

PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

WP 253

Vodítka k uplatnění a stanovení správních pokut pro účely Nařízení 2016/679

Schváleno dne 3. října 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytl Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

Neoficiální překlad

**PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE
ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ**

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice a

s ohledem na svůj jednací řád,

PŘIJALA TATO VODÍTKA:

Obsah:

I. Úvod.....	3
II. Zásady.....	3
III. Kritéria posuzování v článku 83, odst. 2	6
IV. Závěr	12

I. Úvod

EU dokončila všeobecnou regulatorní reformu v oblasti ochrany osobních údajů v Evropě. Reforma stojí na několika pilířích (klíčové komponenty): celistvá pravidla, zjednodušené postupy, koordinované akce, účast uživatele, účinnější informování a silnější vynucovací pravomoci.

Na správce a zpracovatele připadne větší odpovědnost za účinnou ochranu osobních údajů jednotlivců. Dozorové úřady mají pravomoci prosadit, aby zásady Obecného nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“) jakož i práva dotčených jednotlivců byla dodržována v souladu se zněním a duchem Obecného nařízení.

Konzistentní prosazování pravidel ochrany dat je zásadní pro harmonizovaný režim ochrany. Správní pokuty jsou ústředním prvkem nového režimu prosazování práva zavedeného Obecným nařízením a představuje tak mocnou součást balíčku opatření, která dozorové úřady mají k dispozici podle článku 58.

Tento dokument je určen pro využití dozorovými úřady pro zajištění lepšího uplatňování a prosazování Obecného nařízení a vyjadřuje jejich společné porozumění ustanovením článku 83 Obecného nařízení stejně jako jeho provázanost s články 58 a 70 a souvisejícími recitály.

Zejména podle článku 70, odst. 1, písm. e) je Evropský sbor pro ochranu osobních údajů (dále jen „Sbor“) zmocněn vydávat pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování tohoto nařízení a podle článku 70, odst. 1, písm. k) vypracovávat pokyny ohledně stanovení správních pokut.

Tato vodítka nejsou vyčerpávající, ani nemají poskytovat výklad odlišností mezi správním, občanským a trestním právem při ukládání správních sankcí obecně.

V zájmu sourodého přístupu k udělování správních pokut, který by náležitě reflektoval všechny zásady uvedené v těchto vodítkách, se Sbor shodl na jednotném výkladu posuzovacích kritérií podle Obecného nařízení, článek 83, odst. 2 a z toho důvodu se Sbor a jednotlivé dozorové úřady dohodly na používání těchto vodítek jako východiska jednotného přístupu.

II. Zásady

Pokud bylo na základě posouzení případu zjištěno porušení Obecného nařízení, musí příslušný dozorový úřad určit nejvhodnější nápravné (nápravná) opatření k vyřešení dané věci. Ustanovení článku 58, odst. 2, písm. b-j)¹ ukazuje, které nástroje může dozorový úřad uplatnit při řešení nesouladu na straně správce nebo zpracovatele. Při použití těchto pravomocí musí dozorové úřady dodržovat následující zásady:

¹ Článek 58, odst. 2, písm. a) stanoví, že může být vydáno varování, pokud „operace zpracování pravděpodobně porušují toto nařízení“. Jinými slovy, v případě zmíněném tímto ustanovením ještě k porušení Obecného nařízení nedošlo.

1. Porušení Obecného nařízení by mělo vést k udělení „rovnocenných sankcí“.

Koncept „rovnocennosti“ je zásadní při určování šíře povinností dozorových úřadů při zajišťování jednotnosti využití nápravných pravomocí podle článku 58, odst. 2 obecně a uplatňování správních pokut zejména².

S cílem zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci Unie by úroveň ochrany měla být rovnocenná ve všech členských státech (Recitál 10). Recitál 11 rozpracovává skutečnost, že rovnocenná úroveň ochrany osobních údajů v celé Unii vyžaduje, mimo jiné, „rovnocenné pravomoci pro monitorování a zajišťování souladu s pravidly ochrany osobních údajů a rovnocenné sankce za jejich porušování v členských státech“. Rovnocenné sankce ve všech členských státech a účinná spolupráce mezi dozorovými úřady z různých členských zemí jsou navíc nahlíženy, v souladu s recitálem 13 Obecného nařízení, jako cesta k zamezení „rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu“.

Obecné nařízení stanovuje v porovnání se Směrnicí 95/46/ES pevnější základnu pro vyšší hladinu jednotnosti, jelikož je, coby nařízení, přímo aplikovatelné ve všech členských státech. Zatímco dozorové úřady jednájí „cela nezávisle“ (Článek 52) vůči národním vládám, správcům i zpracovatelům, jsou povinny spolupracovat „s cílem zajistit jednotné uplatňování a prosazování tohoto nařízení“ (Článek 57, odst. 1, písm. g).

Obecné nařízení požaduje při udělování sankcí větší jednotnost než Směrnice 95/46/ES. U mezinárodních případů by jednotnosti mělo být dosaženo především spoluprací v rámci mechanismu jediného kontaktního místa a do určité míry také prostřednictvím mechanismu jednotnosti zavedeného novým Obecným nařízením.

