ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 2 | leden 2021

Jak na reaudit

Jak jste si minulý rok vedli v ochraně osobních údajů? Nejde jen o řečnickou otázku, ale také o jednu z povinností dle GDPR – provést reaudit. Jak postupovat, aby vám nic neuniklo? Co všechno reaudit zahrnuje a jak by měla vypadat výsledná auditní zpráva?

Nový rok s sebou vždy přináší změny, ale něco zůstává stejné – zejména povinnosti dle GDPR. Uplynulý rok zásadně změnil náš přístup k interním procesům, **začali jsme pracovat více na dálku a narychlo upravovali své produkty a služby**, aby v této nelehké době obstály. Nebudeme si lhát, že jsme přitom vždy pamatovali na ochranu osobních údajů. Zkrátka to nebylo prioritou.

Tak či tak začíná nový rok a ten s sebou většinou nese **povinnost implicitně vycházející z GDPR**, ale často explicitně zachycenou v interní dokumentaci (zejména v interní směrnici a posouzení vlivu) – **provést reaudit**. V tomto článku se tedy podíváme na to, **jak takový reaudit provést a co by mělo být jeho cílem**.

K čemu bychom měli směřovat?

Ve skutečnosti se reaudit od prvotního auditu zas tak neliší. Ani pro jedno nejsou nikde psaná pravidla, ale postupy jsou víceméně stejné. Cílem je zjistit, **zda naše organizace splňuje podmínky GDPR, nebo jsou naopak někde mezery**, které je nutno vyplnit.

Dlužno dodat, že samo **provedení auditu by mělo mít v závěru určitou formu**, aby bylo možno prokázat, že taková „sebekontrola“ ze strany správce byla vůbec provedena. Jelikož je téma reauditu abstraktní, těžkopádné a obecně nic neříkající, držme se tedy toho, že **výstupem naší činnosti by měla být auditní zpráva** se závěry z reauditu. Do samotné auditní zprávy bychom měli zejména **zaznamenat naše zjištění a návrhy na jejich odstranění**.

Na co se zaměřit?

Teď už víme, že se od nás očekává **sepsání dokumentu, v němž shrneme výstupy z kontroly**. Co ale kontrolovat? Můžeme to rozdělit do několika oblastí, které nám pomohou položit si ty správné otázky a pídit se po správných odpovědích.

Kontrola úplnosti – zjištění skutkového stavu

Nejprve bychom měli provést kontrolu úplnosti – tedy **zjistit, že v mezičase nepřibyla žádná operace zpracování**, žádný nový zpracovatel, žádný důvod výmazu a podobně, který by nebyl zanesen v naší dokumentaci – zejména v záznamech o činnostech zpracování.

Postup by měl být takový, že **projdeme záznamy o činnostech zpracování s odpovědnými osobami** a zkontrolujeme, zda vše sedí. Zároveň nás čeká trochu detektivní práce, abychom odhalili, co z toho všeho, co společnost dělá, se do dokumentace nepropsalo. Je tedy na nás, abychom **pokládali správné dotazy odpovědným osobám**, neboť otázkou, „jaké nové operace zpracování přibyly od minula", se pravděpodobně nikam neposuneme. Každý k tomu může přistoupit různými způsoby, přičemž úrovni detailnosti se meze nekladou.

Skvělým tipem je například **vyžádat si seznam uzavřených smluv s dodavateli za uplynulý rok**. Díky tomu zjistíme, jaké nové služby byly poptány a proč. To nás pak může navést na stopu novým či jinak pojatým operacím zpracování. To vše bychom měli ideálně rovnou **poznačit do nových záznamů o činnostech zpracování** v režimu sledování změn. Jakmile zjistíme celý skutkový stav, můžeme přistoupit k tzv. právnímu auditu.

Právní audit – ověření správnosti

Jakmile máme zjištěný skutkový stav (a zda je správně zanesen do dokumentace jako záznamy o činnostech zpracování), máme takzvaná tvrdá data, u kterých bychom měli **ověřit, zda splňujeme všechny podmínky GDPR k daným operacím**.

