Metodický pokyn ČMKOS

pro postup odborových organizací při implementaci obecného nařízení o ochraně osobních údajů (GDPR)

I.

Úvod

1. Tento metodický pokyn (dále jen „metodika“) doporučuje vhodná organizační a technická opatření pro postup odborových organizací a odborových svazů (dále jen „odborová organizace“) k ochraně osobních údajů jejich zaměstnanců, členů a funkcionářů (dále též „zaměstnanci“) a osob uvedených v odstavci 3 (dále jen „osobní údaje“) ke splnění povinností vyplývajících z obecného 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 Evropského parlamentu 95/46/ES, GDPR (General Data Protection Regulation, které nabývá účinnosti dnem 25. května 2018 – dále jen „nařízení“).

2. Nařízení je přímo závaznou evropskou komplexní právní úpravou v oblasti práv a povinností při zpracování osobních údajů směřující ke zvýšení ochrany osobních údajů občanů ode dne jeho účinností. Počítá se s tím, že ke dni účinnosti nařízení bude zrušen zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který nahradí nový zákon o zpracování osobních údajů, jehož návrh však dosud neprojednala vláda ani Parlament ČR.

3. Tato metodika se týká také shromažďování a zpracovávání osobních údajů jiných fyzických osob, které využívají služeb poskytovaných odborovými organizacemi (např. odborových portálů, odborová rekreace apod.), a které poskytují osobní údaje odborovým organizacím za účelem využití uvedených služeb za podmínek stanovených odborovou organizací pro sebe nebo své rodinné příslušníky (dále jen „jiná osoba“). Pro zaměstnance a jiné osoby používá nařízení a tato metodika společný pojem subjekty osobních údajů.

4. Metodika obsahuje základní popis obsahu nařízení a změn v oblasti ochrany osobních údajů, které přináší oproti současnému stavu, vysvětluje nejdůležitější pojmy a přináší doporučení postupu odborové organizace při implementaci nařízení a vhodných organizačních a technických opatření odborové organizace k ochraně osobních údajů zaměstnanců a jiných osob, jejichž údaje odborové organizace shromažďují a zpracovávají.

5. Metodika je určena všem osobám, které v rámci své činnosti v odborových organizacích nakládají s osobními údaji, zejména pro

a. vedení a funkcionáře odborových organizací,
b. personalisty,
c. účetní,
d. právníky,
e. správce sítí a další IT zaměstnance.

6. Příklady osobních údajů, které shromažďují a zpracovávají odborové organizace, a účel jejich zpracovávání jsou uvedeny v příloze č. 1 této metodiky.

7. Příklady opatření odborových organizací k zajištění ochrany fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů, jsou uvedeny v příloze č. 2 této metodiky.

II.

K obsahu nařízení

1. Nařízení je založeno na stejných základních principech upravujících postup při zpracování osobních údajů jako zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který nahrazuje. Nová právní úprava je kontinuální v přístupu k ochraně osobních údajů s platnou právní úpravou. Dotčeným subjektům stanoví pouze několik málo nových povinností. Pokud odborová organizace dosud zpracovává osobní údaje v souladu se zákonem o ochraně osobních údajů, nebude muset své dosavadní postupy příliš měnit.

2. Osobní údaje jsou podle nařízení veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Podrobnější definice osobních údajů i dalších pojmů používaných v nařízení se nacházejí v čl. 4 nařízení.

3. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Prvky osobních údajů jsou zejména: jméno, pohlaví, věk, datum narození, osobní stav, občanství, IP adresa, fotografie, pracovní nebo osobní adresa, telefonním číslo, e-mail, ověřovací identifikační údaje.

4. I nadále platí, že osobní údaje musí být shromažďovány a zpracovávány korektně a transparentně, v souladu s právními předpisy a uzavřenými smlouvami, pouze pro legitimní účely a v souladu s účely, k nimž byly shromážděny. Shromažďovat osobní údaje je možné pouze v rozsahu nezbytném pro naplnění stanoveného účelu. Uchovávat osobní údaje lze pouze po dobu, která je nezbytně nutná pro naplnění stanoveného účelu. Těchto cílů lze dosáhnout zavedením vhodných technických, organizačních a bezpečnostních opatření při práci s osobními údaji a při jejich uchovávání.

5. Ke zpracování osobních údajů na základě zákona k plnění povinností odborové organizace jako zaměstnavatele se nevyžaduje souhlas zaměstnance. Souhlas není třeba ani pro zpracování osobních údajů dětí a manžela zaměstnance pro účely prohlášení poplatníka daně z příjmů (čl. 6 odst. 1 písm. c nařízení).

