



ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uouu.gov.cz, www.uouu.gov.cz



Čj. UOOU-03154/23-15
Praha 31. května 2024

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z § 50 a § 54 zákona č. 110/2019 Sb., o zpracování osobních údajů, a čl. 58 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Kontrolující:

Ing. Helena Žemličková – zaměstnankyně Úřadu, č. služebního průkazu: 158752453, jako vedoucí kontrolní skupiny, na základě pověření ke kontrole ze dne 28. srpna 2023, čj. UOOU-03154/23-4,

Mgr. Jiří Kodým – zaměstnanec Úřadu, č. služebního průkazu: 134836081, jako člen kontrolní skupiny, na základě pověření ke kontrole ze dne 28. srpna 2023, čj. UOOU-03154/23-4,

Mgr. Ondřej Trnovec – zaměstnanec Úřadu, č. služebního průkazu: 127018294, jako člen kontrolní skupiny, na základě pověření ke kontrole ze dne 28. srpna 2023, čj. UOOU-03154/23-4,

(dále jen „kontrolující“).

Kontrolovaná osoba:

Policie České republiky, Strojnická 27, 170 89 Praha 7 (dále jen „kontrolovaná osoba“ nebo „Policie ČR“).

Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených zákonem č. 110/2019 Sb. a nařízením (EU) 2016/679 při zpracování osobních údajů v souvislosti s využíváním informačního systému Digitálních podob osob (dále jen „IS DPO“ nebo „systém DPO“).

První kontrolní úkon:

Kontrola byla zahájena doručením oznámení o zahájení kontroly, čj. UOOU-03154/23-5, dne 29. srpna 2023. Přílohou oznámení o zahájení kontroly bylo pověření ke kontrole, čj. UOOU-03154/23-4, ze dne 28. srpna 2023.

Poslední kontrolní úkon:

Posledním kontrolním úkonem bylo zařazení spisového materiálu do kontrolního spisu úředním záznamem, čj. UOOU-03154/23-14, dne 31. května 2024.

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Vyjádření kontrolované osoby ze dne 28. července 2023, zaevidováno pod čj. UOOU-03154/23-2, počet listů: 2, přílohy:
 - 1.1. Rozkaz policejního prezidenta č. 194/2022 k zajištění zkušebního provozu informačního systému Digitálních podob osob, počet listů: 1;
 - 1.2. Příloha k Rozkazu policejního prezidenta č. 194/2022 – Zásady zkušebního provozu systému DPO, počet listů: 5;
 - 1.3. Posouzení vlivu na ochranu osobních údajů k informačnímu systému Digitálních podob osob vč. 1 přílohy, čj. PPR-5383/ČJ-2023-990392, počet listů: 31;
 - 1.4. Posudek pověřence pro ochranu osobních údajů k posouzení vlivu na ochranu osobních údajů k informačnímu systému Digitálních podob osob ze dne 27. července 2023, počet listů: 1;
2. Vyjádření kontrolované osoby ze dne 22. září 2023, zaevidováno pod čj. UOOU-03154/23-9, počet listů: 2;
3. Úřední záznam o zařazení audiozáznamu z ústního jednání a místního šetření ze dne 3. listopadu 2023, čj. UOOU-03154/23-12, počet listů: 1, příloha:
 - 3.1. CD nosič s audiozáznamem z ústního jednání a místního šetření konaného dne 2. listopadu 2023 u kontrolované osoby;

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly a, ledaže je níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod kontroly:

Kontrola byla zahájena v návaznosti na úkony provedené Úřadem podle § 3 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), evidované pod sp. zn. UOOU-03154/23, ke kterým Úřad přistoupil s ohledem na informace zveřejněné ve vztahu k IS DPO nevládní organizací Iuridicum Remedium z.s. dne 12. července 2023 a Policií ČR dne 20. července 2023.