Tuto etapu můžeme taktéž rozdělit na dvě další části. Za prvé bychom měli zjistit, **jak se vše propsalo do užívané dokumentace**. Měli bychom si vytvořit checklist přímo pro naši organizaci a **ve vztahu k jednotlivým operacím zpracování například zkontrolovat**, že:

- o všech účelech byly subjekty údajů informovány;
- se všemi zpracovateli je uzavřena zpracovatelská smlouva;
- kde je oprávněný zájem, disponujeme posouzením takového oprávněného zájmu a podobně.

Dokumentaci je třeba posuzovat podle aktuální vodítek, samotný text GDPR nestačí

Díky kontrole úplnosti dokumentace zjistíme ta nejzávažnější porušení GDPR, která můžeme ihned zaznamenat do naší pracovní verze auditní zprávy – tím však náš právní audit nekončí. Teď si musíme vyhrnout rukávy a pustit se do posouzení, **zda je naše dokumentace právně úplná a bezvadná**. Pokud pravidelně čtete náš Zpravodaj, určitě vám neušlo, kolik nových vodítek, pokynů, stanovisek, rozhodovací praxe a doktrinálních názorů bylo jen v minulém roce vydáno. Máme zde **vodítka ke zpracovatelské smlouvě, způsobu získávání souhlasu, informování** a podobně.

Abychom mohli zkontrolovat, zda je skutkový stav v souladu s legislativou, musíme nejprve vědět, jaké jsou požadavky legislativy – **to bohužel nevyčteme ze samotného textu GDPR nebo z dvou let starých publikací**, jakkoliv jsou stále velmi dobré. Naše kroky by tedy měly nyní spočívat v tom, abychom **načerpali aktuální pohled na jednotlivé požadavky GDPR** a aktualizovali si svůj právní názor. Pro ty, kdo čtou naše články a aktuality, by to měla být ve skutečnosti hračka.

Nyní musíme zkontrolovat, že **máme správně nastaveny účely, právní tituly, že zpracovatelské smlouvy**

obsahují, co mají, a že je vše v pořádku. Pokud zjistíme, že je někde chyba, zaznamenáme to do závěrečné zprávy.

Bezpečnostní audit

Poslední fáze reauditu může patřit k těm nejzábavnějším, tedy pokud vše funguje, jak má. Součástí vyhodnocení stavu GDPR v naší organizaci je také ověření, že zásada důvěrnosti a integrity je bez dalšího plně dodržována. Naším úkolem je tak ověřit, **zda jsou stanovená bezpečnostní opatření přiléhavá a také jestli jsou dodržována**. Jeden z klientů například pravidelně zkouší do e-mailu přikládat různé odkazy či soubory a zpovzdálí počítá, kolik zaměstnanců na odkaz či soubor klikne. To je totiž z důvodu ochrany před phishingovými útoky v dané organizaci zakázáno v bezpečnostní směrnici a klient tak ověřuje, nakolik to zaměstnanci dodržují.

V této fázi může být přínosné zapojit do ověření třetí nestrannou osobu, která v tomto oboru podniká. Na druhou stranu se často u svých klientů setkávám s různými **nabídkami „povinných" penetračních testů od třetích osob**, které klient musí udělat, jinak „má zavařeno na průšvih". Pohlídejte si náklady, a pokud nepatříte mezi organizace, jež vyvíjejí vlastní software, popřípadě takový software používají, pravděpodobně to nebude nezbytně nutné a jednalo by se o zbytečný náklad. Stále platí to, co na začátku – **utopit peníze v zajištění bezpečnosti je extrémně jednoduché, ne vždy však účelné**.

Co po provedené kontrole?

