úřad pro ochranu osobních údajů
the office for personal data protection

Zdravice předsedy ÚOOÚ Jiřího Kauckého na konferenci IS2 – Information Security Summit

Vážené dámy, vážení pánové,

na úvod bych rád poděkoval, že jsem mohl za Úřad pro ochranu osobních údajů, jehož mám tu čest být nově předsedou, převzít záštitu nad touto mezinárodní konferencí a popřál letošnímu ročníku mnoho úspěchů.

Kyberbezpečnost, jakožto palčivé téma dneška, samozřejmě prostupuje i činností našeho Úřadu. Dovolte mi proto několik slov.

Ochrana dat je velmi dynamickou agendou, u níž musí docházet, v návaznosti nejen na rozvoj technologií, k neustálým úpravám. V minulých letech si takovou revizí prošel například celý právní rámec ochrany osobních údajů v souvislosti s obecným nařízením o ochraně osobních údajů. Ke změnám se přistoupilo jednoduše proto, že předchozí právní rámec, založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současným potřebám. Týká se to zejména prostředků, které jsou ke zpracování využívány, ale také kvůli mnohem komplexnějšímu zpracování jako takovému, než jakého jsme mohli být svědky před 20 či 30 lety například v oblasti profilování nebo automatizace zpracování osobních údajů.

Na další změny v evropské, ale i světové ochraně dat bychom však neměli jen čekat. Osobní údaje si musíme především chránit my sami. Je proto nutné přiznat této oblasti odpovídající význam a nespoléhat se jen na globální řešení, která často nemusí být ta nejlepší.

Naším cílem by proto mělo být dosažení co největší míry soběstačnosti v technické oblasti ochrany dat. Zmíněná soběstačnost nám poskytne kontrolu zejména nad tím, jak je s našimi daty skutečně nakládáno a že smazaná data nebudou mít nikde svou uloženou záložní verzi. Bohužel ve správě a budování ICT systémů čelí stát přetrvávajícím bezpečnostním problémům, což potvrdila nejedna výroční zpráva BIS nebo NKÚ za poslední roky.

Zmínit je rovněž nutné aktuálně probíhající pandemii onemocnění COVID-19, která má zásadní dopad na evropskou i mezinárodní ekonomiku a celou společnost. Stále zvyšující se počet lidí pracujících na dálku s sebou přináší nejedno bezpečnostní riziko. Zejména malé a střední podniky, které často nebyly zvyklé tolik investovat do bezpečnostních opatření, čelí této nové realitě, na kterou nemusely být zcela připraveny. Přitom se ale stále více stávají závislými na informačních technologiích a musí řešit otázky zabezpečení počítačů (a to často soukromých počítačů zaměstnanců využívaných pro práci z domova), mobilních telefonů zaměstnanců či přenosu dat v souvislosti s cloudovými úložišti.

Společně s nástupem pandemie COVID-19 ale pozorujeme také změny ve státní správě, která musela během krátké doby přejít k významně digitální podobě svého fungování. Přitom jí chybí nejen dlouhodobě obecně zmiňovaní IT odborníci, ale zejména specialisté na kyberbezpečnost, včetně ochrany osobních údajů. Obecně nedostatky v tomto směru mohou způsobit nevratný únik osobních údajů a jejich pozdější zneužití. To je výrazně nebezpečné v případě velkých veřejných databází státu. Víme i o tom, že k takovým únikům dochází, někdy dokonce i bez vědomí dotčených subjektů. Tyto hrozby jsou reálné i v době současné pandemie, obzvlášť citlivé jsou pak v případě nemocnic, či obecně prvků kritické infrastruktury. Je tedy třeba s tímto

faktem počítat a přijmout opatření na úrovni současného vědeckého a odborného poznání, což předpokládá i obecné nařízení o ochraně osobních údajů.

Úřad pro ochranu osobních údajů si je plně vědom reálnosti všech hrozeb souvisejících s probíhající digitalizací společnosti, které samozřejmě nechceme, a navíc ani nemůžeme, bránit. Je třeba si však tyto hrozby jasně pojmenovat, vyhodnotit reálná ohrožení a předcházet případným negativním důsledkům vyplývajícím z užívání komunikačních a informačních technologií, které jsou v dnešní době tak úzce spjaté s možnou hrozbou v podobě zneužití osobních údajů.

Regulace na úrovni státu nebo unijních institucí nemůže v neskutečně dynamickém prostředí digitálního světa natrvalo uspět, aniž bychom se do boje s kyberhrozbami nezapojili my všichni. Důležitý je především odpovědný osobní přístup a neustálé navyšování ochrany, ať již odpovídajícími technickými prostředky či vyhodnocením pravděpodobnosti a závažnosti bezpečnostních rizik, která plynou z našeho vlastního jednání. Před námi je tak jistě nejedna výzva propojující kyberbezpečnost a ochranu osobních údajů.

Přeji vaší konferenci úspěšný průběh, co nejméně technických obtíží a všem účastníkům a jejich blízkým pevné zdraví.