Metodika posuzování dopadu zpracování na ochranu osobních údajů

ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 2016/679
na ochranu fyzických osob v souvislosti se zpracováním osobních údajů (tzv. GDPR)

Posuzování dopadu zpracování na ochranu osobních údajů vyžaduje Nařízení ve svém Oddílu 3 Posouzení vlivu na ochranu osobních údajů a předchozí konzultace, čl. 35 a 36. Nařízení nedefinuje přesnou metodiku posuzování, pouze požaduje, aby posouzení proběhlo a pokud jeho výsledek určí, že riziko je vysoké a Správce nepřijme opatření k jeho zmírnění, je povinen záměr zpracování předem konzultovat s Dozorovým úřadem. Následující metodika představuje aplikaci jen minimálně upravené (upřesněné) metodiky definované za podobným účelem ve Vyhlášce č. 316/2014 Sb. o kybernetické bezpečnosti. Tato Vyhláška v příloze 2 dává návod, jak hodnotit rizika. K tomu používá funkci **riziko = dopad x hrozba** (četnost výskytu incidentu) **x zranitelnost**.

Pro hodnocení použijeme následující stupnice

STUPNICE PRO HODNOCENÍ DOPADU ZPRACOVÁNÍ / INCIDENTU	
úroveň	popis
nízký dopad	**Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický.** Rozsah případných škod nepřesahuje a) 10 zraněných osob s hospitalizací po dobu více než 24 hodin nebo b) finanční nebo materiální ztráty do 5 mil Kč nebo c) dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob nebo d) doplněk nad rámec Vyhl. 316/2014: **dopad se netýká zvláštních kategorií osobních údajů** dle č. 9 a 10 Nařízení, tj. údajů vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení, členství v odborech, jedinečných údajů určených pro identifikaci fyzické osoby (biometrická a genetická data), o zdravotním stavu nebo o sexuální orientaci a životě nebo zpracování údajů o rozsudcích v trestních věcech trestných činech. e) doplněk nad rámec Vyhl. 316/2014: **dopad neumožňuje s vysokou pravděpodobností předvídat chování nebo pohyb dotčených subjektů údajů**
střední dopad	**Dopad je v omezeném časovém období a omezeném rozsahu.** Rozsah případných škod se pohybuje v rozmezí a) 10 mrtvých nebo 11 – 100 osob s hospitalizací po dobu více než 24 hodin nebo b) finanční nebo materiální ztráty od 5 do 50 mil Kč nebo c) dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího 251 – 2 500 osob nebo d) doplněk nad rámec Vyhl. 316/2014: **dopad se netýká zvláštních kategorií osobních údajů** dle č. 9 a 10 Nařízení, tj. údajů vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení, členství v odborech, jedinečných údajů určených

	pro identifikaci fyzické osoby (biometrická a genetická data), o zdravotním stavu nebo o sexuální orientaci a životě nebo zpracování údajů o rozsudcích v trestních věcech trestných činech. e) doplněk nad rámec Vyhl. 316/2014: **dopad neumožňuje s vysokou pravděpodobností předvídat chování nebo pohyb dotčených subjektů údajů**
vysoký dopad	**Dopad je omezeného rozsahu, ale trvalý nebo katastrofický.** Rozsah případných škod se pohybuje v rozmezí a) od 11 do 100 mrtvých nebo 101 – 1000 osob s hospitalizací po dobu více než 24 hodin nebo b) finanční nebo materiální ztráty od 50 do 500 mil Kč nebo c) dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího 2 501 – 25 000 osob nebo d) doplněk nad rámec Vyhl. 316/2014: dopad **se týká zvláštních kategorií osobních údajů** dle č. 9 a 10 Nařízení, tj. údajů vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení, členství v odborech, jedinečných údajů určených pro identifikaci fyzické osoby (biometrická a genetická data), o zdravotním stavu nebo o sexuální orientaci a životě nebo zpracování údajů o rozsudcích v trestních věcech trestných činech. e) doplněk nad rámec Vyhl. 316/2014: dopad **s vysokou pravděpodobností předvídá chování nebo pohyb dotčených subjektů údajů**
kritický dopad	**Dopad je plošný rozsahem, trvalý a katastrofický.** Rozsah případných škod se pohybuje v rozmezí a) od 101 do 1000 mrtvých nebo 1001 a více osob s hospitalizací po dobu více než 24 hodin nebo b) finanční nebo materiální ztráty od převyšující 500 mil Kč nebo c) dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího 2 501 – 25 000 osob nebo d) doplněk nad rámec Vyhl. 316/2014: dopad **se týká zvláštních kategorií osobních údajů** dle č. 9 a 10 Nařízení, tj. údajů vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení, členství v odborech, jedinečných údajů určených pro identifikaci fyzické osoby (biometrická a genetická data), o zdravotním stavu nebo o sexuální orientaci a životě nebo zpracování údajů o rozsudcích v trestních věcech trestných činech. e) doplněk nad rámec Vyhl. 316/2014: **dopad prakticky s jistotou umožňuje předvídat chování nebo pohyb dotčených subjektů údajů**