U národních případů spadajících pod Obecné nařízení uplatní dozorové úřady tato vodítka v duchu spolupráce podle článku 57, odst. 1, písm. g) a článku 63, s cílem zajistit jednotnou aplikaci a prosazování Obecného nařízení. I když jsou dozorové úřady nadále nezávislé při výběru nápravných opatření podle článku 58, odst. 2, měly by se vyvarovat uplatňování odlišných nápravných opatření u srovnatelných případů.

Stejná zásada platí pro ukládání nápravných opatření ve formě pokut.

2. *Správní pokuty, stejně jako veškerá nápravná opatření zvolená dozorovými úřady, by měly být „účinné, přiměřené a odrazující“.*

Podobně jako nápravná opatření obecně, by měly správní pokuty odpovídajícím způsobem reagovat na povahu, závažnost a důsledky porušení, přičemž dozorový úřad musí posoudit veškeré skutečnosti okolo případu, a to konzistentně a objektivně. Posoudit, co je v daném případě účinné, přiměřené a odrazující bude také vyžadovat zvážení, co má zvolené nápravné opatření sledovat, tedy zda má být znovu dosaženo souladu s pravidly nebo zda jde o potrestání nezákonného jednání (nebo obojí).

Dozorové úřady by měly vybírat nápravné opatření, které je „účinné, přiměřené a odrazující“ (Článek 83, odst. 1), a to jak u vnitrostátních případů (Článek 55), tak v případech týkajících se přeshraničního zpracování osobních údajů (podle definice v článku 4, odst. 23).

Tato vodítka připouští, aby v národní legislativě byly zavedeny dodatečné požadavky ohledně postupů prosazování, jež by dozorové úřady musely dodržovat. Sem může patřit například oznámení adresy, způsob a lhůta pro vyjádření stanoviska, odvolání, prosazení, platba³.

Takové požadavky by však neměly bránit dosažení účinnosti, přiměřenosti nebo odrazujícího účinku.

² Byť právní řády v některých zemích EU neumožňují uložení správních pokut v podobě stanovené Obecným nařízením, musí uplatnění tamních pravidel mít účinek rovnocenný správním pokutám uloženým dozorovými úřady (Recitál 151). Soudy jsou vázány Obecným nařízením, avšak nikoliv těmito vodítky Sboru.

³ Jako příklad lze uvést ústavní pořádek a návrh legislativy pro ochranu dat v Irsku, kde je stanoveno, že formální rozhodnutí je činěno na základě vlastního porušení a sděleno všem dotčeným stranám, a to ještě předtím, než se přikročí k posouzení rozsahu sankcí. Rozhodnutí o holé skutečnosti porušení nelze během posuzování rozsahu sankcí znovu otevřít.

Přesnější vymezení, co je účinné, přiměřené a odrazující, bude možné až na základě praxe dozorových úřadů (v oblasti ochrany dat, a také poznatky z jiných regulovaných oblastí), jakož i precedenčních případů, kde tyto zásady budou vykládány.

Dozorový úřad má při ukládání pokut, aby byly účinné, přiměřené a odrazující, použít definici pojmu podnik podle Soudního dvora Evropské unie pro účely aplikace článku 101 a 102 Smlouvy o fungování Evropské unie (SFEU), zejména koncept, kdy podnikem **se rozumí** hospodářská jednotka, která může být vytvořena mateřskou společností včetně všech zainteresovaných poboček. V souladu s právem EU a precedenty⁴, je podnik nutno chápat jako hospodářskou jednotku, která je zapojena do obchodních/hospodářských aktivit, bez ohledu na zapojenou právní osobu (Recitál 150).

3. Příslušný dozorový úřad provede posouzení „v každém jednotlivém případě“.

Správní pokuty mohou být ukládány za širokou škálu porušení. Článek 83 Obecného nařízení ustavuje harmonizovaný přístup k porušení povinností výslovně vyjmenovaných v článcích 4 - 6. Právo členského státu může rozšířit aplikaci článku 83 na orgány veřejné moci a veřejné subjekty tohoto členského státu. Právo členského státu může navíc umožnit nebo dokonce učinit povinným uložení pokuty za porušení dalších ustanovení, kromě těch zmíněných v článku 83, odst. 4 - 6.

Obecné nařízení vyžaduje posoudit každý případ samostatně⁵. Článek 83, odst. 2 je výchozím bodem pro takové individuální posouzení. V článku se říká, že „*Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti ...*“ Podle toho, a také ve světle recitálu 148⁶ je v odpovědnosti dozorového úřadu zvolit nejvhodnější opatření. V případech jmenovaných v článku 83, odst. 4 - 6, **musí** tento výběr vzít v úvahu veškerá nápravná opatření včetně zvážení odpovídající správní pokuty, buď vedle nápravného opatření podle článku 58, odst. 2, nebo samostatně.