Po provedené kontrole by vám měl v ruce zůstat dokument, který obsahuje veškerá zjištění, co je špatně. Naším úkolem je teď, abychom odůvodnili, proč je to špatně, a **ke každému zjištění přidali naše hodnocení, o jak moc velké riziko se jedná**. Klíč k tomu je jednoduchý: čím větší riziko pro subjekt údajů, tím vyšší priorita problému, kterým by se měl správce zabývat. Po uvedení rizikovosti bychom měli následně **připojit náš návrh k odstranění rizika** – tedy jednoduchý návod, co by měl správce udělat, aby byl v souladu s GDPR.

Poslední rada může znít trochu zvláštně, nicméně je nutno si připomenout, že naše úkoly, jakožto pověřenců pro ochranu osobních údajů, jsou spíše poradního a kontrolního charakteru, neboť **za zpracování osobních údajů zodpovídá správce – naším úkolem je ho „pouze" kontrolovat**. Pokud bychom zjištěné chyby začali rovnou sami napravovat, dostali bychom se do střetu zájmů.

Na co dále myslet

Provádět reaudit je naší povinností a měli bychom u toho být obzvláště pečliví. Je výše uvedený návod vyčerpávající? Určitě ne, **v rámci reauditu bychom měli například prověřit i své zpracovatele** (máme u nich právo auditu a v některých případech se naše právo může překlopit do povinnosti). Cílem tohoto článku je poskytnout vodítka k tomu, jak k dané problematice přistupovat. ▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti IT
www.josefbatrla.cz

Ze života pověřence: Podělte se s námi o své zkušenosti!

- Obrátil se na vás jako na pověřence někdo s kuriózním dotazem?
- Byli jste svědkem humorné situace týkající se GDPR?
- Zažili jste jako pověřenci situaci, o kterou byste se s námi chtěli podělit?

Napište nám na zpravodaj.poverenec@forum-media.cz do pondělí 25. 1.

Vaše podněty zpracujeme do mimořádného čísla ke Dni ochrany osobních údajů. Zaručujeme vám zachování anonymity.

Pokuty za **spamy v datovce**

Úřad pro ochranu osobních údajů udělil vysoké pokuty hned několika společnostem, které zneužily bezplatné zasílání poštovních datových zpráv k šíření nevyžádaných obchodních sdělení. Celková výše pokut přesáhla tři miliony korun. Co se Úřadu nelíbilo?

Úřad pro ochranu osobních údajů udělil pokutu jedenácti společnostem **za zneužití osobních údajů k šíření nevyžádaných obchodních sdělení**, která byla zaslána jako poštovní datové zprávy. Úřad uložil předmětným společnostem **pokuty v celkové výši 3 111 000 korun**.

Poštovní datové zprávy zdarma

Od 2. listopadu 2020 až do konce nouzového stavu je na základě usnesení vlády ze dne 30. října 2020 č. 1110 (publikovaného pod č. 441/2020 Sb.) **možné využívat datové schránky kompletně zdarma**. Umožit posílání poštovních datových zpráv zdarma je jedním z krizových opatření, jehož cílem je omezit šíření koronaviru. Usnadnění elektronického styk u občanů i státní správy navzájem má vést k omezení návštěv úřadů občany.

Pokuty uložené ministerstvem vnitra

Ministerstvo vnitra uložilo podle ustanovení § 26a a 26b zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, pokuty již na jaře minulého roku. Celkem **dvaceti pachatelům byly ministerstvem uděleny pokuty** za přestupek rozesílání nevyžádaných obchodních či jiných obtěžujících sdělení prostřednictvím poštovních datových zpráv, které bylo v té době rovněž možné rozesílat zdarma. Ministerstvo vnitra **udělilo pokuty v celkové výši 4,5 milionu korun**.

