č.j. 6/2018-S

Směrnice

„Ochrana osobních údajů“

Gymnázia J. A. Komenského a Jazykové školy s právem státní jazykové zkoušky Uherský Brod

OBSAH

SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

Důvěrnost	Zajištění, že informace (data) jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
Dostupnost a odolnost	Zajištění, že osobní údaje jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby. Jedná se o zničení dat, nebo úmyslné blokování či zahlcení technických prostředků, prostřednictvím kterých mají být tyto osobní údaje přístupné v požadovaném čase.
GDPR	Nařízení evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/es (obecné nařízení o ochraně osobních údajů) (General Data Protection Regulation)
Integrita	Vyjadřuje, jak je důležité, aby informace nebyla neoprávněně změněna.
Osobní údaj	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
Pověřenec pro ochranu osobních údajů	Zaměstnanec Gymnázia J. A. Komenského a Jazykové školy s právem státní jazykové zkoušky Uherský Brod ustanovený do funkce pověřence pro ochranu osobních údajů.
Souhlas	Svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů
Správce	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních

	údajů; jsou-li účely a prostředky tohoto zpracování určeny právem unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení Pro účely této směrnice je správcem Gymnázium J. A. Komenského a Jazyková škola s právem státní jazykové zkoušky Uherský Brod (dále jen „GJAK“)
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují
Vedení GJAK	Ředitel, zástupce
Vedoucí zaměstnanci	Vedoucí zaměstnance stanoví ředitel organizace
Zaměstnanec	Zaměstnanci GJAK Osoby vykonávající práci na základě dohod o pracích konaných mimo pracovní poměr
Zpracování osobních údajů	Jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
Zpracovatelská operace	Proces, agenda nebo činnost, v rámci, které se zpracovávají osobní údaje na základě odpovídajícího právního základu

PREAMBULE

Role definované tímto dokumentem předpokládají, že je bude vykonávat i žena. Avšak z důvodu zjednodušení textu jsou použity názvy jednotlivých rolí v mužském rodě. Bude-li danou roli zajišťovat žena, předpokládá se automatické přechylování názvů jednotlivých rolí, bez nutnosti úpravy směrnice.

1 ÚVOD

1.1 ÚVODNÍ USTANOVENÍ

Gymnázium J. A. Komenského a Jazyková škola s právem státní jazykové zkoušky Uherský Brod vydává tuto směrnici v souladu s těmito předpisy:

- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů" nebo „GDPR"),
- zákon č. 101/2000 Sb., o zpracování osobních údajů a o změně některých zákonů v platném znění, (dále jen „zákon"),

Směrnice upravuje povinnosti osob při ochraně osobních údajů v rámci celého jejich životního cyklu v podmínkách GJAK.

1.2 ROZSAH PŮSOBNOSTI

Ustanovení této směrnice jsou závazná pro všechny zaměstnance GJAK

Odpovědnost za ochranu osobních údajů
Za ochranu osobních údajů u GJAK odpovídá pověřenec pro ochranu osobních údajů v součinnosti s příslušnými vedoucími zaměstnanci.

2 OCHRANA OSOBNÍCH ÚDAJŮ

2.1 ZÁMĚRNÁ OCHRANA OSOBNÍCH ÚDAJŮ PŘI VZNIKU NOVÉ ZPRACOVATELSKÉ OPERACE NEBO ZMĚNY JIŽ EXISTUJÍCÍ ZPRACOVATELSKÉ OPERACE

Pověřenec pro ochranu osobních údajů je povinen v součinnosti s příslušnými vedoucími zaměstnanci navrhnout a předložit ke schválení vedení GJAK