Pokuty představují významný nástroj, kterého by dozorové úřady měly za příčných okolností využívat. Dozorové úřady mají k nápravným opatřením zaujmout uvážlivý a vyvážený přístup, aby se dobraly účinné a odrazující,

⁴ Definice podle precedenčního práva ESD zní (volně přeloženo): „pojem podnik zahrnuje každý subjekt zapojený do hospodářské činnosti bez ohledu na právní status tohoto subjektu a způsob, jakým je financován“ (Případ Hofner a Elsner, odstavec 21, ECLI:EU:C:1991:161). Podnik „musí být v tomto kontextu chápán jako pojem označující hospodářskou jednotku z hlediska cíle dotčené dohody, i když z právního hlediska je tato hospodářská jednotka složena z více fyzických nebo právnických osob“ (Případ Confederación Española de Empresarios de Estaciones de Servicio (odstavec 40, ECLI:EU:C:2006:784).

⁵ Vedle kritérií v článku 83 existují další ustanovení na podporu tohoto přístupu:

- recitál 141 „*Šetření, které následuje po podání stížnosti, by mělo být s výhradou soudního přezkumu provedeno v rozsahu, jenž je v daném případě přiměřený.*“

- recitál 129 „*Pravomoci dozorových úřadů by měly být vykonávány v souladu s vhodnými procesními zárukami stanovenými v právu Unie a členského státu, nestranně, spravedlivě a v přiměřených lhůtách. Každé opatření by zejména mělo být vhodné, nezbytné a přiměřené, aby byl s přihlédnutím k okolnostem každého jednotlivého případu zajištěn soulad s tímto nařízením...*“

- článek 57, odst. 1, písm. f) „*zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s článkem 80, a ve vhodné míře prošetřuje předmět stížnosti.*“

⁶ „*S cílem posílit prosazování pravidel tohoto nařízení by za jakékoliv jeho porušení měly být uloženy sankce včetně správních pokut, a to vedle nebo namísto vhodných opatření uložených dozorovým úřadem podle tohoto nařízení. V méně závažných případech porušení nebo pokud by pokuta, která bude pravděpodobně uložena, představovala pro fyzickou osobu nepřiměřenou zátěž, může být namísto pokuty uloženo napomenutí. Náležitě by se však měla zohlednit povaha, závažnost a doba trvání porušení, úmyslný charakter porušení, kroky, které byly učiněny s cílem zmírnit způsobenou škodu, míra odpovědnosti nebo jakékoli relevantní předchozí porušení, způsob, jakým se dozorový úřad o daném porušení dozvěděl, dodržování opatření, která byla vůči správci nebo zpracovateli nařízena, dodržování kodexu chování nebo jakýkoli jiný přitěžující nebo polehčující faktor. Uložení sankcí včetně správních pokut by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami právních předpisů Unie a Listiny, včetně účinné právní ochrany a spravedlivého procesu.*“

jakož i přiměřené reakce na porušení. Nejde o to brát pokuty jako nejzazší prostředek, ani se bát je dávat, nýbrž uplatňovat je způsobem, který nebude snižovat jejich účinnost coby nástroje.

Sbor, v případě své kompetence podle článku 65 Obecného nařízení, vydá závazné rozhodnutí ve věci sporu mezi úřady týkající se především stanovení, zda nastal případ porušení. Pokud podstatná a odůvodněná námitka pozvedne téma souladu nápravného opatření s Obecným nařízením, bude se rozhodnutí Sboru zabývat také otázkou, jak pokuta předepsaná v návrhu rozhodnutí dozorového úřadu zohledňuje zásadu účinnosti, přiměřenosti a odrazujícího účinku. Pokyn Sboru ve věci uplatnění článku 65 Obecného nařízení dodá další podrobnosti ohledně typu rozhodnutí, která má sbor učinit.

4. Harmonizovaný přístup ke správnímu pokutování na poli ochrany dat vyžaduje aktivní účast a výměnu informací mezi dozorovými úřady

Tato vodítka berou na vědomí, že pravomoc pokutovat je pro některé dozorové úřady novinkou vyvolávající četné otázky ohledně zdrojů, organizace a postupů. Zvláště pak rozhodnutí, při nichž budou dozorové úřady vykonávat své pravomoci pokutovat, se mohou stát předmětem odvolání u vnitrostátního soudu.

Dozorové úřady mají navzájem spolupracovat, a v případě potřeby také s Evropskou komisí, prostřednictvím mechanismů spolupráce ustavených v Obecném nařízení za účelem podpory formální a neformální výměny informací, jako jsou pravidelné semináře. Tato spolupráce se zaměří na zkušenosti a praxi při uplatňování pravomocí udělovat pokuty, přičemž hlavním cílem má být dosažení lepší konzistentnosti.

Toto aktivní sdílení informací, v doplnění k precedenčnímu právu ohledně využití těchto pravomocí, může vést k přehodnocení zásad nebo jednotlivých detailů v těchto vodítkách.

III. Kritéria posuzování v článku 83, odst. 2

Článek 83, odst. 2 poskytuje soupis kritérií, která by dozorové úřady měly používat při posuzování, zda a v jaké výši uložit pokutu. Opakované posuzování stejných kritérií se nedoporučuje, nýbrž posouzení, které vezme v úvahu všechny okolnosti každého jednotlivého případu, jak říká článek 83⁷.