III. Kontrolní zjištění:

Předmětný IS DPO je nástrojem využívaným Policií ČR pro usnadnění ztotožnění neznámých zájmových osob důležitých pro trestní řízení, ať již jde o pachatele, svědka či jinou osobu (např. poškozeného) (přehled podkladů č. 1.3). Základním předpokladem pro využití IS DPO je fotografie obličeje zájmové osoby, kterou musí mít Policie ČR k dispozici v požadované kvalitě. IS DPO pro svoje fungování využívá technologii automatického rozpoznávání tváří (facial recognition), tedy technologii pracující s biometrickými údaji, jejíž cílem je určit či ověřit totožnost jednotlivce pomocí fotografie jeho obličeje. IS DPO pomocí této technologie porovnává vektorové zobrazení obličeje z fotografie zájmové osoby s vektorovými zobrazeními obličejů z fotografií v tzv. referenční databázi. Tato databáze je tvořena průkazovými fotografiemi fyzických osob z informačního systému evidence občanských průkazů a informačního systému evidence cestovních dokladů a k nim přiřazenými jedinečnými identifikátory, přičemž dle názoru kontrolované osoby (přehled podkladů č. 3.1) lze na základě ustanovení § 66a zákona č. 273/2008 Sb., o Policii České republiky, databázi rozšířit o údaje z informačního systému evidence diplomatických a služebních pasů, registru řidičů, centrálního registru řidičů a informačního systému cizinců.

Standardní postup pro využití IS DPO je dle kontrolované osoby (přehled podkladů č. 1.3) následující. Policista disponující vhodnou fotografií neznámé zájmové osoby (tzv. žadatel) podá žádost příslušnému pracovišti, v němž zařazení pracovníci disponují přímým přístupem do IS DPO (tzv. výdejové pracoviště), součástí žádosti je i předmětná fotografie. Pracovník výdejového pracoviště fotografii zájmové osoby vloží do IS DPO, který mu jako výsledek zobrazí fotografie možných kandidátů z referenční databáze spolu s procentuálním vyjádřením shody (standardně je zobrazováno 10 fotografií s nejvyšší mírou shody). Pracovník výdejového pracoviště následně vyhodnocuje shodu a vybírá vhodné kandidáty, pakliže určí alespoň jednoho tzv. „kvalifikovaného“ kandidáta, má pracovník výdejového pracoviště možnost v IS DPO provést ztotožnění takového kandidáta, a to zobrazením identifikačních údajů ze základního registru (registru osob) prostřednictvím agendového informačního systému Policie ČR. Konečný výstup, vč. identifikačních údajů kvalifikovaného kandidáta, je poté zaslán žadateli, který by měl svojí další činností následně ověřit, zda je skutečně kvalifikovaný kandidát předmětnou zájmovou osobou.

Kontrolní zjištění č. 1

Kontrolovaná osoba ve svých vyjádřeních (přehled podkladů č. 1, 2), interních aktech řízení (přehled podkladů č. 1.2) a v posouzení vlivu na ochranu osobních údajů k informačnímu

systému Digitálních podob osob a v posudku k němu (přehled podkladů č. 1.3 a 1.4) jako právní základ pro zpracování osobních údajů prostřednictvím technologie automatického rozpoznání tváře v systému DPO uvádí, nad rámec obecných zmocnění ve smyslu § 2, § 60 a § 79 zákona č. 273/2008 Sb., konkrétně § 66a zákona č. 273/2008 Sb., jehož znění je následující:

„Zpracování digitálních fotografií za účelem identifikace

(1) Policie může od správce evidence nebo zpracovatele získávat a dále zpracovávat digitální fotografie a agendové identifikátory fyzických osob vedené v

- a) informačním systému evidence občanských průkazů,*
- b) informačním systému evidence cestovních dokladů,*
- c) informačním systému evidence diplomatických a služebních pasů,*
- d) registru řidičů,*
- e) centrálním registru řidičů, nebo*
- f) informačním systému cizinců.*

(2) Údaje z evidencí uvedených v odstavci 1 písm. a) a b) se poskytnou způsobem umožňujícím nepřetržitý přístup; údaje z evidencí uvedených v odstavci 1 písm. c) až f) se poskytnou způsobem umožňujícím dálkový a nepřetržitý přístup.

