

Vybrané otázky implementace směrnice 2019/1937 z pohledu předpisů o ochraně osobních údajů

Tento dokument shrnuje výsledky dvou workshopů pořádaných v lednu 2022 Spolkem pro ochranu osobních údajů a Uníí podnikových právníků na téma nastavení zpracování osobních údajů v rámci whistleblowingových systémů. Níže jsou shrnuty závěry těchto workshopů a většinové názory účastníků na řešení některých otázek.¹

Směrnici se v dalším textu rozumí směrnice (EU) 2019/1937, o ochraně osob, které oznamují porušení práva Unie.

Implementačním zákonem se rozumí Sněmovní tisk 1150/0 (minulé volební období), Vládní návrh zákona o ochraně oznamovatelů.

GDPR se rozumí nařízení (EU) 2016/679, obecné nařízení o ochraně osobních údajů

I. Právní základ zpracování osobních údajů v rámci WB systémů

Určení správného právního základu zpracování osobních údajů nezbytného pro whistleblowing systém (WB) je základním předpokladem pro správnou aplikaci GDPR. Obecně je podle našeho názoru při určování právního základu možný dvojí přístup, přičemž většina názorů se kloní k využití jediného základu a tím je čl. 6 odst. 1 písm. c) (plnění právní povinnosti) pro celé zpracování v rámci WB systému. Diskutována byla dvě principiální řešení:

1. Celý WB systém podřadit pod jediný právní základ zpracování

V takovém případě by právním základem zpracování bylo buď:

- a) ustanovení čl. 6 odst. 1 písm. c) GDPR (plnění zákonných povinností). Jak je výše uvedeno, jedná se o většinový názor. Proti tomu bylo namítáno, že sice samotný systém je sice zřizován povinně, nicméně pouze u evidence oznámení předpokládá Implementační zákon dostatečně jednoznačné vymezení zpracování, které by mohlo být považováno za dostatečně určité ve smyslu čl. 6 odst. 1 písm. c) (plnění zákonných povinností) GDPR.
- b) ustanovení čl. 6 odst. 1 písm. e) či f) GDPR (veřejný zájem založený na Směrnici a Implementačním zákoně či oprávněný zájem správce).

2. Odlišovat právní základ zpracování pro jednotlivé součásti WB systému, tedy typicky:

- a. **Pořizování a vedení záznamů o oznámeních** (ve smyslu Směrnice a Implementačního zákona právní základ podle čl. 6 odst. 1 písm. c) GDPR)
- b. **Pro evidenci následných opatření** (čl. 6 odst. 1 písm. e), případně čl. 6 odst. 1 písm. f) GDPR)

¹ Jedná se pouze o pracovní dokument a výslovně upozorňujeme, že výsledný výklad dozorových orgánů může být odlišný od níže uvedených názorů. Taktéž finální verze Implementačního zákona může být odlišná.

- c. **Pro archivaci záznamů a podkladů** (čl. 6 odst. 1 písm. e), případně čl. 6 odst. 1 písm. f) GDPR)
- d. **Pro archivaci souhrnné zprávy o řešení WB případu** (čl. 6 odst. 1 písm. f)).

II. Právní základ zpracování zvláštních kategorií osobních údajů v rámci WB systémů

Pro zpracování zvláštních kategorií osobních údajů ve smyslu čl. 9 GDPR je třeba zvolit vhodný právní základ (vhodnou výjimku ze zákazu) podle tohoto článku. Zde připadají do úvahy zejména výjimky podle čl. 9 odst. 2 písm. f) a 9 odst. 2 písm. g) GDPR, tedy: *zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků* a dále *zpracování nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů* (tímto právním základem by byla Směrnice a Implementační zákon).

Ve specifických případech lze ohledně určitých údajů uvažovat i o zpracování údajů zjevně zveřejněných subjektem údajů (čl. 9 odst. 2 písm. e) GDPR), případně o výslovném souhlasu (zejména v případě oznamovatele, pokud by jej dobrovolně udělil).

Pokud by byly zpracovávány údaje o odsouzení v trestních věcech ve smyslu čl. 10 GDPR (např. v případě zhodnocení důvěryhodnosti dotčené osoby z hlediska jejích předchozích odsouzení), pak by možnost zpracování takových údajů musela být nepřímou vyvozována ze Směrnice a Implementačního zákona, příp. § 316 odst. 4 Zákoníku práce (byť jeho text není zcela příhodný).

