ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR

3. ročník | číslo 9 | duben 2021

Co s osobním spisem bývalého zaměstnance?

Po skončení pracovního poměru zbyde zaměstnavateli osobní spis plný osobních údajů. Které z nich musí okamžitě vymazat a které by měl naopak uchovat pro případ kontroly nebo soudního sporu? A jaké jsou lhůty pro uchování údajů?

Za trvání základního pracovněprávního vztahu zaměstnavatel jako správce zpracovává ve vztahu ke svým zaměstnancům řadu osobních údajů. Základním nástrojem pro jejich zpracování bývá **osobní spis**, který zaměstnavatelé vedou v listinné, elektronické či kombinované podobě a zakládají do něj dokumenty či soubory obsahující osobní údaje. Nabízí se tak otázka, jak zaměstnavatelé mají či mohou s obsahem osobního spisu naložit **po skončení pracovněprávního vztahu**.

Právo na výmaz

Z obecného nařízení o ochraně osobních údajů (GDPR) vyplývá, že jakmile pomine účel zpracování osobních údajů, **musí správce provést jejich likvidaci**. Subjekty, jejichž osobní údaje jsou zpracovávány, mají podle čl. 17 GDPR poté, co jejich osobní údaje přestanou být pro správce nadále potřebné vzhledem k účelům, pro něž byly shromážděny nebo jinak zpracovány, právo na to, aby **jejich údaje byly vymazány** (právo být zapomenut).

> **Při výmazu údajů končícího zaměstnance posuzujte každý údaj zvlášť**

Uvedené ovšem rozhodně nelze chápat tak, že by zaměstnavatel měl po skončení pracovněprávního vztahu celý osobní spis bývalého zaměstnance zlikvidovat. Určité údaje, respektive dokumenty, je zaměstnavatel oprávněn a jiné dokonce **povinen zpracovávat i nadále**. Je nutno vyjít z výše uvedeného východiska – to znamená u každého údaje nebo listiny posoudit, zda **existuje důvod pro další zpracovávání** (zpracování nadále zůstává účelné), nebo zaměstnavatel nemá povinnost tento údaj dále zpracovávat a současně není dán žádný jeho oprávněný zájem či jiný důvod pro další uchování. Při druhé z naznačených variant má zaměstnavatel sám od sebe, aniž by jej k tomu bývalý zaměstnanec musel vyzývat, **přistoupit k výmazu osobních údajů**.

Ochrana oprávněných zájmů

I po skončení pracovněprávního vztahu může zaměstnavatel zpracovávat údaje, které mohou být potřebné pro

PŘÍKLAD:
Zaměstnavatel za trvání pracovního poměru doručil zaměstnanci několik upozornění na možnost rozvázání pracovního poměru výpovědí v souvislosti s porušením povinnosti. Jedno vyhotovení upozornění zaměstnavatel založil do osobního spisu. Pracovní poměr byl poté rozvázán dohodou. Upozornění na možnost výpovědi už nemůže být zaměstnavatelem nijak použito, a tak pominul účel zpracování a zaměstnavatel je povinen tuto listinu zlikvidovat.

ochranu jeho právem chráněných zájmů. Nelze totiž například vyloučit **možnost vzniku právního sporu**, ať už mezi zaměstnavatelem a bývalým zaměstnancem, nebo mezi zaměstnavatelem a třetí osobou (zákazníkem, obchodním partnerem a podobně). V takovémto případném sporu může být pro zaměstnavatele značně důležité předložení určitých informací či údajů (například doložení toho, že zakázku pro určitého zákazníka zpracovával zaměstnanec, který k tomu byl řádně kvalifikovaný a proškolený). Uchování některých údajů vztahujících se k bývalým zaměstnancům může být důležité i **pro případ kontroly** ze strany některého kontrolního orgánu.

Obecná promlčecí lhůta trvá podle občanského zákoníku tři roky. Zaměstnavatelé jsou proto oprávněni uschovat osobní údaje, které by mohly být významné v případném právním sporu (může jít mimo jiné i o podklady pro hodnocení a odměňování zaměstnance pro případ, že by se domáhal zaplacení nějaké části mzdy, na kterou mu podle jeho názoru vzniklo právo), a to **po dobu případně i o něco přesahující tři roky** (pro případ, že by žaloba byla podána těsně před uplynutím promlčecí doby a určitou dobu by trvalo, než by byl zaměstnavatel coby žalovaný s touto skutečností seznámen).