(3) Osobní údaje podle odstavce 1 může policie využívat pouze pro identifikaci konkrétní osoby při plnění účelů uvedených v § 79 odst. 1.

(4) Policie osobní údaje podle odstavce 1 pravidelně aktualizuje.“

Z ustanovení § 66a odst. 3 zákona č. 273/2008 Sb. ve spojení s § 79 odst. 1 téhož zákona vyplývá, že osobní údaje zpracovávané na základě těchto ustanovení mohou být využívány výhradně za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, přičemž takové zpracování osobních údajů se řídí zejména hlavou III zákona č. 110/2019 Sb., která do českého právního řádu transponuje směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Čl. 10 směrnice (EU) 2016/680 přitom stanoví, že zpracování zvláštních kategorií osobních údajů, včetně biometrických údajů za účelem jedinečné identifikace fyzické osoby, „je povoleno pouze tehdy, pokud je zcela nezbytné, pokud existují vhodné záruky práv a svobod subjektu údajů a:

- a) pokud je povoleno právem Unie nebo členského státu;*
- b) na ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; nebo*
- c) pokud se týká údajů zjevně zveřejněných subjektem údajů.“*

Z uvedeného je tak zjevné, že pro možnost takto zpracovávat biometrické osobní údaje je vyžadována explicitní právní úprava, v souvislosti s čímž musí kontrolující konstatovat zřejmou nedostatečnost české právní úpravy, zejména pak úpravy obsažené v hlavě III zákona č. 110/2019 Sb., kde jakékoliv vymezení podmínek pro zpracování zvláštních kategorií

osobních údajů v důsledku nedostatečné transpozice směrnice (EU) 2016/680 zcela absentuje.

Pro srovnání pak kontrolující poukazují na skutečnost, že čl. 9 odst. 1 nařízení (EU) 2016/679 stanovuje obecný zákaz zpracování zvláštních kategorií osobních údajů (vč. biometrických údajů za účelem jedinečné identifikace fyzické osoby) mimo výjimky vymezené v druhém odstavci téhož článku. Kontrolující tedy mají za to, že bylo zjevným záměrem evropského zákonodárce vykládat podmínky pro možnost zpracování biometrických údajů v režimu směrnice (EU) 2016/680 i nařízení (EU) 2016/679 spíše restriktivně, neboť spolu s ostatními zvláštními kategoriemi osobních údajů požívají vyšší míru ochrany.

K výše uvedeným tvrzením kontrolované osoby, že zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby v IS DPO je založeno na oprávnění plynoucím jí z § 66a zákona č. 273/2008 Sb., a mělo by se tak jednat o zpracování povolené právem členského státu ve smyslu čl. 10 písm. a) směrnice (EU) 2016/680, kontrolující konstatují, že ustanovení § 66a zákona č. 273/2008 Sb. explicitně nehovoří o zpracování údajů biometrických, nýbrž pouze o oprávnění Policie ČR získávat (od správce evidence nebo zpracovatele) a dále zpracovávat digitální fotografie a agendové identifikátory fyzických osob vedené v evidencích uvedených v taxativním výčtu pod písmeny a) – f) prvního odstavce dotčeného paragrafu.

Kontrolující uvádí, že si jsou vědomi argumentace k § 66a zákona č. 273/2008 Sb. obsažené v části dvacáté čtvrté zvláštní části důvodové zprávy k zákonu č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, dle které má vložení § 66a přinést Policii ČR možnost softwarového vyhledávání a rozpoznávání obličejů využitelného pro automatickou identifikaci neznámých osob. Zároveň je však nutné vycházet z faktu, že důvodové zprávy nemají normativní závaznost, a ačkoliv k nim lze přihlížet při interpretaci právních norem, mají kontrolující za to, že v případě § 66a zákona č. 273/2008 Sb. a oprávnění zpracovávat biometrické údaje fyzických osob je z důvodu již zmíněné vyšší míry ochrany zvláštních kategorií osobních údajů nutné přistoupit ke spíše restriktivnímu výkladu, dle kterého formulace ustanovení § 66a zákona č. 273/2008 Sb. nemůže obstát jako zákonné zmocnění k takovému zpracování ve smyslu čl. 10 písm. a) směrnice (EU) 2016/680.

