Společné stanovisko EDPB a EIOÚ [4/2026]

k návrhu aktu o kybernetické bezpečnosti 2
a návrhu změn směrnice NIS 2

Přijato dne 18. března 2026

Obsah

Shrnutí

Dne 20. ledna 2026 vydala Evropská komise návrh nařízení o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) a návrh směrnice, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2]. Dne 21. ledna 2026 Komise formálně konzultovala EDPB a EIOÚ v souladu s čl. 42 odst. 2 nařízení (EU) 2018/1725.

EDPB a EIOÚ připomínají, že vztah mezi ochranou údajů a kybernetickou bezpečností je oboustranný. Na jedné straně slouží kybernetická bezpečnost k ochraně osobních údajů tím, že omezuje rizika nežádoucího přístupu k těmto údajům, jejich změny nebo nedostupnosti. Na druhou stranu mohou některá opatření kybernetické bezpečnosti zasahovat do práv a svobod jednotlivců, zejména do práva na soukromí a ochranu údajů. I když je tedy u opatření kybernetické bezpečnosti kladen důraz na účinnost, je třeba zvážit i nezbytnost a přiměřenost.

EDPB a EIOÚ podporují obecný cíl návrhů posílit úlohu agentury ENISA a usnadnit zavádění certifikace kybernetické bezpečnosti, a to s výhradou konkrétních doporučení uvedených v tomto společném stanovisku. Vítají rovněž cíl stanovit ve směrnici (EU) 2022/2555 mechanismy a podmínky, které pomohou usnadnit dodržování požadavků na kybernetickou bezpečnost, a tím učinit jejich provádění soudržnějším a účinnějším, jakož i cíl dále řešit různá rizika pro dodavatelské řetězce IKT, včetně těch netechnických. EDPB a EIOÚ rovněž důrazně podporují cíl zřízení jednotného kontaktního místa pro oznamování případů porušení ochrany osobních údajů, neboť by se tím snížila administrativní zátěž organizací, aniž by to mělo vliv na úroveň ochrany subjektů údajů.

EDPB a EIOÚ rovněž vítají, že návrh aktu o kybernetické bezpečnosti 2 poskytne další objasnění způsobů, jakými agentura ENISA poskytuje podporu různým zúčastněným stranám, a doporučují doplnit také EIOÚ jako možného žadatele o poradenství od agentury ENISA. EDPB a EIOÚ důrazně prosazují, aby takové poradenství následovalo po podání žádosti, čímž se zajistí jasná koordinace a jasné rozdělení odpovědnosti.

Pokud jde o spolupráci mezi agenturou ENISA a dalšími subjekty Unie obecně, EDPB a EIOÚ vítají synergie, které tato spolupráce může umožnit v souladu s jejich příslušnými úkoly a mandáty. Doporučují doplnit výslovný odkaz také na EIOÚ jako instituci Unie, s kterou by agentura ENISA spolupracovala.

EDPB a EIOÚ se domnívají, že pokud by budoucí úkoly agentury ENISA jako informačního centra vyžadovaly zpracování osobních údajů ve značném rozsahu, mělo by to být výslovně uvedeno v ustanoveních základního aktu, kterým se příslušné úkoly řídí, včetně základních prvků jakéhokoli rozsáhlého zpracování a příslušných ochranných opatření. Pokud je naopak cílem umožnit agentuře ENISA především shromažďovat a dále zpracovávat převážně souhrnné neosobní údaje, mělo by to být rovněž objasněno.

EDPB a EIOÚ připomínají, že v zásadě by mělo být v rámci správní autonomie dotčeného orgánu EU (v tomto případě správní rady decentralizované agentury) rozhodováno pouze o velmi technických (praktických) detailech souvisejících se zpracováním osobních údajů. Kromě toho EDPB a EIOÚ doporučují, aby v článku 66 návrhu aktu o kybernetické bezpečnosti 2 byla před přijetím těchto pravidel stanovena předchozí konzultace s EIOÚ.

Pokud jde o Evropský rámec dovedností v oblasti kybernetické bezpečnosti (dále jen „ECSF“), EDPB a EIOÚ doporučují spolunormotvůrcům, aby změnili čl. 19 odst. 2 návrhu aktu o kybernetické bezpečnosti 2 tak, aby se rámec ECSF neomezoval výhradně na „odborníky v oblasti kybernetické bezpečnosti“, ale aby zahrnoval i profily pro obecnou pracovní sílu.

Pokud jde o evropský rámec pro certifikaci kybernetické bezpečnosti, EDPB a EIOÚ doporučují dále vyjasnit oblast působnosti čl. 80 odst. 1 písm. w) aktu o kybernetické bezpečnosti 2 a vztah k certifikaci podle obecného nařízení o ochraně osobních údajů (dále jen „GDPR“). Kromě toho EDPB a EIOÚ doporučují, aby agentura ENISA byla před přijetím schématu certifikace podle čl. 80 odst. 1 písm. w) aktu o kybernetické bezpečnosti 2 povinna konzultovat EDPB, a zajistila se tak jednotnost postupů.

EDPB a EIOÚ zdůrazňují, že je třeba zvážit nejen účinnost opatření kybernetické bezpečnosti, ale také jejich nezbytnost a přiměřenost. EDPB a EIOÚ doporučují vyjasnit, že schémata certifikace by měla v co největší míře zohledňovat bezpečnostní kontroly, které mohou pomoci prokázat splnění požadavků GDPR, zejména pokud se schémata vztahují na produkty IKT, služby IKT, procesy IKT a řízené bezpečnostní služby, které budou pravděpodobně využívány při operacích zpracování údajů.

EDPB a EIOÚ dále vítají navrhované opatření, jehož cílem je zajistit rámec pro důvěryhodné dodavatelské řetězce IKT a řešit netechnická rizika ve vysoce kritických odvětvích.

