GDPR desatero: Doporučení k ochraně osobních údajů na ČVUT

Tento dokument shrnuje hlavní informace a zásady k ochraně osobních údajů, které by měl znát a dodržovat každý zaměstnanec univerzity.

Obsah:

1. Principy a základní informace k ochraně OÚ

Základním dokumentem upravujícím ochranu osobních údajů[1] je Evropské nařízení GDPR[2]. Na univerzitní úrovni je to Příkaz rektora č. 04/2018 k ochraně a zpracování osobních údajů na ČVUT (dále jen Příkaz). Tyto dokumenty stanovují základní pojmy, zásady[3] a postupy při nakládání s osobními údaji, kterými je povinen se řídit každý zaměstnanec, student a spolupracovník univerzity. Základním principem ochrany osobních údajů je *prevence*, předejití možného zásahu do práv těch, kterých se osobní údaje týkají.

2. Pověřenec pro ochranu osobních údajů

Na univerzitě je ustanovena funkce *pověřence pro ochranu osobních údajů*, který dohlíží na celý systém ochrany osobních údajů na ČVUT. Pověřencem je Ing. Josef Svoboda, Ph.D.. Mimo jiné poskytuje informace a poradenství zaměstnancům a studentům provádějícím (nebo připravujícím) zpracování osobních údajů, monitoruje soulad všech činností zpracování OÚ s příslušnými právními předpisy a Příkazem ČVUT, komunikuje se subjekty údajů a s Úřadem na ochranu osobních údajů. Vydává stanovisko k činnostem zpracování OÚ na univerzitě.

Doporučujeme kontaktovat pověřence vždy, když máte nejasnosti nebo pochybnosti k vašim činnostem zpracování osobních údajů, a to na e-mailové adrese dpo@cvut.cz

---

[1] **Osobními údaji** jsou veškeré informace o identifikované nebo identifikovatelné žijící fyzické osobě (subjektu údajů).

[2] **Obecné nařízení o ochraně osobních údajů**, viz https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679

[3] **Zásady zpracování/ochrany OÚ**: Základním pojmem při zpracování osobních údajů je *účel zpracování*, tedy důvod, proč jsou údaje vůbec zpracovávány. Vzhledem k principu prevence je dovoleno zpracovávat jen ty osobní údaje, které jsou zcela nezbytné pro naplnění plánovaného účelu, a to opět jen takovým způsobem, který je vzhledem k danému účelu nezbytný. Osobní údaje je navíc možné uchovávat jen po nezbytně dlouhou dobu vzhledem k danému účelu zpracování, a když účel pomine, je třeba je smazat nebo anonymizovat. Není tedy možné uchovávat soubory s osobními údaji „jen tak pro jistotu“.

3. Ukládání dokumentů

Elektronické dokumenty obsahující osobní údaje je třeba ukládat do bezpečných úložišť[4] a zabezpečit je tak, aby bylo omezeno riziko jejich úniku a zneužití. Pokud jsou uchovány na pracovním počítači, musí být přístup k počítači zabezpečen heslem. Papírové agendy s rozsáhlejšími soubory osobních údajů (personalistika aj.) je třeba uchovávat v zabezpečených prostorách a uzamykatelných skříních. Zvýšenou pozornost je třeba věnovat dokumentům obsahujícím údaje vysoce osobní povahy[5] a osobním údajům týkajících se zranitelných skupin osob[6]; u těchto typů dokumentů či údajů doporučujeme zvážit vyšší stupeň zabezpečení (po domluvě s pověřencem a/nebo se správcem příslušného úložiště).

4. Elektronická komunikace

Elektronická komunikace (především e-mail, ale i další formy jako diskusní fóra aj.) představují z pohledu zabezpečení osobních údajů potenciálně rizikový kanál pro únik informací, takže je nezbytné věnovat pozornost tomu, které informace obsahující osobní údaje a v jaké formě je vhodné těmito kanály šířit. Pro komunikaci pracovní povahy je doporučeno používat výhradně jen komunikační nástroje a služby zajišťované univerzitou (nikoliv veřejné či komerční služby typu Gmail, Seznam apod.). Informace obsahující údaje vysoce osobní povahy doporučujeme předávat pouze v zabezpečené podobě (například šifrované nebo pseudonymizované[7]).

5. Foto a videodokumentace

Při pořizování foto/videodokumentace z akcí pořádaných univerzitou lze využít ustanovení občanského zákoníku o reportážním účelu, kdy není nutné žádat účastníky akce o souhlas s fotografováním/natáčením (pokud však některé osoba vyjádří individuální nesouhlas, je nutné ho respektovat). Tuto obrazovou dokumentaci lze dále uchovávat a využívat nekomerčním způsobem pro potřeby univerzity. U fotografií/videozáznamů, které mají portrétní charakter, je třeba zachovat při jejich využívání přiměřenou opatrnost, v zásadě bude třeba získat souhlas dané osoby (pokud nejde o záznam akademického funkcionáře při výkonu jeho funkce či zveřejnění fotografií přímo ve zpravodajském médiu, např. univerzitním časopise). Zvláštní pozornost je nutné věnovat pořizování a zveřejňování fotografií a videodokumentace nezletilých dětí, kdy je nutný souhlas zákonného zástupce. Oblast bude podrobněji upravena metodickým opatřením ČVUT.

6. Zveřejnění osobních údajů online (weby)

V článku 19 Příkazu jsou uvedeny podmínky, za kterých je možné zveřejnit online (na webu či jiným způsobem) vybrané osobní údaje zaměstnanců univerzity a osob působících v samosprávných akademických či poradních orgánech univerzity bez jejich souhlasu. Ve všech ostatních případech bude zveřejnění osobních údajů na webu podléhat předem udělenému souhlasu dotčených fyzických osob nebo jinému právnímu titulu pro zpracování (bod 9 níže).

