Vážená paní předsedkyně, vážený pane předsedo, vážení hosté a kolegové,

dovolte mi předně poděkovat za možnost zde vystoupit. Dnešní doba vyžaduje věnovat stále více pozornosti oblasti kybernetické bezpečnosti, a to již na strategické úrovni. Proto každé fórum, kde máme příležitost o této oblasti spolu hovořit, vyměňovat si názory a sdílet poznatky, nám všem prospívá a pomáhá nám zlepšovat nejen oblast kybernetické bezpečnosti, ale tím také ochrany osobních údajů.

Je to právě spolupráce a vzájemná komunikace, a to nejenom státních orgánů či orgánů samospráv, ale všech, kdo se pohybují v dnešním globalizovaném kybernetickém prostoru, která je klíčem k tomu, abychom dokázali kybernetické hrozby nejen identifikovat, ale i s nimi bojovat, a to nejlépe ještě předtím, než dojde ke konkrétnímu útoku. Nebude-li kybernetický útok úspěšný, nebudou ohroženy ani osobní údaje, pokud je cíl útoku spravuje.

Působnost Úřadu pro ochranu osobních údajů je samozřejmě širší a týká se nejen ochrany osobních údajů v kybernetickém prostoru, ale jakéhokoliv jejich zpracování. Je to však právě oblast informačních technologií, které jsou dnes v zásadě neoddělitelně spjaty s jakýmkoliv zpracováním osobních údajů. A tím se kybernetické hrozby více či méně, přímo či nepřímo, dotýkají ve svém důsledku téměř vždy naší působnosti – tedy ochrany osobních údajů. Prvotním cílem Úřadu je samozřejmě ochrana soukromí fyzických osob a té lze docílit jen spoluprací se správci či zpracovateli osobních údajů a dalšími subjekty činnými na tomto poli.

GDPR akcentuje koncept nastavení procesů zpracování, jejichž nedílnou součástí je IT zabezpečení, od samého prvopočátku. Úřad se často setkává s tím, že se obecně zabezpečení, a to nejen osobních údajů, nastavuje „jen tak mimochodem“ či zcela formálně a v řadě případů bohužel i „ex post“. A teď nemám na mysli takové drobnosti jako ukradené nezaheslované počítače. Z nedávné doby snad již skončené pandemie řešíme případ, kdy v rámci rezervačního portálu na očkování proti COVIDu došlo k úniku 80 000 rodných čísel. Jakkoliv je pochopitelné, že se v té době mnohé věci dělaly pod tlakem okolností, v tomto případě však došlo k zásadní rezignaci na základy kybernetické bezpečnosti a práci s osobními údaji. V rámci kontroly pak vyplynul další zásadní nedostatek, a to absence řádného a jasného vymezení rolí v rámci nastavení takto citlivého systému. Důsledkem toho je nejen zmatečnost pokynů

při vytváření tohoto systému, ale i následné přehazování odpovědnosti mezi zainteresovanými stranami – v tomto případě za únik desítek tisíc rodných čísel.

Takový případ může být i důsledkem toho, že některé společnosti nijak nevzdělávají své zaměstnance v základním přístupu ke kybernetické bezpečnosti, ani k zodpovědné ochraně osobních údajů. Mnohdy to považují za naprosto zbytné výdaje.

Jsou to pak tyto základní zásady v oblasti kybernetické bezpečnosti – dodržování konceptu nastavení zabezpečení osobních údajů od prvopočátku, důsledné vzdělávání a nastavení rolí jednotlivých aktérů podílejících se na zpracování osobních údajů. To musejí správci vnímat jako samozřejmost i proto, že tyto zásady nacházejí uplatnění nejen v oblasti zabezpečení osobních údajů. Jejich důsledná aplikace je pak nejen prioritou našeho Úřadu, ale musí být i prioritou pro prohlubující se spolupráci na tomto poli jak mezi úřady samotnými, tak hlavně mezi úřady a jednotlivými správci.

Nad rámec této triády (tedy Kybernetické bezpečnosti, Ochrany osobních údajů a Edukace personálu) zmíním ještě dvě povinnosti, které jsou jak pro oblast ochrany osobních údajů, tak pro kybernetickou bezpečnost klíčové, a které je i proto bezpodmínečně nutné dodržovat. Předně – obecné nařízení o ochraně osobních údajů stanoví, že správce osobních údajů má povinnost hlásit našemu Úřadu jakékoli porušení zabezpečení osobních údajů, a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, výjimkou jsou pouze případy, kdy nehrozí riziko ve vztahu k právům a svobodám fyzických osob. V praxi se často setkáváme s tím, že správci nejsou ze strachu z pokuty ochotni buď hlásit takové incidenty, nebo je do jisté míry zkreslují. Na tomto místě musím zdůraznit, že Úřad nechce a nebude pokutovat správce za to, že se nezaviněně stali obětí hackerského útoku. Primárním motivem této povinnosti je potřeba zmapovat příčiny a následky porušení zabezpečení správcem. Úřad pak následně může sledovat trendy v této oblasti a například se zaměřit na určitý typ problému, kterému bude věnovat svoji pozornost. Správce, který poctivě splní svou ohlašovací povinnost, tak může zprostředkovaně napomoci ostatním správcům podobnému incidentu předejít.

Nicméně je faktem, že Úřad je nucen poměrně přísně posuzovat případy, kdy k porušení zabezpečení došlo a ohlašovací povinnost nebyla splněna. Vzhledem k tomu, že to je samo o sobě další protiprávní jednání správce, které navíc svědčí o jeho postoji k ochraně osobních údajů. Je nasnadě, že tento přístup se oproti přístupu správce, který své povinnosti po zjištění porušení zabezpečení řádně

plní, nesmí ani ekonomicky vyplatit. Stejně tak se Úřad velmi přísně zaměřuje a bude nadále zaměřovat na ty případy, kdy má ohlášení porušení zabezpečení za cíl skrýt to, co se skutečně stalo, tedy například to, že se nejednalo o porušení zabezpečení, ale dokonce o vědomý prodej osobních údajů.

Druhou povinností, kterou bych rád zmínil, je hned následující povinnost podle obecného nařízení Evropské unie o ochraně osobních údajů, které říká, že pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů. Nesmíme totiž zapomínat na osoby, jejichž osobní údaje jsou zpracovávány. Ochrana poskytovaná obecným nařízením nemá být abstraktní, ale konkrétní. Tyto osoby mají právo vědět, že došlo ke kompromitaci jejich údajů, neboť jsou to právě ony, jež máme společně chránit a které ponesou následky takového incidentu.

Vážené kolegyně, vážení kolegové, dovolíte-li mi zakončit svůj krátký projev výzvou, která je, jak už to tak bývá, určena těm, kdo se podobných konferencí neúčastní, ale měli by: Je důležité nezatajovat před sebou informace, ale naopak je sdílet, abychom společně vytvářeli podmínky pro bezpečnější kybernetický prostor. Jak i poslední doba kybernetických útoků a hybridní války proti svobodnému světu ukazuje, jedině společně jsme schopni čelit aktuálním výzvám a nebezpečím. Ochrana osobních údajů v úzké vazbě na kybernetickou bezpečnost je naším úkolem v rámci Evropské unie a stává se stále více i globální výzvou.

Děkuji vám za pozornost.