Varování ÚOOÚ

Úřad pro ochranu osobních údajů pak v polovině listopadu 2020 **varoval před využíváním poštovních datových zpráv pro odesílání nevyžádaných obchodních sdělení**. Předseda ÚOOÚ Jiří Kaucký k dané otázce uvedl následující: *„Zprávy odeslané prostřednictvím datových schránek mají sloužit pro standardní bezpečnou písemnou korespondenci. Jde o upřednostňovanou komunikaci uvnitř orgánů veřejné moci a mezi soukromými osobami a orgány veřejné moci navzájem. Jakékoli zneužívání datových schránek je proto špatné, ale v době nouzového stavu jde, při zneužití výjimečné bezplatnosti této služby, o nepřípustný hyenismus.“*

Pokuty za tři miliony

Úřad pro ochranu osobních údajů zahájil na základě desítek stížností držitelů datových schránek správní řízení s celkem jedenácti společnostmi, které **zneužily možnost zasílání poštovních datových zpráv zdarma**. Dle vyjádření úřadu předmětné společnosti *„… zpracovávaly tisíce adres datových schránek fyzických osob a související osobní údaje pro rozesílání nejrůznějších nabídek zboží a služeb prostřednictvím systému datových schránek, a to aniž by tomu předcházel například zákaznický či jiný obdobný vztah, který by z pohledu nařízení (EU) 2016/679 zakládal možnost zasílání sdělení tohoto typu z titulu oprávněného zájmu. Společnosti nedisponovaly ani jiným právním důvodem pro odesílání nabídek zboží a služeb. Došlo tak k porušení článku 6 odst. 1 nařízení (EU) 2016/679.“* Celé vyjádření si můžete přečíst **zde**.

Za uvedená porušení uložil Úřad pro ochranu osobních údajů nepravomocně pokutu v souhrnné výši 3 111 000 korun. Je však nutné poznamenat, že **uvedeným není dotčeno oprávnění ministerstva vnitra** k uložení pokuty za přestupek zneužití poštovních datových zpráv k nevyžádaným a potenciálně nebezpečným spamům podle ustanovení § 26a a 26b zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. ▪▪▪

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

Předávání osobních údajů do VB po brexitu – co se změní?

Je Spojené království považováno z pohledu předávání osobních údajů za třetí zemi? Změnila se po brexitu pravidla pro předávání osobních údajů? Jak má postupovat česká společnost zasílající osobní údaje britským obchodním partnerům? A co když její poskytovatel cloudového řešení sídlí ve Spojeném království?

Je Spojené království považováno od 1. ledna 2021 z pohledu předávání osobních údajů za třetí zemi?

Nikoliv. Evropská unie a Spojené království se v rámci dohody o budoucích vztazích, uzavřené dne 24. prosince 2020, dohodly, že od začátku roku 2021 po přechodnou dobu maximálně šesti měsíců zůstane ve Spojeném království v platnosti režim GDPR.

Změní se od 1. ledna 2021 pravidla pro předávání osobních údajů do Spojeného království?

Nikoliv. Pro předávání osobních údajů od Nového roku po dobu maximálně šesti měsíců zůstává v platnosti dosavadní právní úprava. V tomto období tedy bude možné předávat osobní údaje do Spojeného království jako doposud. Správci osobních údajů, případně zpracovatelé, kteří po Novém roce chtějí předávat osobní údaje do Spojeného království, tak mohou minimálně po dobu šesti měsíců činit za stávajících podmínek. Je přitom jedno, zda se jedná o dceřinou společnost britského holdingu sídlící v České republice, která pravidelně zasílá osobní údaje zaměstnanců mateřské společnosti sídlící ve Spojeném království, českou společnost zasílající osobní údaje britským obchodním partnerům či slovenskou společnost, jejíž poskytovatel webu nebo cloudového řešení sídlí ve Spojeném království. Minimálně po dobu šesti měsíců se pravidla pro předávání osobních údajů do Spojeného království nemění.

Změní se od 1. července 2021 pravidla pro předávání osobních údajů do Spojeného království?

Zatím není zřejmé. Od 1. července 2021 bude Spojené království považováno z pohledu předávání osobních údajů za třetí zemi. Pokud však Evropská komise do té doby vydá rozhodnutí o odpovídající úrovni ochrany osobních údajů umožňující obecně jejich transfer do Spojeného království, bude Spojené království považováno z pohledu předávání osobních údajů za takzvanou bezpečnou třetí zemi (neboli třetí zemi s dostatečnou úrovní ochrany osobních údajů).

