Kodex chování v oblasti osobních údajů
Asociace poskytovatelů personálních služeb

Obsah

Úvod

Personální služby poskytují výhody uživatelům z veřejného i soukromého sektoru, jež zahrnují úspory nákladů, větší flexibilitu, efektivitu a bezpečnost.

Existuje široké spektrum poskytovatelů personálních služeb, respektive agenturního zaměstnávání, kteří své služby poskytují různými způsoby. Rozsah, v jakém poskytovatelé personálních služeb zpracovávají osobní údaje a rozsah kontroly nad zpracováváním těchto údajů, závisí na typu nabízené personální služby. Poskytovatelé různých typů personálních služeb tak mají různé role a odpovědnosti, zejména pokud jde o pravidla ohledně ochrany a zabezpečení osobních údajů.

Například:

Poskytovatel služby v oblasti agenturního zaměstnání a recruitmentu řídí jinou strukturu osobních dat než poskytovatel outsourcingu specializovaných služeb, případně zajišťuje nábor zaměstnanců na hlavní pracovní poměr.

Tento Kodex chování se zaměřuje na poskytovatele personálních služeb. Ti jsou v tomto Kodexu označováni jako členové Asociace poskytovatelů personálních služeb (dále jen APPS).

Účelem tohoto Kodexu je pomoci zákazníkům posoudit, které služby jsou pro ně vhodné ve vztahu ke zpracovávání osobních údajů.

Kodex se skládá ze souboru požadavků pro členy APPS jako správce, případně zpracovatele dat v oddíle 4 (Požadavky na ochranu dat) a v oddíle 5 (Požadavky na transparentnost) - společně požadavky na dodržování Kodexu. Kodex zahrnuje také strukturu řízení v sekci 8 (Management), která má za cíl podpořit implementaci, řízení a aktualizace Kodexu.

Kodex je dobrovolný nástroj, který členům APPS umožňuje vyhodnotit a prokázat jeho dodržováním požadavky na několik svých služeb. Dodržování kodexu může člen APPS dokázat buď osvědčením nezávislými auditory třetí strany, nebo sebehodnocením a vlastním prohlášením o souladu.

Členové APPS, kteří prokázali, že dodržují Kodex v souladu se svými řídícími postupy, mohou použít příslušné známky shody Kodexu.

Zákazníci jsou nabádáni, aby si ověřili, zdali požadavky Kodexu, jakékoli dodatečné smluvní zajištění poskytované členy APPS a i jejich vlastní politiky, splňují požadavky platných právních předpisů EU o ochraně osobních údajů, zejména však nařízení č. 2016/679 – Všeobecné nařízení o ochraně osobních údajů (GDPR). Ověření je možné na webových stránkách, kde jsou uvedeny všechny organizace (dále jen členové APPS) hlásící se k dodržování Kodexu (www.apps.cz, sekce ochrana osobních údajů/Kodex).

1. Struktura Kodexu

Tento Kodex je strukturován následovně:

- **Cíl:** popisuje zaměření Kodexu na platné zákony EU o ochraně osobních údajů.
- **Rozsah:** popisuje oblast působnosti Kodexu.
- **Požadavky na ochranu dat:** popisuje práva a povinnosti členů APPS při jeho dodržování na základě klíčových zásad jako jsou vymezení účelu, práva subjektů údajů, přenosy, zabezpečení, audity, odpovědnosti apod.
- **Požadavky na transparentnost:** popisuje, jakým způsobem členové APPS prokazují přiměřenou úroveň zabezpečení osobních údajů.
- **Dodržování:** popisuje podmínky pro členy APPS, kterými deklarují dodržování Kodexu.
- **Správa:** popisuje způsob řízení, uplatňování a revizí Kodexu, včetně úkolů a povinností pro jeho řídící orgány.

2. Účel

Účelem tohoto kodexu je provést zákazníky procesem posuzování vhodnosti personálních služeb vzhledem k účelům, ke kterým si zákazníci přejí tuto službu využívat. Hlavními službami poskytovanými personálními agenturami jsou: a) recruitment; b) dočasné přidělení; c) outsourcing mezd aj. Druh služby určuje roli člena APPS, buď jako správce, nebo jako zpracovatele. Konečným cílem tohoto Kodexu je pomoci zákazníkům vybrat si pro své specifické potřeby správnou personální společnost zajišťující ochranu osobních údajů. Pro členy APPS je zákazníkem nejenom společnost poptávající zaměstnance, ale i uchazeč o zaměstnání.

Prohlášení členů APPS o dodržování tohoto Kodexu má za cíl přesvědčit zákazníka že:

- mohou tuto službu využívat ke zpracovávání osobních údajů způsobem, který je v souladu s platnými právními předpisy EU o ochraně osobních údajů,
- člen APPS splnil požadavky tohoto Kodexu.

Při využívání personálních služeb jsou ale zákazníci rovněž vyzýváni, aby vytvořili vlastní hodnocení svých specifických činností vzhledem k dodržování platných právních předpisů EU o ochraně osobních údajů. Tento Kodex je určen k tomu, aby zákazníkům v těchto hodnoceních pomáhal, ale nenahrazuje je.

Kodex rovněž nenahrazuje smlouvu mezi členem APPS a jeho zákazníkem. Člen APPS a jeho zákazník mohou volně definovat jakým způsobem je služba poskytována prostřednictvím písemné smlouvy (smlouvy o poskytování služeb). Členové APPS posoudí, zda stávající smlouvy o poskytování služeb, které nabízejí zákazníkům, nejsou v rozporu s požadavky tohoto Kodexu a to zejména před prohlášením o jeho dodržování.

Kodex není právní poradenství a dodržování Kodexu nezaručuje dodržování platných zákonů, a proto by členové APPS i zákazníci měli dbát na to, aby si zajistili další znalosti ohledně dodržování požadavků platných právních norem.

3. Rámec působnosti

Kodex se skládá ze souboru požadavků pro členy APPS jako zpracovatele dat a to se zvláštním důrazem na bezpečnost. Tyto požadavky jsou uvedeny v části 4 (Požadavky na ochranu osobních údajů) a v části 5 (Požadavky na transparentnost) a jsou v Kodexu označovány jako požadavky Kodexu.

Člen APPS může deklarovat dodržování požadavků tohoto Kodexu pro jakoukoli poskytovanou činnost pokud:

- služba splňuje požadavky tohoto Kodexu,
- ve vztahu k této činnosti člen APPS vyhovuje všem zákonům EU o ochraně osobních údajů, které jsou platné a závazné, včetně obecného nařízení o ochraně osobních údajů (**GDPR**),
- součást služby (například cloudové uložiště) člena APPS poskytuje zákazníkovi možnost ukládání a zpracování dat v rámci EHP.[1]

Člen APPS se může rozhodnout, že bude dodržovat Kodex pouze u některých ze svých služeb. To však neznamená, že by takový subjekt neplnil právní povinnosti vyplývající z GDPR na všechny ostatní činnosti, které provádí. Pokud člen APPS prohlásí, že jsou v souladu s Kodexem veškeré jeho služby, musí být schopen splnit všechny požadavky Kodexu pro každou činnost.

Správná identifikace správce dat a všech zpracovatelů dat je zásadní pro právní předpisy EU o ochraně osobních údajů. Tyto koncepty jsou vysvětleny v části 4 (Požadavky na ochranu dat) tohoto Kodexu.

V kontextu personálních služeb funguje člen APPS pro zákazníka jako zpracovatel, nebo správce, a to v závislosti na poskytované službě (například: recruitment a dočasné přidělení – správce; outsourcing mezd - zpracovatel). V ostatních případech může člen APPS působit jako správce, například v interakci k dodavatelům, přidělovaným zaměstnancům aj. Požadavky tohoto Kodexu stanoví zásady, které musí členové APPS jako zpracovatelé a správci osobních údajů dodržovat.

