Šéfka Úřadu pro ochranu osobních údajů: Vysokými pokutami chceme firmy odrazovat, ne likvidovat

Necelý rok zbývá firmám a státním institucím na to, aby se připravily na novou směrnici Evropské unie. Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR) říká, že pokud subjekt nakládá s osobními údaji, bude je nově muset chránit výrazně důsledněji. V opačném případě firmám hrozí až likvidační pokuty. *"Obecné nařízení ukládá, že pokuty musí být odrazující. Tím se budeme řídit,"* upřesňuje Ivana Janů, předsedkyně Úřadu pro ochranu osobních údajů. Ten bude dál plnit roli hlavního tuzemského regulátora.

*** Jak byste postupovala v pozici vedoucího firmy, který se o chystané novince dozví v těchto dnech a není na přizpůsobení se nové legislativě jakkoliv připraven?**

Pokud podnikatel plnil své povinnosti podle zákona o ochraně osobních údajů, tak mu nehrozí žádné revoluční hnutí v jeho podniku, do 25. května se stihne zorientovat a stihne učinit takové kroky, aby ho obecné nařízení nezaskočilo. Pokud neplnil povinnosti a neznal zákon o ochraně osobních údajů, tak je pro něj nejsnazším způsobem udělat revizi povinností podle stávajícího zákona, který je s GDPR hodně kompatibilní.

Nařízení je evropský předpis a je orientovaný jak na malé firmy, tak na gigantický průmysl, který shromažďuje big data, tedy enormní množství údajů o fyzických osobách, které již pro jejich velikost není možné spravovat a zpracovávat běžnými prostředky. Sankce a postihy ovšem musí být nastaveny jednotně na velké, střední a malé podniky. Kdo se řídil stávající právní úpravou a dosud o GDPR nevěděl, tak má akorát čas začít se připravovat.

***Směrnice je hodně obsáhlá, pro firmy jistě nebude snadné se v nových standardech rychle zorientovat. Na co by se měli podnikatelé v přípravě zaměřit především?**

Každý podnikatelský subjekt si musí ujasnit, jaká data se v jeho firmě zpracovávají. Musí si udělat analýzu – prověřit jak systémy, ve kterých se data zpracovávají, tak technologický způsob bezpečnostního servisu. Právě tato analýza by měla sloužit ke snadnějšímu zorientování se v přístupu k povinnostem, které se subjektu nevyhnou.

***Koho všeho se bude GDPR týkat, budou existovat výjimky?**

Postihne většinu všech subjektů, které nakládají s osobními údaji. Budou to všechny orgány státní moci, správy a samosprávy. Pokud jde o podniky, tak jsou to ty, v jejichž hlavní činnosti je systematické zpracovávání těchto údajů. Týká se to skoro každého. Vlastně úplně všech občanů, jde o vyšší bezpečnost našeho soukromí. Osmdesát procent občanů Evropské unie je nespokojeno se stavem, který v zabezpečení našich dat vládne.

***Třetina firem netuší, kolik času jim zabere příprava na novou legislativu, mnoho podniků o GDPR neví vůbec. Vyplynulo to průzkumu společností VMware a Trend Micro, kterého se zúčastnilo 150 českých a slovenských firem. Jak nebezpečné je pro podnikatele či státní instituce podcenění směrnice, jakým rizikům se vystavují?**

Pokud jde o státní instituce, tak ty už nespí a nesní. Koncem loňského roku jsme udělali akci. Upozornili jsme ministerstva a další klíčové úřady, že se 25. květen blíží a že Úřad je připraven

poskytnout základní vstupní informace o celém procesu. Podcenění může vést k vysokým pokutám, které mají být přímo z obecného nařízení odrazující, přičemž jejich limit je proti současnosti nastaven mnohonásobně výše.