Za bezpečné třetí země, tedy za země zajišťující odpovídající úroveň ochrany osobních údajů, je podle čl. 45 odst. 1 GDPR možné považovat jenom ty země, které disponují platným rozhodnutím Evropské komise o odpovídající úrovni ochrany osobních údajů. Třetí země s dostatečnou úrovní ochrany osobních údajů jsou z tohoto hlediska prakticky na úrovni členských států Evropské unie, respektive Evropského hospodářského prostoru. Předání osobních údajů do těchto zemí nevyžaduje ze strany předávajícího správce osobních údajů, případně zpracovatele, přijetí žádných dodatečných opatření.

Pokud Evropská komise do té doby nevydá rozhodnutí o odpovídající úrovni ochrany osobních údajů umožňující obecně jejich transfer do Spojeného království, bude Spojené království považováno z pohledu předávání osobních údajů za třetí zemi s nedostatečnou úrovní ochrany osobních údajů.

Bude Spojené království považováno od 1. července 2021 z pohledu předávání osobních údajů za třetí zemi?

Ano. Od 1. července 2021 bude Spojené království považováno z pohledu předávání osobních údajů za třetí zemi.

Jak postupovat, pokud Evropská komise vydá rozhodnutí o odpovídající úrovni ochrany osobních údajů?

Nic se nemění. V případě, že Evropská komise vydá rozhodnutí o odpovídající úrovni ochrany osobních údajů, nebude předání osobních údajů do Spojeného království vyžadovat ze strany předávajícího správce osobních údajů, případně zpracovatele, přijetí žádných dodatečných opatření. Předávat osobní údaje do Spojeného království bude možné provádět za stávajících podmínek.

Jak postupovat, pokud Evropská komise nevydá rozhodnutí o odpovídající úrovni ochrany osobních údajů?

V případě, že Evropská komise nevydá rozhodnutí o odpovídající úrovni ochrany osobních údajů, budou muset správci osobních údajů, případně zpracovatelé, kteří chtějí předávat osobní údaje do Spojeného království, využít některý z nástrojů umožňujících předávání osobních údajů do třetích zemí, které nejsou považovány za bezpečné, tedy například závazná vnitropodniková pravidla (Binding Corporate Rules), standardní smluvní doložky (Standard Contractual Clauses) nebo schválený kodex chování podle čl. 40 GDPR spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů. Bližší informace o předávání osobních údajů založeném na vhodných zárukách je možné nalézt v čl. 46 GDPR. Volba nejvhodnějšího nástroje bude záležet na konkrétní situaci.

Jak má od 1. 7. 2021 postupovat česká společnost zasílající osobní údaje britským obchodním partnerům?

Česká společnost může v takové situaci využít institut standardních smluvních doložek, který je jedním z nástrojů pro vytvoření vhodných záruk ochrany osobních údajů ve třetí zemi s nedostatečnou úrovní ochrany osobních údajů. Jedná se o vzorový text smlouvy mezi správcem osobních údajů, který hodlá předat osobní údaje do třetí země s nedostatečnou úrovní ochrany osobních údajů, a příjemcem osobních údajů v této třetí zemi.

Smluvní vztah, který ošetří předání osobních údajů českou společností britskému obchodnímu partnerovi, musí zahrnovat jak výše uvedené standardní smluvní doložky, tak i zpracovatelskou smlouvu se všemi náležitostmi vyžadovanými příslušnými ustanoveními GDPR. Může jít přitom buď o dva oddělené smluvní dokumenty, nebo o jeden integrovaný smluvní dokument. V současné době se připravuje nové znění standardních smluvních doložek, o jehož návrhu jsme psali v minulém **čísle**.

Jak má od 1. 7. 2021 postupovat česká společnost, jejíž poskytovatel webu nebo cloudového řešení sídlí ve Spojeném království?