Údaje důležité pro ochranu oprávněných zájmů můžete uchovávat 3 roky po propuštění

Povinné uschování údajů

Povinnost archivovat určité dokumenty zaměstnavateli přímo **ukládají některé právní předpisy**. V těchto případech samozřejmě zaměstnavatel nemůže při skončení pracovněprávního vztahu dané dokumenty zlikvidovat. Je-li uschování určitých listin či informací předepsáno zákonem, pak jejich další **zpracování odpovídající povinnostem** zaměstnavatele nemůže odporovat úpravě v GDPR.

Konkrétně **zákon o organizaci a provádění sociálního zabezpečení** stanovuje zaměstnavatelům například povinnost uchovávat:

- **stejnopisy evidenčních listů** vyhotovených v kalendářním roce, kterého se týkají, nebo v bezprostředně následujícím kalendářním roce po dobu tří kalendářních let po roce, kterého se týkají, a stejnopisy ostatních evidenčních listů po dobu tří kalendářních let po roce, v němž byly vyhotoveny,
- záznamy o skutečnostech vedených v **evidenci o občanech pro účely důchodového pojištění**, a to po dobu 10 kalendářních let po roce, kterého se týkají,

- **mzdové listy nebo účetní záznamy** o údajích potřebných pro účely důchodového pojištění (zejména doklady o druhu, vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a o nemocech z povolání a záznamy o evidenci pracovní doby včetně doby pracovního volna bez náhrady příjmu), a to po dobu dobu 30 kalendářních let následujících po roce, kterého se týkají, a jde-li o mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění vedené pro poživatele starobního důchodu, po dobu 10 kalendářních let následujících po roce, jehož se týkají.

Ze zákona o nemocenském pojištění plyne dále zaměstnavatelům povinnost uschovávat všechny záznamy o skutečnostech, které musí být obsahem jím vedené **evidence o zaměstnancích účastných nemocenského pojištění**, a to po dobu 10 kalendářních let po roce, kterého se týkají. Další archivační lhůty předepisuje například zákon o účetnictví nebo zákon o daních z příjmů.

Vzhledem k tomu, že povinnost uchovávat uvedené dokumenty předepisuje zaměstnavateli zákon, rozhodně od bývalých zaměstnanců v této souvislosti nemusí a **nemá vyžadovat udělení souhlasu**. ▪▪▪

JUDr. Jaroslav Stránský, Ph.D.

Používáním nástroje Mailchimp dochází k porušování GDPR

Bavorský dozorový úřad (*Bayerisches Landesamt für Datenschutzaufsicht*, zkráceně *BayLDA*) dospěl ve svém rozhodnutí sp. zn. LDA-1085.1-12159/20-IDV k závěru, že používání marketingového nástroje Mailchimp, který **umožňuje rozesílat newslettery** či jiné hromadné e-maily, není v souladu s požadavky GDPR na ochranu osobních údajů.

Provozovatelem služby Mailchimp je americká společnost The Rocket Science Group LLC. Při využívání předmětného nástroje je tudíž nutné brát v potaz skutečnost, že dochází **k předávání osobních údajů do USA** (e-mailové adresy odběratelů newsletterů či jiných hromadných e-mailů zasílaných pomocí předmětného marketingového nástroje jsou předávány do USA). Dozorový úřad BayLDA dospěl k závěru, že Mailchimp může být podle právních předpisů USA, konkrétně podle FISA702 (50 U.S.C. § 1881), kvalifikovaný jako **poskytovatel služeb elektronických komunikací**. To by znamenalo, že e-mailové adresy, na které jsou pomocí nástroje Mailchimp zasílány newslettery či jiné hromadné e-maily, mohou být zpřístupněny americkým zpravodajským službám.

Bavorský dozorový úřad vytýkal v případě řešeném pod sp. zn. LDA-1085.1-12159/20-IDV nejmenované společnosti, na niž byla podána stížnost a kvůli které se otázkou používání Mailchimpu zabýval, že výše uvedené skutečnosti nevzala v potaz a ve světle rozsudku Soudního dvora EU ze dne 16. července 2020 ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) nezhodnotila, zda je případně nutné (a vůbec možné) přijmout doplňující opatření, která by zajistila **soulad nástroje Mailchimp s požadavky GDPR** na ochranu osobních údajů. Nejmenovaná společnost se v daném případě vzdala používání předmětného marketingového nástroje, a to s okamžitou účinností. BayLDA z toho důvodu nepřistoupil k uložení pokuty.