***Jak přísně tedy bude váš Úřad zpočátku přistupovat k těm, kteří nová pravidla poruší?**

Nově budeme moci ukládat pokutu až do čtyř procent hrubého celosvětového obratu firmy nebo do dvaceti milionů eur. Obecné nařízení říká, že pokuty musí být odrazující. Tím se budeme řídit. Pokuty mohou být velmi velmi vysoké, doteď nebyly. Při výpočtu výše sankce se ale budou zvažovat stejné okolnosti jako dosud. Záleží na závažnosti porušení, na kontextu. Jakýkoliv únik dat musí podnik oznámit do tří dnů Úřadu, ale i postiženým fyzickým osobám.

Snaha o nápravu a okamžité ohlášení hraje velkou roli coby polehčující okolnost při stanovování sankce. Naopak pokud budou firmy vyčkávat s ohlášením až do doby, než začnou hackeři prodávat ukradená data na trhu, tak pak je to špatné, jak pro firmy, tak pro občany. Firmy musí být schopny dokázat, kdy se o úniku dat dozvěděly. Od tohoto okamžiku se počítá jejich 72hodinová lhůta na oznámení. Peníze vybrané na pokutách poputují, stejně jako je tomu nyní, do státního rozpočtu.

***Takže nebudete zpočátku tolerantnější, ale naopak vysokými pokutami tvrdě odrazovat ostatní podniky od porušování GDPR?**

Nespekulovala bych takto. Každá pokuta musí být obecně přiměřená, ne likvidační. O výši pokuty rozhoduje i to, jak si podnik ekonomicky stojí. Takže odrazovat, ale nelikvidovat.

***K masivnímu úniku dat došlo naposledy v T-Mobilu v dubnu minulého roku, operátorovi jste vyměřili pokutu 3,6 milionu korun. Jak by Úřad postupoval, kdyby již platilo GDPR?**

V té době jsme mohli uložit pokutu do výše deseti milionů. T-Mobile se mohl odvolat, neudělal to. Společnosti unikla data i v Německu, tam poškozeným klientům, jak jsem informována, operátor nabídl nová telefonní čísla. V Česku nenabídl vůbec nic. I to hraje roli při stanovování výše pokuty – snaha zhojit nastalé újmy. Pokud by v té době platilo GDPR, pokuta by byla vyšší.

***Bude se nějak lišit přístup v pokutování veřejných a soukromých subjektů?**

O tom nyní nemám informace. Existují úvahy, proč dávat pokuty veřejným institucím, když peníze směřují nakonec stejně zpět do státního rozpočtu. Má to ale hlubší filozofii. Když se udělí pokuta, musí se najít viník, který karambol způsobil. Zejména ve státních institucích, kde by k porušování ochrany osobních údajů nemělo docházet, to má výchovnou funkci. Udělování pokut se zatím na bruselské úrovni neprojednávalo. Zásadní je, že nově poslední slovo bude mít vždy Evropský sbor. Nemůže to být tak, že by si nějaký stát řekl, že zpočátku nebude udělovat pokuty vůbec.

***Tušíte, kolik subjetků v Česku nová legislativa postihne?**

Náš Úřad nemá možnosti, jak by toto číslo zjistil. Proč je to důležité? Abychom všechny zkontrolovali?

***Zajímá mne, jak chce Úřad kontrolovat tak širokou masu subjektů podléhajících nařízení.**

Ani dnes nehlídáme všechny přímo. Zdrojem pro naše kontrolní kroky jsou stížnosti, které nám chodí, a problémy, které hýbou společností. Kontrolu ale můžeme nařídit i tam, kde k úniku dat ještě nedošlo. Máme vyšetřovací, edukativní, školící a kontrolní pravomoci, které budou nově modifikované v kontextu GDPR.

Vždycky jsme trestali i orgány veřejné správy, například ministerstva. Takhle to ale ve všech státech dosud nechodí. Je to i otázka diskuse, jestli se tak dál bude pokračovat. Státní instituce zpracovávají obrovské množství dat, kontrola je podle mě naprosto nutná. Napětí vzniká, pokud jde o výši sankcí a rozsah shromažďovaných dat.

