných údajov SR je prijatie nového zákona v čo najväčšom časovom predstihu. Ak pôjde legislatívny proces hladko, predpokladá sa schválenie zákona v januári, najneskôr vo február 2018. Prijatie ostatných všeobecne záväzných predpisov, ktoré vydá Úrad je závislé od prijatia a znenia samotného zákona.

.....

13. v ramci GDPR GAP analyzii nam bolo odporucene nasadiť sifrovanie. Odporucate ist touto cestou ?

Berthoty Jakub: ano, vo všeobecnosti odporúčame. Otázka skor je, čo konkrétne vám bolo odporúčané sifrovať a na základe čoho. GDPR neodpovedá na tieto otázky, ktoré si musíte zodpovedať v spolupráci s IT a právny poradcom. Čo by bolo vo Vasom prípade primerané je vždy o okolnostiach konkrétneho prípadu.

ZIMEN Ondrej: Súhlas s Jakubom. GDPR výrazne povzbudzuje regulované subjekty nasadzovať pseudonymizáciu (i.e. aj šifrovanie) všestranne. Treba používať ratio a aplikovať to na základe klasifikácie aktív tam, kde to je ľahké a nest'ážuje to procesy (napr. full disk encryption na cloudovom úložisku alebo SSL komunikačný protokol) alebo tam kde to je nevyhnutné z hľadiska citlivosti a bezpečnosti spracovateľskej operácie (napr. zabezpečený súbor s výpisom z bankového účtu zasielaný na email

klienta, či vynášanie a prenos určených dát na prenosnom médiu napr. USB z chránených priestorov firmy niekde mimo).

NAGY Zoltán: Súhlasím. Súčasne je však potrebné mať na pamäti, že aj po zabezpečení ochrany osobných údajov šifrovaním či pseudonymizáciou, majú tieto dáta naďalej povahu osobných údajov (nepôjde teda o anonymizované údaje), a preto je potrebné aj po zašifrovaní údajov zabezpečiť splnenie ostatných relevantných povinností GDPR.

Ivan Makatura: GDPR vám neodporúča implementáciu žiadnych konkrétnych opatrení na riziká. Nechajte si vykonať analýzu rizík od nezávislej, odborne spôsobilej osoby a následne sa budete môcť (opäť v spolupráci s odborníkmi) rozhodnúť, aké opatrenia na ochranu osobných údajov budete implementovať. Z môjho pohľadu sa šifrovanie ako odporúčanie v GDPR vôbec nemalo vyskytnúť, pretože to zachádza do roviny, ktorá je závislá od konkrétneho prostredia a architektúry. Legislatívna naivita.

.....

14. Ako sa bude uplatňovať GDPR v prípade predaja dát medzi právnymi subjektmi .

Berthoty Jakub: Na 'predaj' dát je potrebné najst osobitný právny základ. V princípe je možné hovoriť o súhlase alebo opravných zaujmoch.

.....

15. aký je dopad ePrivacy na statne weby?

Ivan Makatura: **Otázka na Prevádzkovateľov**

.....

16. Co v pripade ze nezistim unik alebo narusenie ochrany osobnych udajov a tym padom to nenahlasim

ZIMEN Ondrej: Modlite sa, aby to nezistili dotknute osoby a dozorný organ.

Ivan Makatura: aj samotné GDPR v tejto požiadavke tápa v neznámom. Princípy manažmentu incidentov autori GDPR celkom zjavne nepochopili. Je totiž veľmi problematické definovať presný čas, kedy nastali prvé malígne aktivity, ktoré by bolo možné vyhlásiť za incident – a najmä stanoviť, kedy v priebehu incidentu došlo ku porušeniu práv na ochranu osobných údajov. Odporúčam riešiť túto otázku z nezávislými, odborne spôsobilými osobami, ktoré majú reálnu skúsenosť s riešením bezpečnostných incidentov. (Advokátske kancelárie to však pri všetkej úcte nie sú...)

Tatiana Valentová:

Ak nezistíte porušenie ochrany osobných údajov s dopadom na práva fyzických osôb, nie ste povinný takýto bezpečnostný incident hlásiť úradu. Uvedené však predpokladá dôsledný manažment rizík, nastavené mechanizmy, na základe ktorých budete schopný posúdiť, či daný bezpečnostný incident je porušením ochrany

osobných údajov a zároveň povedie k rizikám pre práva a slobody fyzických osôb. Až po tejto identifikácii začne plynúť lehota na nahlásenie porušenia úradu (ak bolo vyhodnotenie pozitívne).

.....