Kromě výše popsaného institutu standardních smluvních doložek může v této situaci přicházet v úvahu i využití institutu závazných vnitropodnikových pravidel pro zpracovatele (Binding Corporate Rules for Processors neboli BCR-P). Tento druh závazných vnitropodnikových pravidel je určen pro velké nadnárodní zpracovatele osobních údajů, typicky například pro poskytovatele cloudových služeb, kteří provádějí zpracování osobních údajů pro velké množství správců osobních údajů.

Pracovní skupina WP29 shrnula požadavky kladené čl. 47 GDPR na závazná vnitropodniková pravidla pro zpracovatele do pracovního dokumentu, kterým se zavádí tabulka s prvky a zásadami nacházejícími se v závazných podnikových pravidlech pro zpracovatele (WP257). Dokument si můžete přečíst **zde**.

Závazná vnitropodniková pravidla pro zpracovatele podléhají schválení. Formulář žádosti a přehled informací, které musí žádost o schválení závazných vnitropodnikových pravidel pro zpracovatele obsahovat, jsou uvedeny v dokumentu Standardní žádost o schválení závazných podnikových pravidel předávání osobních údajů pro zpracovatele (WP265), který je dostupný **zde**.

Závazná vnitropodniková pravidla pro zpracovatele by měla být přiložena ke zpracovatelské smlouvě, která musí splňovat veškeré náležitosti vyžadované příslušnými ustanoveními GDPR. V případě popsaném v otázce je však iniciativa spíše na straně poskytovatele webu či cloudového řešení. Pokud nedojde ke schválení závazných vnitropodnikových pravidel pro zpracovatele, bude se muset česká společnost poohlédnout po jiném zpracovateli (tedy zpracovateli sídlícím v EU či třetí zemi s dostatečnou úrovní ochrany osobních údajů nebo po zpracovateli se schválenými závaznými vnitropodnikovými pravidly pro zpracovatele), nebo využít institut standardních smluvních doložek.

Jak to je od 1. ledna 2021 s takzvaným mechanismem jediného kontaktního místa?

Na mechanismus jediného kontaktního místa se nevztahuje žádné přechodné období. Správci osobních údajů a zpracovatelé usazení pouze ve Spojeném království a podléhající GDPR ve smyslu jeho čl. 3 odst. 2 (tedy zpracovávající osobní údaje subjektů údajů, které se nacházejí v EU) budou muset podle čl. 27 GDPR jmenovat svého zástupce v EU. Zástupce musí být správcem osobních údajů nebo zpracovatelem zmocněn v tom smyslu, že se na něj vedle správce nebo zpracovatele či místo nich mohou obracet zejména dozorové úřady a subjekty údajů ohledně všech otázek souvisejících se zpracováním osobních údajů za účelem zajištění souladu s GDPR.

Jak má od 1. 7. 2021 postupovat dceřiná společnost britského holdingu sídlící v České republice, která pravidelně zasílá osobní údaje zaměstnanců mateřské společnosti sídlící ve Spojeném království?

Kromě výše popsaného institutu standardních smluvních doložek může v takové situaci přicházet v úvahu i využití institutu závazných vnitropodnikových pravidel. Jedná se o nástroj pro vytvoření vhodných záruk ochrany osobních údajů ve třetí zemi s nedostatečnou úrovní ochrany osobních údajů, vhodný zejména pro skupiny podniků nebo uskupení podniků vykonávající společnou hospodářskou činnost. Závazná podniková pravidla jsou tudíž ideálním nástrojem pro přeshraniční předávání osobních údajů v rámci velkých nadnárodních korporací. Tento druh závazných vnitropodnikových pravidel bývá označován jako závazná vnitropodniková pravidla pro správce (Binding Corporate Rules for Controllers neboli BCR-C).

Pracovní skupina WP29 (dnes Evropský sbor pro ochranu osobních údajů) shrnula požadavky kladené čl. 47 GDPR na závazná vnitropodniková pravidla pro správce do pracovního dokumentu, kterým se zavádí tabulka s prvky a zásadami nacházejícími se v závazných podnikových pravidlech (WP256). Dokument si můžete přečíst **zde**.