Pokud jde o návrh, kterým se mění směrnice NIS 2, EDPB a EIOÚ vítají označení evropských peněženek digitální identity a evropských podnikatelských peněženek jako „základních subjektů“ a plně podporují důležitý cíl, kterým je zabránit budoucím ransomwarovým útokům a narušit a zlikvidovat zločinecké organizace, které za nimi stojí.

Evropský sbor pro ochranu osobních údajů a evropský inspektor ochrany údajů

s ohledem na čl. 42 odst. 2 nařízení (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES

přijali toto společné stanovisko (dále jen „stanovisko“)

1 SOUVISLOSTI

1. Dne 20. ledna 2026 vydala Evropská komise (dále jen „Komise“) návrh nařízení o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2)[1] a návrh směrnice, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2][2] (dále jen „návrh aktu o kybernetické bezpečnosti 2“, „návrh změn směrnice NIS 2“ a společně „návrhy“). Dne 21. ledna 2026 Komise formálně konzultovala EDPB a EIOÚ v souladu s čl. 42 odst. 2 nařízení (EU) 2018/1725 (dále jen „EUDPR“)[3].
2. Cílem návrhu aktu o kybernetické bezpečnosti 2 je nahradit stávající akt o kybernetické bezpečnosti [4], aby se 1) posílila úlohu agentury ENISA se zaměřením na potřeby zúčastněných stran ve stále nepřátelštějším prostředí hrozeb, 2) oživilo provádění evropského rámce pro certifikaci kybernetické bezpečnosti, 3) snížila složitost a rozmanitost politik souvisejících s kybernetickou bezpečností a 4) dále řešila bezpečnostní rizika dodavatelského řetězce IKT[5].
3. Návrh změn směrnice NIS 2 se zaměřuje zejména na třetí cíl, a to zavedením upřesnění a zjednodušením dodržování předpisů pro regulované subjekty[6].
4. Cílem tohoto společného stanoviska je zabývat se příslušnými aspekty návrhů, které mají zvláštní význam pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů.

2 OBECNÉ INFORMACE

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).
[4] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj), ve znění nařízení Evropského parlamentu a Rady (EU) 2025/37 ze dne 19. prosince 2024, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby (Úř. věst. L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] Důvodová zpráva, COM(2026) 11 final, s. 1.
[6] COM(2026) 13 final.

5. Cílem návrhu aktu o kybernetické bezpečnosti 2 je rozšířit mandát agentury ENISA a zvýšit její operativnost. EDPB a EIOÚ podporují posílení úlohy agentury ENISA a cíl usnadnit zavádění certifikace kybernetické bezpečnosti, obojí s výhradou níže uvedených konkrétních doporučení.

6. EDPB a EIOÚ rovněž vítají cíl stanovit ve směrnici (EU) 2022/2555[7] (dále jen „směrnice NIS 2“) mechanismy a podmínky, které pomohou usnadnit dodržování požadavků na kybernetickou bezpečnost, a tím učinit jejich provádění soudržnějším a účinnějším, jakož i cíl dále řešit různá rizika pro dodavatelské řetězce IKT, včetně netechnických.

7. Jak již uvedli ve svém společném stanovisku k návrhu souhrnného balíčku pro digitální oblast[8], EDPB a EIOÚ důrazně podporují cíl zřízení jednotného kontaktního místa pro oznamování případů porušení ochrany osobních údajů, neboť by to snížilo administrativní zátěž organizací, aniž by to mělo vliv na úroveň ochrany subjektů údajů.

8. Ustanovení čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679 (GDPR) stanoví bezpečnost jako jednu z hlavních zásad týkajících se zpracování osobních údajů. Článek 32 GDPR dále definuje tuto povinnost, která se vztahuje na správce i zpracovatele, a to zajistit odpovídající úroveň zabezpečení. Z obou ustanovení jasně vyplývá, že zabezpečení zpracování osobních údajů je nezbytné pro dodržení právních předpisů EU o ochraně údajů.

9. Vztah mezi ochranou údajů a kybernetickou bezpečností je oboustranný. Na jedné straně slouží kybernetická bezpečnost k ochraně osobních údajů tím, že omezuje rizika nežádoucího přístupu k těmto údajům, jejich změny nebo nedostupnosti. Na druhou stranu mohou některá opatření kybernetické bezpečnosti zasahovat do práv a svobod jednotlivců, zejména do práva na soukromí a ochranu údajů[9].

10. EDPB a EIOÚ připomínají, že 49. bod odůvodnění GDPR uznává, že opatření v oblasti kybernetické bezpečnosti zahrnující zpracování osobních údajů představují oprávněný zájem dotčeného správce údajů, a zároveň zdůrazňuje, že tato opatření by měla být přísně nezbytná a přiměřená pro účely zajištění bezpečnosti sítě a informací. V důsledku toho by se opatření v oblasti kybernetické bezpečnosti neměla řídit pouze hlediskem účinnosti, ale měla by také zvažovat, zda jejich dopad na základní práva zůstává omezen na to, co je nezbytné a přiměřené.

3 PODPORA AGENTURY ENISA PŘI PROVÁDĚNÍ POLITIKY A PRÁVA UNIE A SPOLUPRÁCE S OSTATNÍMI SUBJEKTY UNIE

11. Podle čl. 5 odst. 1 návrhu aktu o kybernetické bezpečnosti 2 přispívá agentura ENISA k provádění politiky a práva Unie v různých oblastech tím, že poskytuje podporu různým zúčastněným stranám uvedeným v tomto článku.

[7] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).
[8] Společné stanovisko EDPB a EIOÚ 2/2026 k návrhu nařízení, pokud jde o zjednodušení digitálního právního rámce (souhrnný balíček pro digitální oblast), přijaté dne 10. února 2026.
[9] Viz EIOÚ stanovisko 5/2021 ke strategii kybernetické bezpečnosti a směrnici NIS 2.0, 11. března 2021, body 10–11, EIOÚ stanovisko 7/2022 k návrhu nařízení o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie, 17. května 2022, body 9–10, a EIOÚ stanovisko 2/2024 k návrhu nařízení, kterým se mění akt o kybernetické bezpečnosti, pokud jde o řízené bezpečnostní služby, 10. ledna 2024, bod 5.