Závěry učiněné v první fázi posouzení mohou být použity ve druhé části, kdy půjde o výši pokuty, čímž se předejde nutnosti posuzovat ta samá kritéria dvakrát.

Tento oddíl nabízí dozorovým úřadům pokyny, jak ve světle kritérií v článku 83, odst. 2 vykládat jednotlivá fakta případu.

(a) povaha, závažnost a délka trvání porušení;

Skoro všechny povinnosti správců a zpracovatelů podle Obecného nařízení jsou utříděny podle jejich **povahy** v ustanoveních článku 83, odst. 4 – 6. Obecné nařízení už stanovením dvou různých maximálních výší pokuty (10/20 miliónů eur) naznačuje, že porušení některých ustanovení Obecného nařízení může být závažnější, než v případě jiných ustanovení. Příslušný dozorový úřad však při posouzení skutečností případu ve světle obecných kritérií v článku 83, odst. 2 může rozhodnout, že v konkrétním případě je větší nebo omezenější potřeba reagovat nápravným opatřením ve formě pokuty. Pokud byla pokuta vybrána jako samostatné řešení nebo jako součást několika náležitých nápravných opatření, použije se pro stanovení výše pokuty, která může být udělena podle povahy daného porušení, odstupňovaný systém v Obecném nařízení (Článek 83, odst. 4 - 6).

Recitál 148 zavádí pojem „méně závažné případy porušení“. Taková porušení mohou spočívat v nedodržení jednoho nebo několika ustanovení Obecného nařízení vyjmenovaných v článku 83, odst. 4 nebo 5. Posouzení podle

⁷ V některých zemích může zvážení sankce, která má být uložena, přijít až následně po vyhodnocení, zda vůbec došlo k porušení, a to podle vnitrostátních procedurálních pravidel vyplývajících z ústavy. Proto obsah a rozsah informací v návrhu rozhodnutí vydaného vedoucím dozorovým úřadem může být v těchto zemích omezen.

Neoficiální překlad

kritérií v článku 83, odst. 2 však může dozorový úřad přivést k přesvědčení, že za konkrétních okolností nepředstavuje porušení významné riziko pro práva dotčených subjektů údajů a nepostihuje podstatu příslušné povinnosti. V takových případech může místo pokuty (ale ne vždy) přijít napomenutí.

Recitál 148 nemluví o žádné povinnosti dozorového úřadu vždy sáhnout k napomenutí v případech méně závažných porušení („*může být namísto pokuty uloženo napomenutí*“), ale spíše o možnosti, která je po ruce v závislosti na konkrétním posouzení všech okolností případu.

Recitál 148 otevírá stejnou možnost nahradit pokutu napomenutím, pokud správce je fyzická osoba a pokuta, která bude pravděpodobně uložena, by představovala nepřiměřenou zátěž. Dozorový úřad musí tedy nejprve posoudit, s ohledem na všechny okolnosti daného případu, zda je udělení pokuty žádoucí. Přikloní-li se dozorový úřad k udělení pokuty, musí posoudit, zda tato nebude pro fyzickou osobu představovat nepřiměřenou zátěž.

Obecné nařízení nestanovuje konkrétní finanční výši pro specifická porušení, pouze strop (maximální částku). Může to svědčit o poměrně nižším stupni závažnosti u porušení povinností uvedených v článku 83, odst. 4 ve srovnání s případy vyjmenovanými v článku 83, odst. 5. Účinná, přiměřená a odrazující reakce na porušení ustanovení článku 83, odst. 5 však bude záviset na okolnostech případu.

Je třeba si uvědomit, že porušení Obecného nařízení, která svou povahou mohou spadat do kategorie „až do výše 10 miliónů eur nebo až do výše 2% celkového ročního obrátu celosvětově“ stanovené v článku 83, odst. 4, by za jistých okolností mohlo nakonec spadnout do vyšší úrovně (20 miliónů eur). Mohlo by to být v případě, kdy taková porušení byla předtím předmětem nějakého nařízení od dozorového úřadu⁸, které správce nebo zpracovatel nesplnil⁹ (Článek 83, odst. 6). Ustanovení vnitrostátního práva mohou v praxi mít dopad na toto posouzení¹⁰. Povaha porušení s přihlédnutím k „*rozsahu, účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody*“, budou vypovídat o **závažnosti** porušení. Při výskytu několika různých porušení spáchaných společně v rámci jednoho určitého případu může dozorový úřad uplatnit správní pokuty, které budou účinné, přiměřené a odrazující a v rozsahu odpovídajícímu nejzávažnějšímu porušení. Proto bude-li odhaleno porušení článku 8 a článku 12, může dozorový úřad uplatnit nápravná opatření podle článku 83, odst. 5, která budou odpovídat kategorii nejzávažnějšího porušení, zejména článku 12. Podrobnější pojednání by v této fázi bylo nad rámec tohoto dokumentu (podrobná kalkulace může být předmětem případné nové verze těchto vodítek).

Dále uvedené faktory by měly být posouzeny v kombinaci např. s počtem subjektů údajů a možným dopadem na ně.