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

ÚOOÚ za rok 2020 v číslech

Jaké trendy v ochraně osobních údajů odhalila výroční zpráva ÚOOÚ za rok 2020? Počet stížností klesá, ale zpřísňují se pokuty za neposkytnutí součinnosti. Na co si lidé nejčastěji stěžují? A na jaké oblasti se Úřad zaměří v roce 2021?

Úřad pro ochranu osobních údajů zveřejnil výroční zprávu za rok 2020. Pro nás se tím otevírá příležitost zjistit, jaké jsou trendy v ochraně osobních údajů, kolik lidí si stěžuje, co je předmětem stížností a mnoho dalšího. Tyto informace nám pomůžou lépe plánovat interní audity či se specificky zaměřovat na oblasti, u nichž víme, že na ně padá nejvíce stížností. Kromě pohledu do minulosti se podíváme také na oblasti, **na které se ÚOOÚ zaměří v tomto roce**.

Dotazy a konzultace

V rámci konzultační činnosti se v roce 2020 ÚOOÚ věnoval **celkem 1 751 písemným dotazům** a prostřednictvím GDPR linky jich vyřídil celkem 1 351. Počet písemných dotazů zůstává meziročně v podobném rozsahu (v roce 2019 bylo dotazů 1 836) a ÚOOÚ si pravděpodobně může oddychnout, že období roku 2018, kdy vešlo v účinnost GDPR a Úřad se musel vypořádat s celkem 4 161 dotazy, je definitivně pryč. Tento trend se pravděpodobně promítl i **do počtu volajících na GDPR linku**, neboť za rok 2020 je takřka poloviční oproti roku minulému (kdy telefon v ÚOOÚ zazvonil celkem 2 667x) a 3,5krát menší než počet hovorů za rok 2018 (tehdy to bylo 2 800 hovorů a dalších 1 900 na telefonní lince pro kamerový systém).

Otázkou je, zda z tohoto můžeme vyvodit, že podnikatelé jsou rok od roku zkušenější a **ochrana osobních údajů je brána již jako samozřejmost**, anebo naopak opadl jakýkoliv zájem podnikatelů tuto otázku vůbec řešit – to pravděpodobně zjistíme z informací týkajících se stížností a kontrol níže.

Co však vzbuzuje údiv, je celkový počet konzultací, které ÚOOÚ provedl v souvislosti s **povinnostmi správců ve vztahu k předchozím konzultacím** s ÚOOÚ dle čl. 36 GDPR. Pokud totiž správce při posuzování vlivu narazí na zpracování, jež by měla za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, je povinen takové zpracování před jeho zahájením konzultovat s ÚOOÚ. Stejně jako v minulém roce se i **letos toto stalo přesně nulakrát**, přičemž minimálně ve vztahu k „novým" technologiím, jež stát využívá pro boj se současnou pandemií (nikoliv ze zákonné povinnosti), ale i s ohledem na modernizaci některých procesů je to poměrně zajímavé zjištění.

> **Lidé si nejčastěji stěžují na obchodní sdělení a zveřejnění osobních údajů**

Podněty a stížnosti

Co nás ale zajímá nejvíce, je pochopitelně to, jak si minulý rok stál, co se týče přijatých podnětů. Zatímco v roce 2018 přijal ÚOOÚ celkem 3 616 podnětů, o rok později to bylo již jen 2 482. Tento **sestupný trend se projevil i v roce 2020**, neboť počet podnětů klesl poprvé od roku 2017 pod hranici dvou tisíc na **celkem 1 855 podnětů**. Ve stejné tendenci, ale nikoliv stejným poměrem, také klesl počet případů, kdy byl podnět předán ke kontrolnímu či jinému řízení, neboť zatímco v roce 2018 bylo takových podnětů předáno 193, v roce 2019 už to bylo 145 a **za rok 2020 celkem 125**. Ačkoliv tedy klesl celkový počet podnětů, na činnosti ÚOOÚ to prakticky nebylo poznat (k tomu viz níže).