12. V souladu s čl. 5 odst. 1 písm. h) návrhu aktu o kybernetické bezpečnosti 2 by agentura ENISA mimo jiné poskytovala na žádost Evropského sboru pro ochranu osobních údajů poradenství ohledně provádění konkrétních aspektů kybernetické bezpečnosti politiky a práva Unie souvisejících s ochranou údajů a soukromí. EDPB a EIOÚ konstatují, že čl. 5 odst. 1 písm. h) návrhu aktu o kybernetické bezpečnosti 2 není zcela novým ustanovením. Ustanovení čl. 5 odst. 5 písm. c) stávajícího aktu o kybernetické bezpečnosti již stanoví, že agentura ENISA může podporovat „členské státy při provádění konkrétních aspektů kybernetické bezpečnosti v rámci politiky a práva Unie ve vztahu k ochraně údajů a soukromí a to též poskytováním poradenství Evropskému sboru pro ochranu osobních údajů na jeho žádost“.

13. EDPB a EIOÚ vítají, že návrh aktu o kybernetické bezpečnosti 2 poskytne další vyjasnění způsobů spolupráce při zachování základních prvků čl. 5 odst. 5 písm. c) aktu o kybernetické bezpečnosti. Nový čl. 5 odst. 1 písm. h) by vyjasnil, že EDPB jako orgán Unie je oprávněn přímo požádat agenturu ENISA o poradenství (aniž by bylo vázáno na provádění konkrétních aspektů kybernetické bezpečnosti politiky a práva Unie týkajících se ochrany údajů a soukromí členskými státy).

14. Současně EDPB a EIOÚ doporučují doplnit do čl. 5 odst. 1 písm. h) aktu o kybernetické bezpečnosti 2 jako možného žadatele také EIOÚ, a to s ohledem na jeho úlohu dozorového úřadu pro zpracování osobních údajů orgány, institucemi a jinými subjekty Evropské unie. Budou-li mít EDPB i EIOÚ možnost využívat technické kompetence agentury ENISA v oblasti kybernetické bezpečnosti, může to přispět k tomu, aby jejich pokyny a rozhodnutí v oblasti ochrany údajů vycházely z nejnovějších poznatků v oblasti kybernetické bezpečnosti. Poradenství a spolupráce by mohly být přínosné v několika oblastech, včetně standardů a provozních postupů kybernetické bezpečnosti, jakož i používání technologií zvyšujících ochranu soukromí v souvislosti s kybernetickou bezpečností.

15. EDPB a EIOÚ důrazně podporují, aby se poradenství uvedené v čl. 5 odst. 1 písm. h) aktu o kybernetické bezpečnosti 2 poskytovalo pouze na základě předchozí žádosti EDPB nebo, jak je zde navrhováno, EIOÚ. Stanovením toho, že agentura ENISA jedná pouze na žádost EDPB nebo EIOÚ, by čl. 5 odst. 1 písm. h) zajistil jasnou koordinaci a jasné rozdělení odpovědnosti[10].

16. EDPB a EIOÚ poznamenávají, že čl. 5 odst. 1 písm. h) návrhu aktu o kybernetické bezpečnosti 2 se jeví jako konkrétní projev obecnější povinnosti spolupráce zakotvené v článku 68 návrhu aktu o kybernetické bezpečnosti 2, který upravuje spolupráci agentury ENISA s dalšími subjekty Unie. Podle článku 68 agentura ENISA spolupracuje v záležitostech týkajících se kybernetické bezpečnosti s dalšími orgány EU, včetně Evropského sboru pro ochranu osobních údajů, aby zajistila soudržnost, vytvořila synergie a řešila otázky společného zájmu. Tuto spolupráci lze zajistit prostřednictvím výměny know-how a osvědčených postupů; poskytováním poradenství a vydáváním pokynů týkajících se otázek souvisejících s kybernetickou bezpečností a uzavíráním praktických ujednání pro výkon konkrétních úkolů, po konzultaci s Komisí.

[10] Tím, že je zapojení agentury ENISA podmíněno žádostí dozorových úřadů, je zachován strukturovaný konzultační proces, v jehož rámci agentura ENISA poskytuje technické odborné znalosti, zatímco dozorové úřady si ponechávají plnou kontrolu nad rozhodnutími týkajícími se ochrany údajů. Zajišťuje také, aby byl jakýkoli zásah agentury ENISA koordinovaný, přičemž EDPB nebo EIOÚ převezme vedení a určí vhodný postup. Toto respektování stanovených rolí podporuje konzistentnost, zabraňuje roztříštěnosti regulace a posiluje odpovědnost orgánů pro ochranu údajů v jejich dozorové funkci.

17. EDPB a EIOÚ vítají spolupráci a součinnost mezi agenturou ENISA a dalšími subjekty Unie v souladu s jejich příslušnými úkoly a mandáty. V této souvislosti EDPB a EIOÚ doporučují v zájmu právní jasnosti změnit článek 68 návrhu aktu o kybernetické bezpečnosti 2 doplněním výslovného odkazu také na EIOÚ jako orgán Unie, s nímž by agentura ENISA spolupracovala[11].

4 OPERATIVNÍ SPOLUPRÁCE, SDÍLENÉ POVĚDOMÍ O KYBERNETICKÉ BEZPEČNOSTI A OCHRANA OSOBNÍCH ÚDAJŮ

18. Podle článků 10 a 11 návrhu aktu o kybernetické bezpečnosti 2, který by byl dalším rozpracováním stávajícího článku 7 aktu o kybernetické bezpečnosti, by agentura ENISA rozšířila svou úlohu ústředního centra pro operativní spolupráci, včetně zpracování značného množství zpravodajských informací o hrozbách[12]. Z toho lze vyvodit, že informace, které agentura ENISA v rámci své funkce zpracovává, mohou zahrnovat osobní údaje, jako jsou IP adresy, přihlašovací údaje uživatelů, záznamy o aktivitách uživatelů, finanční transakce nebo podrobnosti o kompromitovaných účtech.