***Nakolik je přechod ze stávající právní úpravy na novou legislativu radikální, co všechno se změní?**

Celá proměna spočívá ve filozofii přístupu k naší bezpečnosti. Bude se vyhodnocovat riziko, které ochraně osobních údajů hrozí, a podle toho se bude provádět zabezpečení – budeme důsledně sledovat, aby bylo plněno, co je subjekty dokumentováno a deklarováno. Takže když přijde náš audit, tak bude začínat zjišťováním, jak jsou data zabezpečená. Oni předloží svá deklarovaná opatření a my verifikujeme, jak to funguje ve skutečnosti.

***Co pozitivního nařízení přináší, chápete ho jako krok vpřed?**

Jsme v digitálním věku prudce se rozvíjejících komunikačních technologií. S každou pracovní silou putují osobní údaje. Není možné, aby v EU, kde existují čtyři svobody – volný pohyb zboží, služeb, pracovních sil a kapitálu – nebyla sjednocená pravidla pro pohyb informací, které volně se pohybujícího člověka provázejí. To je významný přínos GDPR, kdy se ke zmíněným čtyřem svobodám musí nutně přiřadit jednotná úprava ochrany soukromí.

***Čím může nové nařízení vnést naopak zmatek do běžného fungování firem, čím je může brzdit?**

Proč zmatek? Ukáže až praxe, zda existují nějaké slabiny. Tak už to u práva spojeného s prudkým rozvojem technologií chodí. Musí se přehodnocovat. Proto se změnil způsob kontroly. Díky pověřencům DPO (Data Protection Officers), které musí jmenovat některé firmy, dostala kontrola horizontální podobu.

Jako úřad vysunujeme svá chapadla do prostoru, kde máme spolupracovníky – pověřence. Ti sami testují, zda firma postupuje v souladu s pravidly GDPR. Dokonce testují i to, zda jsou zabezpečení dostatečná. To je jedna rovina. A do toho přicházejí integrační procesy z EU – měly by ale jít až na úroveň globalizovaného světa. Všichni lidé chtějí ochranu soukromí, ale i výdobytky digitálního věku.

***Když zmiňujete pověřence, doporučujete firmám pověřit touto agendou spíše některého ze stávajících zaměstnanců, nebo tuto činnost outsourcovat?**

My jednoznačně zastáváme názor, že by to měl být interní pracovník, který zná firemní prostředí. Ani v menších podnicích nic nebrání tomu, aby to byl člověk zevnitř. Náklady nemusí být vysoké, protože lze funkce kumulovat. Vzniká tu nová profese, která je kombinací právníka a IT specialisty.

***Jaká bude role Evropského sboru pro ochranu osobních údajů?**

Z orgánu, který dříve jen radil Evropské komisi, se stává suverénní samostatný orgán, takzvaný Sbor. Bude mít rozhodovací pravomoci. Budou ho tvořit šéfové úřadů z jednotlivých států, připravení plnit své úkoly. Pro mě je důležité, aby byl v Evropě slyšet i náš hlas a abychom nebyli jen tichým zúčastněným. GDPR dostává v Evropě samostatnost, důležitost a nepřehlédnutelnost.

***Jak se na svou novou roli připravuje Úřad?**

Komplikaci vidíme v udržení odborně zdatných pracovníků a získání nových. Jde nám hlavně o to, abychom se platově dostali na úroveň ministerstev. Je vysoká poptávka po znalcích problematiky osobních údajů – právnících, IT specialistech, analyticích. Soukromé firmy mohou oproti nám nabídnout dvojnásobné peníze, hrozí nám odkrvení. Hlavně banky přichází s lukrativními podmínkami. Tenhle problém je prakticky stejný v celé Unii. Určité odbornosti v Úřadu musí být platově konkurenceschopné soukromému byznysu.

JUDr. Ivana Janů
Od roku 2015 předsedá Úřadu pro ochranu osobních údajů. V období let 1993 až 2001 byla soudkyní a místopředsedkyní Ústavního soudu, poté do roku 2004 zasedala jako soudkyně v Mezinárodním trestním tribunálu pro bývalou Jugoslávii. Od roku 2004 znovu působila coby soudkyně v Ústavním soudu, a to až do roku 2014. V období let 1989 až 1993 pracovala jako poslankyně českého parlamentu, zúčastnila se prací na současné Ústavě ČR z roku 1993.

Autor: Jiři Liebreich