Počet dotčených subjektů údajů by měl být posouzen s ohledem na zjištění, zda jde o izolovanou nebo symptomatickou událost nebo o systémovější porušení či chybějící náležité postupy. Tím není řečeno, že u izolovaných případů by neměla být vymahatelnost, neboť i osamocené případ může postihnout mnoho subjektů údajů. Bude to, podle okolností případu, záviset například na celkovém počtu registrovaných v dané databázi, na počtu uživatelů služby, počtu zákazníků nebo na poměru k počtu obyvatel dané země.

⁸ Podle článku 58, odst. 2 lze:

- nařídit správci a zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;
- nařídit správci či zpracovateli, aby uvedli operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;
- nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle článku 17, odst. 2 a článku 19;
- nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;
- nařídit přerušování toků údajů příjemci ve třetí zemi nebo toku údajů mezinárodní organizaci.

⁹ Aplikace článku 83, odst. 6 musí nutně zohlednit vnitrostátní procesní právo. Vnitrostátní právo stanoví, jakým způsobem má být vydáno nařízení, jak ho oznámit, od jakého okamžiku nabývá účinnosti, zda existuje doba odkladu, po kterou lze pracovat na souladu. V potaz by zejména měl být vzat účinek odvolání vůči vymahatelnosti nařízení.

¹⁰ Zákonná ustanovení ohledně omezení mohou způsobit, že předchozí nařízení dozorového úřadu už nebudou brána v úvahu kvůli době, která uplynula od vydání předchozího nařízení. V některých jurisdikcích mají pravidla zakazující, aby po uplynutí promlčecí lhůty určitého nařízení byly udělovány pokuty za nesplnění daného nařízení podle článku 83, odst. 6. Bude na jednotlivých dozorových úřadech, aby zjistily, jaký účinek jejich příslušný právní řád v tomto ohledu má.

Účel zpracování musí být rovněž posouzen. Stanovisko WP 29 o „účelovém omezení“¹¹ už dříve analyzovalo dva hlavní stavební kameny této zásady v právu na ochranu osobních údajů: stanovení účelu a slučitelné použití. Při posuzování účelu zpracování v kontextu článku 83, odst. 2, by se měl dozorový úřad podívat, do jaké míry zpracování odpovídá oněm dvěma klíčovými složkami této zásady¹². V jistých situacích může dozorový úřad shledat, že bude nutné při analýze článku 83, odst. 2 vzít v potaz hlubší rozbor účelu zpracování jako takového.

Utrpí-li subjekty údajů **újmou**, musí být vzata v úvahu úroveň této škody. Zpracování osobních údajů může vyvolávat rizika pro práva a svobody jednotlivce, jak ukazuje recitál 75:

„Různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činech či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů.“

Pokud byla újma utrpěna, nebo by k ní mohlo dojít v důsledku porušení Obecného nařízení, měl by to dozorový úřad vzít v potaz při výběru nápravného opatření, byť úřad sám není příslušný pro konkrétní odškodnění této utrpěné škody.

Uložení pokuty není odvislé od schopnosti dozorového úřadu určit příčinnou souvislost mezi porušením a hmotnou ztrátou (viz například článek 83, odst. 6).

Doba trvání porušení může vypovídat například o:

- a) úmyslném jednání správce, nebo
- b) nepřijetí náležitých preventivních opatření, nebo
- c) neschopnosti zavést požadovaná technická a organizační opatření.

(b) zda k porušení došlo úmyslně nebo z nedbalosti;

Obecně řečeno, „záměr“ vyjadřuje jak vědomost, tak úmysl ve vztahu k povaze porušení zákona, přičemž „neúmyslný“ znamená, že neexistoval žádný záměr zapříčinit porušení, ačkoliv správce/zpracovatel porušil povinnost řádné péče vyžadované zákonem.

Obecně se připouští, že záměrná porušení ukazující pohrdání právem jsou závažnější, než ta neúmyslná a proto u nich bude spíše přikročeno k udělení správní pokuty. Příslušné závěry ohledně úmyslnosti nebo nedbalosti budou učiněny na základě objektivních prvků chování zjištěných ze shromážděných faktů o případu. Kromě toho, právní precedenty a praxe na poli ochrany dat, které se budou utvářet v průběhu aplikace Obecného nařízení, budou názorně dokreslovat okolnosti naznačující jasnější rozhraní pro posuzování, zda porušení bylo záměrné.

Okolnostmi ukazujícími na záměrná porušení mohou být nezákonná zpracování povolená výslovně vrcholovým vedením správce, nebo skutečněná přes radu pověřence pro ochranu osobních údajů či nerespektování stávající

¹¹ WP 203, Stanovisko 03/2013 k účelovému omezení, dostupné na:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

¹² Viz také WP 217, Stanovisko 6/2014 k pojmu legitimního zájmu správce podle článku 7, strana 24, k otázce: „Co dělá zájem „legitimním“ nebo „nelegitimním“?“

firemní politiky, například získávání a zpracování dat zaměstnanců od konkurence se záměrem diskreditovat ho na trhu.