19. V návaznosti na vysvětlení poskytnuté Evropskou komisí[13] EDPB a EIOÚ chápou, že agentura ENISA nemá podle aktu o kybernetické bezpečnosti 2[14] v úmyslu nařídit a povolit žádné rozsáhlé zpracování osobních údajů.

    EDPB a EIOÚ berou na vědomí skutečnost, že agentura ENISA bude shromažďovat a dále zpracovávat především souhrnné neosobní údaje, nicméně připomínají, že pokud by budoucí úkoly agentury ENISA jako informačního centra vyžadovaly zpracování osobních údajů ve značném rozsahu, mělo by to být výslovně uvedeno v ustanoveních základního aktu, kterým se příslušné úkoly řídí, včetně základních prvků jakéhokoli rozsáhlého zpracování a příslušných ochranných opatření. Pokud je naopak cílem umožnit agentuře ENISA shromažďovat a dále zpracovávat především souhrnné neosobní údaje, mělo by to být rovněž objasněno, alespoň formou bodu odůvodnění.

[11] EDPB a EIOÚ se domnívají, že čl. 7 odst. 2 stávajícího aktu o kybernetické bezpečnosti, který agentuře ENISA ukládá povinnost spolupracovat na operativní úrovni a navazovat synergie s orgány, institucemi a jinými subjekty Unie, mimo jiné s dozorovými úřady zabývajícími se ochranou soukromí a osobních údajů, s cílem řešit otázky společného zájmu, se již vztahuje i na EIOÚ.

[12] Srov. COM(2026) 11 final, Legislativní finanční a digitální výkaz, s. 19: „Nové prvky/úkoly v návrhu přinesou přidanou hodnotu evropským zúčastněným stranám, které by měly prospěch z toho, že agentura ENISA bude informačním centrem, přispěje ke sdílení informací a bude poskytovat varovná oznámení jejich členům“ a s. 95: „V posledních letech se agentura ENISA stala informačním centrem, které shromažďuje informace z různých zdrojů. V tomto smyslu je mnoho úkolů agentury ENISA spojeno s opakovaným použitím a recyklací informací pro účely různých analýz.“

[13] Jak bylo uvedeno na zasedání *ad hoc* podskupiny technologických expertů EDPB dne 27. února 2026.

[14] Komise objasnila, že agentura ENISA nemá mandát k provádění operativní analýzy incidentů a nemá přístup k údajům ze samotných incidentů. Místo toho budou zpracovávány souhrnné údaje. Upozornění od národních týmů CSIRT obvykle neobsahují operativní osobní údaje, ale spíše administrativní údaje, jako jsou kontaktní informace. Stejně tak mohou poskytnout své kontaktní údaje společnosti, které se přihlásí k odběru včasných varování. Podle Evropské komise by ve vzácných případech, kdy by souhrnné informace o hrozbách nebo incidentech poskytnuté agentuře ENISA obsahovaly IP adresy, neměla agentura ENISA žádnou provozní potřebu, a tudíž ani žádnou právní a faktickou možnost vyšetřovat účastníka, který se za IP adresou skrývá. Evropská komise dále upřesnila, že asistenční služba podle článku 13 má poradenský charakter a poskytuje například informace o tom, na který příslušný orgán členského státu se obrátit.

20. EDPB a EIOÚ konstatují, že agentura ENISA by nadále zpracovávala osobní údaje pro administrativní účely[15]. Ustanovení čl. 66 odst. 1 návrhu aktu o kybernetické bezpečnosti 2, podobně jako stávající akt o kybernetické bezpečnosti[16], obsahuje obecný odkaz na platné právní předpisy o ochraně údajů, tj. nařízení EUDPR, aniž by stanovilo další konkrétní pravidla.

21. Stejně tak čl. 66 odst. 2 návrhu aktu o kybernetické bezpečnosti 2 přebírá stávající čl. 41 odst. 2 aktu o kybernetické bezpečnosti, který stanoví možnost správní rady agentury ENISA přijmout „další opatření nezbytná pro uplatňování nařízení (EU) 2018/1725“ agenturou[17], aniž by správní rada měla povinnost přijmout konkrétní opatření. Ustanovení čl. 66 odst. 2 návrhu aktu o kybernetické bezpečnosti 2 neupřesňuje rozsah a druh těchto dodatečných opatření na ochranu údajů ani použitelný postup pro jejich přijetí. Neobjasňuje také úlohu EIOÚ v tomto procesu[18].

22. EDPB a EIOÚ mají za to, že pokud správní rada agentury ENISA přistoupí k uplatňování čl. 66 odst. 2 návrhu aktu o kybernetické bezpečnosti 2, měla by ve svém rozhodnutí (rozhodnutích) uvést další podrobnosti o tom, jak agentura ENISA provádí zpracování osobních údajů.

23. EDPB a EIOÚ připomínají, že v zásadě by mělo být v rámci správní autonomie dotčeného orgánu EU, v tomto případě správní rady decentralizované agentury, rozhodováno pouze o velmi technických (praktických) detailech souvisejících se zpracováním osobních údajů. Je tomu tak proto, že povolování zásahů do základních práv by mělo být vyhrazeno spíše normotvůrci a nanejvýš Komisi prostřednictvím prováděcích aktů nebo aktů v přenesené pravomoci[19]. Proto by mělo být v normativním ustanovení nařízení výslovně vyjasněno, co přesně se rozumí druhou větou návrhu čl. 66 odst. 2 „další opatření nezbytná pro uplatňování nařízení (EU) 2018/1725 ze strany agentury ENISA“.