---

[4] Za **bezpečná datová úložiště** lze považovat především úložiště poskytovaná ČVUT (uložiště VIC a IT oddělení fakult a součástí) a dále také úložiště sdružení CESNET a úložiště v rámci služby o365.cvut.cz.

[5] **Údaje vysoce osobní povahy** zahrnují jednak zvláštní kategorie osobních údajů (dříve označované termínem citlivé osobní údaje, jako jsou informace o rasovém či etnickém původu, politických názorech, náboženském vyznání, zdravotním stavu, sexuální orientaci aj. – viz čl. 16 Směrnice), jednak další typy osobních údajů, které mohou zvyšovat riziko pro práva a svobody subjektu údajů (jako například finanční údaje, které by mohly vést k podvodům s platbami, lokalizační údaje, jejichž shromažďování zpochybňuje svobodu pohybu apod.)

[6] **Zranitelné skupiny osob** představují skupiny, pro které může být obtížnější vykonávat či hájit svá práva, jako například nezletilé děti, osoby s duševní poruchou, žadatelé o azyl, starší osoby nebo pacienti.

[7] **Pseudonymizace** znamená skrytí identity fyzické osoby, například nahrazením jména neveřejným kódem.

7. Mobilní zařízení

Pokud pracovník používá mobilní zařízení (notebook, tablet, mobilní telefon aj.) k ukládání osobních údajů pracovní povahy, je povinen zabezpečit zařízení tak, aby v případě jeho ztráty či odcizení nedošlo k úniku osobních údajů. Přístup k informačnímu obsahu musí být vždy zabezpečen silným heslem a informace obsahující údaje vysoce osobní povahy či rozsáhlé soubory osobních údajů doporučujeme zabezpečit šifrováním, pseudonymizací či jiným vhodným způsobem. Obdobný přístup platí rovněž pro externí osobní úložiště dat (HDD disky, CD/DVD, flash-disky aj.) obsahující osobní údaje.

8. Nová zpracování osobních údajů

Při přípravě nového zpracování osobních údajů[8] je třeba respektovat zásady ochrany osobních údajů, jako je například zásada limitace účelem, zásada minimalizace údajů a nezbytnost připravit plánované zpracování tak, aby bylo k fyzickým osobám a jejich právům co nejšetrnější. Dále je nutné posoudit vliv zpracování na práva a svobody fyzických osob, jichž se údaje týkají a prostřednictvím Registru činností zpracování osobních údajů ČVUT oznámit a popsat úmysl pověřenci pro ochranu osobních údajů (viz čl. 13 Směrnice). Navrhovatel má právo zahájit nové, resp. změnit dosavadní zpracování, až poté, kdy od pověřence obdrží stanovisko a je ustanoven garant zpracování.
V případech, kdy má osobní údaje zpracovávat student v rámci plnění svých povinností (diplomová práce, projekt či jiná činnost), je školitel povinen seznámit studenta s povinnostmi dle nařízení GDPR a Příkazu ČVUT a zajistit případné další kroky (viz čl. 8 Směrnice).

9. Zákonnost zpracování osobních údajů

Pro každé zpracování osobních údajů je třeba mít stanoven právní titul, který zpracování umožní – jen tak je zpracování osobních údajů zákonné. Nařízení GDPR uvádí šest možných právních titulů (viz článek 15 Směrnice). Nejznámější je souhlas se zpracováním, který může udělit fyzická osoba, jíž se údaje týkají. Se souhlasy je však třeba být opatrný; nařízení požaduje, aby byl souhlas vyžadován pouze v těch případech, kdy nelze uplatnit jiný právní titul, jako je splnění zákonné povinnosti správce, plnění smlouvy, ochrana oprávněných zájmů správce, veřejný zájem aj. Pokud si nejste jisti, na který právní titul se v daném konkrétním případě spolehnout, kontaktujte právní odbor rektorátu ČVUT.

10. Porušení ochrany OU

Podle nařízení GDPR má správce osobních údajů povinnost ohlásit Úřadu pro ochranu osobních údajů incidenty, při nichž dojde k porušení zabezpečení zpracovávaných osobních údajů. Incidentem se rozumí zejména situace, kdy dojte k úniku nebo zneužití osobních údajů, či kdy dojde ke ztrátě případně odcizení zařízení, na kterém jsou zpracovávané osobní údaje uloženy. V případě, že zaznamenáte takový incident, ohlaste tento fakt neprodleně univerzitnímu pověřenci pro ochranu osobních údajů na adresu dpo@cvut.cz.
Incidentům je třeba pokud možno předcházet dodržováním zásad bezpečnosti zařízení a zabezpečení přístupu k údajům. Všichni zaměstnanci a studenti, kteří přichází do styku s osobními údaji, jsou povinni *zachovávat mlčenlivost* o osobních údajích a o bezpečnostních opatřeních pro jejich zabezpečení. Povinnost mlčenlivosti trvá i po ukončení pracovního poměru, studia nebo výkonu příslušných prací (viz čl. 7 odst. 4 Příkazu).

Verze 1.0, 24. 5. 2018

[8] **Zpracováním osobních údajů** se rozumí jakákoliv operace (ruční nebo automatizovaná) nebo soubor operací s osobními údaji. Zpracováním je již pouhé shromáždění či zaznamenání osobních údajů, stejně jako jakákoliv další operace s nimi, včetně jejich zpřístupnění.