6. Pokud má odborová organizace členy, nepotřebuje jejich souhlas se zpracováním osobních údajů (čl. 9 odst. 2 písm. d) nařízení).

7. Ke splnění povinností vyplývajících pro odborovou organizaci z nařízení postačí stručný interní předpis o zpracovávání osobních údajů, dobře vedený archív a kvalitní zabezpečení

počítačové sítě s jasně vymezenými a zabezpečenými přístupovými oprávněními pro úzce vymezený okruh osob.

III.

Hlavní změny v ochraně osobních údajů vyplývající z nařízení pro odborovou organizaci

1. Vedení záznamů o činnostech zpracování – Oznamovací povinnost vůči Úřadu pro ochranu osobních údajů při zahájení zpracovávání osobních údajů je nahrazena povinností vést záznamy o zpracovávání osobních údajů. Odborové organizace jsou povinny v záznamech uvádět především jak, kdo a za jakým účelem zpracovává jakou kategorii údajů a subjektů a komu budou tyto údaje zpřístupněny včetně případného předávání do zahraničí. Záznamy by měly být vedeny tak, aby se v nich dalo zpětně orientovat, a Úřad pro ochranu osobních údajů si je může vyžádat k nahlédnutí (čl. 30 nařízení).

2. **Ohlašování porušování zabezpečení** – Porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (čl. 4 odst. 12 nařízení). Porušení zabezpečení osobních údajů by měly odborové organizace předcházet vhodnými technickými a organizačními zabezpečeními osobních údajů. Dojde-li k porušení zabezpečení osobních údajů, mají odborové organizace povinnost bez zbytečného odkladu a pokud možno nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděly, ohlásit tuto skutečnost Úřadu pro ochranu osobních údajů a též bez zbytečného odkladu informovat všechny dotčené subjekty údajů. Povinnost ohlásit tuto skutečnost Úřadu pro ochranu osobních údajů odborová organizace nemá, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Povinnost informovat dotčené subjekty údajů odborová organizace nemá, pokud je nepravděpodobné, že by toto porušení mělo za následek vysoké riziko pro práva a svobody fyzických osob (čl. 33 a 34 nařízení). Odborovým organizacím se doporučuje, aby dokumentovaly též odůvodnění rozhodnutí přijatých v reakci na porušení zabezpečení osobních údajů.

3. **Pověřenec** (čl. 37 až 39 nařízení)

a) Při naplnění stanovených kritérií má odborová organizace povinnost jmenovat pověřence pro ochranu osobních údajů, který má za úkol především poskytovat informace a poradenství osobám, které v rámci odborové organizace zpracovávají osobní údaje, monitorovat soulad zpracování s právní úpravou a sloužit jako kontaktní místo při spolupráci s Úřadem pro ochranu osobních údajů. Pověřence lze však i bez naplnění podmínek stanovených v nařízení jmenovat dobrovolně, považuje-li to odborová organizace za potřebné.

b) Povinnost odborové organizace jmenovat pověřence pro ochranu osobních údajů vzniká v případě, kdy množství zpracovávaných údajů o členství v odborech či jiných údajů zvláštní kategorie lze považovat za „rozsáhlé“. Při posuzování „rozsáhlosti“ zpracovávání údajů by měly odborové organizace vzít v úvahu především faktory jako počet členů odborů, ať už jako

konkrétní číslo či podíl obyvatelstva nebo zaměstnanců, objem a spektrum údajů, trvání a stálost činností zpracování či jejich zeměpisný rozsah.

c) Požadavky nařízení pro osobu vykonávající funkci pověřence v odborové organizaci jsou profesní kvality a odbornost v oblasti ochrany osobních údajů, které mu umožní plnění úkolů uvedených v nařízení. Specifické vzdělání či certifikace takové osoby nařízení nevyžaduje.

d) Pověřencem může být jmenován i stávající zaměstnanec odborové organizace, který může plnit i jiné úkoly a povinnosti, avšak musí mu být poskytnut dostatek prostoru pro výkon této funkce bez hrozby střetu zájmů.

4. **Povinnosti odborové organizace jako správce osobních údajů** - Odborová organizace zavádí vhodná technická, organizační a bezpečnostní opatření a to nejen v průběhu samotného zpracování, ale již v době navrhování jeho řešení, aby osobní údaje byly chráněny před neoprávněným zpracováním.