Ohlášení porušení zabezpečení

Jak víme z předchozích článků Zpravodaje týkajících se kontrol ÚOOÚ, některé z nich byly zahájeny na základě **předchozího ohlášení o porušení zabezpečení** osobních údajů ve smyslu čl. 33 GDPR. Zatímco v roce 2018, kdy tato povinnost vstoupila v účinnost až téměř v polovině roku, obdržel ÚOOÚ těchto oznámení celkem 260, předminulý rok, kdy Úřad obdržel 416 ohlášení, byl rekordní. V minulém roce však nastal opět propad takových ohlášení na celkový počet 292.

Otázkou zůstává, nakolik to lze považovat za důkaz, že dochází k méně případům porušování zabezpečení (o čemž lze s ohledem na obrovský **meziroční nárust kybernetických útoků** v některých sektorech až o 40 % velmi pochybovat), nebo že správci neplní tuto svoji povinnost důsledně.

Kontrolní činnost

Nejzásadnějším údajem pro nás jsou data o kontrolní činnosti, a proto vás nebudeme napínat – za rok 2020 bylo **zahájeno celkem 54 kontrol**, což je o 9 méně než předchozí rok a o 22 mé-

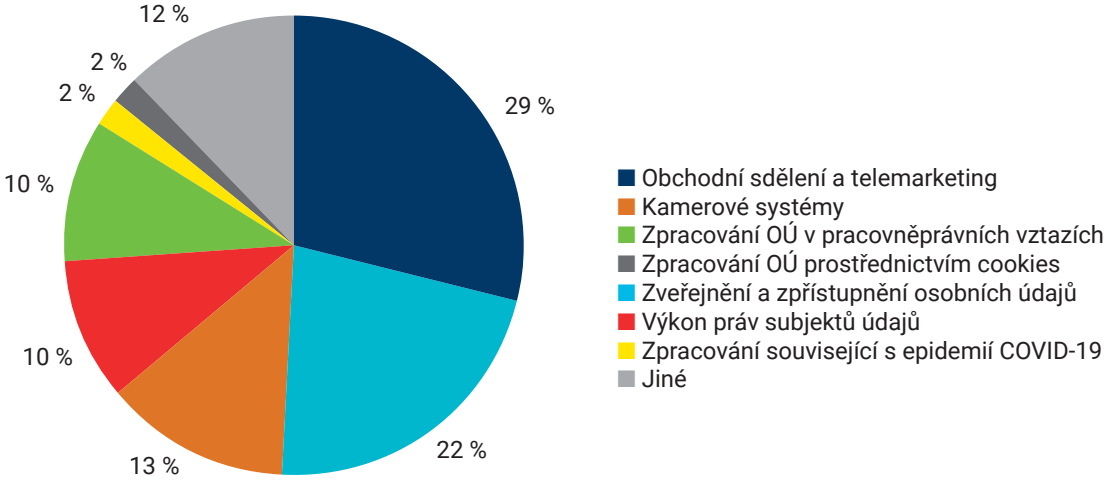
ně než za rok 2018. Stejně tak se letos podařilo ÚOOÚ **ukončit celkem 48 kontrol** (z toho 16 bylo z předchozích let). V roce 2019 se mu dařilo lépe, neboť bylo ukončeno celkem 75 kontrol (z toho 32 z předchozích let), a pochopitelně je to méně než za rok 2018 (ukončeno 89, z toho 36 bylo z předchozích let). Ačkoliv počet provedených kontrol mírně klesá, **zvyšuje se nekompromisní přístup ÚOOÚ** v případě, že kontrolovaný subjekt neposkytuje součinnost – v tomto roce totiž padlo již **pět pokut za neposkytnutí součinnosti** (v minulých letech se k tomu ÚOOÚ uchýlil pokaždé celkem čtyřikrát).

Obchodní sdělení

S příchodem pandemie a různých forem lockdownů se spousta firem s nadějí uchýlila k internetovému marketingu, a to zejména formou zasílání obchodních sdělení. Je proto zajímavé, jak se tento **trend přesunu do digitálního marketingu** projevil v počtu stížností. V roce 2018 obdržel ÚOOÚ celkem 2 901 stížností na obchodní sdělení (z čehož zahájil 22 kontrol), což navzdory silné medializaci s příchodem GDPR bylo jen o cca 200 stížností více než rok předcházející, a nadto o 900 méně než v roce 2016. Bylo to dokonce o 2 500 stížností méně než za rok 2015. Ostatně v roce 2014 a letech předcházejících ÚOOÚ obdržel standardně okolo 8 000 stížností – celkově se tedy projevil trend, že **těchto stížností skutečně ubývá**. Potvrzují to i čísla za rok 2019, kdy ÚOOÚ obdržel celkem 2 007 podnětů (z nichž zahájil pět kontrol).