Zde jsou další příklady:

- upravování osobních údajů, aby vznikl zavádějící (pozitivní) dojem ohledně dosažení určitých cílů – viděli jsme to v souvislosti s cílovou čekací dobou v nemocnici
- firma obchodující s osobními údaji pro marketingové účely například prodává data získaná formou „opt in“, aniž by si ověřila přání subjektů údajů, nebo na ně vůbec nebrala ohled, jak má být s jejich daty naloženo

Další okolnosti, jako neprostudování nebo neuplatnění stávající firemní politiky, lidská chyba, neprověření osobních údajů ve zveřejňovaných informacích, neuplatnění technických aktualizací včasným způsobem, nepřijetí politiky (spíše než jen její neuplatnění) jsou případy, které mohou naznačovat nedbalost.

Podniky by měly nést odpovědnost za zajištění struktur a zdrojů odpovídajících povaze a složitosti jejich podnikání. Správci ani zpracovatelé nemohou ospravedlňovat porušování práva na ochranu osobních údajů nedostatkem zdrojů. Obvyklé postupy a dokumentace činností zpracování musí zohledňovat přístup na základě rizika podle Obecného nařízení.

Existují šedé zóny, které ovlivní rozhodování, zda uložit nebo neuložit nápravné opatření, přičemž úřady mohou mít potřebu provést rozsáhlejší šetření ke zjištění skutečností okolo případu a pro zajištění, aby byly dostatečně zohledněny všechny konkrétní okolnosti každého jednotlivého případu.

(c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

Správci a zpracovatelé mají povinnost zavést technická a organizační opatření pro zajištění takové úrovně zabezpečení, která bude odpovídat riziku, zpracovat posouzení vlivu na ochranu osobních údajů a zmírnit rizika, která zpracování přináší pro práva a svobody jednotlivců. Pokud však dojde k porušení a subjekt údajů utrpí škodu, měla by odpovědná strana udělat vše, co je v jejích silách, aby omezila důsledky tohoto porušení pro dotčeného jednotlivce. K takovému odpovědnému chování (nebo jeho absenci) by měl dozorový úřad přihlídnout při výběru nápravných opatření, jakož i při výpočtu výše sankce, která má být v daném případě udělena.

Přitěžující nebo polehčující faktory se zejména hodí k doladění výše pokuty podle konkrétních okolností případu, přesto by neměla být podceňena ani jejich role při výběru náležitého nápravného opatření. V případech, kdy po posouzení ostatních kritérií zůstane dozorový úřad na pochybách ohledně vhodnosti správní pokuty jako jediného nápravného opatření nebo kombinovaného s dalšími opatřeními podle článku 58, mohou tyto přitěžující nebo polehčující okolnosti pomoci při výběru náležitých opatření nastolením rovnováhy ve prospěch toho, co se v daném případě ukáže jako účinnější, přiměřenější nebo více odrazující.

Toto ustanovení funguje jako nástroj posouzení míry odpovědnosti správce za nastalé porušení. Může se vztahovat na případy, kdy správce/zpracovatel zřetelně nezaujal lehkomyšlný/nedbalý přístup, nýbrž učinil vše, co mohl pro nápravu svého konání poté, co se o porušení dozvěděl.

Dosavadní zkušenosti dozorových úřadů z regulační činnosti podle Směrnice 95/46/ES ukazují, že je dobré projevit jistý stupeň flexibility vůči těm správcům/zpracovatelům, kteří porušení připustili a přijali odpovědnost za nápravu nebo omezení dopadu své činnosti. Uvést lze následující příklady (i když nemusí vždy vést k pružnějšímu přístupu):

- Kontaktování dalších správců /zpracovatelů, kteří mohli být dotčeni rozšířením zpracování, např. pokud došlo k mylnému sdílení nějakých dat se třetími stranami.
- Včasné kroky učiněné správcem/zpracovatelem k zamezení, aby se porušení svým pokračováním nebo rozšířením dostalo na úroveň nebo do fáze, kdy by mělo daleko vážnější dopad, než dosud.

(d) míra odpovědnosti správce či zpracovatele s přihlídnutím k technickým a organizačním opatřením jimi zavedenými podle článků 25 a 32;

Obecné nařízení zavedlo mnohem vyšší míru odpovědnosti správce v porovnání se Směrnicí 95/46/ES.

Míra odpovědnosti správce nebo zpracovatele posuzovaná na pozadí výběru náležitých nápravných opatření může zahrnovat tyto aspekty:

- Zavedl správce technická opatření respektující zásady záměrné a standardní ochrany osobních údajů (Článek 25)?
- Zavedl správce organizační opatření, která účinně uplatňují zásady záměrné a standardní ochrany osobních údajů (Článek 25) na všech úrovních organizace?
- Má správce/zpracovatel zabezpečení na náležité úrovni (Článek 32)?
- Je povědomí o postupech/politikách týkajících se ochrany a jsou v organizaci uplatněny na příslušné úrovni řízení (Článek 24)?