17. Ak su osobne udaje tiež kamerovy zaznam, co s datami napríklad pri kamerovom systéme v aute?

ZIMEN Ondrej: Ak to robíte ako súkromná osoba - občan jednotlivec výlučne pre svoju osobnú potrebu napr. preukazovanie priebehu vlastnej poistnej udalosti alebo vlastného priestupkového konania je to úplne mimo aktuálnej i budúcej GDPR regulácie spracúvania osobných údajov. Ide o tzv. house-hold exemption. Určite však takéto záznamy nikdy nezverejňujte, ak sú tam identifikovateľní ľudia to by z Vás spravilo prevádzkovateľa. Je tiež vhodné dodať, že aktuálne sa právne názory dozorných orgánov na využívanie autokamier značne a podstatne líšia. Náš úrad k tejto veci zverejnil metodické usmernenie dostupné na jeho webe.

.....

18. Tyka sa gdprv plnom rozsahu aj neziskovych organizacii a zdruzeni? Predpoklada sa kontrola aj takychto institucii?

ZIMEN Ondrej: Áno GDPR sa nevyhnute dotkne aj tohto typu subjektov. Neplanovanu mimoriadnu kontrolu na základe podnetu alebo kvalifikovaného podania, resp. sťažnosti dotknutej osoby nikdy nie je možné úplne vylúčiť.

Tatiana Valentová: Doplním, výnimky z pôsobnosti GDPR sú definované v čl. 2 ods. 2 nariadenia.

.....

19. V prípade ak je osobny udaj suborom dat a vykona sa anonymizacia (odnatie casti z tychto dat) zostane tento subor dat osobnym udajom?

Berthoty Jakub: Tak ako to popisujete, nepojde o anonymizáciu, takže s pravdepodobne ano zostane.

ZIMEN Ondrej: Otázne je či tu oddelenu časť dát, ktorá bude podrobená anonymizácii (trvalá ireverzibilita) budú tvoriť identifikátory bez ktorých tie dáta už neumožnia identifikáciu konkrétneho človeka. Ak áno pôjde o anonymizáciu, ak nie pôjde o pseudonymizáciu, pretože oddelené súbory po ich spojení s ďalšími súbormi údajov vytvoria zas osobný údaj. Pseudonymizované údaje sú v zmysle GDPR považované za osobné údaje, aj keď môžu byť na prvý pohľad nečitateľné z hľadiska možnosti určenia identity konkrétneho človeka.

Tatiana Valentová:

O anonymizácii môžeme hovoriť výlučne v prípade, ak prevádzkovateľ údaje upraví takým spôsobom, že ich nikdy nebude možné priradiť k ďalším dátam, na základe

ktorých je možné dotknutú osobu identifikovať (osoba na základe nich nikdy nebude identifikovaná alebo identifikovateľná).

V prípade, že dáta budú od osobných údajov „len“ oddelené a bude ich možné v prípade potreby opätovne priradiť k fyzickej osobe, pôjde o pseudonymizáciu.

.....

20. Budu sa považovať za anonymizované prípady, keď v danom IT systéme dojde k prepisaniu osobných údajov, ale umelý identifikátor zaznamu o osobe zostane zachovaný?

Berthoty Jakub: Nie, toto je pseudonymizácia. Stále pôjde o osobné údaje.

NAGY Zoltán: Pseudonymizácia prevádzkovateľovi pomáha pri plnení jednotlivých povinností vyplývajúcich z GDPR, nemá však za následok vyňatie týchto osobných údajov spod pôsobnosti GDPR. Zásadný rozdiel medzi pseudonymizáciou a anonymizáciou spočíva v tom, že anonymizácia údajov musí byť trvalá nezvratná. Inými slovami tak z anonymizovaných údajov nemožno identifikovať konkrétnu fyzickú osobu, ktorej údaje patria, a to ani v prípade spojenia týchto údajov s inými údajmi, ktoré má prevádzkovateľ k dispozícii.

.....

21. otázka na p. Hudecovu ..poznáte princíp jedenkrát a dost? ak áno nebolo by vhodné sa pri oznamovaní incidentov vhodne abstrahovať ho do návrhu zákona?

Irena Udecová: návrh zákona upravuje oznámenie incidentov (oznámenie porušenia ochrany osobných údajov úradu) len vo vzťahu k spracúvaniu, ktoré nespadá do pôsobnosti GDPR. Aby nebola v SR odlišná úprava pre spracúvanie, ktoré spadá do pôsobnosti GDPR a spracúvanie, ktoré do pôsobnosti GDPR nespadá a na ktoré sa teda bude aplikovať nový zákon o ochrane osobných údajov, nový zákon preklopil povinnosť oznamovania incidentov 1:1 v súlade s GDPR. Spoločnú úpravu oznamovania incidentov bolo potrebné riešiť v procese prijímania samotného GDPR.