III. Ochrana totožnosti jednotlivých osob účastných na řešení WB případů

III. a Ochrana dotčených osob

Směrnice poskytuje velmi silnou ochranu osobám dotčeným (v širokém slova smyslu) šetřením WB případů. **Bohužel je podle našeho názoru poněkud nejasná zejména ohledně úrovně ochrany, která má být poskytována dotčeným (oznámeným) osobám. Naopak je z ní zjevné, že ochrana oznamovatelů má být velmi široká a výjimky z ní velmi omezené.** Tato otázka byla účastníky workshopů široce diskutována, zejména z toho pohledu, že pokud by měla být poskytnuta dotčeným osobám (oznámeným) v principu stejná ochrana, jako oznamovatelům, znemožnilo by to pověřeným osobám řádně vyšetřit dotčený případ (např. informovat vedoucího dotčené osoby za účelem získání dalších podkladů). Domníváme se, že de facto absolutní ochrana (až na výslovně stanovené výjimky) je tak Směrnicí poskytována pouze oznamovatelům samotným, úroveň ochrany poskytované dotčeným osobám musí být vykládána funkčně a není na stejné úrovni jako ochrana oznamovatelů.

Rozhodujícími ustanoveními Směrnice jsou podle našeho názoru:

- **Rec. 76:** *Členské státy by měly zajistit, aby příslušné orgány zavedly náležité postupy ochrany při zpracovávání oznámení a pro ochranu osobních údajů osob, jichž se oznámení týká. Tyto postupy by měly zajistit, aby ve všech fázích postupu byla chráněna totožnost každé oznamující osoby, dotčené osoby a třetích osob uvedených v oznámení, například svědků nebo kolegů.*
- **Rec. 82:** *Zajištění utajení totožnosti oznamující osoby v průběhu procesu oznamování a šetření podněceného oznámením je zásadním opatřením ex-ante k zabránění odvetným opatřením.*
- **Rec. 100:** *Práva dotčené osoby by měla být chráněna, aby se zabránilo poškození její dobré pověsti či jiným nepříznivým důsledkům. V každé fázi postupu na základě oznámení by mělo být mimoto plně respektováno právo dotčené osoby na obhajobu a na přístup k právní ochraně v*

souladu s články 47 a 48 Listiny. **Členské státy by měly chránit utajení totožnosti dotčené osoby a zajistit právo na obhajobu**, včetně práva na přístup ke spisu, práva být vyslechnut a práva využít účinný opravný prostředek proti rozhodnutí týkajícímu se této osoby podle platných postupů stanovených ve vnitrostátním právu v rámci vyšetřování nebo následných soudních řízení.

- **Čl. 9 odst. 1 písm a): kanály pro přijímání oznámení**, které jsou navrženy, zavedeny a provozovány bezpečným způsobem, jenž **zajišťuje ochranu utajení totožnosti oznamující osoby a veškerých třetích osob zmíněných v oznámení** a zabraňuje přístupu neoprávněných pracovníků
- **Čl. 16 odst. 1:** Členské státy zajistí, aby **totožnost oznamující osoby nebyla sdělena bez jejího výslovného souhlasu** nikomu kromě oprávněných pracovníků příslušných k přijímání oznámení nebo následných opatření. Totéž se vztahuje i na jakékoli další informace, z nichž by mohla být přímo či nepřímo vyvozena totožnost oznamující osoby.
- **Čl. 22 odst. 2 a 3: Příslušné orgány v souladu s vnitrostátním právem** zajistí, aby **totožnost dotčených osob** byla chráněna po celou dobu průběhu šetření podníceného oznámením nebo zveřejněním. Pravidla stanovená v článcích 12, 17 a 18² týkající se ochrany totožnosti oznamující osoby se vztahují i na ochranu totožnosti dotčených osob.

Z výše uvedených ustanovení podle našeho názoru vyplývá, že by sice měla být dotčeným osobám poskytnuta silná ochrana, ta by však neměla jakkoliv bránit samotnému šetření WB případu, uplatnění odpovídajících sankčních opatření vůči dotčeným osobám a **to, ani kdyby bylo v průběhu těchto činností nutné totožnost dotčené osoby sdělit jiným osobám**; neměla by ani bránit předání údajů o dotčené osobě orgánům veřejné správy v odůvodněných případech (např. podání trestního oznámení apod.).