Právní povinnosti správců osobních údajů, které jsou stanoveny v platných právních normách EU o ochraně osobních údajů, jsou širší než právní předpisy zpracovatelů. Zpracovatelé osobních údajů mohou hrát podpůrnou úlohu při plnění povinností správce dat. Kodex stanovuje závazky jednotlivým členům APPS jako správcům OÚ, a zároveň Kodex usiluje o vysvětlení toho, jakým způsobem členové APPS, pakliže jsou v roli zpracovatelů osobních údajů, mohou podporovat ty zákazníky, kteří jsou buď správci dat, nebo samotní zpracovatelé osobních údajů v dodavatelském řetězci.

Co se týče dat zpracovávaných jménem zákazníka pomocí personální služby, pak člen APPS buďto nebude mít k těmto údajům přístup a nebude je využívat, s výjimkou případů, kdy je to nezbytné k poskytování personálních služeb, nebo člen APPS zpracovává tato data pro vlastní účely, včetně účelů jako vytěžování dat, profilování, nebo přímý marketing.

Člen APPS může působit jako správce dat, pokud jde o určité osobní údaje poskytnuté zákazníkem a přiděleným zaměstnancem. Patří sem například informace o účtu (jako jsou uživatelská jména, e-mailové adresy nebo fakturační údaje), které zákazník poskytuje členu APPS v souvislosti s vytvořením nebo správou účtu používaného pro přístup ke službě člena APPS.

4. Požadavky na ochranu dat

Všeobecné nařízení o ochraně osobních údajů EU rozlišuje mezi správcem dat - stranou, která určuje účel a prostředky zpracovávání osobních údajů a zpracovatelem dat, který zpracovává osobní údaje jménem správce.

---

[1] Evropský hospodářský prostor

V návaznosti na poskytovanou službu, členové APPS poskytují na vyžádání uživatele (zákazníka) dočasně přidělované zaměstnance, kteří jsou řízeni a kontrolováni zákazníky. Člen APPS předá osobní údaje o přiděleném zaměstnanci uživateli a ten tyto údaje využívá pro zpracování OU. V případě náboru zaměstnanců[2] pro zákazníka člena APPS je člen do umístění zaměstnance v roli správce.

Zákazník jako správce nebo zpracovatel

Personální služby jsou využívány jako součást řady různých služeb, ve kterých může být zapojeno více stran. Někdy je zákazník ten, kdo ukládá nebo jinak zpracovává osobní údaje, ale v jiných případech je správcem právě člen APPS. Zákazník (odběratel služeb, nebo uživatel přidělovaných zaměstnanců) zde vystupuje jako správce nebo zpracovatel.

- Zákazník je ve vztahu ke zpracování osobních údajů správcem, pokud si určuje účel a způsob zpracování dat.
- Zpracovatelem je v případě, pokud zpracovává osobní údaje jménem a dle zadání třetí strany (ta může být správcem, nebo jinou třetí stranou v dodavatelském řetězci).
- Zákazník v roli přidělovaného nebo nabíraného zaměstnance je subjekt údajů.

Člen APPS jako správce i jako zpracovatel

Pokud člen APPS poskytuje agenturní zaměstnávání, nebo nábor nových zaměstnanců, kteří jsou následně zaměstnáni u zákazníka (odběratele služeb), je člen APPS v roli správce. Pokud je zákazníkům vedena personální agenda (mzdová aj.), pak je člen APPS v roli zpracovatele OÚ. Pokud se zákazník rozhodne uchovávat nebo jinak zpracovávat osobní údaje pomocí personálních služeb člena APPS, pak bude člen APPS jeho zpracovatel.

Účel této sekce Kodexu ohledně ochrany osobních údajů

Cílem této části (Požadavky na ochranu dat) je objasnit úlohu člena APPS jako správce i jako zpracovatele dat, a to podle platných právních předpisů EU o ochraně osobních údajů v souvislosti s poskytováním personálních služeb.

Kodex sleduje tento cíl:

(a) určení požadavků na správce a zpracovatele dat s ohledem na platné právní předpisy EU o ochraně osobních údajů (**požadavky na ochranu dat**),

(b) uplatnění požadavku na ochranu osobních údajů v kontextu personálních služeb, přidělení odpovědností pro tyto požadavky mezi členy APPS, zákazníky a definování specifických požadavků pro členy APPS podle Kodexu (**požadavky na členy APPS**).

(c) Jedním z prvků, jimiž lze doložit, že člen APPS plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 GDPR, nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42 GDPR.

Vedle respektování Kodexu je důležité, aby členové APPS i zákazníci respektovali právní předpisy EU o ochraně osobních údajů v souvislosti s využíváním personálních služeb.

Důležitým cílem Kodexu je také řešit klíčové požadavky pro členy APPS v souvislosti s nařízením o ochraně osobních údajů. Jedná se zejména o požadavky nařízení General Data Protection Regulation (dále „GDPR“) jakmile vstoupí v platnost. Tyto požadavky jsou v Kodexu definovány s odkazem na nařízení GDPR. Kodex bude revidován a aktualizován

---

[2] Zaměstnanci jsou po jejich vyhledání a umístění na specifikované místo zaměstnáváni a řízeni zákazníkem člena APPS.

s ohledem na změny platných právních předpisů EU o ochraně osobních údajů v souladu s oddílem 8 (Management), včetně jakýchkoliv specifikací, týkajících se GDPR, které mohou příslušné orgány dozoru poskytnout.

4.1. Zpracovávání osobních údajů dle GDPR:

Požadavky na ochranu dat:

Člen APPS zavede taková technická a organizační opatření (s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, k různě pravděpodobným a různě závažným rizikům týkajících se práv a svobod fyzických osob), aby zajistil a byl schopen doložit, že zpracování dat je prováděno v souladu s nařízením. Tato opatření musí být podle potřeby revidována a aktualizována. Člen APPS dat musí zajistit, aby byly osobní údaje zpracovávány zákonně. Zpracování je legální pouze tehdy, jsou-li splněny určité podmínky tohoto kodexu a dalších vnitropodnikových dokumentovaných postupů vydaných v souladu s nařízením GDPR. Pokud člen APPS zpracovává osobní údaje jako zpracovatel, pak je zpracovává i v souladu s pokyny zákazníka, které jsou úplně a kompletně definovány ve smlouvě o poskytování služeb, případně v jiném dokumentu určeným zákazníkem.

4.2. Smluvní podmínky služeb členů APPS

Požadavky na ochranu dat:

Zpracování OÚ pro člena APPS se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči členu APPS a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. (GDPR čl. 28 odst. 3). Člen APPS tímto ustanovením zcela jednoznačně garantuje zákazníkům a subjektům údajů neporušenost řetězce všech subjektů, které mohou přijít do kontaktu s osobními údaji člena APPS.

Požadavky na členy APPS:

Člen APPS definuje vlastnosti služeb, způsob jejich poskytování a práva a povinnosti zákazníka ve smlouvě o poskytování služeb, jak je stanoveno v pododstavcích a) a b) níže.

a) Popis zpracovávání dat

Pro usnadnění služby zákazníkům je vhodné popis zpracovávání dat ve smlouvě popsat tak, aby se smlouva nemusela měnit pokaždé, když si zákazník nebo kterýkoli koncový uživatel bude přát změnit způsoby či účely využití personální služby.

Z důvodu flexibility je tedy vhodné ve smlouvách řešit popis zpracovávání dat například obecnějším výkladem, jako například: „výpočty, ukládání a doručování dat v síti člena APPS“.

b) Forma smlouvy o poskytování služeb

Pokud je smlouva mezi členem APPS a zákazníkem právně závazná, pak může mít formu například:

- jedné smlouvy,

- souboru dokumentů, jako je smlouva o základních službách s příslušnými přílohami (dohody o zpracovávání dat, SLA[3], podmínky poskytování služeb, bezpečnostní zásady s ohledem na ISMS a nařízení GDPR atd.),
- standardních online podmínek.