.....

22. V akom stadiu je vypracovanie kodexov na ktoré sa odvoláva článok 40? Mali by ich vypracovať členské štáty.

Berthoty Jakub: Nie, kodexy môžu - nemusia - vypracovať asociácie a združenia zastresujúce subjekty z určitého segmentu. Nejde o povinnosť.

23. Čo v prípade keď poskytovateľ cloudovej služby nie je viazaný právom EÚ?

Berthoty Jakub: sprostredkovateľ primárne vždy spracováva osobné údaje podľa práva prevádzkovateľa. Ak nie je z EÚ, mali by ste riešiť cezhraničný prenos, pričom jeho inštitúty zabezpečujú to isté na zmluvnej báze (napr. štandardné zmluvné doložky).

NAGY Zoltán: Ak sa zákazník (prevádzkovateľ) rozhodol outsourcovať spracúvanie osobných údajov na poskytovateľa cloudu (sprostredkovateľa), zákazník v prvom rade zodpovedá podľa čl. 28 ods. 1 GDPR za voľbu *vhodného sprostredkovateľa* – poveriť spracúvaním osobných údajov tak možno len sprostredkovateľa (napr. poskytovateľa cloudu), ktorý poskytol dostatočné záruky na to, že má implementované primerané technické a organizačné opatrenia tak, aby spracúvanie, ktoré vykonáva, spĺňalo požiadavky GDPR a aby sa zabezpečila ochrana práv dotknutej osoby. Následne musí byť medzi zákazníkom a poskytovateľom cloudu uzatvorená písomná zmluva, obsahujúca jednotlivé náležitosti vymedzené v ustanovení čl. 28 ods. 3 GDPR.

To znamená, že prostredníctvom zákazníka (prevádzkovateľa) sa relevantné ustanovenia GDPR budú vzťahovať aj na poskytovateľa cloudu, poskytujúceho svoje služby zákazníkovi v pôsobnosti práva EÚ.

Tatiana Valentová:

Ak prevádzkovateľ využíva služby subjektu, ktorý nie je v pôsobnosti GDPR a nového zákona o ochrane osobných údajov, postupuje podľa ustanovení pre prenos do tretích krajín (rozhodnutie o primeranosti, primerané záruky, vnútropodnikové pravidlá a pod.)

.....

24. V akej štruktúre a v akom detaile má byť odpoveď na dotaz osoby, aké údaje o nej máme (právo na prístup)?

ZIMEN Ondrej: Toto je vždy vhodné nastaviť individuálne, a to aj s ohľadom na povinnosť chrániť práva a slobody iných dotknutých osôb, ktoré by mohli byť dotknuté pri realizácii tohto práva v časti týkajúcej sa poskytovania kópií spracúvaných osobných údajov. Dôležitá je úprimná snaha, deklarovanie potvrdenia o tom, že údaje sú spracúvané v presne stanovenom rozsahu a poskytnutie regulačných informácií, ktoré ste aj tak povinný dotknutej osobe dávať už pri získavaní osobných údajov. Odkaz na dobrú Privacy Policy na webe môže tiež pomôcť.

.....

25. aký je rozdiel v dopadoch na procesy spracovania údajov orgánmi verejnej moci a beznou právnickou osobou?

ZIMEN Ondrej: To je dosť analytická otázka a veľmi všeobecná otázka. Orgány verejnej moci by mali vždy spracovávať osobné údaje občanov iba na základe zákonov s poukazom na ústavu iba v rozsahu a spôsobom stanoveným zákonom. Zakony by mali byť tvorené s ohľadom na základné právo na ochranu súkromia a rodinného života občanov...Základný

.....

26. Ake su konkretne opatrenia, ku ktorym moze firma pristupit a v ktorých prípadoch sa odporuca použiť ktore (pseudonymizacia, sifrovanie...)

ZIMEN Ondrej: Toto je predmetom individualneho riešenia zohľadňujúceho prostredie, procesy, citlivosť dát, zavaznosť a pravdepodobnosť rizika pre práva a slobody dotknutých osôb apod. Vo všeobecnosti je potrebné zachovať zdravý rozum a cieľavedome sa usilovať dosiahnuť primeranú bezpečnosť dát bez toho, aby Vás to zruinovalo finančne alebo to vytvorilo neumernú ťažko dodržiavateľnú procesno-administratívnu záťaž či znefunkčnilo využívané biznis modely.

.....

27. Je potrebné riešiť anonymizáciu operatívnych údajov aj v prípade, že pri spracovávaní len prechádzajú technologickou platformou, ale nie sú fyzicky ukladané?