24. Pokud se přesto považuje za nezbytné, aby správní rada přijala opatření, která jdou nad rámec technických (praktických) podrobností zpracování již stanovených v právních předpisech nebo aktech v přenesené pravomoci či prováděcích aktech, měla by být opatření, která má správní rada přijmout, jasná a přesná a jejich použití by mělo být pro dotčené osoby předvídatelné. To zahrnuje i náležité zveřejnění uvedených pravidel. Kromě toho by měly stanovit nezbytná ochranná opatření, aby byl zajištěn soulad s klíčovými zásadami ochrany údajů a ochrannými opatřeními, jako je omezení účelu, omezení úložiště a záměrná a standardní ochrana údajů. Jako důležitou dodatečnou záruku v takových případech navíc EDPB a EIOÚ doporučují, aby článek 66 návrhu aktu o kybernetické bezpečnosti 2 stanovil povinnost předběžné konzultace s EIOÚ před přijetím takových pravidel[20].

---

[15] Například v procesu posuzování žádostí o udělení oprávnění k výkonu funkce poskytovatele potvrzení v rámci evropského schématu potvrzování individuálních dovedností v oblasti kybernetické bezpečnosti (článek 22), v průběhu odvolacího řízení proti přijatým rozhodnutím (článek 36 a následující), při vyřizování stížností fyzických nebo právnických osob v souvislosti s certifikací nebo EU prohlášeními o shodě (čl. 88 odst. 6 písm. h)) nebo v souvislosti s certifikací kybernetické bezpečnosti (článek 96).

[16] Viz čl. 41 odst. 1 nařízení (EU) 2019/881.

[17] Dne 21. listopadu 2019 přijala správní rada agentury ENISA rozhodnutí o vnitřních pravidlech týkající se omezení některých práv subjektů údajů v souvislosti se zpracováním osobních údajů v rámci fungování agentury ENISA podle článku 25 nařízení EUDPR.

[18] Například čl. 18a odst. 5 nařízení (EU) 2016/794 (nařízení o Europolu) stanoví, že správní rada Europolu na návrh výkonného ředitele a **po konzultaci s EIOÚ** upřesní podmínky týkající se poskytování a zpracování osobních údajů […] (doplněno zvýraznění).

[19] Viz „Pokyny pro spolunormotvůrce ke klíčovým prvkům legislativních návrhů“ EIOÚ, které jsou k dispozici na adrese https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, bod 76.

[20] Podobně jako je stanoveno v čl. 18a odst. 5 nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (nařízení o Europolu) (Úř. věst. L 135, 24.5.2016, s. 53).

5 JEDNOTNÉ KONTAKTNÍ MÍSTO PRO OZNAMOVÁNÍ INCIDENTŮ (ČLÁNEK 15 AKTU O KYBERNETICKÉ BEZPEČNOSTI 2)

25. Podle článku 15 návrhu aktu o kybernetické bezpečnosti 2 musí agentura ENISA zřídit, poskytovat, provozovat, udržovat a podle potřeby aktualizovat mimo jiné jednotnou platformu pro podávání zpráv podle čl. 16 odst. 1 nařízení (EU) 2024/2847 a jednotné kontaktní místo pro oznamování incidentů zřízené podle článku 23a směrnice (EU) 2022/2555. Cílem těchto nástrojů je zjednodušit různé povinnosti týkající se podávání zpráv o kybernetické bezpečnosti[21].

26. Jak již uvedli ve svém společném stanovisku k návrhu souhrnného balíčku pro digitální oblast[22], EDPB a EIOÚ důrazně podporují cíl zřízení jednotného kontaktního místa pro oznamování případů porušení ochrany osobních údajů, neboť by to snížilo administrativní zátěž organizací, aniž by to mělo vliv na úroveň ochrany subjektů údajů. EDPB již ve svém Helsinském prohlášení[23] zdůraznil, že podporuje možné řešení pro vzájemné evropské oznamování, protože by to pomohlo usnadnit dodržování GDPR. EDPB a EIOÚ rovněž připomínají, že je důležité zajistit bezpečnost oznámení zasílaných a předávaných prostřednictvím jednotného kontaktního místa, neboť oznámení o narušení bezpečnosti údajů často obsahují citlivé informace[24].

6 EVROPSKÝ RÁMEC DOVEDNOSTÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI (DÁLE JEN „ECSF“) (ČLÁNEK 19 AKTU O KYBERNETICKÉ BEZPEČNOSTI 2)

27. Článek 19 návrhu aktu o kybernetické bezpečnosti 2 by vyžadoval, aby agentura ENISA vypracovala a zveřejnila Evropský rámec dovedností v oblasti kybernetické bezpečnosti (dále jen „ECSF“). Rámec ECSF by pomohl zajistit, aby se odborníci na kybernetickou bezpečnost, zaměstnavatelé, poskytovatelé odborné přípravy a orgány veřejné správy ve všech členských státech opírali o společné porozumění tomu, co konkrétní pracovní místa v oblasti kybernetické bezpečnosti vyžadují. Podpořil by jasné pracovní profily, transparentní kvalifikační požadavky a lepší sladění vzdělávání s potřebami trhu práce. Agentura ENISA by využívala rámec ECSF jako základ pro poskytování odborné přípravy, zejména na podporu provádění právních předpisů EU v oblasti kybernetické bezpečnosti, operativní spolupráce mezi členskými státy a činností zaměřených na zvyšování povědomí. To znamená, že rámec ECSF funguje jako základ pro strukturované programy školení v oblasti kybernetické bezpečnosti, zejména pro orgány veřejné správy a subjekty, na které se vztahují právní předpisy EU v oblasti kybernetické bezpečnosti.