STUPNICE PRO HODNOCENÍ (četnosti) HROZEB	
úroveň	popis
nízká hrozba	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za pět let. doplněk nad rámec Vyhl. 316/2014: Hrozba se vyskytuje izolovaně.
střední hrozba	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od jednoho roku do pěti let. doplněk nad rámec Vyhl. 316/2014: Hrozba se vyskytuje izolovaně.
vysoká hrozba	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí jednoho měsíce až jednoho roku.

	doplněk nad rámec Vyhl. 316/2014: Hrozba se vyskytuje s souvislosti s dalšími hrozbami, hromadně, případně i koordinovaně s dalšími hrozbami.
kritická hrozba	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace je častější než jednou za měsíc. doplněk nad rámec Vyhl. 316/2014: Hrozba se vyskytuje s souvislosti s dalšími hrozbami, hromadně, případně i koordinovaně s dalšími hrozbami.

STUPNICE PRO HODNOCENÍ ZRANITELNOSTI	
úroveň	popis
nízká zranitelnost	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, která jsou schopná včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
střední zranitelnost	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání bezpečnostních opatření je omezená. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
vysoká zranitelnost	Zranitelnost je pravděpodobná až vel mi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí pokusy o překonání bezpečnostních opatření.
kritická zranitelnost	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy o bezpečnostních opatření.

STUPNICE PRO HODNOCENÍ RIZIK	
úroveň	popis
nízké riziko	Riziko je považován za přijatelné.
střední riziko	Riziko může být sníženo méně náročnými opatřeními nebo, v případě vyšší náročnosti opatření, je riziko přijatelné.
vysoké riziko	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
kritické riziko	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Doporučená organizace hodnocení rizika a vlivy hodné zřetele

Oprávněná osoba určí skupina určí skupinu hodnotitelů, kteří jako celek znají všechny důležité aspekty zpracování, možnosti a účinnost bezpečnostních opatření, znají účel a rozsah posuzovaného zpracování osobních údajů. Hodnotitelé (v souladu s doporučením WP 29, dok WP 248 Pokyny pro posuzení vlivu na ochranu osobních a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely Nařízení 2016/679) při posouzení mimo jiné berou v potaz, zda:

a) je uveden systematický popis zpracování. Přitom přihlíží k povaze, rozsahu, kontextu a účelům zpracování; zda jsou zaznamenány osobní údaje, příjemci a doba zpracování; zda jsou popsány funkční operace zpracování, zda jsou stanoveny prostředky na nichž je zpracování závislé (HW, SW, komunikační kanály, …), zda je zohledněn soulad s definovaným chováním zpracovatelů (např. kodexy, pokyny apod.)
b) jsou stanovena opatření k zajištění souladu s požadavky Nařízení, zejména

a. s požadavkem na přiměřenost a nezbytnost na základě definovaných účelů, zákonnosti, na přiměřenost a minimalizaci zpracovávaných osobních údajů a na omezení doby zpracování.
b. s opatřeními za účelem podpory práv subjektů (transparentnost zpracování, přístup subjektu k vlastním osobním údajům, právo na opravu a výmaz, právo na námitku a na ometzení zpracování, sesmluvnění zpracování se zpracovatelem a ochranu údajů při předávání mezinárodním subjektům)

c) jsou řízena rizika vzniklá zpracováním pro práva svobody subjektů údajů; zda je známa povaha a původ rizika, jeho dopad, četnost a zranitelnost zpracování, zda jsou známy a určeny možné vlivy na práva a svobody subjektu údajů, zda jsou známy a popsány hrozby vůči zabezpečení zpracování a zda jsou známa a stanovena opatření určeníé k řešení těcho rizik.

U každého posuzovaného zpracování (agendy) hodnotitelé napřed vyplní jeho dopad, četnost hrozby a zranitelnost. Následně posoudí kombinovaný vliv všech tří aspektů na konečné riziko. Obecně platí, že vyšší hodnota aspektů by měla převažovat. Tedy například pokud máme střední dopad, nízkou hrozbu a nízkou zranitelnost, mělo by být výsledné riziko střední. Pokud ovšem skupina hodnotitelů na základě relevantních znalostí dojde k názoru, že vliv některého z hodnocených aspektů je dominantní, může zvolit jako určení konečného rizika hodnotu nižší nebo naopak větší, než by odpovídalo prostému součinu všech aspektů.