Požadavek na určitou míru kvality vnitrostátní právní úpravy je kladen např. v recitálu 33 směrnice (EU) 2016/680, dle které by právo, právní předpisy, právní základ či legislativní opatření členského státu „měly být jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují“. Ostatně potvrzení tohoto požadavku na dostatečně jasný a přesný právní základ pro zpracování biometrických údajů policejními orgány za účelem vyšetřování s cílem bojovat proti trestné činnosti a udržovat veřejný pořádek byl formulován též v rozsudku Soudního dvora EU ze dne 26. ledna 2023 ve věci C-205/21, Ministerstvo na vatrešnite raboty (Zpracování biometrických a genetických údajů policejními orgány).

Podobně se pak v Pokynech Evropského sboru pro ochranu osobních údajů 5/2022, k používání technologie rozpoznávání obličejů v oblasti vymáhání práva¹ (dále jen „Pokyny“), v bodě 44. uvádí, že by pro většinu případů používání takové technologie měla existovat

¹ Pozn.: Pracovní překlad

dedikovaná právní úprava popisující takové používání a podmínky pro ně. V bodě 70. Pokynů je pak uvedeno, že vnitrostátní právní předpisy musí být dostatečně jasné, aby subjektům údajů dostatečně objasnily okolnosti a podmínky, za nichž jsou správci oprávněni využít takových prostředků. Pokyny v bodě 71. dále uvádí, že pokud by obecné ustanovení čl. 10 směrnice (EU) 2016/680 mělo být do právní řádu členského státu pouze bez dalšího převzato, tak toto nelze vykládat jako dostatečný právní základ umožňující zpracování biometrických údajů pro účely vymáhání práva prostřednictvím technologie rozpoznávání obličejů. K tomu kontrolující podotýkají, že ani k takovému prostému převzetí však v případě transpozice do českého právního řádu nedošlo, resp. došlo neúplně, kdy § 79 odst. 3 zákona č. 273/2008 Sb. sice stanovuje omezení zpracovávání některých zvláštních kategorií osobních údajů, nicméně absenteje jakákoliv zmínka o údajích biometrických.

Po zvážení shora uvedeného tak kontrolující konstatují, že zpracování biometrických údajů v souvislosti s využíváním IS DPO je rozporu s čl. 10 směrnice (EU) 2016/680, neboť § 66a zákona č. 273/2008 Sb. nestanoví explicitně, že by pro v tomto ustanovení zakotvené zpracování osobních údajů bylo možné zpracovávat též biometrické údaje za účelem jedinečné identifikace fyzické osoby. Zároveň však nelze shledat, že by předmětné zpracování bylo v rozporu s konkrétním ustanovením hlavy III zákona č. 110/2019 Sb., a to vinou nedostatečné transpozice směrnice (EU) 2016/680 do českého právního řádu.

K uvedenému závěru se však zároveň doplňuje, že jakkoli český zákonodárce netransponoval čl. 10 směrnice (EU) 2016/680, zakotvil porušení související s principem vyjádřeným v tomto článku jako přestupky, a to například přestupky uvedené v § 63 odst. 1 písm. s), resp. v § 63 odst. 2 písm. i) zákona č. 110/2019 Sb., vztahující se k porušení omezení zpracování zvláštních kategorií osobních údajů. Navíc s přihlédnutím k nutnosti vyšší míry ochrany zvláštních kategorií osobních údajů, a s tím souvisejícím požadavkem na dostatečně jasný a přesný právní základ pro zpracování biometrických údajů, může být příléhavým přestupek podle § 63 odst. 1 písm. a) zákona č. 110/2019 Sb., kterého se právnická osoba dopustí tím, že při zpracování osobních údajů překročí oprávnění vyplývající z jiného zákona.