III. b Ochrana oznamovatelů v případech, kdy oznámení není podáváno v rámci věcné působnosti Směrnice/Implementačního zákona

Rozhodujícími ustanoveními Směrnice jsou podle našeho názoru:

- **Čl. 6 odst. 1: Oznamující osoby mají nárok na ochranu podle této směrnice, jestliže:**
 - a) **měly oprávněné důvody se domnívat**, že oznámené informace o porušení byly v době oznámení **pravdivé** a že tyto informace **spadaly do oblasti působnosti této směrnice** a
 - b) **podaly oznámení** buď interně v souladu s článkem 7 nebo externě v souladu s článkem 10, nebo učinily zveřejnění v souladu s článkem 15
- Rec. 36: Základním důvodem pro zajištění ochrany těchto osob je jejich ekonomická zranitelnost plynoucí ze vztahu k osobě, na níž jsou fakticky pracovně závislé. **Neexistuje-li takováto nerovnováha sil v souvislosti s prací, například v případě běžných stěžovatelů nebo nezúčastněných osob z řad občanů, není ochrana před odvetnými opatřeními nutná.**
- Rec. 46: Ochrana by se současně neměla vztahovat na osoby, které oznámí informace, které již jsou zcela zpřístupněny veřejnosti, nebo na **nepodložené zvěsti a zprávy z doslechu.**

² Zde považujeme za důležité upozornit na to, že toto ustanovení neodkazuje na čl. 16, který je základním ustanovením pro zvýšenou ochranu oznamovatelů a dále na to, že adresáty této normy jsou „příslušné orgány“, nikoliv samotné subjekty, které přijímají WB oznámení.

- Rec. 82: *Ochrana utajení totožnosti by se neměla uplatnit, pokud oznamující osoba úmyslně odhalí svou totožnost v souvislosti se zveřejněním informací.*

Pokud by oznámení bylo podáno mimo rámec těchto ustanovení, nevztahovala by se na oznamovatele široká ochrana podle Směrnice. **Bylo by však nutné plně aplikovat GDPR, tedy zejména dodržovat požadavky na kompatibilitu účelů a v případě dalšího zpracování na základě čl. 6 odst. 1 písm. f) GDPR řádně provést balanční test.**

IV. Charakter vyjádření oznamovatele ve smyslu § 20 odst. 3 návrhu Implementačního zákona

Podle tohoto ustanovení: *Poskytují-li příslušná osoba nebo pověřený zaměstnanec informaci o totožnosti oznamovatele orgánu veřejné moci podle odstavce 2, jsou povinni o tom předem oznamovatele vyrozumět společně s důvody, pro které jsou povinni informaci o totožnosti poskytnout, a umožnit oznamovateli, aby se k poskytnutí informace vyjádřil.*

Podle našeho názoru toto vyjádření je institutem sui generis WB práva a nelze je považovat za námitku ve smyslu čl. 21 GDPR a to mj. proto, že při předání podle § 20 odst. 3 návrhu Implementačního zákona se jedná o plnění právní povinnosti (viz text § 20 odst. 2), kde námitka podle GDPR nepřichází pojmově v úvahu. Vyjádření je tak spíše procesní zárukou; o kombinaci s námitkou podle GDPR by se u vyjádření však mohlo jednat tehdy, pokud by příslušná osoba předávala ve smyslu § 20 odst. 2 další, nikoliv výslovně státním orgánem vyžádané údaje. Zde by se pak mohlo jednat o zpracování ve veřejném zájmu ve smyslu čl. 6 odst. 1 písm. e) GDPR, kde by již námitka pojmově v úvahu přicházela.

V. Informační povinnost podle čl. 13 a čl. 14 GDPR

U plnění informační povinnosti je třeba dle našeho názoru rozlišovat tyto skupiny osob:

- **Oznamovatele**
- **Dotčenou osobu (oznámeného)**
- **Svědky**
- **Ostatní osoby**

Zde bylo zejména diskutováno, zda postačuje obecné neadresné poučení např. na webových stránkách příslušného správce. Zatímco totiž u oznamovatele bude obvykle možné splnit individuálně poučovací povinnost bez problémů, u ostatních kategorií osob již může narazit splnění této povinnosti na právní či faktické překážky. Např. u dotčené osoby (oznámeného) by brzké splnění informační povinnosti mohlo fakticky zmařit šetření či dokonce vést k vyzrazení totožnosti oznamovatele.