Samozřejmě nám výše uvedená čísla bez kontextu spíše nepomohou, neboť neznáme statistiky, kolik bylo posláno obchodních sdělení, kolik z nich bylo v souladu se zákonem a kolik z nich trpělo jinými vadami. Jediné, co víme, je to, že za rok 2020 **obdržel ÚOOÚ celkem 3 031 podnětů**, z nichž **zahájil celkem 15 kontrol**, tedy trojnásobně více než za předchozí rok. Ostatně právě minulý rok

Na co si lidé nejčastěji stěžují



Zdroj: Výroční zpráva ÚOOÚ za rok 2020

ÚOOÚ udělil **rekordní pokutu ve výši šesti milionů korun** a předseda Úřadu k tomu v úvodu závěrečné zprávy dodal: *„Naším cílem je individuální, a především generální prevence. Nejen výše hrozící sankce, ale především její neodvratnost by měly pomoci kultivovat prostředí v této oblasti. Nevyžádaná obchodní sdělení přestanou být problémem v okamžiku, kdy se podstatné části těch, kteří je rozesílají, přestanou vyplácet.“* Z výše uvedeného nelze než vyčíst, že bychom si měli **dát na zasílání obchodních sdělení pozor.**

Jak pandemie zasahuje do činnosti ÚOOÚ

Klíčovou otázkou je, jak bude ÚOOÚ v rámci současné pandemie postupovat v této oblasti nadále. Co se týče prozatím nezveřejněného kontrolního plánu, Úřad se plánuje zaměřit na **věrnostní programy, zpracování v rámci doručovatelských služeb**, ale také zpracování ve vztahu k nabídce a prodeji zprostředkování energií, a to i co se týče telemarketingu, což je téma, které rezonovalo i ve výroční zprávě za rok 2020. Ostatně plánovaným kontrolám **neunikne ani šíření obchodních sdělení** prostřednictvím telefonních operátorů.

Přestože v rámci veřejného sektoru je vynucování pravomoci ÚOOÚ značně osekané, měli bychom si dát pozor na zveřejňování údajů na **elektronických úředních deskách** či u **městských kamerových systémů** – i sem zamíří pozornost ÚOOÚ. Obecně vzato lze ale předpokládat i další sérii kontrol v oblastech týkajících se zpracování osobních údajů v souvislosti s aktuální pandemií, a to nejen ve vztahu k rezervačnímu systému na očkování, ale i CovidPassu a podobně. Alespoň takto můžeme usuzovat z tiskových zpráv ÚOOÚ.

MINULÝ ROK ÚOOÚ:

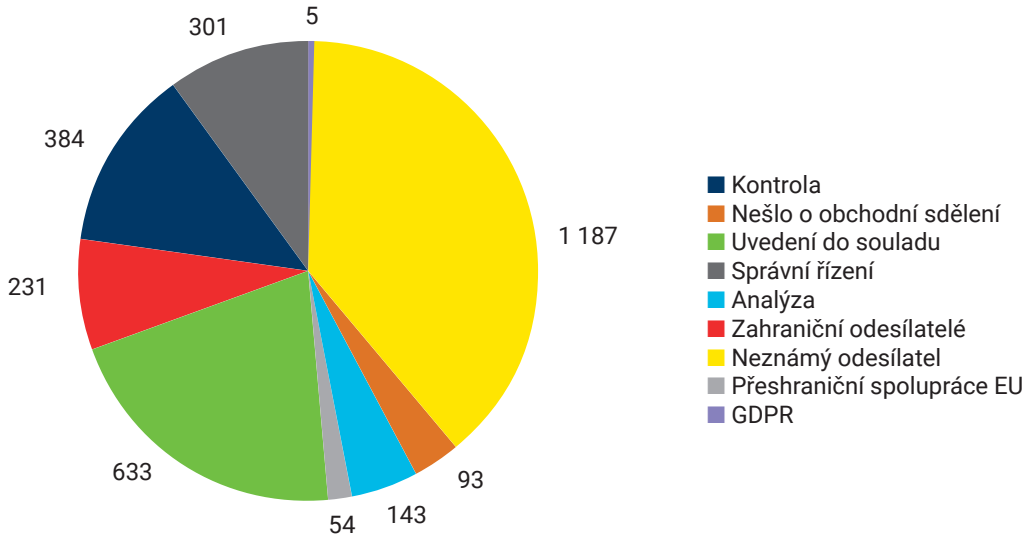
- **obdržel 1 751 písemných a 1 351 telefonických dotazů**
- **neposkytl žádnou konzultaci v souvislosti s povinností správce dle čl. 36 GDPR**
- **přijal 1 855 stížností, z nichž 125 předal k dalšímu kontrolnímu či jinému řízení**
- **obdržel 292 ohlášení o porušení zabezpečení osobních údajů**
- **zahájil 54 kontrol a 48 z nich ukončil**
- **udělil 5 pokut za neposkytnutí součinnosti kontrolovaným subjektem**
- **obdržel 3 031 stížností na obchodní sdělení, z čehož zahájil 15 kontrol**
- **udělil rekordní pokutu 6 milionů korun za nevyžádané obchodní sdělení**