Kontrolní zjištění č. 2

Kontrolovaná osoba předložila dokument Posouzení vlivu na ochranu osobních údajů k informačnímu systému Digitálních podob osob (přehled podkladů 1.3, dále jen „posouzení vlivu“). Vzhledem k absenci metodiky pro vypracování posouzení vlivu na ochranu osobních údajů podle směrnice (EU) 2016/680, resp. hlavy III zákona č. 110/2019 Sb., využila kontrolovaná osoba pro jeho vypracování metodiku Úřadu podle nařízení (EU) 2016/679 (dále jen „metodika Úřadu“). Tento postup je kontrolujícími považován za přiměřený a umožňující systematický přístup. Kontrolující považují za nutné uvést, že ačkoliv technicky obsahuje prvky vyžadované § 37 zákona č. 110/2019 Sb., tak posouzení vlivu a jeho příloha č. 1 (dále jen „tabulka“) trpí určitými nedostatky uvedenými níže.

V jistých částech by posouzení vlivu, dle názoru kontrolujících, mělo být podrobnější, aby přispělo komplexnějšímu pochopení celého zamýšleného zpracování osobních údajů.

Například by bylo vhodné zahrnout komparaci postupu ztotožňování osob před nasazením IS DPO (respektive bez jeho využívání) a ztotožňování za jeho pomoci, zejména je-li jeho využívání kontrolovanou osobou označované za „pouhé zrychlení procesu“.

Ve vymezení kategorií subjektů údajů na straně 22 posouzení vlivu pak nejsou zahrnuty všechny zdrojové evidence, ze kterých by dle kontrolované osoby mělo být možno čerpat osobní údaje do referenční databáze IS DPO. Konkrétně absentuje zmínka o informačním systému evidence diplomatických a služebních pasů, registru řidičů a centrálním registru řidičů, a to byť jen v podobě konstatování, že tyto toho času nebyly využívány.

Na straně 22 posouzení vlivu je dále nedostatečně objasněn rozsah kategorií osobních údajů předávaných příjemcům, tedy, zda zamýšlení příjemci obdrží vždy všechny osobní údaje včetně biometrických, nebo jen některé. V této věci dále není kontrolovanou osobou uvedeno, na čem se zakládá případné předávání osobních údajů do zahraničí.

Kontrolující dále zastávají názor, že v případě, kdy se kontrolovaná osoba rozhodla do posouzení vlivu zařadit též část posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů (tzv. test proporcionality), měla v této části provést bližší vyhodnocení zvažovaných variant, např. z hlediska míry zásahu, nákladů na jednotlivé varianty a úspor nákladů jednotlivých řešení, aby bylo zřejmé, že vybraná varianta je nezbytná.

V jiných částech posouzení vlivu kontrolující konstatují jistou zmatečnost.

Kupříkladu není zcela jasné, jakým způsobem kontrolovaná osoba hodnotila míru zranitelnosti. Zdá se, že vycházela ze seznamu zranitelností, který si připravila (strany 43-45 posouzení vlivu, celkem 10 zranitelností) a pro každou zranitelnost stanovila její míru. Proč postupovala takto není zřejmé, metodika Úřadu předpokládá, že míra zranitelnosti může být různá u každé trojice aktivum-zranitelnost-hrozba. Ostatně ani sama kontrolovaná osoba se následně již vlastního uvedeného hodnocení nedrží, když u stejných zranitelností má v tabulce uvedenu různou míru zranitelnosti. Např. zranitelnost *„nedostatečná údržba informačních a komunikačních technologií podporujících zpracování osobních údajů“* je v posouzení vlivu na str. 44 ohodnocena mírou zranitelnosti Střední (stupeň 2). V tabulce je však následně tato zranitelnost ohodnocena mírou zranitelnosti stupeň 3 (řádek 11) a stupeň 2 (řádek 12). Obdobně se toto opakuje např. na řádcích 24 a 25, 30 a 31, 37 a 38, 42 a 43 tabulky, které se vždy týkají stejné zranitelnosti.