Diskutováno bylo taktéž možné využití § 11 zákona č. 110/2019 Sb., kde sice lze WB systémy považovat za zpracování vyhovující podmínkám § 6 odst. 2 písm. b) a c) tohoto zákona (předcházení, vyhledávání nebo odhalování trestné činnosti a jiný důležitý cíl veřejného zájmu Evropské unie nebo členského státu Evropské unie), a proto by bylo možné splnit informační povinnost pouze v přiměřeně upraveném rozsahu či ji odložit, nicméně s ohledem na absenci jakýchkoliv konkrétních výjimek v návrhu Implementačního zákona je třeba k aplikaci § 11 přistupovat obezřetně. Bylo by také nutné provést oznámení ÚOOÚ podle § 11 odst. 2 zákona č. 110/2019 Sb.

Pokud se jedná o obecné neadresné poučení např. na webových stránkách příslušného správce, zde bylo upozorněno na to, že dříve zveřejněná doporučení zahraničních dozorových orgánů (DSK, EDPS) spíše požadují individuální poučení (zejména u oznamovatele, dotčené osoby a případně vybraných svědků). Nelze však zcela vyloučit, že by i neadresné poučení dotčené osoby a ostatních osoby (vyjma

oznamovatel) postačovalo v případě, kdy WB oznámení bylo odloženo, či naopak byla dotčená osoba seznámena s šetřením (aniž by musela být specificky odkazována na poučení). V konkrétním případě lze rovněž aplikovat výjimky z informační povinnosti podle čl. 14 odst. 5 GDPR.

Pokud by však v důsledku splnění informační povinnosti hrozilo odhalení totožnosti oznamovatele, je podle našeho názoru vždy třeba upřednostnit jeho ochranu (a tomu přizpůsobit formu a dobu splnění informační povinnosti, případně její splnění odložit). Viz i dále komentář k čl. 15 GDPR.

Vždy je ale třeba zvážit i splnění informační povinnosti ad hoc (např. při předání informací orgánu veřejné moci).

VI. Právo na přístup podle čl. 15 GDPR

Subjekty údajů mají podle čl. 15 GDPR právo na přístup k údajům o zpracování, které zahrnuje i právo získat kopii zpracovávaných údajů. Toto právo tedy náleží jak oznamovatelům, tak dotčeným osobám (oznámeným) tak jakýmkoliv dalším osobám v oznámení zmíněným či osobám, jejichž osobní údaje byly shromážděny v souvislosti s interním vyšetřováním WB případu. Právo na přístup je přitom velmi důležitým právem subjektů údajů, které zásadním způsobem zvyšuje jejich kontrolu nad procesem zpracování.

Z pohledu GDPR zahrnuje právo na přístup možnost získat celkové přehledové informace o zpracování (čl. 15 odst. 1 a 2) a konkrétní kopii zpracovávaných údajů (čl. 15 odst. 3). GDPR u celkových přehledových údajů v principu neumožňuje poskytnutí této informace odmítnout (až na velmi specifické případy podle čl. 12, či případně výjimky ve zvláštních předpisech podle čl. 23 GDPR). U poskytnutí kopie údajů umožňuje toto právo omezit v čl. 15 odst. 4: *Právem získat kopii uvedenou v odstavci 3 nesmějí být nepříznivě dotčena práva a svobody jiných osob.*

Ustanovení Směrnice týkající se ochrany oznamovatele (čl. 16), je však třeba považovat za výjimku z pravidel GDPR přijatou ve smyslu čl. 23 GDPR, a tedy vůči GDPR lex specialis. Proto v případě, kdy by splnění informační povinnosti v rámci práva na přístup znamenalo vyjádření totožnosti oznamovatele, je možné její splnění odepřít.

Na osobu, která bude na žádost o přístup k osobním údajům podle čl. 15 GDPR odpovídat, však tato konstrukce klade vysoké nároky a bude vždy nutné postupovat případ od případu podle konkrétních skutkových okolností.

Zde je podle našeho názoru třeba vycházet z těchto hledisek:

1. V rámci odpovědi na žádost podle čl. 15 GDPR **nelze uvádět nepravdivé informace** (např. že údaje nejsou zpracovávány, pokud ve skutečnosti zpracovávány budou)
2. V některých **případech i samotné sdělení informace, že údaje jsou (za konkrétním účelem) zpracovávány, mohou vést ke ztotožnění oznamovatele** (oznámený bude mít podezření, že konkrétní zaměstnanec využil WB linku a samotné potvrzení zahájení WB šetření by toto potvrzení potvrdilo). Zde sice stále platí, že nelze poskytnout nepravdivou informaci, ovšem zároveň je nutné ochránit oznamovatele. Jako vhodné řešení se jeví např. standardizovaná odpověď „*údaje nejsou zpracovávány nebo není možné tuto informaci poskytnout*“, která by byla předávána při všech žádostech o přístup, kdy buď nedochází ke zpracování, nebo poskytnutí této informace brání zákonné překážky, případně prosté neposkytnutí informace. Totéž platí i ve vztahu k dalším osobám, jejichž informace jsou zpracovávány (potenciální svědci apod.).