Závěr

Počet stížností a kontrol klesá, v oblasti marketingu (zejména obchodních sdělení) je však trend spíše opačný. Do jisté míry to má svoji logiku – čím dál více jsme uzavřeni ve svých domovech a nakupujeme na internetu. Z daných čísel sice nelze přesně vyčíst, jak se tyto trendy budou vyvíjet do budoucna, nicméně i tak nám zmíněná data umožňují odhadnout, **na co si dát v rámci našich organizací pozor** a jakým oblastem se věnovat především. ■■■

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Podané stížnosti z oblasti obchodních sdělení a způsob jejich vyřízení



Zdroj: Výroční zpráva ÚOOÚ za rok 2020

Facebooku unikla data 500 milionů uživatelů

Ze služby Facebook unikla data o více než 500 milionech uživatelů na hackerská fóra – e-maily, telefonní čísla, data narození a další osobní údaje. Mezi postiženými je i milion Čechů. Jste mezi nimi i vy? A jak ochránit svá data?

Na začátku dubna se do světa rozletěla zpráva, která rezonovala snad všemi médii – **data o více než 500 milionech uživatelů Facebooku unikla** a jsou volně dostupná na hackerských fórech. V návaznosti na to doslova vystřelily titulky, z nichž byste jen velmi těžko pochopili, že se ve skutečnosti úplně nejednalo o hackerský útok, respektive o nabourání systému Facebooku. Facebook k tomu následně dodal své vyjádření a situace se trochu zklidnila, otázkou však je – oprávněně?

Informace k útoku

Jaká jsou tedy čísla? Zdroje hovoří o tom, že unikly údaje celkem 533 milionů uživatelů Facebooku, a to do srpna roku 2019, než byla daná chyba definitivně opravena. V předmětné databázi, která se šíří na hackerských fórech, jsou tak k mání údaje jako **e-mailové adresy, telefonní čísla, identifikátor uživatelů**, jména a příjmení, data narození a další informace. Už zde dlužno dodat, že předmětná data byla mnohdy „veřejně dostupná" kvůli zabezpečení soukromí profilů jednotlivými uživateli – k tomu však dále.

Co se týče rozsahu, dle odhadu **Lupa.cz** mohlo být unikem zasaženo něco mezi **třetinou až polovinou českých uživatelů** Facebooku v rozhodné době. **iRozhlas** doplňuje, že šlo o něco více než milion českých uživatelů.

Jak k úniku došlo

Ať už to nazveme útokem, či únikem, pravdou je, že za incidentem stojí s trochou nadsázky touha Facebooku rozšířit svoji síť co nejdál a mezi co nejvíce uživatelů. Pamatujete si na články z předchozích dílů Zpravodaje, kde jsme řešili **funkci tell-a-friend**? V tomto případě šlo prakticky o totéž: funkce spočívala v pomocníkovi pro vyhledávání přátel, kteří mají účet na Facebooku. Pokud jste zadali do vyhledávání telefonní číslo či e-mail svého kamaráda, sociální síť vám umožnila **ověřit si, zda kamarád má facebookový účet**.