IV.

Jak postupovat při implementaci nařízení?

1. Do 25. května 2018 je třeba provést:

a) **Zpracovat přehled o současném zpracovávání osobních údajů** – Odborovým organizacím se doporučuje zpracovat přehled dosavadních postupů při shromažďování a nakládání s osobními údaji včetně kategorizace těchto osobních údajů (osobní údaje zaměstnanců a jiných osob, které využívají služeb odborové organizace). Dále ověřit a uvést, které osoby mají k údajům přístup, kde a v jaké formě se osobní údaje ukládají a jak jsou chráněna před zneužitím, zda je prokazatelný souhlas se zpracováním osobních údajů, k jakému účelu se zpracovávají, po jakou dobu, kde a jak se archivují, pravidla pro likvidaci osobních údajů poté, co pominul legální účel jejich shromažďování a zpracování, popřípadě kdy byl odvolán souhlas dotčených osob.

b) **Kontrola zákonnosti a nezbytnosti zpracovávání** – Zpracovávat osobní údaje lze jen na základě zákona nebo souhlasu subjektu a v rozsahu a době nezbytných pro naplnění stanoveného účelu. V případě, že zpracování údajů probíhá v rozporu s právními předpisy nebo není potřebné pro činnost odborové organizace, má organizace povinnost od tohoto zpracování upustit (čl. 5 a 6 nařízení).

c) **Kontrola smluv** – Pokud odborová organizace uzavřela smlouvy, jejichž předmět zahrnuje zpracování osobních údajů, typicky smlouvy s IT společnostmi provozujícími externí informační systémy, je třeba zkontrolovat soulad těchto smluv se zákonem a nařízením, především dostatečné možnosti omezení či zákazu předávat nabyté informace dál třetím osobám v rozporu se zájmy odborové organizace či subjektů osobních údajů. Text smluv by měl odpovídat záměru předcházet jakémukoliv nezákonnému zpracování osobních údajů. Průběh plnění smlouvy v souladu s právními předpisy je odpovědností obou smluvních stran. V případě nedostatků je třeba smlouvy změnit, v případě nesouhlasu druhé smluvní strany s takovou změnou smlouvu vypovědět pro rozpor s právními předpisy či ukončit dohodou.

d) **Nastavení vnitřních mechanismů** – Odborovým organizacím se doporučuje přijmout vnitřní předpis, který nastaví pravidla pro nakládání s jednotlivými druhy osobních údajů

včetně postupu pro jejich likvidaci, způsobu uchovávání a výčtu osob pověřených shromažďováním a zpracováváním osobních údajů. Výsledkem by mělo být vytvoření funkčního systému ochrany osobních údajů s jasným vymezením oprávnění pro přístup k nim a pro přehlednou archivaci dříve proběhlých úkonů, která umožní odborové organizaci doložit, že zpracování probíhá v souladu s právními předpisy (čl. 24, 25, 30 a 32 nařízení).

2. Od 25. května 2018 je třeba zajišťovat následující činnosti:

a) **Vyřizovat žádosti ze strany zaměstnanců a jiných osob** – Subjekty osobních údajů mají právo na informace o jejich osobních údajích, které jsou zpracovávány a o způsobu jejich zpracování (čl. 13 až 15 nařízení), právo na přístup k samotným údajům, včetně práva přístupu k údajům, které mohou tvořit přílohy e-mailů, nebo které jsou uloženy na interních (odborových) nebo externích úložištích, právo na jejich přenesení, právo na opravu či výmaz nebo na omezení jejich zpracovávání (čl. 16 až 20 nařízení) a též právo vznést námitku proti jakémukoliv zpracování údajů. (čl. 21 nařízení). Pokud jsou uloženy nesprávné údaje, odborová organizace je na žádost zaměstnance nebo jiné osoby opraví; umožní přitom podávat žádosti o opravu nesprávných údajů on-line. Odborová organizace předá subjektům osobních údajů na jejich žádost jejich osobní údaje ve strojově čitelném formátu.

b) **Porušení zabezpečení** – V případě porušení zabezpečení osobních údajů budou odborové organizace postupovat podle článku III, bod 2 metodiky. Jako nejvhodnější se jeví elektronická metoda, zvláště při větším počtu subjektů údajů (čl. 33 a 34 nařízení).

c) **Součinnost s Úřadem pro ochranu osobních údajů** – Odborovým organizacím mohou za určitých okolností vyplývat z nařízení povinnosti vůči Úřadu pro ochranu osobních údajů (např. konzultace při rizikovém zpracování). Odborové organizaci musí vyřizovat též případné žádosti a umožnit zásahy Úřadu pro ochranu osobních údajů na základě stížností či z vlastní iniciativy tohoto státního orgánu.