Kromě toho sama míra zranitelnosti, jak je definována (s výjimkou stupně 4), v sobě předpokládá přijetí nějakých opatření – například míra zranitelnosti stupeň 1 (definována jako *„Využití zranitelnosti se nejeví jako možné. Existují opatření, která jsou schopna včas detekovat pokusy o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům (úspěšné pokusy nejsou známy) o narušení integrity, dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována“*). Sama kontrolovaná osoba uvádí (strana 50 posouzení vlivu), že *„Vzhledem k tomu, že s obdobným systémem, jako je IS DPO, ještě v rámci policie jako organizace pracováno nebylo, je s ním nakládáno jako s novým řešením.“* V takovém případě by měla být míra zranitelnosti před přijetím opatření u všech hrozeb na stupni 4 a na systém by se mělo pohlížet, jako by žádná opatření nebyla přijata. To umožní

spravujícímu orgánu uvést úplný seznam technických a organizačních opatření které hrozby redukuje na přijatelnou úroveň nebo je zcela eliminují, a to bez ohledu na to, jestli jsou to opatření „zděděná“ v rámci nastavení opatření společných pro všechny informační systémy Policie ČR nebo opatření přijatá speciálně k řešení IS DPO.

V posouzení vlivu jsou technická a organizační opatření uvedena poněkud nepřehledně na více místech – viz zejména části 6.6 a 7.6 a některá i v částech 7.2, 7.3 posouzení vlivu.

Dále není z posouzení vlivu zřejmé, jak kontrolovaná osoba došla k závěru o míře dopadů, pokud dojde k narušení dostupnosti nebo důvěrnosti nebo integrity osobních údajů nebo kombinovanému narušení. Například, že při ztrátě důvěrnosti osobních údajů prostřednictvím různých hrozeb mohou být dopady na různém stupni. Pokud vycházíme z předpokladu, že výsledkem působení hrozby je, že osobní údaje jsou v cizích rukou a je pravděpodobné, že budou zneužity, pak by neměly být dopady hodnoceny odlišně (např. řádky 49, 50 a 51 tabulky, kdy jsou dopady ztráty důvěrnosti hodnoceny odlišně tj. 1, 2 i 3 stupněm).

Kontrolující konstatují, že výše popsané nedostatky posouzení vlivu svojí povahou a intenzitou nezakládají porušení povinnosti stanovené kontrolované osobě § 37 zákona č. 110/2019 Sb.

Kontrolní zjištění č. 3

Kontrolující se nemohou ztotožnit se závěrem formulovaným kontrolovanou osobou (přehled podkladů č. 1), dle kterého zpracování osobních údajů pomocí systému DPO nebylo nutné projednat s Úřadem, neboť „využití nové technologie [...] nevede k vysokému riziku zásahu do práv a svobod subjektů údajů“.

Podle § 38 odst. 1 písm. b) zákona č. 110/2019 Sb. je spravující orgán povinen podat Úřadu žádost k projednání připravovaného zpracování, má-li jím vzniknout nová evidence a pokud druh zpracování osobních údajů, s přihlédnutím k využití nových technologií nebo postupů, vede k vysokému riziku zásahu do práv a svobod subjektů údajů.

Pro potřeby využívání IS DPO byla jako jeho součást kontrolovanou osobou vytvořena tzv. referenční databáze (přehled podkladů č. 1.2, 1.3, 3.1) obsahující v době kontroly fotografie fyzických osob z informačního systému evidence občanských průkazů a informačního systému evidence cestovních dokladů a k nim přiřazené jedinečné identifikátory. Vzhledem k tomu, že kontrolovaná osoba považuje za právní základ pro předmětné zpracování osobních údajů § 66a zákona č. 273/2008 Sb., je nadto nutno doplnit, že uvedené ustanovení umožňuje získávat a zpracovávat i údaje z informačního systému evidence diplomatických a služebních pasů, registru řidičů, centrálního registru řidičů a informačního systému cizinců, přičemž z vyjádření kontrolované osoby (přehled podkladů č. 1, 3.1) je zjevná snaha doplnit referenční databázi alespoň o údaje z informačního systému cizinců.