Jenže tato funkce, určená lidem, **nebyla dostatečně zabezpečena** proti zneužívání pomocí automatizovaných systémů a právě tak mělo k úniku pravděpodobně dojít. Představte si, že máte v ruce super mobilní telefon, do nějž nahrajete několik tisíc telefonních čísel – třeba i jen těch, co vás prostě napadnou – a ty postupně zadáváte do vyhledávání na Facebooku. Pokud se číslo spojí s uživatelem, jehož nastavení profilu umožňovalo zobrazení daných informací, problém je na světě. Pak už totiž stačí tyto data stáhnout. Takto nějak daný únik mohl probíhat, a sice že **útočníci si nainstalovali emulátor** Android zařízení do svého počítače a pomocí něj postupně vytahovali předmětná data.

> **Uniklá data mohou být zneužita k prolomení dvoufázové autentifikace**

Pravděpodobné je, že předmětná databáze bude složena z několika různých úniků, které probíhaly již od roku 2018.

Je to problém?

Sám Facebook celou věc relativizuje tím, že se jedná o stará data a že předmětná bezpečnostní díra byla záplatovaná už v roce 2019. Ve spojení s informací, že ve většině případu se **jednalo o veřejně dostupné informace** z důvodu nastavení viditelnosti jednotlivých uživatelů, se tedy nabízí otázka – znamená to, že na tuto epizodu můžeme zapomenout? Pravděpodobně ne – předmětná databáze mnohdy obsahuje e-maily i telefonní čísla, a **umožňuje tak návaznou podvodnou činnost** či jiná nebezpečná jednání, jako je stalking.

Dle informací **iRozhlas** bylo v předmětné databázi například dva tisíce českých uživatelů, kteří uvádí jako svého zaměstnavatele **policii či ministerstva, úřady nebo soudy**. Tyto informace pak mohou sloužit i k podvrhování identit či phishingu.

Neméně problematický je právě únik telefonních čísel, která mohou být mnohdy využívána pro **účely dvoufázové autentifikace**. Zde se pak nástroj k zajištění bezpečnosti stává sám nebezpečný, a to kvůli útoku typu SIM swapping. Útočník totiž může

díky informacím, které má o subjektu k dispozici, kontaktovat například telefonního operátora a požádat ho o vystavení nové SIM karty. Jakmile ji obdrží, odpadne mu problém s dvoufázovou autentifikací, neboť pokud nějaká služba zasílá SMS kód pro ověření, obdrží jej rovnou útočník (to vše díky nové SIM kartě).

Přijde vám to nepravděpodobné? V tom případě si přečtěte, jak o svůj twitterový profil přišel sám CEO Twitteru (například **zde**). A co když se útočníkovi podaří rovnou **nabourat do databáze operátora** a všechna důležitá hesla pro správu zákaznického účtu si prostě odnese? Zdá se vám to také nemožné? Tak si přečtěte **oznámení** společnosti T-Mobile o porušení zabezpečení, které tato společnost vydala právě potom, co došlo k blíže neurčenému počtu SIM swapp podvodů.

Co tedy s tím?

Obecně první, co bychom měli udělat, je zjistit, zda je možné, že jsme součástí tohoto úniku. Díky **službě** Have I Been Pwned je to velmi jednoduché – stačí zadat e-mail či telefonní číslo a zjistíme, zda se naše osobní údaje neobjevily v souvislosti s únikem na internetu.

Zadat lze i pracovní e-maily zaměstnanců či firemní čísla, popřípadě i pomoci rodinným příslušníkům. Následně **zkontrolujeme své nastavení na sociálních sítích** – měli bychom co nejvíce omezit přístup mimo okruh přátel (samozřejmě nejbezpečnější nastavení účtu na sociální síti je tento účet smazat a nikdy si jej už nezaložit – to ovšem není úplně praktická rada).

To je základní minimum, co můžeme udělat – pochopitelně by bylo lepší, pokud bychom rovnou **vyměnili e-mail i telefonní číslo**, popřípadě alespoň pro účely dvoufázové autentifikace. V každém případě je dobré zachovat zdravou úroveň obezřetnosti a dát si pozor na to, komu svoje osobní údaje svěřujeme.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Poradna

Jaké vzdělání, osvědčení či akreditaci máme požadovat od pověřence osobních údajů, abychom měli zajištěno, že jde o kompetentní osobu znalou problematiky?