V.

Hlavní zásady činnosti odborových organizací při implementaci nařízení

1. Nařízení je přímo závazný právní předpis Evropské unie, který má přednost před zákony České republiky. Proto musí odborové organizace od 25. května 2018 bez dalšího jednat v souladu s nařízením a plnit v něm uvedené povinnosti. Doporučuje se proto odborovým organizacím upravit do té doby veškeré jejich postupy, smlouvy a jiné právní dokumenty tak, aby byl zajištěn jejich plný soulad s úpravou obsaženou v nařízení.

2. Je třeba ctít základní zásady zpracování osobních údajů, které jsou uvedené v čl. 5 nařízení, tedy zákonnost, korektnost, transparentnost, účelové omezení, minimalizace údajů, přesnost, omezené uložení, integritu a důvěrnost a odpovědnost správce. Vždy je na místě zvážit především nezbytnost zpracovávání údajů a možnost pseudonymizace dat.

3. Je nutné rozlišovat zpracování osobních údajů na základně zákona a na základě souhlasu. Kde má zpracování osobních údajů oporu v zákoně, tam se již nevyžaduje souhlas subjektu údajů.

4. Odborové organizace nepotřebují souhlas svých členů ke zpracování jejich osobních údajů (čl. 9 odst. 2 písm. d) nařízení) a také nepotřebují souhlas svých zaměstnanců ke zpracování jejich osobních údajů, které jsou nezbytné pro splnění povinností odborové organizace jako zaměstnavatele, povinností daňových (čl. 6 odst. 1 písm. c) nařízení), popř. souhlas jiných osob, jde-li o splnění závazků vyplývajících z uzavřených smluv (čl. 6 odst. 1 písm. b) nařízení).

5. Podle čl. 9 odst. 2 písm. d) nařízení je členství v odborech považováno za „osobní údaj zvláštní kategorie“ („citlivý údaj“ podle původní úpravy). Odborové organizace jsou oprávněny zpracovávat údaje o tom, kdo je jejich členem, pokud jde o jejich současné nebo bývalé členy nebo o osoby, s nimiž udržují pravidelné styky související s odborovými cíli, a za podmínky, že tyto údaje nejsou bez souhlasu příslušné osoby zpřístupněny komukoliv jinému. Doporučuje se, aby odborové organizace nezpracovávaly jiné osobní údaje zvláštní kategorie (např. genetická či biometrická data).

6. Subjekty údajů by měly být pravidelně informovány a poučovány o nezbytnosti a potřebě zpracování údajů v souladu se zásadou transparentnosti. Mají právo být informováni o jejich osobních údajích, které jsou zpracovávány a o způsobu jejich zpracování. Doporučuje se uvést:

a) kdo tuto agendu v odborové organizaci zajišťuje a má za ni odpovědnost,
b) rozsah a účel zpracování osobních údajů
c) sídlo toho, kdo jejich osobní údaje zpracovává (odborová organizace, popř. jiná právnická osoba,
d) pokud odborová organizace předává osobní údaje jiným subjektům (než stanoveným zákonem), musí uvést komu a proč.

7. Dozorovým úřadem v oblasti ochrany osobních údajů v České republice je Úřad pro ochranu osobních údajů.

8. Pokud místo odborové organizace jako správce zpracovává osobní údaje jako zpracovatel podle jejích pokynů jiný subjekt, nese odpovědnost za řádné zpracování osobních údajů a za ochranu osobních údajů jak odborová organizace, tak i jiný subjekt, který jako zpracovatel pro odborovou organizaci osobní údaje zpracovává.

9. Nařízení je právní předpis přispívající ke zvýšení bezpečnosti a ochrany práv zaměstnanců a členů odborových organizací a další zúčastněných osob v dnešní moderní době rychle se rozvíjejících informačních technologií.