Článek 25 a článek 32 Obecného nařízení požadují, aby správci „[přihlédli] ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu, a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese“. Nejedná se ani tak o povinnost dosáhnout nějakého cíle, spíše tato ustanovení zavádí povinnosti ohledně prostředků, to jest, správce musí vypracovat nezbytné posudky a dobrat se k náležitým závěrům. Dozorový úřad pak musí nalézt odpověď na otázku, do jaké míry správce „učinil, co od něho mohlo být očekáváno“ vzhledem k povaze, účelům nebo velikosti zpracování, viděno ve světle povinností uložených mu Obecným nařízením.

Při tomto posouzení je třeba zohlednit všechny existující „dobré postupy“ nebo metody a uplatnit je. Odvětvové standardy i kodexy chování pro příslušnou oblast nebo profesi je rovněž důležité vzít v úvahu. Kodexy správné praxe mohou ukázat, jaké jsou sdílené postupy v dané oblasti a jaká má být úroveň znalostí ohledně různých způsobů zvládnutí typických bezpečnostních problémů souvisejících se zpracováním.

Zatímco dobré postupy by obecně měly představovat následovníhodný ideál, musí být při posuzování míry odpovědnosti přihlédnuto ke zvláštním okolnostem každého jednotlivého případu.

(e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

Účelem tohoto kritéria je posoudit dosavadní historii záznamů o subjektu, který se dopustil porušení. Dozorové úřady by si měly uvědomit, že širší posouzení tu může být docela rozsáhlá, protože jakýkoliv druh porušení Obecného nařízení, jakkoliv jiné povahy, než ten právě šetřený dozorovým úřadem, by mohl být pro posouzení „relevantní“, jelikož by mohl naznačovat obecnou míru nedostatečnosti znalostí nebo ignorování pravidel ochrany osobních údajů.

Dozorový úřad by měl posoudit následující:

- Dopustil se správce/zpracovatel stejného porušení už dříve?
- Dopustil se správce/zpracovatel porušení Obecného nařízení stejným způsobem? (například v důsledku nedostatečné znalosti stávajících postupů v organizaci nebo následkem nedostatečného posouzení rizika, nereagováním včas na žádosti subjektu údajů, nepodloženým zpožděním při reagování na tyto žádosti a podobně).

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

Článek 83, odst. 2 stanoví, že míra spolupráce se „řádně zohlední“ při rozhodování o tom, zda uložit správní pokutu a při rozhodování o výši správní pokuty. Obecné nařízení nedává přesnou odpověď na otázku, jak zohlednit snahu správce nebo zpracovatele napravit porušení již zjištěné dozorovým úřadem. Je navíc jasné, že tato kritéria budou obvykle uplatněna při výpočtu výše ukládané pokuty.

Pokud ovšem zásahem správce dojde k zamezení negativních důsledků pro práva jednotlivců nebo jejich dopad bude menší, než by jinak mohl být, může i to být zohledněno při výběru pro daný případ přiměřeného nápravného opatření.

Příklad případu, kdy spolupráce s dozorovým úřadem může být vzata v úvahu:

- Reagoval subjekt během šetření mimořádným způsobem na žádosti dozorového úřadu v daném konkrétním případě a tím ve výsledku významně omezil dopad do práv jednotlivců?

Přesto by nebylo vhodné brát dodatečný zřetel na spolupráci, která je už vyžadována zákonem, například když je subjekt každopádně povinný umožnit dozorovému úřadu vstup do svých prostor za účelem kontroly/inspekce.

(g) kategorie osobních údajů dotčené daným porušením;

Několik příkladů klíčových otázek, na které může dozorový úřad požadovat odpověď, je-li relevantní pro daný případ:

- Týká se porušení operací zpracování zvláštních kategorií dat vyjmenovaných v článku 9 nebo 10 Obecného nařízení?
- Jsou data přímo identifikovatelná/nepřímo identifikovatelná?
- Zahrnuje zpracování údaje, jejichž rozšíření by jednotlivci způsobilo bezprostřední škodu/nepohodu (spadající mimo kategorie zmíněné v článku 9 nebo 10)?
- Jsou údaje dostupné přímo bez technické ochrany nebo jsou zašifrovány¹³?

(h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

Dozorový úřad by se o porušení mohl dozvědět na základě šetření, stížností, článků v tisku, anonymních tipů nebo ohlášení správcem. Správce má podle Obecného nařízení povinnost ohlásit dozorovému úřadu případ porušení zabezpečení osobních údajů. Pokud správce pouze plní tuto povinnost, nemůže to být vykládáno jako zmírňující/polehčující okolnost. Obdobně, i správce/zpracovatel, který jednal lehkomyšlně a neučinil ohlášení nebo přinejmenším neohlásil veškeré informace o porušení z důvodu neprovedení náležitého posouzení rozsahu případu, může si od dozorového úřadu vysloužit přísnější trest, tj. věc pravděpodobně nebude klasifikována jako drobnější porušení.

(i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s tímž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

Správce nebo zpracovatel už může být v hledáčku dozorového úřadu poté, co se dříve dopustil porušení a následně styky s pověřencem pro ochranu osobních údajů, pokud existuje, byly pravděpodobně četnější. Proto bude dozorový úřad brát v potaz dřívější kontakty.

Tato posuzovací kritéria, v protikladu ke kritériím podle (e), mají dozorové úřady pouze upozornit, aby pamatovaly na opatření, která samy dříve nařídily stejnému správci či zpracovateli „v souvislosti s tímž předmětem“.