3. Pokud z nějakého důvodu odpadne ochrana oznamovatele (např. oznamovatel svoji identitu zveřejní), není nutné ex post poslat dodatečnou reakci na původní žádost o přístup ze strany oznámeného. Informace mu bude poskytnuta pouze v případě, kdy znovu požádá. **I v takovém případě je však třeba pečlivě zvažovat, jaké informace budou poskytnuty (např. obsah oznámení) a to v návaznosti povinnost podle čl. 15 odst. 4 GDPR (k tomu i např. rec. 76 a 84 Směrnice).** Zde se nabízí otázka, zda by nebylo vhodnější, aby Implementační zákon výslovně omezil právo na přístup ve smyslu rec. 84 Směrnice, resp. stanovil vhodné výjimky a omezení.

V rámci praktického vyřizování žádosti považujeme za přípustný taktéž takový postup, kdy osoba pověřená agendou ochrany osobních údajů v případě doručení žádosti o přístup vyřídí tuto žádost co do své kompetence a pokud se jedná o WB, předá tuto žádost pověřené osobě k vyřízení, pokud jde o údaje zpracovávané v rámci WB systému. Pokud pověřená osoba zjistí, že v rámci WB systému nejsou vedeny žádné údaje nebo případně že se uplatní výjimky z povinnosti poskytnout informaci, takovou žádost bez dalšího odloží, aniž by informovala žadatele. I v takovém případě by však v poučení ohledně zpracování osobních údajů v rámci vyřizování žádostí o přístup mělo být alespoň obecně uvedeno, že tento případ může nastat. Pokud by osoba pověřená agendou ochrany osobních údajů přímo vyřizovala žádost i ohledně údajů zpracovávaných v rámci WB systému, je třeba zajistit takové nastavení procesů, které zajistí důvěrnost totožnosti zejména oznamovatele.

V rámci diskuze o praktickém vyřizování žádosti byla dále zvažována možnost, aby správce v rámci svých zveřejněných zásad k výkonu práv dle GDPR žadatele předem obecným způsobem poučil, že žádá-li právo na přístup k osobním údajům zpracovávaným v rámci vnitřního oznamovacího systému, je nezbytné, aby tento požadavek v rámci práva na přístup uvedl. I v tomto případě platí, že je nutné následně při odpovědi k takto vyžádanému právu na přístup chránit oznamovatele a další osoby, jak uvedeno v odstavci 2. výše, a odpověď vhodně formulovat.

VII. Doba zpracování

Diskutovanou otázkou byla taktéž doba uchovávání zpracovávaných údajů v rámci WB systémů.

Zde se může jednat o tyto okruhy dokumentů:

1. **Záznamy o oznámeních**
2. **Dokumentace týkající se šetření WB případu a následných opatření**, kde lze rozlišit dvě subvarianty
 - a. Šetření potvrdilo podezření
 - b. Šetření toto podezření nepotvrdilo
3. **Souhrnná zpráva o WB případu**

Návrh Implementačního zákona řeší výslovně pouze dobu uchovávání oznámení, kde v § 21 odst. 2 stanoví pětiletou retenční dobu.

Domníváme se, že tato pětiletá doba od zahájení šetření (doručení oznámení) by měla být aplikována na všechny dokumenty spojené s WB případem, byť jsme si vědomi, že některé zahraniční dozorové orgány navrhuje pro případ, kdy se podezření nepotvrdí, výrazně kratší retenční dobu. Výjimky vedoucí k prodloužení pětileté doby by měly být přípustné pouze ve zvláštních případech (např. stále běžící šetření orgánu veřejné správy nebo soudní spor, nebo je povinnost stanovena jiným právním předpisem – zákon č. 499/2004 Sb., o archivnictví a spisové službě). Po uplynutí retenční doby mohou být uvedené dokumenty uchovávány v zásadě jen v anonymizované podobě. Domníváme se však, že s ohledem na nutnost prokazovat funkčnost WB systému, by mělo být možné tuto zprávu uchovávat

v podobě, která bude i pouze pseudonymizovaná (s ohledem na široký koncept identifikovatelnosti v GDPR), nicméně by taková pseudonymizace měla být provedena důsledně (např. spíše obecné označení organizační jednotky, v níž je dotčená osoba činná, neuvádění ani iniciál dotčených osob apod.).