Ivan Makatura: Táto otázka je závislá na výsledkoch analýzy rizík. Nie je možné zo všeobecne položenej otázky stanoviť, či na OÚ pôsobia riziká v jednotlivých podprocesoch (získavanie ukladanie, prenos, proces, entita).

.....

28. K akej interpretácii požiadavky na datovú minimalizáciu sa prikláňa UOOU? Je zmazanie údajov jediným spôsobom ako naplniť požiadavku GDPR po uplynutí účelu?

Tatiana Valentová:

Po uplynutí účelu spracúvania osobných údajov, ak neexistuje iný zákonný dôvod na ich ďalšie spracúvanie (napr. na základe tzv. privilegovaných právnych základov – archivácia) je prevádzkovateľ povinný tieto likvidovať. Ak ste mali na mysli napr. ich anonymizáciu, tak v takom prípade anonymizované údaje už nie sú osobnými údajmi a teda sa na ne nevzťahuje zákon/GDPR (samozrejme za splnenia podmienok anonymizácie).

.....

29. Nie je lacnejšie usporiadať referendum EU o zrušení GDPR a rozpustení úradov?

Ivan Makatura: Vzhľadom na odhadované náklady protiopatrení by to zrejme bola lacnejšia alternatíva. ☺ Ale nebrala by do úvahy realitu súčasných rizík spracúvania informačných aktív.

.....

30. Poskytujete službu, napríklad depozitu cennosti, Vy data po case vymazete. Klient však príde s originalom a pýta sa: "Kde mám svoje cennosti?" Co s tým?

Berthoty Jakub: Ak ma na to klient pravo, tak potom to pravo musi od niekoho vyplývať (zakon alebo zmluva). Ak to tak je, potom by ste nemali mazat ani vy, az do kym toto pravo klient nema. Opat ide len o jeden ucel, mozno ich mate viac a je potrebne k nim pristupovat odbobne.

.....

31. Rodne cislo nemoze byt povazovane za vseobecny identifikator, pretoze obsahuje navyse udaje o veku a pohlavi.

Irena Hudecová: skutočnosť, že rodné číslo obsahuje údaje o veku a pohlaví osoby nevylučuje, aby sa považoval za všeobecný identifikátor.

.....

32. Môže eshop výmenou za súhlas so sprac. OU + získaním OU návštevníkom ponúknuť zákazníkom / návštevníkom zľavy, členstvo, kupóny či iné výhody?

Berthoty Jakub: Moze a podľa mojho osobneho nazoru je to buducnost marketingovych dat.

NAGY Zoltán: Súhlasím, ide o pomerne štandardnú formu „motivovania“ zákazníka k udeleniu jeho súhlasu na spracúvanie osobných údajov výmenou za poskytnutie určitej zákaznickej výhody. Zákazník sa v takom prípade môže dobrovoľne rozhodnúť o udelení súhlasu so spracúvaním jeho osobných údajov na marketing výmenou za získanie výhody. Na druhej strane však treba dbať na to, že zákazníkovi nemožno odmietnuť poskytnutie samotnej služby len z toho dôvodu, že odmietol prevádzkovateľovi udeliť tento súhlas. Je preto potrebné rozlišovať medzi službou (napr. predaj tovaru v e-shope), ktorej poskytnutie nemožno podmieňovať udelením súhlasu a medzi poskytovaním určitej zákaznickej výhody (napr. zľavové kupóny).

.....

33. Stačí pri požiadavke na vymazanie údajov daný údaj označiť ako vymazaný? ved' aj klasické mazanie na filesystéme takto funguje, a to nestačí?!

????

.....

34. Udaje FO pre eshop (prevádz.) na marketing spracúvajú viacerí prevádzkovatelia. Ako má vyzerat' súhlas FO? Nutné spomenúť mena sprost. Alebo stačí všeob. Súhlas?

NAGY Zoltán: Jednou zo základných náležitostí súhlasu je aj to, že tento súhlas musí byť informovaný. Vo všeobecnosti tak prevádzkovateľ musí dotknutú osobu pri získavaní jej údajov informovať o katalógu informácií v rozsahu čl. 13 GDPR, a to v stručnej, transparentnej, zrozumiteľnej, jednoduchej a ľahko dostupnej forme. Podľa uvedenej úpravy by mal prevádzkovateľ dotknutú osobu informovať o všetkých

konkrétnych príjemcoch alebo aspoň o kategóriách príjemcov, ktorým budú osobné údaje poskytnuté (napr. o sprostredkovateľoch alebo o iných prevádzkovateľoch).