Závazná vnitropodniková pravidla podléhají schválení vedoucího dozorového úřadu pro závazná podniková pravidla (takzvaný BCR Lead). Závazná podniková pravidla tedy není nutné předložit ke schválení dozorovému úřadu v každé členské zemi EU zvlášť. Schvalovací procedura se spouští v okamžiku, kdy skupina podniků, která se je rozhodla přijmout, podá u vedoucího dozorového úřadu pro závazná podniková pravidla žádost o jejich schválení. Formulář a přehled informací, které musí daná žádost obsahovat, jsou uvedeny v dokumentu Standardní žádost o schválení závazných podnikových pravidel předávání osobních údajů pro správce (WP264), který je dostupný **zde**.

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

Poradna

JOSEF BÁTRLA ADVOKÁT

Je třeba ve vztahu k žákům a škole někde vyžadovat informovaný souhlas zákonných zástupců? Tedy je nějaké zpracování povoleno pouze na základě informovaného souhlasu rodičů, nebo je k něčemu vysloveně vyžadován a měli bychom jej od rodičů mít?

V současné době máme souhlas k:

- **evidenci úrazů,**
- **nahlížení do zdravotní dokumentace (jsme škola pro žáky s kombinovaným postižením),**
- **pořizování audiovizuálních záznamů a fotografií,**
- **zpracování OÚ v rámci školní matriky,**
- **objednávky stravy,**
- **hrazení školného a svozové dopravy,**
- **poskytování OÚ v ubytovacím zařízení (při školních výletech).**

Informovaný souhlas nám ukládá zákon a vyhláška pouze v případě doporučení školského poradenského zařízení a zajímá nás, zda je třeba zajišťovat informovaný souhlas ještě k některým dalším operacím v rámci GDPR.

Zpracování osobních údajů v rámci školství je určitě kapitolou samo o sobě, nicméně vykazuje velmi podobné znaky, jako zpracování osobních údajů na pracovišti. Společným jmenovatelem obojího je pravidlo, že souhlas se zpracováním osobních údajů by neměl být nadužívaný, byť u každého oboru je to trochu z jiných důvodů. Příčinou, proč bychom se měli se souhlasem v rámci školství potkávat co nejméně, je právě sama podstata souhlasu, který musí být vždy svobodný a vždy odvolatelný, aniž by to mělo následky pro subjekt údajů – v tomto případě pro žáka (potažmo jeho rodiče).

Zkuste se vrátit k vámi uvedeným příkladům a odpovědět si na otázku – pokud je tato operace zpracování založena na základě souhlasu, jaký následek pro žáka, školu či rodiče by mělo, pokud by byl tento souhlas odvolán? Pro tyto případy vydalo Ministerstvo školství, mládeže a tělovýchovy Metodickou pomůcku k aplikaci obecného nařízení o ochraně osobních údajů (GDPR), kde na 88 stránkách nalezneme metodické pokyny, jak ke zpracování osobních údajů přistupovat.

Kupříkladu ve vztahu k pořizování fotografií MŠMT uvádí totéž, co ÚOOÚ, tedy že v takovém případě se může dost často jednat o nadužívání souhlasu. Taktéž si lze těžko představit situaci, že by uprostřed školy v přírodě došlo k odvolání souhlasu pro poskytování OÚ v ubytovacích zařízeních. Ještě hůře představitelným je postup v případě odvolání souhlasu s evidencí úrazů, popřípadě v rámci školní matriky – oboje totiž MŠMT uvádí ve své metodice jako příklad, kdy souhlas není třeba (viz například strana 27 metodiky).

S ohledem na skutečnost, že zvolení špatného právního titulu (a tedy nadužívání souhlasu) má za následek porušení zásady transparentnosti, doporučuji projít zmíněnou metodiku a zkontrolovat, zda nejdete proti praxi, kterou se snaží MŠMT zavést.