Příloha č. 1: Příklady osobních údajů, které shromažďují a zpracovávají odborové organizace, a účel jejich zpracovávání

a) Příklady osobních údajů, které shromažďují a zpracovávají odborové organizace

- osobní údaje o zaměstnancích v základním pracovněprávním vztahu a na základě dohod o pracích konaných mimo pracovní poměr: jméno a příjmení, příp. rodné příjmení, adresu trvalého bydliště, doručovací adresu, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, čísla bankovních účtů, podpis zaměstnance, zdravotní znevýhodnění, fotografie, e-mailové adresy, telefonní čísla – soukromá a pracovní, čísla občanských a řidičských průkazů, údaje o exekucích, vzdělání, příjem ze zaměstnání, členství v odborech, smlouvy včetně dodatků, potvrzení z předchozích zaměstnání, údaje o zdravotní způsobilosti zaměstnance k výkonu zaměstnaní, údaje o dětech zaměstnance,
- osobní údaje o členech odborové organizace: jméno a příjmení, případně rodné příjmení, adresu trvalého bydliště, doručovací adresu, pohlaví, věk, datum narození, den vzniku členství v odborové organizaci, výše odváděných příspěvků,
- osobní údaje o osobách, které publikují v časopisu odborové organizace a využívají služeb odborové organizace: jméno a příjmení, příp. rodné příjmení, adresu trvalého bydliště, doručovací adresu, pohlaví, věk, datum narození, místo narození, rodné číslo, osobní stav, čísla bankovních účtů, podpis zaměstnance, zdravotní znevýhodnění, fotografie, e-mailové adresy, telefonní čísla – soukromá a pracovní, čísla občanských a řidičských průkazů,

b) Za jakým účelem jsou osobní údaje zpracovávány

– Zaměstnanci: účelem zpracování osobních údajů zaměstnanců je běžná personální agenda, zpracování mezd; právním důvodem zpracování je plnění zákonem stanovené povinnosti, plnění smlouvy a souhlas subjektu údajů (zveřejnění fotografie na internetových stránkách odborové organizace apod.).

– Členové odborové organizace: účelem zpracování osobních údajů členů je evidence členů a výběru členských příspěvků, na jejichž základě poskytuje odborová organizace svým členům své služby; právním důvodem zpracování je sledování odborových cílů a ke zpracování osobních údajů členů není třeba jejich souhlas (čl. 9 odst. 2 písm. d) nařízení). Jedná se také o příspěvek či podporu z fondů odborové organizace a údaje o členech, kteří jsou právně zastupováni prostřednictvím odborové organizace.

– Jiné osoby publikující v odborovém časopise: účelem zpracování osobních údajů je vyplacení odměny za jejich články; právním důvodem zpracování je plnění smlouvy.

– Osoby, které se účastní odborových akcí: členové odborových organizací, úředníci, představitelé zaměstnavatelů, zejména v případech, kdy se vyhotovuje prezenční listina: účelem je evidence účastníků odborových akcí, např. pro účely dokumentace projektů, v jejichž rámci se takové akce uskutečňují, či pro poskytnutí cestovní náhrady. Součástí může být i informace o členství v odborové organizaci.

– Fyzické osoby, s nimiž odborová organizace uzavřela smlouvu (smlouva o dílo, smlouva o koupi apod.): účelem zpracování osobních údajů těchto osob je plnění závazků odborové organizace plynoucích z takových smluv.

c) Jak se osobní údaje shromažďují

Osobní údaje se shromažďují v listinné i elektronické podobě.

d) Jak se osobní údaje uchovávají

Osobní údaje se uchovávají v listinné i elektronické podobě.

Příloha č. 2: Příklady opatření odborových organizací k zajištění ochrany fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů.

a) Přístup k osobním údajům má v rámci odborové organizace jen vymezený okruh osob, např. mzdová účetní, personalista, vedoucí finančního oddělení, právník, předseda,

b) Osobní údaje jsou uchovávány:
   - v tištěné podobě, ve složkách, které jsou uchovávány v plechové skříni v zamykatelné místnosti, popř. v trezoru, ke kterým má přístup jen vymezený okruh osob za přítomnosti personalisty, účetní či pověřeného vedoucího zaměstnance,
   - v elektronické podobě, v počítači pověřeného zaměstnance s ochranou jedinečným přístupovým kódem nebo heslem a se zálohováním např. na serveru odborové organizace se stejnou ochranou s přístupem pouze vymezeného okruhu osob,

c) Za evidenci osobních údajů odpovídá pověřený pracovník,

d) Databáze s osobními údaji je zabezpečena hesly a včetně programu na evidenci členské základny uložena na serveru, k databázi mají přístup pověřené osoby z hlediska plnění svých povinností přes své osobní certifikáty.