[21] Viz čl. 16 odst. 1 nařízení (EU) 2024/2847 a COM(2025) 837 final, s. 8.
[22] Společné stanovisko EDPB a EIOÚ 2/2026 k návrhu nařízení, pokud jde o zjednodušení digitálního právního rámce (souhrnný balíček pro digitální oblast), přijaté dne 10. února 2026.
[23] EDPB, Helsinské prohlášení o větší srozumitelnosti, podpoře a zapojení, Přístup k inovacím a konkurenceschopnosti založený na základních právech, přijaté dne 2. července 2025.
[24] Viz kapitola 8.3. společného stanoviska EDPB a EIOÚ 2/2026 k návrhu nařízení, pokud jde o zjednodušení digitálního právního rámce (souhrnný balíček pro digitální oblast), přijatého dne 10. února 2026.

28. EDPB a EIOÚ vítají cíl posílit pracovní sílu v oblasti kybernetické bezpečnosti v EU a zdůrazňují, že pro fungování jednotného digitálního trhu je důležité, aby byly dovednosti přenosnější a více uznávané v zahraničí.

29. Zároveň si všímají, že profily definované v čl. 19 odst. 2 návrhu aktu o kybernetické bezpečnosti 2 jsou v současné době omezeny na odborníky v oblasti kybernetické bezpečnosti. Návrh neobsahuje profil potřebných dovedností pro občany, úředníky nebo nespecializované pracovníky. Jak je uvedeno v 21. bodě odůvodnění návrhu aktu o kybernetické bezpečnosti 2, digitální gramotnost je zásadní pro posílení odolnosti občanů, avšak téměř polovina dospělé populace nemá základní digitální dovednosti, přestože je vyžaduje více než 90 % pracovních míst. Proto by měl rámec ECSF zahrnovat profil „Kybernetická bezpečnost pro všeobecné pracovníky“, který by zahrnoval minimální dovednosti, které by měl mít každý obyvatel EU v produktivním věku, aby mohl bezpečně komunikovat v rámci jednotného digitálního trhu a chránit nejen sebe, ale i svou organizaci a ostatní, zejména před phishingem s pomocí umělé inteligence, deepfakes, vydáváním se za někoho jiného a útoky využívajícími sociálního inženýrství. Takový profil by mohly využívat veřejné nebo soukromé organizace pro školení svých zaměstnanců, aby minimalizovaly rizika vyplývající z lidského faktoru, a tím snížily celkové riziko narušení bezpečnosti údajů.

30. EDPB a EIOÚ poznamenávají, že 45. bod odůvodnění návrhu výslovně odlišuje rámec ECSF od evropského rámce digitálních kompetencí (DigComp 3.0) a upřesňuje, že rámec DigComp je určen pro každodenní život, účast ve společnosti, práci a učení a mohou jej využívat dospělí i děti[25], zatímco rámec ECSF je určen pro specializované publikum a nabízí jednoduchý rámec, který určuje role v oblasti kybernetické bezpečnosti a související úkoly, znalosti a dovednosti potřebné k jejich plnění.

31. EDPB a EIOÚ podporují všechny uvedené iniciativy, ať už je provádí agentura ENISA nebo v případě rámce DigComp Společné výzkumné středisko Evropské komise (JRC), neboť by v případě dostatečného zájmu mohly přispět ke snížení rizika narušení ochrany osobních údajů. Proto se všechny zúčastněné strany vyzývají, aby hledaly způsoby, jak dopad rámců zvýšit.

[25] EDPB a EIOÚ dále připomínají, že Evropská komise v letech 2022 až 2024 zkoumala možnost vytvoření evropského certifikátu digitálních dovedností (EDSC) na základě rámce DigComp. Tento certifikát by lidem pomohl zajistit, aby jejich digitální dovednosti byly rychle a snadno uznány zaměstnavateli, poskytovateli vzdělávání a dalšími subjekty. Tato iniciativa měla nabídnout značku kvality pro certifikaci digitálních dovedností v celé Evropě. V návaznosti na studii proveditelnosti (viz CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. a TROIA, S., Studie proveditelnosti Evropského certifikátu digitálních dovedností (EDSC), Úřad pro publikace Evropské unie, Lucemburk, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344) a pilotním projektu s několika zeměmi EU dospěla Evropská komise k závěru, že takové označení kvality by evropským občanům nepřineslo dostatečnou přidanou hodnotu. Rámec DigComp, poprvé publikovaný v roce 2013, však stále existuje (COSGROVE, J. a CACHIA, R., DigComp 3.0: Evropský rámec digitálních kompetencí – páté vydání, Úřad pro publikace Evropské unie, Lucemburk, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121). Popisuje, co je potřeba pro získání digitálních kompetencí v dnešní společnosti, a podporuje rozvoj digitálních kompetencí u jednotlivců všech věkových kategorií. Zahrnuje širokou škálu úrovní dovedností, od základních až po vysoce pokročilé. Některé kompetence v rámci DigComp se výslovně týkají kybernetické bezpečnosti, například 4.1 Ochrana zařízení, 4.2 Ochrana osobních údajů a soukromí a dokonce 4.4 Ochrana životního prostředí (prevence úniku dat z vyřazených zařízení). Ostatní oblasti se rovněž týkají příslušných dovedností, takže obsahují dovednosti z oblasti 1, které jsou klíčové pro obranu proti sociálnímu inženýrství, snižují rizika z oblasti 2, která se týkají vnitřních hrozeb, a zabraňují náhodnému vyzrazení informací, a zvyšují rychlost odhalování incidentů v oblasti 5.

32. Zároveň se EDPB a EIOÚ domnívají, že rámec DigComp nenahrazuje specializovaný systém kybernetické bezpečnosti pro všeobecné pracovníky[26], a doporučují spolunormotvůrcům, aby změnili čl. 19 odst. 2 návrhu aktu o kybernetické bezpečnosti 2 tak, aby se rámec ECSF neomezoval výhradně na „odborníky v oblasti kybernetické bezpečnosti“, ale aby zahrnoval i profily pro všeobecné pracovníky nebo občany. K tomu by měla být připojena odpovídající změna 45. bodu odůvodnění.