Exekutor v rámci žádosti o poskytnutí součinnosti žádá o sdělení rodného čísla zaměstnance, dále o jeho e-mail a telefonní číslo. Měl by mu zaměstnavatel tyto informace poskytnout?

Jak jsme již jednou v rámci naší poradny řešili, poskytování součinnosti exekutorovi je naší povinností, které se nemůžeme jednoduše zříci. I nyní stále panuje v praxi rozkol, jak je možno na jednotlivé žádosti o poskytnutí informace reagovat a kde jsou mantinely toho, co by měl exekutor zjišťovat sám od povinného (v tomto případě vašeho zaměstnance), nebo co si může zjistit právě dotazem na zaměstnavatele.

Z předchozí odpovědi na toto téma víme, že si úplně nemůžeme dovolit poskytnout součinnost jen tak (viz Nález II. ÚS 456/14) a že v případě, že zaměstnavatel má dané údaje u sebe a nemusí si hrát na detektiva, tedy zjišťovat dané údaje za exekutora sám – měl by žádosti vyhovět.

Sečteno podtrženo, ze zákona má zaměstnavatel povinnost poskytnout exekutorovi součinnost (viz § 33 exekučního řádu, respektive § 128 občanského soudního řádu), přičemž poskytnutí výše zmíněných informací nelze vnímat jako excesivní. Na základě nezbytnosti pro splnění právní povinnosti by zaměstnavatel měl výše uvedené informace o povinném exekutorovi sdělit, přičemž z pohledu GDPR můžeme těžko hovořit o nezákonnosti takového zpracování.

Je možné využít v rámci pracoviště živé vysílání? A jak to případně formálně ošetřit? Pro zrychlení expedice bychom chtěli do oddělení logistiky instalovat monitor s trvalým živým přenosem z našeho oddělení expedice, aby měli logistici neustálý přehled o tom, co se právě nakládá. Standardně je naše společnost vybavena kamerovým systémem, platí pro živé vysílání stejná pravidla?

Kamerový systém a zpracování osobních údajů jde ruku v ruce, ale jen pokud se skutečně prostřednictvím kamerového systému zpracovávají osobní údaje. Tak tomu však nebývá v situacích, kdy kamerový systém nepořizuje záznam. V takovém případě se totiž neukládá ani podobizna osob (nebo jiných osobních údajů jako registrační značka vozidel), tudíž nelze mluvit o zpracování osobních údajů.

To však neznamená, že se tak nemůže stát nebo že bychom mohli takový kamerový systém nainstalovat všude s odůvodněním, že se nejedná o zpracování osobních údajů. Co se týče prvního případu, pokud nebude mít kamerový systém odpovídající zabezpečení a předmětný „stream" z kamer bude „unikat" ven, můžete se jednoduše dostat do pozice správce osobních údajů (ačkoliv o tom ani nemusíte vědět). Pokud vám to přijde absurdní – podívejte se na tuto stránku, kde můžete vidět stream nejen z průmyslových kamer, ale i domácích IP kamer nebo kamer z chůviček (viz **zde**).

Co se týče druhé připomínky – ačkoliv na vaši situaci GDPR nemusí dopadnout, stále platí ochrana soukromí osob podle občanského zákoníku a taktéž ochrana před sledováním zaměstnanců podle zákoníku práce. K těmto tématům doporučuji článek Skrytá kamera na pracovišti z dubnového čísla Zpravodaje, který si můžete přečíst **zde**.

▪▪▪

Nevíte si s něčím rady? Pošlete nám svůj dotaz a my vám zprostředkujeme odpověď! Dotazy pokládejte e-mailem na:
zpravodaj.poverenec@forum-media.cz

V příštím čísle Zpravodaje se dozvíte:
- **Jak napsat oznámení o ochraně osobních údajů**
- **Jsou trestné body za dopravní přestupky osobními údaji?**

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM, s. r. o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Editorka: Anna Pěkná | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 Jazyková redakce: Bc. Vendula Pazderová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2 490 Kč bez DPH Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 14. 1. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.