VIII. Specifika zpracovatelské smlouvy s externím dodavatelem WB systému

Čl. 28 GDPR vyžaduje uzavření smlouvy o zpracování osobních údajů mezi správcem a zpracovatelem. V případě externího dodavatele WB systému bude obvykle tento dodavatel tzv. zpracovatelem osobních údajů (ponecháváme zde prozatím stranou otázku sdílení WB systémů podle čl. 8/6 směrnice).

Ačkoliv co do povinných náležitostí takové smlouvy se zpracovatelem – dodavatelem WB systému se smlouva s ním nebude odlišovat od běžných smluv o zpracování osobních údajů, je přesto třeba již při přípravě smlouvy mít na paměti specifika takové smlouvy pro takové zpracovatele. Zejména se jedná o:

- Určení pověřené osoby jako osoby kontaktní tak, aby se omezilo riziko vyrazení totožnosti oznamovatele.
- Zvláštní úpravu auditů a kontroly souvisejícího zpracování osobních údajů, např. vedení evidence oznámení (zejména pokud by měla být v jejich rámci kontrolována „ostrá“ data).
- Zvýšené požadavky na zabezpečení a ujednání o mlčenlivosti, zejména pokud se týká poučení o mlčenlivosti podle Směrnice a Implementačního zákona.
- Zvláštní ujednání o střetu zájmů, které může mít specifické požadavky (viz např. rec. 56 Směrnice).

IX. Další otázky

Dále jsme se zabývali několika dílčími otázkami s tímto výsledkem:

1. Domníváme se, že **zpracování údajů v rámci WB systému samo o sobě nepodléhá povinnosti provedení DPIA** (posouzení vlivu na zpracování osobních údajů), a to s ohledem na ustanovení § 10 Zákona č. 110/2019 Sb. o zpracování osobních údajů (byť je možné zejména u větších organizací jeho provedení zvážit).
2. Domníváme se, že **pověřenec pro ochranu osobních údajů může vykonávat funkci pověřené osoby**, je však nutné jasně oddělit kanály pro přijímání oznámení v rámci WB systému a v rámci GDPR, aby pověřenec vždy věděl, v jakém režimu je povinen oznámení zpracovávat. Je rovněž nutné dořešit případ, kdy WB oznámení směřuje do oblasti zpracování osobních údajů, protože takové oznámení DPO kvůli střetu zájmů prošetřit nemůže.
3. **Vztah jednotlivých správců při sdílení zdrojů podle čl. 8 odst. 6 Směrnice** může být podle charakteru spolupráce vztahem samostatných správců, vzájemných správců a zpracovatelů a také vztahem společných správců. Vždy bude záležet na konkrétním nastavení spolupráce.
4. **V případě data breach (porušení zabezpečení osobních údajů) je i pověřená osoba povinna takové porušení zabezpečení ohlásit běžnými kanály užívanými v dané organizaci**, případně zajistit oznámení subjektům údajů ve smyslu čl. 34 GDPR. Domníváme se, že v zájmu zachování důvěrnosti by mělo být dobrou praxí, že takové oznámení provede pověřená osoba za případné součinnosti osoby pověřené agendou ochrany osobních údajů.

X. Závěr

Spolek pro ochranu osobních údajů a Unie podnikových právníků vítají možnost diskutovat návrh Implementačního zákona včetně specifických bodů týkajících se zpracování osobních údajů. V tomto dokumentu jsou zdůrazněny některé nevyjasněné otázky, které v praxi mohou velmi reálně ztížit řádné zavedení či provoz whistleblowing systému, resp. související míru ochrany soukromí dotčených osob.

Spolek i Unie podnikových právníků proto uvítají, pokud návrh Implementačního zákona bude předložen k veřejné diskusi, a jsou připraveny zprostředkovat poznatky svých členů, kteří již nejen výše uvedené otázky v praxi řeší.

Praha, 6.2.2022

Zpracovali: Vladan Rámiš, Alice Selby, Jitka Pišl Drábková, František Nonnemann, Vladimír Valenta