(j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42;

Dozorový úřad „monitoruje a vymáhá uplatňování tohoto nařízení“ (Článek 57, odst. 1, písm. a). Dodržování schválených kodexů chování může být správcem nebo zpracovatelem využito jako způsob doložení souladu ve smyslu článků 24, odst. 3, 28, odst. 5 a 32, odst. 3.

V případě porušení některého z ustanovení Obecného nařízení může dodržování schváleného kodexu chování napovědět, jak rozsáhlá je ze strany dozorového úřadu potřeba zásahu účinnou, přiměřenou a odrazující správní pokutou nebo jiným nápravným opatřením. Schválené kodexy chování mají podle článku 40, odst. 4 obsahovat „mechanismy, které umožňují (dohledovému) subjektu provádět povinné monitorování dodržování jeho ustanovení“.

¹³ Skutečnost, že porušení se týká jen nepřímo identifikovatelných údajů nebo dokonce dat pseudonymních/šifrovaných, by neměla být pokaždé brána jako bonusový polehčující činitel. V případě takových porušení může teprve celkové posouzení ostatních kritérií více či méně ukázat na nutnost udělení pokuty.

Tam, kde správce nebo zpracovatel dodržuje schválený kodex chování, může dozorový úřad nabýt přesvědčení, že ti z okruhu vázaného kodexem, kteří mají na starosti správu kodexu, sami podniknou náležité kroky vůči svým členům, například prostřednictvím postupů monitorování a prosazování zakotvených v kodexu. Dozorový úřad se zde může domnívat, že taková opatření jsou v daném konkrétním případě dostatečně účinná, přiměřená nebo odrazující, aniž by bylo nutné ukládat dodatečná opatření ze strany dozorového úřadu. Určité formy sankcionování nevyhovujícího chování mohou být uplatněny skrze monitorovací postupy v souladu s článkem 41, odst. 2, písm. c) a článkem 42, odst. 4, včetně pozastavení členství nebo vyloučení správce nebo zpracovatele ze společenství subjektů hlásících se ke kodexu. Pravomoci monitorovacího subjektu však jsou takové „*aniž tím jsou dotčeny úkoly a pravomoci [příslušných] dozorových úřadů*“, což znamená, že dozorový úřad není povinen vzít v úvahu předchozí uložené sankce týkající se samoregulačního nástroje.

Neplnění samoregulačních opatření by také mohlo odhalit správce/zpracovatele nedbalost nebo záměrné nedodržování pravidel.

(k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

Toto ustanovení samotné uvádí příklady, jejichž další prvky by mohly být zohledněny při rozhodování o náležitosti správní pokuty za porušení ustanovení zmíněných v článku 83, odst. 4 - 6.

Informace o zisku obdržené následkem porušení mohou být pro dozorové úřady zvláště důležité, jelikož hospodářský výnos z porušení nelze vyvážit opatřením, které nebude mít peněžní složku. Skutečnost, že správce měl z porušení Obecného nařízení zisk, může tedy představovat silný důvod k uložení pokuty.

IV. Závěr

Úvahy o problematice předložené v tomto materiálu mají dozorovým úřadům pomoci určit, na základě podstatných skutečností, ta kritéria, která jsou nejvíce užitečná pro dosažení rozhodnutí, zda udělit náležitou správní pokutu v doplnění nebo namísto dalších opatření podle článku 58. Dozorový úřad, s uvážením kontextu posuzování, stanoví v reakci na porušení nejúčinnější, nejprůměrnější a nejvíce odrazující nápravné opatření.

Článek 58 poskytuje určitý návod ohledně opatření, která dozorový úřad může zvolit, neboť jednotlivá nápravná opatření se ve své podstatě liší a jsou vhodná k dosažení různých účelů. Některá z opatření v článku 58 lze dokonce kumulovat a tím dosáhnout regulatorní akce sestávající z více než jednoho nápravného opatření.

Není vždy nezbytné doplňovat jedno opatření uplatněním dalšího. Například: účinnosti a odrazujícího vlivu zásahu ze strany dozorového úřadu může, při náležitém zvážení přiměřenosti danému případu, být dosaženo samotnou správní pokutou.

Úřady v podstatě musí znovu nastolit soulad prostřednictvím všech nápravných opatření, která mají po ruce. Dozorové úřady také budou muset vybírat nejvhodnější cestu k uskutečnění regulatorní akce. Mohou to být například trestněprávní sankce (tam, kde jsou na vnitrostátní úrovni k dispozici).

Praxe ukládání správních pokut konzistentně v celé Evropské unii je ve vývoji. Dozorové úřady by průběžně měly pořádat akce, během nichž budou spolupracovat na prohlubování konzistentnosti. Toho může být dosaženo pomocí pravidelných debat během seminářů zaměřených na vyřizování případů nebo umožňujících srovnání případů, které se objevily na zemské, národní a nadnárodní úrovni. Na podporu této činnosti se doporučuje vytvářet stále podskupiny s vazbou na příslušnou část Evropského sboru pro ochranu osobních údajů.