Sama kontrolovaná osoba pak v posouzení vlivu (přehled podkladů č. 1.3) na str. 15 uvádí, že „*ke zpracování osobních údajů v rámci IS DPO je nezbytné přistupovat jako k novému řešení a způsobu využití technologie, se kterým dosud nejsou žádné zkušenosti*“, a že „*V systému DPO jsou obsaženy prvky umělé inteligence.*“, přičemž tuto skutečnost kontrolovaná osoba vyhodnotila jako jednu z oblastí dosahujících při hodnocení rizikivosti kritických hodnot.

Předmětná technologie se využívá v plné šíři na všechny osoby jejichž fotografie jsou uloženy v referenční databázi, neboť dle vyjádření kontrolované osoby (přehled podkladů č. 3.1) dochází k biometrickému zpracování všech fotografií v referenční databázi, a to v podobě jejího převodu na vektorové zobrazení. V důsledku tak dochází (stav ke dni realizovaného místního šetření) ke zpracování biometrických údajů všech držitelů občanských průkazů (tedy v zásadě všech občanů ČR starších patnácti let) a všech držitelů cestovních dokladů. Lze tak hovořit řádově o milionech subjektů údajů, jejichž osobní údaje zvláštní kategorie jsou s pomocí nové technologie zpracovávány. I sama kontrolovaná osoba v posouzení vlivu (přehled podkladů č. 1.3.) na str. 14 uvádí, že „*předmětné zpracování [...] je nutné považovat za zpracování velkého rozsahu*“, a i tento aspekt byl v rámci hodnocené rizikivosti kontrolovanou osobou vyhodnocen jako oblast dosahující kritických hodnot.

Zároveň kontrolující poukazují na bod 98. Pokynů, kde Sbor uvádí, že většina případů zavádění a používání technologie rozpoznávání obličejů ze své podstaty představuje vysoké riziko pro práva a svobody subjektů údajů, a proto by orgán, který takovou technologii nasazuje, měl kromě provedení posouzení vlivu také konzultovat příslušný dozorový úřad.

Kontrolující s ohledem na výše uvedené konstatují, že kontrolovaná osoba porušila povinnost podat Úřadu žádost k projednání připravovaného zpracování, jež jí vyplývá z § 38 odst. 1 písm. b) zákona č. 110/2019 Sb.

IV. Povinnost podat zprávu dle §10 odst. 2 zákona č. 255/2012 Sb., o kontrole (kontrolní řád)

Kontrolující v souladu s ustanovením § 10 odst. 2 zákona č. 255/2012 Sb. žádají kontrolovanou osobu o podání písemné zprávy o odstranění nedostatků zjištěných kontrolou, a to ve lhůtě 60 dnů ode dne formálního ukončení kontroly ve smyslu § 18 zákona č. 255/2012 Sb. Za splnění této povinnosti lze považovat i podání zprávy o opatřeních, která budou v danou dobu stále ve fázi přípravy nebo realizace.

Kontrolující v dané věci upozorňují, že v souladu s § 15 zákona č. 255/2012 Sb. je nesplnění povinnosti dle § 10 odst. 2 tohoto zákona považováno za přestupek, za který lze uložit pokutu do výše 500 000 Kč. V případě, že kontrolovaná osoba nebude z objektivních důvodů schopna podat písemnou zprávu o odstranění nebo prevenci nedostatků zjištěných kontrolou ve stanoveném termínu, lze před vypršením stanovené lhůty písemně požádat kontrolní orgán o její prodloužení.

V. Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

Ing. Helena Žemličková	pověřená zaměstnankyně Úřadu vedoucí kontrolní skupiny	<u>(podepsáno elektronicky)</u> podpis
Mgr. Jiří Kodym	pověřený zaměstnanec Úřadu	<u>(podepsáno elektronicky)</u> podpis
Mgr. Ondřej Trnovec	pověřený zaměstnanec Úřadu	<u>(podepsáno elektronicky)</u> podpis