4.3. Bezpečnostní požadavky

Požadavky na ochranu dat:

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou **členové APPS** vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (GDPR čl. 32 odst. 1).

Požadavky na členy APPS:

a) Bezpečnostní opatření

Členové APPS se budou řídit závaznými zásadami, jakým způsobem implementovat a udržovat vhodná technická a organizační opatření pro svá datová centra, servery, síťová zařízení a hostitelské softwarové systémy, které jsou pod jejich kontrolou a slouží jako podpora k poskytování personálních služeb. Tato technická a organizační opatření mají být navržena tak, aby pomohla zákazníkům zabezpečit osobní údaje před neoprávněným užitím, zpracováním, přístupem nebo zveřejněním a před náhodnou nebo nezákonnou ztrátou dat. Za bezpečnost dat odpovídají členové APPS. Pokud člen APPS využívá k uchování OÚ cloudová uložiště (OneDrive, GoogleDrive, Cloud aj., měl by mít od poskytovatele těchto uložišť vyjádření o všech zárukách vyplývajících z nařízení GDPR.[4]

Příloha 1 (Rozdělení bezpečnostních odpovědností) definuje bezpečnostní odpovědnosti členů APPS a zákazníků v rámci personálních služeb.

Zákazníci musí přezkoumat:

(a) informace, týkající se bezpečnosti poskytovaných služeb, jak je uvedeno v oddílu 5 (Požadavky na spravedlivost a transparentnost),

(b) použití funkcí a ovládacích prvků služeb a své konfiguraci těchto služeb,

(c) zda bezpečnostní opatření, která jsou v jejich odpovědnosti a bezpečnostní opatření zpracovatelů (dodavatelů zákazníků), společně poskytují odpovídající úroveň zabezpečení pro vybranou službu.

Toto určení má být založeno na povaze, rozsahu, kontextu a účelu služby, kterou chce zákazník využívat. Rozhodovací pravomoc ohledně zpracovávaných dat má zákazník, tedy hlavně on může určit, která úroveň zabezpečení je vhodná pro zpracovávání osobních údajů, které ukládá a zpracovává. Členové APPS nesledují, neomezují ani nijak neovlivňují, jakým způsobem bude zákazník služby využívat a není tedy schopen posoudit vhodnost úrovně zabezpečení zákazníka.

b) Program zabezpečení informací

---

[3] Service Level Agreement, zkratka SLA, je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby. SLA (Service Level Agreement), používá se zkratka SLA, překládá se jako dohoda o úrovni poskytovaných služeb.

[4] Členové APPS nejsou za zabezpečení dat výlučně odpovědní například při využití cloudových služeb u třetích poskytovatelů. Některé z klíčových aspektů zabezpečení si zákazníci musí zajistit sami. Zákazník je například odpovědný za zabezpečení hostovaných operačních systémů, aplikací, tranzitních dat a přihlašovacích údajů pro své zaměstnance.

Člen APPS bude s cílem identifikovat předvídatelná vnitřní rizika pro bezpečnost své sítě udržovat program zabezpečení, a to nejen osobních údajů. Tento program (nebo organizační opatření) pomůže bezpečnostní rizika minimalizovat a bude také obsahovat hodnocení rizik a pravidelné testování popsané v dokumentovaném vnitropodnikovém postupu.

Člen APPS určí jednoho nebo více pracovníků, kteří budou program zabezpečení dat (nebo jiná organizační opatření) informací koordinovat a budou za něj odpovědní.

c) Průběžné přezkoumávání

Člen APPS provádí pravidelné přezkoumávání bezpečnosti sítě a přiměřenosti programu informační bezpečnosti. Program průběžného přezkoumávání se provádí dle jednoho nebo více bezpečnostních standardů a slouží ke zjištění, zda bude nutné provést dodatečná či další bezpečnostní opatření. Člen APPS má povinnost reagovat na nová bezpečnostní rizika nebo výsledky z vlastních periodických přezkumů bez zbytečného odkladu.

Bezpečnostní standardy mohou být průběžně upravovány, ale takovým způsobem, aby během celé doby trvání smlouvy poskytovaly přinejmenším stejnou úroveň, jak je popsáno v bezpečnostních právních předpisech k datu účinnosti smlouvy o poskytování služeb.

4.4. Převod osobních údajů do třetích zemí

Požadavky na ochranu dat:

K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel v závislosti na dalších ustanoveních nařízení podmínky stanovené v této kapitole, včetně podmínek pro další předávání osobních údajů z dané třetí země nebo mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizace. Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená tímto kodexem nebyla znehodnocena. (GDPR, čl. 44).

Požadavky na členy APPS:

a) Umístění

K jakémukoli předání osobních údajů, které jsou předmětem zpracování, nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít jen za předpokladu zajištění všech požadavků nařízení GDPR (pakliže jsou relevantní) ve všech místech určení osobních údajů, kde je s nimi nakládáno. Tzn.: člen APPS garantuje zákazníkům a subjektům údajů, že jejich data jsou uložena jen u těch subjektů, se kterými jsou uzavřeny písemné dohody o plnění požadavků nařízení GDPR k dotčeným osobním údajům. Člen APPS bude vždy upřednostňovat možnost, aby všechny osobní údaje byly ukládány a bylo s nimi nakládáno v rámci prostoru EHP. V případě ukládání osobních údajů na cloudová uložiště, člen APPS musí znát místa uložení jejich infrastruktury.

b) Informace

Člen APPS poskytuje zákazníkům informace o regionu a zemi, kde jsou jejich data uchovávána a zpracovávána členy APPS nebo jménem členů APPS, včetně případů, kdy jsou subdodávky zpracovávány třetími stranami.

Z bezpečnostních důvodů se poskytují informace pouze ohledně obecného umístění (například oblast města nebo oblasti městského regionu). Tento obecný popis umožní zákazníkovi určit, pod kterou jurisdikci členského státu EU zpracovávání jeho dat spadá.

Pokud na základě platných právních předpisů vznikne členu APPS tato povinnost a za předpokladu, že důvěrné informace jsou odpovídajícím způsobem chráněny, může člen APPS sdělit příslušnému orgánu dozoru přesnou adresu příslušných zařízení.

c) Úroveň ochrany

Členové APPS zpřístupní zákazníkům uznávaný standard pro přenos osobních údajů do příslušných zemí (včetně například standardních smluvních doložek EU, závazných firemních pravidel, nebo štítu ochrany osobních údajů EU-USA pro přenos osobních údajů do Spojených států amerických), pokud:

a) zákazník předává osobních údaje, které jsou ukládány prostřednictvím služeb členů APPS, z EHP do jakékoli země mimo EHP, která není evropskou komisí uznána jako země poskytující odpovídající úroveň ochrany osobních údajů, nebo
b) je člen APPS oprávněn přistupovat k osobním údajům, uloženým prostřednictvím jeho služby, v rámci EHP ze země uvedené v bodě a) výše.

4.5. Dílčí zpracování (subdodavatelé)

Požadavky na bezpečnost dat:

Člen APPS nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky (GDPR čl. 28 odst. 2).

Pokud člen APPS v roli **zpracovatele** zapojí dalšího zpracovatele, aby jménem správce (zákazníka) provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo České republiky stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto kodexu a nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel (GDPR čl. 28 odst. 4).

Požadavky na členy APPS:

a) Informace

Členové APPS vedou aktualizovaný seznam subdodavatelů (společně, nebo individuálně) se schváleným přístupem k datům zákazníků. Tento seznam obsahuje umístění dílčího úložiště a musí být snadno přístupný zákazníkům před podpisem smlouvy o poskytování služeb i během jejího trvání. Lokalita je uvedena pouze obecně (například oblast města).