Vzdělání a vlastně celková způsobilost osoby vykonávat funkci pověřence byla i jedna z věcí, na kterou narážel ÚOOÚ v rámci jedné z kontrol (viz **článek**). Důvodem byla chybná právní kvalifikace ze stany pověřence, který ohlásil porušení zabezpečení ÚOOÚ, jež však porušením ve skutečnosti nebylo. ÚOOÚ doslova zapsal: *„Při výběru a jmenování pověřence pro ochranu osobních údajů dle čl. 37 obecného nařízení je nutno pamatovat nejen na to, aby tento byl jmenován na základě svých profesních kvalit, odborných znalostí práva a praxe v oblasti ochrany osobních údajů, ale také na základě schopnosti plnit úkoly stanovené čl. 39 obecného nařízení. Uvedené však musí být též podpořeno postavením pověřence pro ochranu osobních údajů ve smyslu čl. 38 obecného nařízení a správce či zpracovatel musí zajistit, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.“*

Byť tak GDPR výslovně podmínku vzdělání nepožaduje, přece jen v čl. 37 odst. 5 GDPR zmiňuje, že *„Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39.“* Ačkoliv tedy pověřenec nemusí mít právní vzdělání, měl by se v této problematice velmi dobře orientovat a pokud tyto

znalosti nemá, jde to k tíži správce (který jmenoval nekvalifikovaného pověřence). WP29 k tomu ve svých vodítkách k pověřencům na straně č. 13 doplňuje, *„že pověřenci pro ochranu osobních údajů musí mít odborné znalosti v oblasti vnitrostátní a evropské praxe a právních předpisů na ochranu údajů a důkladně chápat obecné nařízení o ochraně osobních údajů“.*

Co se týče osvědčení či akreditací, ty jsou v dnešní době vydávány pouze na základě soukromého práva, přičemž jejich udělení může, ale nemusí garantovat, že daný pověřenec splňuje odborné a kvalifikační předpoklady. Můžete tak narazit na skvělého pověřence, který nemá vysokoškolské vzdělání, a přesto se perfektně orientuje v dané problematice, ale také na pověřence s vysokoškolským vzděláním a všemožnou certifikací od soukromých subjektů, jehož odborné znalosti zůstanou v rovině předpokladů a nepodaří se je přetavit do praxe. Z těchto důvodu doporučujeme spíše než hledět na získané certifikáty, ověřit si dosažené vzdělání a znalosti pověřence důkladně otestovat. K tomu vám může velmi dobře posloužit jakýkoliv článek ze Zpravodaje, abyste si ověřili, zda daný pověřenec sleduje aktuální dění na poli ochrany osobních údajů a neodvozuje svoje profesní kvality od jednoho školení, které absolvoval v roce 2018 v rámci třídenního rychlokurzu.

Kde najdu shrnutí problematiky anonymizace údajů ve smlouvách v rámci registru a uveřejnění smluv?

Kromě článku ve Zpravodaji, který toto téma aktuálně připravujeme, lze vyjít alespoň z metodiky, kterou v minulosti připravovalo Ministerstvo vnitra (viz **zde**). Poněkud starší a kratší návod naleznete i na stránkách ÚOOÚ (viz **zde**). Na straně 55 metodiky pro veřejné subjekty je uvedena tabulka, v níž najdete jednotlivé typy údajů a způsob jejich anonymizace. V zásadě se lze těmito doporučeními řídit, aniž by došlo k porušení zákona.

V každém případě je však vhodné jednotlivé postupy anonymizace zapracovat do interní metodiky, která bude popisovat jednotlivé kroky v rámci uveřejnění smluv v registru smluv. Co se týče veřejných zakázek, předmětná legislativa je založena na stejné logice (ostatně zákon o registru smluv výslovně stanovuje, že v případě uveřejnění smlouvy v registru smluv je splněna i povinnost uveřejnit smlouvu dle zákona o zadávání veřejných zakázek), tudíž i v případě anonymizace daných údajů lze postupovat podle stejných pravidel.

JOSEF BÁTRLA ADVOKÁT

Nevíte si s něčím rady? Pošlete nám svůj dotaz a my vám zprostředkujeme odpověď! Dotazy pokládejte e-mailem na:
zpravodaj.poverenec@forum-media.cz

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM, s. r. o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Editorka: Anna Pěkná | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 Jazyková redakce: Bc. Vendula Pazderová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2 490 Kč bez DPH Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 20. 4. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.