33. Kromě toho se EDPB a EIOÚ domnívají, že je nezbytné, aby byl do odborných profilů rámce ECSF začleněn modul o potřebě zajistit soulad opatření kybernetické bezpečnosti s právem EU v oblasti ochrany údajů, zejména pokud jde o praktické provádění zásady záměrné a standardní ochrany údajů (článek 25 GDPR), a vyzývají spolunormotvůrce, aby za tímto účelem doplnil bod odůvodnění.

7 EVROPSKÝ RÁMEC PRO CERTIFIKACI KYBERNETICKÉ BEZPEČNOSTI (HLAVA III)

34. Článek 71 a čl. 80 odst. 1 písm. w) návrhu aktu o kybernetické bezpečnosti 2 upravují rozsah certifikace kybernetické bezpečnosti. V čl. 80 odst. 1 písm. w) se jako bezpečnostní cíl evropských schémat certifikace kybernetické bezpečnosti doplňuje „zajistit, aby subjekt byl schopen zajistit bezpečnost zpracování osobních údajů“.

35. EDPB a EIOÚ konstatují, že znění čl. 80 odst. 1 písm. w) návrhu aktu o kybernetické bezpečnosti 2 je velmi blízké požadavkům GDPR na bezpečnost zpracování údajů[27]. V tomto smyslu lze oblast působnosti nového schématu certifikace vykládat tak, že zahrnuje požadavky podle GDPR. Právní a operativní působnost však není zcela jasná, neboť ustanovení neodkazuje na ustanovení GDPR (např. čl. 5 odst. 1 písm. f), článek 32, článek 25 GDPR) a je umístěno uvnitř seznamu „bezpečnostních cílů“ (čl. 80 odst. 1 první věta).

36. EDPB a EIOÚ připomínají, že bezpečnost podle GDPR se týká rizik pro základní práva a svobody fyzických osob. Zatímco právní definice kybernetické bezpečnosti podle práva Unie zahrnuje v širokém smyslu ochranu uživatelů a dalších osob[28], rozsah opatření kybernetické bezpečnosti obvykle zahrnuje rizika všeho druhu pro danou organizaci. Přesto existuje možnost vytvořit synergie, aby hodnocení rizik mohlo zahrnovat ochranu práv a svobod jednotlivců.

37. EDPB a EIOÚ dále připomínají, že GDPR má vlastní certifikační mechanismus (články 42–43 GDPR), a domnívají se, že certifikace kybernetické bezpečnosti se liší od certifikace ochrany údajů podle článku 42 GDPR.

[26] V rámci DigComp je bezpečnostní obsah rozptýlen do 21 kompetencí, chybí explicitní modely hrozeb, nezohledňuje bezpečnostní rizika na úrovni organizace a není přímo provázán s povinnostmi v oblasti dodržování předpisů. Zatímco rámec ECSF by se ve své současné podobě vztahoval na dovednosti odborníků v oblasti kybernetické bezpečnosti, pro zaměstnance mimo tuto oblast strukturovaný rámec na úrovni EU chybí. EDPB a EIOÚ připomínají, že většina narušení bezpečnosti pochází z phishingu, sociálního inženýrství, zneužití pověření, chybné konfigurace a používání „stínových systémů IKT“. Jedná se o obecné vzorce chování. Obecný rámec kybernetické bezpečnosti by mohl jasně stanovit rizika, poskytnout očekávání zohledňující role (např. pro lidské zdroje, finance) a podpořit měřitelné výsledky.

[27] Viz čl. 5 odst. 1 písm. f) a článek 32 GDPR.

[28] Viz čl. 2 bod 1 návrhu aktu o kybernetické bezpečnosti 2, který používá dřívější ustanovení a zní: „‚kybernetickou bezpečností‘ [se rozumí] činnosti nezbytné k ochraně sítě a informačních systémů, uživatelů těchto systémů a jiných osob dotčených kybernetickými hrozbami“.

38. Přesto se EDPB a EIOÚ domnívají, že mezi certifikací kybernetické bezpečnosti a certifikací ochrany údajů mohou existovat synergie. Například certifikace aktu o kybernetické bezpečnosti 2 by mohla být použita jako podpůrný důkaz k prokázání splnění některých požadavků certifikace GDPR, pokud jde o kybernetickou bezpečnost. EDPB a EIOÚ však upozorňují, že čl. 80 odst. 1 písm. w) návrhu aktu o kybernetické bezpečnosti 2 jasně nevyjadřuje vztah k certifikaci podle článků 42–43 GDPR. V zájmu právní jistoty doporučují EDPB a EIOÚ dále vyjasnit oblast působnosti čl. 80 odst. 1 písm. w) aktu o kybernetické bezpečnosti 2 a vztah k certifikaci podle GDPR. Kromě toho EDPB a EIOÚ doporučují, aby agentura ENISA byla před přijetím schématu certifikace podle čl. 80 odst. 1 písm. w) aktu o kybernetické bezpečnosti 2 povinna konzultovat EDPB, a zajistila se tak jednotnost postupů.

39. EDPB a EIOÚ zdůrazňují, že je třeba zvážit nejen účinnost opatření kybernetické bezpečnosti, ale také jejich nezbytnost a přiměřenost. Některé kontroly kybernetické bezpečnosti vytvářejí specifická rizika pro ochranu údajů. Může se jednat o monitorování a protokolování, hloubkovou kontrolu paketů nebo analýzu chování uživatelů. Dobře navržené schéma certifikace bezpečnosti zpracování by mohl zahrnovat kontroly, které zajistí, že bezpečnostní opatření lze provádět způsobem, který je v souladu s pravidly ochrany údajů (např. některé aspekty by měly být konfigurovatelné; mohlo by se jednat například o podrobnost údajů, které jsou zaznamenávány pro bezpečnostní účely, protože to může správci umožnit nebo usnadnit dodržování zásad bezpečnosti a minimalizace údajů podle GDPR; obdobně by měly být doby uchovávání konfigurovatelné, aby správce mohl v kontextu prováděného zpracování rozhodnout, jak dlouho by měly být osobní údaje uchovávány, než budou vymazány nebo anonymizovány pomocí certifikovaných technik).