O posouzení rizika se vede u jednotlivých zpracování písemný záznam, který identifikuje nejméně: posuzované zpracování (agendu), hodnotitele, hodnocení dopadu, hrozby a zranitelnosti a výsledné zjištěné riziko.

Doporučená forma ochrany zpracování osobních údajů dle zjištěného rizika

OSOBNÍ ÚDAJE NA FYZICKÝCH NOSIČÍCH (papír, mikrofiše, apod.)	
úroveň	popis zabezpečení při zpracování
nízké riziko	V době přítomnosti oprávněného personálu volně v (otevřených) organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) či na policích. V době nepřítomnosti oprávněného personálu v (uzavřených) organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) či policích, místnost uzamčena. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě podezření na narušení ochrany dat.
střední riziko	V době přítomnosti oprávněného personálu volně v (otevřených) organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) či policích. V době nepřítomnosti oprávněného personálu v uzamčených organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.), místnost uzamčena. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě podezření na narušení ochrany dat.
vysoké riziko	V době přítomnosti oprávněného personálu v uzavřených organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) zvýšené odolnosti (např. plechová skříň s cylindrickým zámkem). V době nepřítomnosti oprávněného personálu v uzamčených organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) zvýšené odolnosti (nap. plechová skříň s cylindrickým zámkem), místnost uzamčena. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě podezření na narušení ochrany dat.

kritické riziko	Osobní údaje jsou udržovány v místnosti s řízeným vstupem (vstup povolen pouze oprávněnému personálu), odkud jsou vynášeny pouze v případě dalšího zpracování, vždy jednotlivě a po skončení zpracování jsou okamžitě vraceny zpět. Místnost je osazena dveřmi se zvýšenou odolností a vstup je osazen zámkem vyšší třídy odolnosti (s klíči chráněného profilu). V době přítomnosti oprávněného personálu v uzamčených organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.) V době nepřítomnosti oprávněného personálu v uzamčených organizačních schránách (skříních, šanonech, lístkovnicích, boxech apod.), místnost uzamčena. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě podezření na narušení ochrany dat. Je ověřována účinnost tohoto postupu.

OSOBNÍ ÚDAJE V ELEKTRONICKÉ PODOBĚ	
úroveň	popis zabezpečení při zpracování
nízké riziko	Jednoduchá jednofaktorová autentizace uživatele (např. standardní Microsoft přihlášení), postačuje jednoduché heslo. Obměna hesla vyžadována jednou za tří měsíce. Jsou sledovány a zaznamenávány neúspěšné pokusy o přihlášení, při překročení povoleného počtu pokusů je účet zablokován. Tyto záznamy jsou namátkově kontrolovány. Aktivity uživatelů jsou alespoň na základní úrovni (přihlášení a odhlášení, ze které stanice) logovány a logy jsou udržovány po dobu umožňující účinnou reakci na incident. Existují popsané, řízené systémy přidělování oprávnění do IT systému, je řešen nástup a ukončení pracovního poměru zaměstance/ externího pracovníka. Je prováděna kontrola konfliktu rolí. Data nejsou šifrována. Data jsou chráněna standardními firewally s podporou od výrobce HW a SW. Infrastruktura je rozdělená do logických síťových zón. Servery vnitřní sítě jsou odděleny od uživatelských segmentů a DMZ síť je oddělena pomocí firewallů. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě nestandardního chování systému nebo při podezření na zneužití dat. Je ověřována znalost tohoto postupu.
střední riziko	Platí to co nízke riziko a rozšíření o: Jsou sledovány a zaznamenávány neúspěšné pokusy o přihlášení, při překročení povoleného počtu pokusů je účet zablokován. Tyto záznamy jsou pravidelně kontrolovány. Konstrukce hesel je prováděná minimálne 8 znaků, jedno velke pismeno, jedna číslice a jeden speciální znak. Aktivity uživatelů jsou alespoň na základní úrovni (přihlášení a odhlášení, ze které stanice) logovány a logy jsou udržovány po dobu umožňující účinnou reakci na incident. Logy jsou pravidelně vyhodnocovány v bezpečnostním dohledu. Existují popsané, řízené systémy přidělování oprávnění do IT systému, je řešen nástup a ukončení pracovního poměru zaměstance/ externího pracovníka. Je prováděna kontrola konfliktu rolí. Jsou pravidelně nasazovány aktualizované verze SW OS a aplikací vč záplat. Servery a na nich provozovaný SW jsou evidovány ve znalostní databázi, kde je evidovaná verze SW komponety a OS serveru. Pravidelně alespoň jednou týdne je zkoumána zranitelnost OS, aplikace, FW, přepínačů a směrovačů oproti znalostní databázi a alespoň jednou měsíčně je plánováno nasazení změn bezpečnostních balíčků. Na koncových stanicích a serverech je nasazen antivir, antispam a personální FW.