Před udělením oprávnění novému subdodavateli poskytnou členové APPS informace o tomto subdodavateli zákazníkům.

b) Uspořádání subdodávek

Člen APPS ukládá takové smluvní povinnosti svým subdodavatelům, které jsou shodné jako ty, které má uvedeny ve smlouvách o poskytování personálních a souvisejících služeb se svými zákazníky.

Člen APPS zavede taková provozní opatření týkající se jeho dodavatelů, aby poskytoval úroveň ochrany dat přesně dle smlouvy o poskytování služeb. Člen APPS musí být předložením příslušných dokladů zákazníkům schopen prokázat, že tato opatření přijal.

Člen APPS musí omezit zpracovávání dat zákazníka u subdodavatelů na míru, která je nezbytná pro poskytování nebo údržbu služeb.

Člen APPS zůstává odpovědným za dodržování svých povinností týkajících se ochrany osobních údajů, obsažených ve smlouvě o poskytování služeb i za jakékoli jednání nebo opomenutí subdodavatele, které by způsobilo, že člen APPS poruší některé ze svých závazků vyplývajících ze smlouvy o poskytování služeb.

Bez ohledu na pododstavce a) až b) a podle platných zákonů mohou členové APPS volně využívat subdodavatele nebo dodavatele (např. dodavatele energie, zařízení, dopravce, poskytovatele technických služeb, poskytovatele IP, prodejců hardwaru atd.), aby vykonávali své povinnosti podle smlouvy o poskytování služeb, bez povinnosti informovat nebo požadovat předchozí povolení od zákazníka za předpokladu, že takoví subdodavatelé nebo dodavatelé nemají oprávnění přístupu k datům zákazníků.

4.6. Prokazování shody

Požadavky na ochranu dat:

Člen APPS poskytne zákazníkovi[5] v případě jeho žádosti veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto kodexu, a umožní audity (včetně inspekcí), prováděné zákazníkem nebo jiným nezávislým auditorem, kterého zákazník pověřil, a k těmto auditům poskytne dostatečnou součinnost. (GDPR čl. 28 odst. 3 písm. h).

Požadavky na členy APPS:

a) Informace

Člen APPS poskytne dostatek informací o konaných bezpečnostních kontrolách, aby si zákazníci mohli jednoduše ověřit, zda člen APPS skutečně dodržuje bezpečnostní pravidla ustanovená ve smlouvě o poskytování služeb.

Pokud nejsou informace důvěrné nebo zneužitelné, budou zákazníkům zpřístupněny prostřednictvím přímé informace na webových stránkách člena APPS. Pokud jsou informace důvěrné, zpřístupní je člen APPS na vyžádání zákazníka, přičemž může požadovat od zákazníků dohodu o mlčenlivosti. Člen APPS se může dle vlastního uvážení rozhodnout nezveřejnit některé vysoce důvěrné bezpečnostní informace.

Člen APPS může vyžadovat po zákaznících poplatek za doplňující informace. Poplatek musí být v rozumné výši tak, aby se nepoužíval k zabránění přístupu k informacím o bezpečnostních auditech.

Je vhodné na internetových stránkách zveřejňovat aktuální informace o aktualizacích týkajících se bezpečnosti IS potažmo osobních údajů.

Člen APPS nabídne zákazníkům možnost k pokládání dotazů týkajících se ochrany dat, osobních údajů, nebo otázek týkajících se bezpečnosti systému zpracovávajících osobní údaje a to například v podobě diskuzního fóra, blogu aj. Zákazníkům poskytne kontakt na zaměstnance, kteří byli pověřeni řešením těchto záležitostí a Pověřence pro ochranu

---

[5] V Případě, že zákazník je v roli správce.

osobních údajů[6], který je jmenován APPS. Ustálené postupy mají být vhodné a přiměřené pro danou službu a mohou mít formu telefonického kontaktu, e-mailového kontaktu, chatovacích systémů nebo jiných metod, které umožňují zákazníkovi komunikovat s příslušným zástupcem člena APPS. Pro přístup k případné zákaznické lince nejsou vyžadovány po zákaznících žádné údaje.

b) Audit

Kromě výše uvedených požadavků využívá člen APPS k ověření adekvátnosti kontrol bezpečnosti nezávislé auditory třetích stran a to v pravidelných intervalech, nejméně však jednou za 12 měsíců.

Pokud jsou audity objednány členem APPS, pak budou prováděny:

- ve shodě s uznávaným bezpečnostním standardem (včetně např. ISO 27001),
- pravidelně podle platných norem a nařízení,
- kvalifikovaným nezávislým auditorem s osvědčením pro provádění auditů dle ISO 27001 a s osvědčením o absolvování kurzu k problematice GDPR v rozsahu nejméně 32 hodin.

O auditech budou vytvářeny hodnocení a zprávy.

Pokud člen APPS využívá k ověření adekvátnosti bezpečnostních kontrol nezávislých auditorů, může zákazníkům poskytnout kopie zpráv z auditů a to na základě písemné žádosti. Zprávy z auditů slouží k tomu, aby si zákazníci, auditoři zákazníků nebo příslušné dohledové orgány mohli ověřit soulad bezpečnostních povinností, který je definován ve smlouvě o poskytování služeb. Zpráva z auditu je zprávou důvěrnou. Člen APPS může tedy před dodáním zprávy po zákaznících požadovat podpis dohody o mlčenlivosti.7 Požadavky ohledně subjektu údajů

<u>Požadavky na ochranu dat:</u>

Člen APPS v roli zpracovatele zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III; (GDPR čl. 28 odst. 3 písm. e)

<u>Požadavky na členy APPS:</u>

Člen APPS poskytuje všem subjektům údajů (zákazníci, uchazeči, zaměstnanci aj.) možnost opravit, vymazat, omezit zpracovávání nebo poskytnout data (požadavek přenositelnosti údajů). Zákazníkům tak pomáhá reagovat na žádosti o uplatnění práv subjektů údajů.

Člen APPS může poskytnout všem subjektům údajů možnost opravit, vymazat, omezit nebo přenášet jeho data jako součást služby, nebo umožní zákazníkům navrhnout a nasadit vlastní řešení.

4.7. Požadavky na zaměstnance člena APPS:

<u>Požadavky na ochranu dat:</u>

---

[6] **Data Protection Officer – „DPO“,** <u>Článek 37 a násl.</u> GDPR

[7] Kodex nevyžaduje, aby člen APPS dal souhlas zákazníkovi nebo jiné osobě k provedení auditu svých procesů a systémů. Fyzický přístup třetích osob může znamenat potencionální bezpečnostní riziko pro všechny ostatní zákazníky. Poskytnutím zprávy z auditu konkrétního člena APPS toto riziko lze eliminovat a zároveň uspokojit přání zákazníka ohledně ověření bezpečnosti služeb.

Člen APPS zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti; (GDPR čl. 28 odst. 3 písm. b).

Požadavky na členy APPS:

Důvěrnost:

Člen APPS uloží veškerým zaměstnancům pověřeným přístupem datům zákazníků příslušné smluvní povinnosti týkající se mlčenlivosti a vypracuje vnitropodnikový dokumentovaný postup obsahující odpovědnosti a kompetence všech zaměstnanců zainteresovaných do procesu nakládání s OÚ.

Kontroly přístupu:

Člen APPS zavede a bude udržovat systém kontrol přístupů a takovou politiku, aby přístup k datům zákazníků měli skutečně jen ti zaměstnanci, kteří jej potřebují ke zpracovávání osobních údajů v rámci poskytování služeb. Pokud již zaměstnanec tento přístup nepotřebuje, člen APPS jej okamžitě zruší.

4.8. Požadavky na vymáhání práva

Požadavky na ochranu dat:

Rozhodnutí soudního orgánu a rozhodnutí správního orgánu třetí země, jež po správci nebo zpracovateli požadují předání nebo zpřístupnění osobních údajů, lze jakýmkoli způsobem uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem, aniž jsou dotčeny jiné důvody pro převod podle této kapitoly nařízení (GDPR čl. 48).

Požadavky na členy APPS:

Člen APPS předá orgánům ze třetích zemí činným v trestním řízení data zákazníků až poté, co obdrží platný a právně závazný soudní rozsudek, příkaz nebo požadavek a nebude poskytovat více zákaznických dat, než je nezbytně nutné.

V případě, že člen APPS obdrží závazný soudní rozsudek, bude o předání dat orgánům činným v trestním řízení informovat zákazníka s předstihem, aby mu poskytl možnost se dostatečně hájit.

Člen APPS může vydat veřejné pokyny určené orgánům činným v trestním řízení, žádajícími informace člena APPS a minimálně jednu zprávu o typech a objemech žádostí, které zpracoval.

4.9. Úniky dat

Požadavky na ochranu dat:

Jakmile **člen APPS** zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci. (GDPR čl. 33 odst. 2).

Člen APPS v roli **zpracovatele** je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici (GDPR čl. 28 odst. 3 písm. f)

Požadavky na členy APPS:

Politika správy bezpečnostních incidentů

Člen APPS má zavedenu politiku řízení bezpečnostních incidentů, která stanoví postupy pro identifikaci a reakci na bezpečnostní incidenty.

Tato politika zahrnuje:

- pokyny ohledně rozhodnutí, které typy incidentů musí být oznámeny zákazníkovi, případně UOOU, na základě možného dopadu na jeho data,
- pokyny k řešení incidentů,
- specifikace informací, které mají být zákazníkům po úniku dat zpřístupněny.

Oznámení o porušení bezpečnosti

Záznam a načasování oznámení

Pokud se člen APPS dozví o neoprávněném přístupu k jakýmkoliv osobním údajům a takový neoprávněný přístup vede ke ztrátě, zveřejnění, nebo změně těchto dat, oznámí tuto skutečnost bez zbytečného odkladu zákazníkům, případně UOOU.

Při vytváření podrobných pravidel týkajících se formátu a postupů ohlašování případů porušení zabezpečení osobních údajů člen APPS náležitě zohledňuje okolnosti porušení, včetně otázky, zda byly osobní údaje chráněny vhodnými technickými opatřeními, jež pravděpodobnost zneužití totožnosti a jiných forem zneužívání účinně omezují. Pakliže míra rizika zneužití OU díky přijatým opatřením člena APPS jsou minimální, ohlášení provést nemusí.

Obsah oznámení

Oznámení bude obsahovat: popis povahy narušení bezpečnosti; popis důsledků narušení bezpečnosti, popis opatření, která byla přijata či navržena v reakci na incident; jméno a kontaktní údaje zodpovědného zaměstnance.

4.10. Výmaz nebo obnova osobních údajů

Požadavky na ochranu dat:

Člen APPS se zavazuje striktně dodržovat ustanovení článku 17 nařízení GDPR. Pokud je člen APPS v roli zpracovatele, pak v souladu s rozhodnutím správce, všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů (GDPR čl. 28 odst. 3 písm. g).

Požadavky na členy APPS:

Člen APPS poskytuje možnost data přenést i smazat. Každý subjekt údajů může tuto možnost využít k portabilitě nebo smazání dat na konci smluvního vztahu, jak v případě zákazníka, tak i zaměstnance. Zpracování osobních údajů je možné jako součást služby, ale zákazník může navrhnout i své vlastní řešení.

5. Požadavky na transparentnost a spravedlivost

Každý z členů APPS se podpisem tohoto kodexu zavazuje, že všechny informace a všechna sdělení týkající se zpracování osobních údajů jsou snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Fyzické osoby budou upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva.

Zákazníci musí být při zpracovávání dat v schopni provádět spolehlivé hodnocení bezpečnostních rizik a jejich možný dopad na ochranu osobních údajů.

Člen APPS pomáhá zákazníkům tím, že transparentně komunikuje ohledně bezpečnostních opatření, která provádí. Tato komunikace zahrnuje:

1. Jasně dané rozdělení odpovědností mezi členem APPS a zákazníkem, které je zakotveno ve smlouvě o poskytování služeb.
2. Prohlášení člena APPS o vysoké úrovni bezpečnostních cílů a norem (důvěryhodnost, dostupnost a bezúhonnost).
3. Informace ohledně správy služeb, díky kterým zákazníci porozumí možným hrozbám a zranitelným místům.
4. Informace ohledně ověření procesů řízení rizik a bezpečnostních kritérií pro službu.
5. Informace o zavedených bezpečnostních opatřeních.
6. Dokumentace ohledně systému řízení informační bezpečnosti člena APPS.

Níže uvedené pododdíly popisují kroky, které by měl člen APPS podniknout, aby zajistil odpovídající úroveň transparentnosti a spravedlivosti pro každou službu, u které prohlašuje, že je v souladu s Kodexem.

Těchto cílů je možné dosáhnout zavedením a udržování systému řízení bezpečnosti informací. Tímto se pokryje všech šest žádaných cílů, což je v souladu s Kodexem.

Člen APPS se může, kromě požadavků specifikovaných ve smlouvě o poskytování služeb, rozhodnout sdílet informace, které jsou uvedeny v oddílu 5 (Požadavky na transparentnost a spravedlivost).

Jedná se o:

- informace o bezpečnostních a kontrolních postupech,
- informace o získání certifikace v oboru bezpečnosti informací a o osvědčení nezávislých auditorů (certifikačních orgánů),
- poskytování certifikátů, zpráv z auditů a dalších dokumentů.

Pokud tyto informace člen APPS považuje za důvěrné, může po zákazníkovi požadovat prohlášení o mlčenlivosti.

5.1. Požadavky na smlouvu o poskytování služeb z hlediska rozdělení bezpečnostních odpovědností mezi členem APPS a zákazníkem

Ve smlouvě o poskytování služeb jsou definovány bezpečnostní odpovědnosti člena APPS a bezpečnostní odpovědnosti zákazníka. Zákazník pak zůstává odpovědný za veškeré aspekty bezpečnosti, na které se smlouva nevztahuje.

5.2. Prohlášení o bezpečnostních cílech a normách vztahující se na poskytování služeb

Člen APPS uvádí, že stanovil cíl sledovat bezpečnostní opatření jím zavedená, případně právního předpisu, nebo normy, které bude člen APPS udržovat při provádění bezpečnostních opatření.

Upravovat požadavky bezpečnostních právních požadavků a norem je možné pouze za předpokladu, že úroveň bezpečnosti služeb bude nadále poskytovat přinejmenším stejnou úroveň bezpečnosti, která je popsána v právních předpisech či normách platných k datu počátku účinnosti smlouvy o poskytování služeb.

Člen APPS bude informovat zákazníky o úmyslech rozšířit služby zákazníkům o informace ohledně pravidel dodržování zvláštních standardů nebo právních požadavků vztahujících se k určitému typu zpracovávání dat (např. zpracovávání údajů o zdravotní péči, biometrické údaje, rasa, náboženství, členství v odborech aj.). Tyto informace může obsahovat smlouva o poskytování služeb a mohou být uvedeny v popisu služby na webových stránkách člena APPS nebo v jiných veřejně dostupných materiálech.

5.3. Shromažďování osobních údajů;

Člen APPS poskytuje zákazníkům, v případě jejich zájmu, informace o systémovém zabezpečení a o tom, jakým způsobem jsou informace o zařízení, síti, hardwaru a provozním softwaru využívána v rámci poskytování služeb.

Tyto informace mohou například obsahovat:

- Seznam subdodavatelů, kteří mají autorizaci k přístupu k datům zákazníků,
- bezpečnostní prvky služeb,
- seznam možností, které může zákazník využít k vyššímu zabezpečení služeb,
- obecné umístění hostitelských zařízení.

5.4. Informace ověřující procesy řízení rizik a kritéria pro člena APPS

Člen APPS poskytuje zákazníkům informace, ověřující existenci a vhodnost programu řízení rizik. Zákazníci tyto programy mohou začlenit do vlastního rámce řízení rizik. Tyto informace mohou například obsahovat hodnocení vnitřních a vnějších rizik ze zpráv z auditů.

Při hodnocení rizik se člen APPS řídí metodikou založenou na metodách vysokého technického a vědeckého poznání v dané problematice

5.5. Informace ohledně implementovaných bezpečnostních opatřeních

Člen APPS poskytuje informace o zavedených bezpečnostních opatřeních takovým způsobem, aby zákazníkům pomohli porozumět, jak jsou tato bezpečnostní opatření zavedena, používána a ověřena.

Zákazníci pak mohou vyhodnotit, jakým způsobem konfigurovat nastavení svých služeb, aby byla úroveň bezpečnosti odpovídající.

Zejména budou specifikovány:

- fyzické a operační bezpečnostní procesy pro síťové a serverové infrastruktury,
- bezpečnostní prvky a ovládací prvky, které mohou zákazníci využívat a konfigurovat v rámci služeb.

Dále budou obsahovat například informace o:

- fyzické a environmentální bezpečnosti,
- zabezpečení sítě,
- řízení nepřetržitosti provozu,
- změny řízení,
- funkce zabezpečení účtu.

5.6. Dokumentace ověřující řízení systému informační bezpečnosti

Člen APPS poskytuje v souvislosti s poskytovanými službami dostatek informací o implementovaném systému bezpečností informací. Zákazníci si tak mohou ověřit, jak je popsáno v odstavci 4.6 (Prokazování shody), že člen APPS dodržuje závazky týkající se bezpečnosti obsažené ve smlouvě o poskytování služeb.

6. Ostatní závazky členů APPS

6.1. Oprávněné zájmy správců, které v konkrétních situacích sledují

V případě, že zpracování je nezbytné pro účely oprávněných zájmů příslušného člena APPS[8] je takové zpracování zákonné. Oprávněné zájmy člena APPS se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem. Například pokud je subjekt údajů zákazníkem správce nebo mu naopak poskytuje služby. Takové situace neplatí, jestliže ke zpracování osobních údajů dochází za okolností, kdy subjekt údajů jejich další zpracování důvodně neočekává. Zpracování osobních údajů členy APPS pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu.

6.2. Shromažďování osobních údajů

Žádný ze členů APPS nepoužívá osobních údajů dětí pro účely marketingu nebo vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání služeb nabízených přímo dětem. Takové služby členové APPS neposkytují.

6.3. Pseudonymizace osobních údajů

Člen APPS se zavazuje implementovat vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně pseudonymizace a šifrování osobních údajů. Člen APPS přijme vnitřní koncepci a zavede opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření mimo jiné spočívají v minimalizaci zpracování osobních údajů a co nejrychlejší pseudonymizaci osobních údajů.

Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů, zohlední člen APPS jako správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.

6.4. Informace poskytované veřejnosti a subjektům údajů

Člen APPS se zavazuje, že všechny informace určené veřejnosti nebo subjektu údajů budou stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech navíc i vizualizace. Pokud budou tyto informace určeny veřejnosti, mohly by být poskytovány v elektronické podobě, například prostřednictvím internetových stránek.

Kromě informací zveřejňovaných subjektům údajům a veřejnosti, asociace zveřejní na svých stránkách i tento Kodex, stejně tak by ho měl zveřejnit i UOOU.

6.5. Výkon práv subjektů údajů

Člen APPS přijal vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých

---

[8] Kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

jazykových prostředků veškeré informace, které musí sdělit v případě, že osobní údaje (ne) byly získány od subjektu údajů dle článku 13 a 14 Nařízení a učinil veškerá sdělení podle práva subjektu údajů na přístup k osobním údajům.

Člen APPS stanovil postupy, které usnadnily výkon práv subjektů údajů podle nařízení, včetně mechanismů pro podávání žádostí a obdržení přístupu k osobním údajům a opravy nebo výmazu osobních údajů a pro uplatnění práva vznést námitku. Člen APPS zajišťuje podmínky pro to, aby žádosti mohly být podávány elektronicky, a reaguje na žádosti subjektu údajů bez zbytečného odkladu a nejpozději do jednoho měsíce.[9]

Člen APPS zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III Nařízení.

6.6. Postupy a opatření k zajištění bezpečnosti zpracování

Člen APPS stanovil vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s nařízením. Mezi tato opatření patří tento Kodex chování a vnitropodniková dokumentace člena APPS. Tato opatření jsou pravidelně revidována a aktualizována.

Člen APPS zavede jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky Nařízení a ochránil práva subjektů údajů.

Člen APPS implementuje vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provede Člen APPS vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně: pseudonymizace a šifrování osobních údajů; schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti Člen APPS vždy zohledňuje zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. Člen APPS přijímá opatření pro zajištění toho, aby jakákoliv fyzická osoba, která má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce.

6.7. Mimosoudní vyrovnání a řešení sporů

Aniž jsou dotčeny jakékoliv jiné prostředky správní nebo soudní ochrany, má každý subjekt údajů právo podat stížnost u UOOU, pokud se subjekt údajů domnívá, že zpracováním jeho

---

[9] Pokud má člen APPS pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů.

osobních údajů je porušeno Nařízení GDPR. Příslušný dozorový úřad informuje stěžovatele o pokroku v řešení stížnosti a o jeho výsledku.

Právo na účinnou soudní ochranu vůči členovi APPS

Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle Nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto Nařízením.

Řízení proti členovi APPS se zahajuje u soudů v ČR, pokud provozovna, kde k porušení došlo, není v jiném státě než toho členského státu, v němž má daný správce nebo zpracovatel provozovnu.

7. Prohlášení o dodržování Kodexu

Člen APPS nemůže prohlásit, že bude dodržovat pouze vybranou část požadavků Kodexu, nebo určitou část požadavků vyloučit. Pokud se zavázal Kodex dodržovat, musí vyhovět požadavkům všem, které jsou v Kodexu uvedené a to pro každou ze svých služeb.

Člen APPS se zavazuje podrobit se požadavkům z části 8 (Management). Pokud člen APPS nebude plnit některé z požadavků Kodexu, budou se na něj vztahovat prostředky k vymáhání nápravy. Tímto nejsou dotčeny případné jiné sankce příslušných orgánů dohledu.

a) Prohlášení o dodržování Kodexu

Aby člen APPS mohl označit své služby značkou shody, musí vyplnit a předložit prohlášení o dodržování Kodexu (Prohlášení o shodě) v souladu s pokyny pro dodržování Kodexu schválenými Prezídiem (pokyny pro dodržování Kodexu). Současná podoba Prohlášení o dodržování je uvedena v příloze 2. Prohlášení může být průběžně aktualizováno. Sekretariát zveřejňuje prohlášení o dodržování a pokyny pro dodržování Kodexu ve veřejném registru členů APPS. Prohlášení o dodržování potvrzuje, že služby splňují požadavky tohoto Kodexu.

Člen APPS si k podpoře svého prohlášení o dodržování Kodexu může zvolit mezi následujícími dvěma postupy:

- certifikace nezávislým auditem třetí strany,
- sebehodnocením.

Značky shody se vztahují na prohlášení o dodržování, které je podporováno oběma těmito postupy. Oba postupy jsou podrobněji vysvětleny v pododstavcích (b) a (c) níže.

Sekretariát APPS přezkoumá prohlášení dle pokynů pro dodržování Kodexu. Do 20 pracovních dnů od obdržení dokumentu sekretariát APPS oznámí členům APPS, zda je prohlášení úplné.

Pokud v dokumentu některé náležitosti chybí, sekretariát může požádat o doplnění chybějících dokumentů či informací.

V případě přijetí prohlášení sekretariát začlení člen APPS do veřejného rejstříku uvedeném na WWW.APPS.cz to do deseti pracovních dnů po oznámení o přijetí.

Po začlenění prohlášení o dodržování Kodexu do veřejného rejstříku je člen APPS oprávněn používat toto prohlášení a příslušnou značku shody (jak je uvedeno v části 7.1 níže).

Člen APPS je povinen neprodleně sekretariátu APPS ohlásit jakoukoli změnu, která znamená nutnost aktualizovat dokumenty a na aktualizaci se sekretariátem spolupracovat.

b) certifikace nezávislým auditorem

Proces

Člen APPS prokazuje shodu s Kodexem předložením certifikátů, auditorských zpráv, prohlášeními o shodě a podobnými dokumenty pokrývajícími požadavky Kodexu.

APPS získá certifikát tím, že využije služeb některé z kvalifikovaných a uznávaných auditorských firem (například QISO-MIRAIS, s.r.o.), které provedou audit, vypracují z auditu zprávu a vystaví osvědčení o shodě. Zprávy a certifikáty vystavené certifikační autoritou slouží jako osvědčení pro splnění účelů této části Kodexu.

Pokud člen APPS již vlastní certifikát nebo zprávu z auditů, může ji pro účely osvědčení o dodržování Kodexu použít jako osvědčení, které prokazuje, že jeho služby splňují požadavky Kodexu, aniž by musel podstoupit nový audit k získání certifikátu nebo zprávy z auditu.

Obnova prohlášení o dodržování Kodexu

Prohlášení o dodržování požadavků Kodexu získané prostřednictvím certifikátu (interního auditu) je platné pouze jeden rok ode dne jeho zapracování do veřejného rejstříku uvedeném na WWW.APPS.cz.

Aby člen APPS mohl značky shody nadále používat, musí prohlášení o dodržování Kodexu každý rok obnovit (certifikací nezávislým auditem třetí strany, nebo sebehodnocením).

c) Sebehodnocení prováděné členy APPS

Proces

Člen APPS může prokázat, že jedna nebo více jeho služeb je ve shodě s požadavky Kodexu, sebehodnocením provedeným v souladu s pokyny níže.

Člen APPS, který si zvolí tento postup, musí předložit své prohlášení o dodržování Kodexu sekretariátu APPS společně s veškerými požadovanými doplňujícími informacemi, které jsou uvedeny v požadavcích na dodržování Kodexu.

Obnova prohlášení o dodržování Kodexu

Prohlášení o dodržování Kodexu získané prostřednictvím sebehodnocení je platné pouze jeden rok od data, kdy je člen APPS zapsán do veřejného rejstříku uvedeném na WWW.APPS.cz.

Pokud si člen APPS přeje využívat prohlášení o dodržování Kodexu získané sebehodnocením a nadále značky shody používat, musí každý rok prohlášení obnovovat.

7.1. Značky shody

APPS vytvoří **značky shody**, které se budou využívat jako veřejný status shody služeb s požadavky na Kodex (značky shody)[10]. Značka shody je schválena Prezídiem APPS v níže uvedeném vyobrazení:

---

[10] OUR SERVICES WE PROVIDE ACCORDANCE WITH THE GDPR CODE ISSUED BY APPS; NAŠE SLUŽBY POSKYTUJEME V SOULADU S GDPR KODEXEM VYDANÝM APPS.

Sekretariát APPS tyto pokyny zveřejní a aktualizuje na webových stránkách.

Jakmile je prohlášení o dodržování Kodexu začleněno do veřejného rejstříku, je člen APPS oprávněn používat příslušnou značku shody, dokud prohlášení o shodě s Kodexem zůstane platné a za předpokladu, že člen APPS použije značky shody v souladu s pokyny pro používání značky.

8. Management

8.1. Struktura managementu

Asociace poskytovatelů personálních služeb (APPS) odpovídá za správu Kodexu.

8.2. Stížnosti a prostředky k vymáhání nápravy

a) Prezídium

Prezídium asociace bude zodpovědné za:

a) posouzení stížností ohledně služeb, na něž se vztahuje prohlášení člena APPS o dodržování požadavků Kodexu,

b) převzetí povinnosti využít prostředky vymáhání proti nevyhovujícímu členu ASPP a v případě potřeby doporučení konkrétních donucovacích opatření správní radě.

b) Řízení o stížnostech

Sekretariát APPS navrhne Prezídiu pravidla a proces pro vyřizování, rozhodování, odvolávání a sdělování výsledků stížností na soulad služeb, na něž se vztahuje prohlášení o dodržování požadavků Kodexu (proces podávání stížností).

Po schválení Prezídiem bude sekretariát zveřejňovat, provádět a řídit proces stížností. Sekretariát APPS bude zveřejňovat a aktualizovat informace o procesu podávání stížností ve veřejném registru na webových stránkách APPS.

Člen APPS, zákazník, uchazeč, zaměstnanec nebo příslušný orgán dozoru může tomuto Prezídiu podat stížnost. Prezídium je přezkoumá a rozhodne v souladu s procesem pro vyřizování stížností.

c) Vymáhání nápravy

Pokud Prezídium ve svém konečném rozhodnutí sezná, že člen APPS není v souladu s požadavky Kodexu, pak bude postupovat následujícím způsobem:

- Požádá člena APPS, aby přijal konkrétní nápravná opatření, a to v rozumném časovém rámci,
- v případě extrémních nebo opakovaných případů nedodržení požadavků Kodexu nebo v případě, že člen APPS neprovede požadovaná nápravná opatření (vůbec nebo včas), doporučuje správní radě, aby prohlášení o dodržování Kodexu člena APPS bylo pozastaveno nebo zrušeno s ohledem na nevyhovující službu.

Pokud je prohlášení o dodržování Kodexu pozastaveno nebo zrušeno:

- sekretariát okamžitě odstraní člena APPS z veřejného rejstříku členů asociace APPS,
- Prezídium určí přiměřený časový rámec, kdy člen APPS musí přestat používat značku shody,
- člen APPS přestane používat značku shody v souvislosti ve lhůtě stanovené Prezídiem asociace.

V případě pozastavení platnosti prohlášení o dodržování Kodexu platí tato opatření až do zrušení tohoto pozastavení. Tato vynucovací opatření jsou jediné a výlučné opravné prostředky při nedodržení požadavků Kodexu. Vynucovacími opatřeními nejsou dotčena práva zákazníka podle příslušného zákona o ochraně osobních údajů nebo smlouvy o poskytování služeb.

Možnost zákazníka podat stížnost neposkytuje zákazníkovi žádná přímá práva nebo opravné prostředky vůči členu APPS na základě nebo v souvislosti s Kodexem.

APPS nepřijímá žádnou odpovědnost za dodržování Kodexu členem APPS. Asociace nebude odpovědná žádné straně, za žádnou žalobu ani za tezi odpovědnosti za ztráty nebo škody, vyplývající z jednání nebo opomenutí člena asociace v souvislosti s Kodexem.

8.3. Přezkum Kodexu a pokynů pro dodržování Kodexu

a) Znění Kodexu

Asociace bude nadále přezkoumávat Kodex na základě změn platných právních předpisů EU o ochraně údajů. Asociace se zavazuje kompletně přezkoumat aktuálnost kodexu každé dva roky, aby byl zohledněn právní a technologický vývoj, jakož i vývoj v oblasti osvědčených postupů v odvětví.

Prezídium může zahájit zvláštní revizi Kodexu společnou žádostí nejméně pěti členů. Prezídium může zahájit takové přezkoumání z vlastního podnětu, nebo proto, že je o to požádána příslušným orgánem dohledu, jednajícím jako úřední osoba.

- **b) Změny v Kodexu**

Po přezkoumání může asociace doporučit změny Kodexu Prezídiu. Změny kodexu musí být přijaty asociací ještě před tím, než vstoupí v platnost.

Každá změna Kodexu musí být přijata členy APPS a to tímto postupem:

- předložena Prezídiu a valnému shromáždění,
- schválena Prezídiem,
- schválena valným shromážděním zvláštním usnesením.

Před přijetím změny ze strany asociace může Prezídium rozhodnout o předložení změny Kodexu k posouzení a připomínkám UOOU.

Po přijetí změny asociací zveřejní sekretariát aktualizovanou verzi tohoto kodexu ve veřejném registru.

Členové APPS jsou povinni obnovit nebo znovu potvrdit svá prohlášení o dodržování Kodexu do dvou měsíců od zveřejnění aktualizované verze Kodexu. Člen APPS, který prokáže, že jeho činnost splňuje požadavky Kodexu předložením certifikátu společně s prohlášením o dodržování, může využít stávající certifikáty, aniž by musel podstoupit nový nebo zvláštní audit a získat tak nové certifikáty nebo zprávy z auditů.

PŘÍLOHA 1

Rozdělení bezpečnostních odpovědností

Předmět

Tato příloha definuje bezpečnostní odpovědnosti člena APPS a zákazníka v rámci poskytování personálních služeb.

Člen APPS je odpovědný za službu, kterou poskytuje, ale nikoli za systémy a aplikace, které zákazník prostřednictvím personální služby obsluhuje. Za tuto část odpovídá zákazník.

1) Management bezpečnosti informací

a) Odpovědnosti člena APPS

Člen APPS má čitelný systém řízení a podpory zabezpečení služeb.

Člen APPS má zavedenou politiku bezpečnosti informací, které upravují zabezpečení služeb a jsou schváleny managementem.

Člen APPS má zavedený systém managementu informační bezpečnosti nebo jeho ekvivalent. Rozsah systému managementu bezpečnosti informací se vztahuje na služby.

Člen APPS jmenoval zaměstnance, kteří budou koordinovat a budou odpovědní za systém managementu bezpečnosti informací.

B) Odpovědnost zákazníka

Zákazník určí kontaktní místo pro otázky bezpečnosti vzhledem k využívání personálních služeb.

Zákazník provede zhodnocení rizik, aby zajistil vhodnost personálních služeb pro zpracovávání dat vzhledem k platným právním předpisům EU o ochraně osobních údajů.

2) Bezpečnost lidských zdrojů

a) Odpovědnost člena APPS

Člen APPS má organizační strukturu odpovědnou za zavedení a udržování managementu bezpečnosti informací s jasně definovanými úlohami a odpovědnostmi.

b) Odpovědnost zákazníka

Zákazník je výhradně odpovědný za své zaměstnance a za třetí osoby, které mají přístupy nebo využívají personální služby (včetně smluvních dodavatelů, zástupců nebo koncových uživatelů).

3) Řízení uživatelských přístupů

a) Odpovědnost člena APPS

Člen APPS poskytuje zákazníkům systém správy přístupu jako součást některých služeb. Systém správy přístupů zahrnuje jmenovité účty, přístup do služby za účelem plnění úkolů a hesla nebo jiné prostředky ověřování.

Člen APPS není odpovědný za přístupová řešení a aplikace, které využívá pomocí personálních služeb zákazník.

b) Povinnosti zákazníka

Zákazník je výhradně odpovědný za používání a konfiguraci přístupových systémů. Zákazník je odpovědný za přidělování přístupových práv příslušným zaměstnancům.

Zákazník je odpovědný za přístupová řešení k systémům a aplikacím, které využívá prostřednictvím personálních služeb.

4) Bezpečnostní opatření

a) Odpovědnost člena APPS

Člen APPS zavádí a udržuje bezpečnostní opatření pro personální služby, jejichž cílem je pomoci zákazníkům zabezpečit osobní údaje před neoprávněným zpracováním a náhodnou nebo nezákonnou ztrátou, přístupem nebo zveřejněním.

b) Odpovědnost zákazníka

Zákazníci posuzují:

a) informace poskytnuté členy APPS týkající se bezpečnosti,

B) zda zavedená bezpečnostní opatření jeho i bezpečnostní opatření zpracovatele společně poskytují odpovídající úroveň zabezpečení.

5) Servery a zařízení

a) Odpovědnosti člena APPS

APPS je výhradně zodpovědný za umístění, provoz a zabezpečení jakéhokoli fyzického hardwaru používaného k poskytování personálních služeb, včetně všech konfigurací potřebných pro poskytování služeb.

b) Odpovědnosti zákazníka

Zákazník je výhradně odpovědný za správu vhodné konfigurace jakéhokoli systému a aplikací, které zákazník využívá v rámci personálních služeb.

6) Konec životnosti hardware a jiných zařízení

a) Odpovědnosti člena APPS

Člen APPS maže data zákazníků z paměťových médií před jejich konečnou likvidací. Tento proces je prováděn v souladu se stanovenými standardními postupy, tak aby data zákazníků nemohly být nikdy zpět získány z příslušných typů paměťových médií žádnými nástroji pro získávání dat nebo jinými prostředky.

b) Povinnosti zákazníka

Zákazníci posuzují:

a) informace poskytnuté členem APPS ohledně vyřazování paměťových médií z provozu,

b) bezpečnostní aspekty v jeho odpovědnosti a bezpečnostní opatření, která zákazník provádí v souvislosti s využíváním personálních služeb, aby se ujistil, že společně tato opatření poskytují odpovídající úroveň zabezpečení pro zpracovatele, který bude služby využívat.

PŘÍLOHA 2

Šablona PROHLÁŠENÍ o dodržování Kodexu

Toto je prohlášení o dodržování Kodexu (dále jen "Prohlášení") pro poskytovatele personálních služeb. Pokud není vymezeno jinak, termíny používané v tomto Prohlášení budou mít význam, který je jim dán v Kodexu.

2. Člen APPS, který Prohlášení vydal

Toto Prohlášení je vydáváno subjektem, který je poskytovatelem personálních služeb (dále jen "člen APPS"). Pokud je toto Prohlášení vydáváno více než jedním členem APPS, uveďte podrobnosti pro každého člena níže a také v části číslo 5. Tyto informace budou k dispozici ve veřejném registru.

	Název právnické osoby	Adresa
Poskytovatel personálních služeb 1	…	…
Poskytovatel personálních služeb 2	…	…
Atd.	…	…

3. Způsob podpory Prohlášení

Prohlášení je podpořeno:

- certifikací provedenou nezávislým auditorem třetí strany,

- sebehodnocením člena APPS.

Je na Vás, který způsob využijete a kterou značku shody pak budete mít možnost využívat.

4. Požadavky na auditovatelné položky Prohlášení (pro Prohlášení potvrzená certifikátem)

Požadavky v tabulce A jsou požadavky na auditovatelné položky. Prosím vyplňte tabulku a přiložte kopie všech certifikátů.

5. Prohlášení o dodržování Kodexu

Podpisem tohoto dokumentu člen APPS potvrzuje, že:

a) všechny jeho činnosti splňují požadavky tohoto Kodexu, a to k datu podpisu tohoto prohlášení,

b) člen APPS bude dodržovat postupy pro případ stížností uvedené v oddíle 8 (Management),

c) pokud nastanou u člena APPS změny, které jsou důležité ve vztahu ke Kodexu a toto prohlášení bude nutné aktualizovat, pak to člen APPS neprodleně oznámí sekretariátu APPS a bude spolupracovat na aktualizaci.

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………

Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: ……………………
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy

Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: ……………………
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….

Jméno: …………………….
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: …………………….
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: …………………….
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: …………………….
Datum: ……………………

Člen APPS – název firmy
Podpis: …………………….
Jméno: …………………….
Datum: ……………………