1) V případě vzniku nové zpracovatelské operace nebo změny již existující deklaraci a návrh řešení:
   a) dodržení zásad zpracování osobních údajů dle čl. 5 GDPR,
   b) definici právního titulu pro zpracování dle čl. 6 GDPR,
   c) v případě, že právním důvodem zpracování je souhlas subjektu údajů se zpracováním, stanovit podmínky jeho vyjádření, prokazatelnosti a postupů v případě jeho odvolání dle čl. 7 GDPR,
   d) v případě, že budou zpracovávány zvláštní kategorie osobních údajů, zajistit jejich zpracování v souladu s čl. 9 GDPR, tj. zejména:
      a. deklarovat zákonnost zpracování,
      b. stanovit právní titul zpracování,
      c. v případě, že se bude jednat o zpracování těchto údajů na základě uděleného výslovného souhlasu, v případě vyhodnocení nezbytnosti tohoto zpracování vydat písemný souhlas k tomuto zpracování.
2) Návrh smlouvy se zpracovatelem, v případě, že se na zpracování bude podílet zpracovatel a zmocnění ke zpracování nevyplývá z právního předpisu. Smlouva musí mít náležitosti dle čl. 28 GDPR. Smlouva může být uzavřena formou:
   a) samostatné smlouvy,
   b) příslušná ustanovení mohou být zapracována do jiné smlouvy,
   c) dodatku ke smlouvě.
3) Závěry z vyhodnocení rizik pro práva a svobody subjektů údajů. V případě, že riziko bude vyhodnoceno jako vysoké, provést posouzení vlivu zamýšlené operace zpracování na ochranu osobních údajů a případně zahájit konzultační činnost s dozorovým úřadem.

4) Návrh požadavků na zabezpečení osobních údajů, přičemž bude vycházet z posouzení rizika zpracování pro práva a svobody subjektů údajů. Bude vyhodnocena vhodnost nasazení opatření dle článku čl. 32 GDPR k:

   a) případnému šifrování osobních údajů,

   b) zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování osobních údajů,

   c) obnovitelnosti a zajištění dostupnosti osobních údajů,

   d) testování, posuzování a hodnocení účinnosti zavedených bezpečnostních opatření.

2.2 ZÁMĚRNÁ OCHRANA OSOBNÍCH ÚDAJŮ V PRŮBĚHU ZPRACOVATELSKÉ OPERACE

Pověřenec pro ochranu osobních údajů je povinen v součinnosti s příslušnými vedoucími zaměstnanci průběžně ověřovat, zda jsou stávající technická a organizační opatření dostatečná, případně předložit návrh k úpravě existujících opatření. Za realizaci schválených změn jsou odpovědní příslušní vedoucí zaměstnanci.

2.3 ZÁMĚRNÁ OCHRANA OSOBNÍCH ÚDAJŮ PŘI ZÁNIKU ZPRACOVATELSKÉ OPERACE NEBO JAKÉKOLI JEJÍ ČÁSTI

Pověřenec pro ochranu osobních údajů je povinen v součinnosti s příslušnými vedoucími zaměstnanci navrhnout a předložit ke schválení vedení GJAK procesy a návrhy řešení související s:

1) dobou uchování osobních údajů za účelem archivace, pokud není určena platným skartačním plánem,

2) rozsahem a typy osobních údajů, které budou pro případnou archivaci uchovány,

3) způsobem likvidace zbývajících osobních údajů v elektronické i listinné podobě.

2.4 STANDARDNÍ OCHRANA OSOBNÍCH ÚDAJŮ

Pověřenec pro ochranu osobních údajů je povinen v součinnosti s příslušnými vedoucími zaměstnanci navrhovat a systematicky kontrolovat principy minimalizace osobních údajů spočívající v:

1) zajištění pouze nezbytně nutného rozsahu zpracovávaných osobních údajů pro daný účel spočívající v:

   a) zpracování záznamů o činnostech zpracování,

   b) vyřazením případných „nerelevantních nepřiměřených nebo nadbytečných údajů“,

   c) dodržováním postupů záměrné ochrany uvedených v předcházejících článcích této části směrnice,

   d) systematické kontrolní činností při zpracování osobních údajů, realizované v součinnosti s odpovědnými vedoucími zaměstnanci (kontrola pravidel bezpečnosti, aktuálnost záznamů, relevantnost údajů atd.).