	Je kontrolován nainstalovány SW a prováděno pravidelné skenování nastavení koncových zařízení. Data nejsou šifrována, výjimku tvoří disky přenosných stanic (notebooků). Jsou prováděny pravidelné penetračni testy z Internetu a ze vnitřku organizace. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě nestandardního chování systému nebo při podezření na zneužití dat. Je ověřována znalost tohoto postupu.
vysoké riziko	Platí to co pro střední a rozšířené o: Dvoufaktorová autentizace uživatele, je vyžadováno silné heslo. Obměna hesla vyžadována jednou měsíčně. Jsou sledovány a zaznamenávány neúspěšné pokusy o přihlášení, při překročení povoleného počtu pokusů je účet zablokován. Tyto záznamy jsou pravidelně kontrolovány a vyhodnocovány. Aktivity uživatelů jsou rozsáhle logovány (přihlášení a odhlášení, ze které stanice, jaké aktivity provádí, četnost přihlášení a doba) a logy jsou udržovány po dobu umožňující účinnou reakci na incident. Logy jsou systematicky, pravidelně vyhodnocovány.Na podstatných aplikacích a aktivitách je vyžadována autorizace. Akce v aplikaci jsou logovány (prohlížení dat, modifikace, vytváření a mazání), data jsou zasílána do bezpečnostního monitoringu. Existují popsané, řízené systémy přidělování oprávnění do IT systému, je řešen nástup a ukončení pracovního poměru zaměstance/ externího pracovníka. Je prováděna kontrola konfliktu rolí. Data jsou šifrována dostatečně silnou šifrou. Na mobilních zařízeních je naistalován specializovany SW pro lokalizaci zařízení. Je aplikován SW pro ochranu OS a aplikace (Pesonal FW, IPS/HIDS, Antivir, kontrola patch managementu). Jsou řízena připojení externích datových nosičů a jejich použití podléhá autorizaci. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě nestandardního chování systému nebo při podezření na zneužití dat. Je ověřována účinnost tohoto postupu.
kritické riziko	Osobní údaje jsou udržovány v místnosti s řízeným vstupem (vstup povolen pouze oprávněnému personálu), zařízení nejsou zapojeny do lokalní sítě a nejsou žádným prostředkem připojeny k Internetu či podobné síti. Doufaktorovová autentizace, systém autentizace a autorizace využívá biometrické mechanismy pro zvýšení úrovně zabezpečení. Jsou sledovány a zaznamenávány neúspěšné pokusy o přihlášení, při překročení povoleného počtu pokusů je účet zablokován a automaticky je vyvolán poplach v místě s trvalým dohledem obsluhy. Záznamy o aktivititách uživatele jsou zaznamenány do logů a jsou automaticky kontrolovány. Aktivity uživatelů jsou plně logovány (přihlášení a odhlášení, ze které stanice, jaké aktivity provádí, četnost přihlášení a doba, jaké změny uživatel dělal, … aktivity uživatele v aplikaci) a logy jsou udržovány po dobu umožňující účinnou reakci na incident. Logy jsou systematicky, automaticky vyhodnocovány, vybočení ze standardního chování uživatele vyvolává poplach. Na podstatných aplikacích a aktivitách je vyžadována autorizace. Existují popsané, řízené systémy přidělování oprávnění do IT systému, je řešen nástup a ukončení pracovního poměru zaměstance/ externího pracovníka. Je prováděna kontrola konfliktu rolí. Data jsou šifrována dostatečně silnou šifrou. Na mobilních zařízeních je naistalován specializovany SW pro lokalizaci zařízení. Je aplikován SW pro ochranu OS a aplikace (Pesonal FW, IPS/HIDS, Antivir, kontrola patch managementu). Jsou

	řízena připojení externích datových nosičů a jejich použití podléhá autorizaci. Plošné exporty dat jsou možné pouze v rámci pravidla čtyř očí. Existuje mechanismus / postup, podle kterého se zaměstnanci chovají v případě nestandardního chování systému nebo při podezření na zneužití dat. Je ověřována účinnost tohoto postupu. Je ověřována účinnost tohoto postupu.