40. Proto EDPB a EIOÚ doporučují v bodě odůvodnění vysvětlit, že schémata certifikace by měla být pokud možno navržena, zavedena a udržována tak, aby zohledňovala bezpečnostní kontroly, které mohou pomoci prokázat splnění požadavků GDPR, pokud se systémy vztahují na produkty IKT, služby IKT, procesy IKT a řízené bezpečnostní služby, které se pravděpodobně používají při operacích zpracování údajů. Je třeba také poznamenat, že některé kontrolní mechanismy mohou být nástrojem pro záměrnou a standardní ochranu údajů.

8 RÁMEC PRO DŮVĚRYHODNÉ DODAVATELSKÉ ŘETĚZCE IKT (HLAVA IV)

41. Návrh aktu o kybernetické bezpečnosti 2 doplňuje opatření pro bezpečnost dodavatelských řetězců IKT a zabývá se zejména netechnickými riziky, jako jsou geopolitické a právní faktory, faktory týkající se vlastnictví, závislosti a strategické interference, které ovlivňují dodavatelské řetězce IKT ve vysoce kritických odvětvích a v dalších kritických odvětvích. Ačkoli jsou tato bezpečnostní opatření v dodavatelském řetězci zaměřena především na řešení rizik, která přímo nesouvisejí s ochranou údajů, mohou mít také příznivý dopad na ochranu základních práv tím, že omezí zahraniční zásahy do údajů subjektů údajů v EU prostřednictvím činností, jako je špionáž a sledování.

42. EDPB a EIOÚ vítají navrhované opatření, jehož cílem je zajistit rámec pro důvěryhodné dodavatelské řetězce IKT a řešit netechnická rizika ve vysoce kritických odvětvích.

9 DALŠÍ ZÁKLADNÍ SUBJEKTY V RÁMCI NÁVRHU ZMĚN SMĚRNICE NIS 2

43. Návrh, kterým se mění směrnice NIS 2, by zahrnoval evropské peněženky digitální identity a evropské podnikatelské peněženky jako „základní subjekty“ bez ohledu na jejich velikost. Subjekty klasifikované jako „základní“ podléhají v plném rozsahu povinnostem řízení rizik kybernetické bezpečnosti podle směrnice NIS 2 a musí zavést bezpečnostní opatření požadovaná podle článku 21 směrnice NIS 2, včetně analýzy rizik a politik bezpečnosti, řešení incidentů, kontinuity provozu a krizového řízení, bezpečnosti dodavatelského řetězce, řešení zranitelností, politik v oblasti kryptografie a šifrování a kontroly přístupu a správy aktiv.

44. EDPB a EIOÚ vítají označení poskytovatelů evropských peněženek digitální identity a evropských podnikatelských peněženek za „základní subjekty“. EDPB a EIOÚ se domnívají, že peněženky digitální identity jsou klíčovou součástí digitální infrastruktury EU, takže incidenty, které je ovlivní, by mohly mít široký přeshraniční dopad. Jsou základem bezpečné identifikace, autentizace a elektronických potvrzení. Pro digitální ekonomiku jsou podnikatelské peněženky stejně důležité jako evropské peněženky digitální identity. S oběma typy poskytovatelů peněženek se proto zachází podobně jako s poskytovateli služeb vytvářejících důvěru, kteří již byli označeni za „základní subjekty“ podle směrnice NIS 2, a s dalšími provozovateli vysoce kritické infrastruktury.

10 SHROMAŽĎOVÁNÍ ÚDAJŮ O RANSOMWAROVÝCH ÚTOCÍCH

45. Podle čl. 5 odst. 8 návrhu změn směrnice NIS 2, kterým se navrhuje doplnit nové odstavce 12 a 13 do článku 23 směrnice NIS 2, mohou být dotčené subjekty v případě ransomwarového útoku požádány, aby pro reakce na počítačové bezpečnostní incidenty (CSIRT) poskytly určité informace týkající se ransomwarových incidentů, včetně informací o tom, zda subjekt zaplatil výkupné, a pokud ano, jakou částku a komu (kryptoaktiva / poskytovatelé služeb), a totožnost osoby, která působí jako kontaktní místo.

46. Podle čl. 23 odst. 11 směrnice NIS 2 je Komise zmocněna k přijímání prováděcích aktů, které blíže určují druh informací, formát a postup při plnění oznamovací povinnosti. Působnost tohoto prováděcího aktu by byla rozšířena tak, aby zahrnovala i nové oznamovací povinnosti v případě ransomwarových útoků.

47. EDPB a EIOÚ plně podporují důležitý cíl, kterým je zabránit budoucím ransomwarovým útokům a narušit a zlikvidovat zločinecké organizace, které za nimi stojí. EDPB a EIOÚ berou na vědomí, že informace, které mají být sdíleny v souvislosti s ransomwarovými útoky, by mohly být potenciálně citlivé povahy, jak Komise dále vysvětluje v 10. bodě odůvodnění návrhu změn směrnice NIS 2. Takové hlášení může navíc znamenat zpracování osobních údajů. EDPB a EIOÚ vítají odstupňovaný přístup zvolený v odstavcích 12 a 13, kdy citlivější informace v odstavci 13 budou oznamovány pouze na vyžádání.

48. Současně s ohledem na citlivost hlášených údajů a v souladu se zásadami nezbytnosti a přiměřenosti doporučují EDPB a EIOÚ v případě, že by hlášení ransomwarových útoků zahrnovalo zpracování osobních údajů, upřesnit v prováděcím aktu podle čl. 23 odst. 11 směrnice NIS 2 použitelné záruky ochrany údajů. V této souvislosti rovněž připomínají požadavek, aby Komise podle čl. 42 odst. 1 nařízení EUDPR konzultovala s EIOÚ návrhy prováděcích aktů a aktů v přenesené pravomoci, pokud mají dopad na ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů.