GDPR 2018: Změny v ochraně osobních údajů v návodech a vzorech

Praktické nástroje, šablony a formuláře v souladu s nařízením EU

Březen 2024

FORUM

Obsah tištěné příručky

GDPR 2018: Změny v ochraně osobních údajů v návodech a vzorech

5 Jaká práva mají fyzické osoby vůči svým osobním údajům

6 Nakládání s osobními údaji při zaměstnávání

7 Marketingová a obchodní činnost ve světle GDPR

3.2.3 Co musí být ve smlouvě společných správců?

Zamysleli jste se, zda při zpracování osobních údajů **nevystupujete v roli společného správce**? Je to častější, než jste si mysleli. Společným správcům GDPR ukládá několik povinností včetně uzavření smlouvy. V této kapitole se podíváme, jak na to.

Současný stav

Vztahy povinných osob v rámci GDPR jsou kapitola sama o sobě. Ačkoliv GDPR je zde s námi již přes pět let (a tato povinnost dokonce vychází z původní směrnice), stále se setkáváme s obchodními případy, kde GDPR **nehraje žádnou roli** a je zcela opomíjeno.

Dlužno dodat, že situace je o něco lepší než dříve a v okamžiku **předložení zpracovatelské smlouvy** z jedné strany už většinou nepřicházejí zvídavé dotazy, proč takovou smlouvu uzavřít. Obě strany už zpravidla akceptují skutečnost, že dochází ke zpracování osobních údajů a že kdyby nedošlo k uzavření zpracovatelské smlouvy, **mohou obě strany dostat pokutu**.

Vztah společných správců

Jenže **vztah správce a zpracovatele** není jediným vztahem, s nímž se můžeme v rámci GDPR setkat. Naopak, s rozvojem business modelů různých služeb se stále častěji potkáváme se situacemi, kdy předmětný vztah není tvořen správcem a zpracovatelem (či správcem a správcem), ale zpracování probíhá **v rovině společných správců**. Někdy se však na tento fakt úplně zapomíná, stejně jako na povinnosti, které v takových případech GDPR aktérům ukládá.

Častá chyba

Nedávno udělil francouzský dozorový orgán (CNIL) pokutu poskytovateli remarketingových služeb, který se svými partnery neuzavíral předmětné smlouvy, a tím docházelo k porušení GDPR.

Smlouva společných správců

Co by taková **smlouva společných správců tedy měla obsahovat**? Pro účely této kapitoly se obejdeme bez podrobného rozboru definice společných správců (najdete ji v předchozí kapitole 3.2.1). Tato definice sice může v praxi působit potíže, ze strany WP29 či EDPB nicméně již **přišlo mnoho vodítek a pokynů** s praktickými příklady, díky nimž by si s tím každý člověk, který je v organizaci odpovědný za GDPR, měl poradit.

Pro společné správce je příznačné, že **společně určují účely a prostředky zpracování**, nicméně stejně jako v případě vztahu správce a zpracovatel není vhodné tuto definici interpretovat pouze jazykovým výkladem.

Zaměřme se spíše na to, jaké povinnosti GDPR v takových případech ukládá. Nastavení vzájemných pravidel se věnuje GDPR relativně stroze v jednom článku (čl. 26) o třech odstavcích. Primárním způsobem regulace vztahů je **požadavek na uzavření smlouvy** (respektive slovy GDPR ujednání) mezi aktéry, jež má upravovat vzájemná práva a povinnosti, ale také povinnosti vůči třetím osobám.

Co se týče formálních náležitostí, GDPR žádné bližší podmínky neupravuje. Vlastně stanovuje

12 GDPR ve zdravotnictví

12.1 Jak bude fungovat Evropský prostor pro zdravotní data?

Předávání lékařských zpráv na CD, chybějící standardy pro elektronizaci zdravotnictví či **nejasná pravidla pro zpracování osobních údajů** pro účely vědy a výzkumu. To jsou jen některé z problémů, o nichž se mluví v souvislosti s digitalizací českého zdravotnictví. Tyto i mnohé další si klade za cíl vyřešit navrhované **evropské nařízení o evropském prostoru pro zdravotní data** (dále jen „nařízení").

Co je cílem EHDS?

Evropský prostor pro zdravotní data (European Health Data Space, dále jen „EHDS") představuje **rámec pro sdílení zdravotních dat** se společnými pravidly pro fungování, infrastrukturou a technickými standardy. Stojí na dvou relativně autonomních pilířích. Jeden je určený pro takzvané **primární využití zdravotních dat**, tedy pro účely poskytování zdravotních služeb, druhý je **pro sekundární využití**, tedy pro účely výzkumu, vývoje, inovací, statistik či tvorby politik.

Evropská komise návrhem reaguje na **nízkou úroveň elektronizace zdravotních systémů** v mnoha členských zemích EU, která se zejména v období pandemie covidu-19 ukázala jako hlavní překážka efektivního **řízení hrozeb pro veřejné zdraví**. Současně však EU usiluje o to stát se lídrem na digitálním trhu a vysoce efektivní společností založenou na datech. EHDS je prvním konkrétním návrhem

ze skupiny společných evropských datových prostorů, které mají být postupně vytvořeny v rámci **Evropské digitální strategie** vyhlášené na roky 2020–2030.

Mezi hlavní cíle EHDS patří zaprvé umožnit jednotlivcům **kontrolu nad jejich zdravotními daty**, zadruhé podpořit využívání dat pro zvýšení kvality poskytovaných zdravotních služeb, zatřetí podpořit výzkum, inovace a tvorbu politik a začtvrté stanovit pravidla pro uvádění informačních **systémů pro vedení elektronických zdravotních záznamů** na trh.

Aktuální stav legislativního procesu

Tato kapitola vychází z **druhého kompromisního návrhu nařízení** ze dne 8. května 2023, do něhož byly promítnuty některé připomínky Evropského hospodářského a sociálního výboru, Evropského výboru regionů, ale též společné připomínky Evropského sboru pro ochranu dat a Evropského inspektora pro ochranu údajů. V současné době se připravuje třetí kompromisní návrh. Jeho **přijetí se předpokládá do konce roku 2023**.

První pilíř EHDS

Základem a smyslem celého EHDS je sdílení elektronických zdravotních dat, která se nejčastěji generují při poskytování zdravotních služeb. Nařízení **dělí elektronická zdravotní data na osobní a anonymizovaná**. Osobními daty jsou zdravotní a genetická osobní data ve smyslu nařízení (EU) 2016/679 (dále jen „GDPR"), zpracovávaná v elektronické podobě. Anonymními elektronickými zdravotními daty jsou pak údaje týkající se zdraví zpracovávané v elektronické podobě, které se nevztahují k identifikované nebo identifikovatelné fyzické osobě,

13 Příklady dobré praxe podle GDPR

13.1 Jak postupovat při zavádění kamerového systému

S kamerovými systémy se v současné době setkáváme téměř na každém kroku a někdy už ani nevnímáme, že v určitém prostoru jsou na nás kamery namířeny. Nicméně **legitimní provozování kamerového systému** je spjato s celou řadou povinností, které vyplývají především z GDPR. Již **před samotnou instalací** musí budoucí provozovatel kamerového systému provést několik kroků, aby neporušil právní předpisy.

Jednotlivé povinnosti jsou podrobně popsány v kapitole 3.9 Kamerové systémy. Zde se zaměříme na časté chyby při provozování kamerových systémů a na **praktická doporučení a návody.**

Kamery pro strýčka Příhodu

V praxi se lze poměrně často setkat s tím, že kamerové systémy jsou provozovány, aniž by k tomu měl provozovatel (správce z pohledu GDPR) nějaký závažný důvod. Je to čistě **preventivní opatření pro případ, že by se něco stalo**. Takový přístup ovšem z pohledu GDPR ani jiných právních předpisů neobstojí. Správce musí mít předem jasně stanovený a popsaný účel pro provozování kamerového systému. Navíc kamerový systém není často tím prvním opatřením, ke kterému by měl správce přistoupit.

Praktický příklad

Ne každý problém může vést k zavedení kamerového systému. Například pokud chce zaměstnavatel kontrolovat své zaměstnance, jak pilně pracují, kamerový systém určitě není ten správný prostředek, jak toho dosáhnout. Na druhou stranu umístění kamerového systému v rámci obchodu s klenoty z důvodu ochrany majetku, ale i zdraví a života zaměstnanců může být oprávněným důvodem.

Důležitou roli také hraje okruh subjektů údajů, které mají být kamerovým systémem sledovány. Pokud se jedná o **zranitelné osoby nebo osoby ve slabším postavení**, jako jsou například děti, pacienti nebo zaměstnanci, musí být důvod k jejich sledování závažnější než při sledování běžné veřejnosti.

Před zavedením kamerového systému

Jestliže chce tedy správce zavést kamerový systém, musí být schopen toto opatření **obhájit z hlediska účelu, jeho nezbytnosti a přiměřenosti**. Dále je nutné zpracování osobních údajů prostřednictvím kamerového systému opřít o nějaký právní titul uvedený v článku 6 GDPR. Jak bylo uvedeno v kapitole o kamerových systémech, nejčastějším právním titulem je **oprávněný zájem správce nebo třetích osob**. V tomto případě je ale třeba také zpracovat takzvaný balanční test, ve kterém je nutné porovnat oprávněný zájem s právy a zájmy subjektů údajů, které budou předmětem sledování, jímž může být neoprávněně zasahováno do jejich soukromí. Teprve když si je správce jistý, že jeho oprávněné zájmy či zájmy jiných osob jsou **silnější než práva subjektů údajů**, může uvažovat o instalaci kamerového systému.

13.2 Jak pracovat se službou ChatGPT a neohrozit osobní údaje?

Už jste zkoušeli ChatGPT? Kontroverzní podobu umělé inteligence navrženou jako takzvaný **chatbot spustila společnost OpenAI** v listopadu 2022. Od té doby stihla proniknout do nejedné obchodní korporace či domácnosti. Je však s touto inovací vše v pořádku? A jaké hrozby může používání ChatGPT přinést v rámci ochrany osobních údajů?

ChatGPT (Generative Pre-trained Transformer) je jazykový model, který za poslední rok **změnil způsob komunikace a samozřejmě i způsob tvorby textů**. Funguje jako klasický chat umožňující komunikaci (dialog) s umělou inteligencí, která je od té lidské takřka k nerozeznání. Avšak i když ChatGPT a jemu podobné jazykové modely nepochybně znamenají inovaci a větší pohodlí při tvorbě článků nebo třeba postů pro sociální sítě, **přinášejí také řadu rizik z hlediska ochrany osobních údajů**.

Dejte si pozor, na co se ptáte

Jednou z nejnebezpečnějších hrozeb spojených s chatovacími modely je **riziko úniku citlivých dat**. Tyto modely totiž pracují na základě obrovských „datasetů" (úložišť informací), jejichž obsah často tvoří data vkládaná samotnými uživateli, která jsou následně uchovávána a zpracovávána chatovacím modelem. Z těchto vložených údajů pak chatovací model čerpá při tvorbě svých odpovědí.

13.3 Využití umělé inteligence při náboru zaměstnanců

Proces nabírání nových zaměstnanců může být značně úmorný – zejména ve velkých společnostech, které **hledají nové členy týmu téměř neustále**. Personalisté musejí vytvářet vhodné pracovní inzeráty, potom se probírat hromadou obdržených životopisů, vyřazovat na první pohled nevhodné uchazeče a obvolávat ty, které vybrali k pozvání na osobní pohovor. Následně někdo musí osobní pohovory s kandidáty absolvovat, což také **zabere hodně času**. V náborovém procesu některých firem proto hrají čím dál tím důležitější roli stroje, které jej mají usnadnit.

Pomocník v podobě AI

Všemožné systémy umělé inteligence (AI) jsou naprogramovány tak, aby shromažďovaly co největší množství dat (včetně osobních údajů), jež následně **samy analyzují a zpracovávají**. Přečtou životopisy, zhodnotí silné i slabé stránky kandidáta, dokážou si s kandidátem chatovat nebo zhodnotí jeho prezentaci zachycenou na videu. Oblast lidských zdrojů tedy přináší pro AI mnoho příležitostí – dokáže **zrychlit poměrně dost aktivit**, které jsou jinak pro personalisty zdlouhavé a repetitivní.

S umělou inteligencí se proces nalezení ideálního zaměstnance mezi stovkami profilů v databázi může stát záležitostí pár sekund a náboráři tak **ušetří čas strávený probíráním se životopisy**. Zní to tak idylicky, až by se mohlo zdát, že díky umělé inteligenci personalisté nebudou mít co na práci. Stane se však takový postup při náboru zaměst-

nanců postupně standardem? Je možné zcela pominout osobní kontakt při výběru budoucího kolegy? A nebude využívání strojů v náboru narážet na **limity při nutnosti dodržování právní regulace osobních údajů**?

Umělá inteligence v běžném životě

AI využíváme téměř každý den, aniž bychom si to uvědomovali. Vyhledáváme na internetu, přičemž vyhledávače se neustále učí podle toho, jaké údaje jsou do nich zadávány nejčastěji, a **automaticky vyhodnocují chování lidí na síti**. Stále častěji nakupujeme online a na základě našich předchozích nákupů jsou nám nabízena **personalizovaná doporučení ohledně produktů**, jež bychom si mohli zakoupit. Chytrý telefon má již téměř každý z nás – můžeme na něm využít nespočet aplikací, které **pomáhají se zvládáním každodenních úkolů**: překladač textu, aplikace pro korekturu gramatiky, virtuální asistenti, automatické vytváření videí či úprava fotografií, našeptávání při psaní zpráv, ale také personalizované reklamy. Rovněž automobily jsou dnes už vybaveny funkcemi využívajícími umělou inteligenci, ať už se jedná o automatizované senzory schopné detekovat nebezpečné situace, o takzvané autopiloty nebo o zabudované navigace.

Asi nejvíce diskutovaným systémem umělé inteligence je potom v dnešní době ChatGPT (Generative Pre-trained Transformer) spuštěný firmou OpenAI v listopadu 2022. Jedná se o chatbot neboli **počítačový program určený k automatizované komunikaci** s lidmi, který je schopen samostatně diskutovat v podstatě na libovolné téma a disponuje širokou zásobou znalostí.

14 Whistleblowing a ochrana oznamovatelů v praxi

14.1 Whistleblowing podle českého zákona o ochraně oznamovatelů

Dne 1. srpna 2023 nabyl účinnosti zákon č. 171/2023 Sb., o ochraně oznamovatelů (dále jen „zákon o ochraně oznamovatelů" nebo „zákon"), a zákon č. 172/2023 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o ochraně oznamovatelů (dále jen „změnový zákon"). Zákon transponuje do českého právního řádu **evropskou legislativu na ochranu a podporu oznamovatelů** protiprávního jednání, především pak její klíčové aspekty týkající se oznamování protiprávních jednání v pracovním prostředí.

Co znamená whistleblowing

Hlavním účelem této nové legislativy o takzvaném whistleblowingu **je poskytnout ochranu oznamovatelům** (whistleblowerům), tedy osobám, které se staly svědky, zjistily anebo jsou si vědomy protiprávního jednání v organizaci a rozhodnou se tuto skutečnost oznámit. Zákon pokrývá **různé formy protiprávního jednání** (včetně trestných činů, přestupků a jiných porušení právních předpisů), **upravuje mechanismy** pro jejich řádné hlášení a řešení, **definuje role**, jež jsou za příjem oznámení a jejich prověřování odpovědné, a především vymezuje **odvetná opatření**, před kterými jsou oznamovatelé chráněni.

Praktický příklad

Pojem whistleblowing (též whistle-blowing nebo whistle blowing, z anglického „to blow a whistle", doslova „zapískat na píšťalku") označuje situace, kdy stávající nebo bývalý zaměstnanec nějaké organizace nebo osoba v obdobném postavení, takzvaný whistleblower („ten, kdo píská na píšťalku"), upozorní v dobré víře či nezištně organizaci, orgán dozoru či dohledu nebo jinou instituci oprávněnou k prověření či postihu protiprávního jednání nebo k zakročení proti němu na nelegitimní, neetické nebo nezákonné praktiky na pracovišti, které se dějí se souhlasem či z nedbalosti jeho nadřízených a jdou proti veřejnému zájmu či ohrožují veřejnost. Jde o termín z 19. století, v aktuálním významu poprvé užitý na počátku 70. let 20. století americkým politickým a občanským aktivistou Ralphem Naderem a definovaný M. P. Micelim a J. P. Nearem v roce 1985 (viz *Organizational Dissidence: The Case of Whistle-Blowing, Journal of Business Ethics 4*).

Následující úvod do problematiky whistleblowingu má za cíl **poskytnout základní přehled o nové legislativě** a nastínit hlavní pojmy a témata, která budou dále rozpracována v navazujících kapitolách o rozhraní mezi whistleblowingem a ochranou osobních údajů (14.2) a o praktických krocích, jak zvládnout vytvoření a nastavení odpovídajícího systému pro příjem a vyšetřování oznámení (14.3).

Transpozice evropské směrnice

Zákon o ochraně oznamovatelů a související změnový zákon **transponují do českého právního řádu směrnici** Evropského parlamentu a Rady (EU)

14.2 Právní úprava whistleblowingu vs. ochrana osobních údajů

Zákon o ochraně oznamovatelů je nezbytné **aplikovat i v kontextu jiných právních norem** týkajících se ochrany údajů požívajících právní ochrany dle zvláštních právních předpisů. Takovými právními předpisy jsou zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 (dále jen „GDPR") a zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon o zpracování osobních údajů").

Následující kapitola nejdříve představí osoby, jejichž osobní údaje jsou v rámci fungování oznamovacího systému zpracovávány (dále jen „subjekty údajů"), a **osoby, které tyto údaje spravují a zpracovávají**. Pozornost bude věnována také otázce **zákonnosti zpracování osobních údajů** v rámci vnitřního oznamovacího systému, která má bezprostřední vliv na rozsah a možnosti uplatnění práv subjektů údajů. Poté následují praktické aspekty povinností příslušné osoby při:

- přijetí osobních údajů;
- zabezpečování osobních údajů;
- sdílení osobních údajů s třetími osobami;
- vyřizování žádostí subjektů údajů o uplatnění práv vyplývajících z GDPR.

Subjekty údajů zpracovávaných v rámci oznamovacího systému

V rámci fungování oznamovacího systému může docházet ke zpracovávání osobních údajů zejména

14.3 Implementace whistleblowingu do organizace v praxi

Příprava na tvorbu vnitřních řídicích dokumentů

Prvním krokem v rámci přípravy řídicích dokumentů v oblasti ochrany oznamovatelů je **definování konkrétního nastavení systému** pro řešení oznámení. Organizace si primárně musí **určit šíři záběru svého oznamovacího systému**.

Praktický tip

- Lze řešit pouze zákonné minimum, tedy porušení právních předpisů dle § 2 odst. 1 zákona o ochraně oznamovatelů (trestné činy, přestupky s horní hranicí sazby pokuty alespoň 100 tisíc korun, porušení zákona o ochraně oznamovatelů, porušení v definovaných oblastech práva Evropské unie).
- Záběr lze ale rozšířit také na porušení dalších předpisů, například vnitřních předpisů organizace (například etického kodexu) – to doporučujeme pro posílení právní jistoty organizací.
- Dále lze nastavit i okruh osob oprávněných podávat oznámení – vedle zaměstnanců a dalších osob vykonávajících činnost pro organizaci ve smyslu § 2 odst. 3 a 4 zákona o ochraně oznamovatelů lze umožnit podávání oznámení také dalším osobám, například zákazníkům – to však spíše nedoporučujeme (pro řešení podnětů a stížností od zákazníků efektivněji slouží jiné postupy, například reklamační řízení).

Organizace si dále musí **ověřit, které předpisy budou dopadat na její oznamovací systém**. Vedle