2) zajištění pouze nezbytně nutné doby uchování osobních údajů pro daný účel, a to jak v listinné, tak i v elektronické podobě, spočívající ve:

   a) zpracování záznamů o činnostech zpracování,

   b) stanovení lhůt pro uchování osobních údajů vycházející buď z/ze:

      a. spisového a skartačního řádu a jeho lhůt, nebo

      b. přiměřenosti vzhledem k účelu zpracování,

      c. zajištění jejich zachování jak u listinného, tak i elektronického zpracování, realizace skartačních lhůt v elektronické podobě,

      d. systematické kontrolní činností při zpracování osobních údajů, realizované v součinnosti s vedoucími zaměstnanci a správcem IT z hlediska realizace skartačních lhůt v elektronické podobě.

3) Zajištění dostupnosti pouze nezbytně nutnému počtu osob spočívající ve:

   a) zpracování záznamů o činnostech zpracování,

   b) stanovení pravidel pro řízení přístupu,

   c) stanovení pravidel pro zveřejňování, sdílení nebo předávání informací,

   d) systematické kontrolní činností při zpracování osobních údajů, realizované v součinnosti s vedoucími zaměstnanci.

2.5 PORUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

1) Zaměstnanci jsou povinni v případě zjištění porušení zabezpečení osobních údajů (nebo nabytí podezření) neprodleně informovat svého nadřízeného, který následně informuje pověřence pro ochranu osobních údajů.

2) Pověřenec pro ochranu osobních údajů na základě hlášení o porušení zabezpečení osobních údajů v součinnosti s příslušným vedoucím zaměstnancem:

   a) vyhodnotí zdroje porušení (interní, externí atd.),

   b) vyhodnotí základních informace o narušení, a

   c) rozhodne o klasifikaci narušení, tj. zda se jedná o bezpečnostní událost nebo bezpečnostní incident:

      a. bezpečnostní událost je situace, kdy mohlo dojít k selhání některého z bezpečnostních opatření a tím mohlo dojít k porušení zabezpečení ochrany osobních údajů,

      b. bezpečnostní incident je situace, kdy došlo k selhání některého z bezpečnostních opatření a tím došlo k porušení zabezpečení ochrany osobních údajů.

3) Pokud je informace vyhodnocena jako bezpečnostní událost, provede pověřenec pro ochranu osobních údajů v rámci šetření následující kroky:

   a) prověří v záznamech, zda se jedná o nahodilou událost nebo se jedná o událost, která se opakuje,

   b) vypracuje návrh na opatření k nápravě,

   c) návrh na opatření k nápravě předá vedení GJAK k posouzení a vyjádření.

4) Pokud je informace vyhodnocena jako bezpečnostní incident, pověřenec pro ochranu osobních údajů přizve další osoby, které jsou kompetentní pro jeho posouzení, a provedou se následující činnosti:

   a) pokud je to možné, provedou odpovědní zaměstnanci okamžitou nápravu (zastavení provozu, zablokování přístupových oprávnění atd.),

   b) identifikace kategorie porušení:

      a. důvěrnosti,

      b. dostupnosti a odolnosti,

      c. integrity,

   c) identifikace typů osobních údajů, u kterých došlo k porušení bezpečnosti,

   d) stanovení přibližného objemu údajů, u kterých došlo k porušení bezpečnosti,

   e) identifikace pravděpodobného zdroje úniku, či případného porušení zabezpečení osobních údajů,

f) popis pravděpodobných důsledků dopadů na subjekty údajů,

g) vyhodnocení rizika dopadů na práva a svobody subjektů údajů:

   a. bez rizika,

   b. riziko,

   c. vysoké riziko.

5) Po vyhodnocení rizika bude kontaktován pověřený zástupce z vedení GJAK

6) Pověřenec pro ochranu osobních údajů společně s pověřeným zástupcem z vedení GJAK přijme rozhodnutí (o povinnosti ohlášení nebo oznámení) a v případě vyhodnocení:

   a) rizika – provede ohlášení dozorovému úřadu, (bez zbytečného odkladu do 72 hodin od zjištění bezpečnostního incidentu),

   b) vysokého rizika – provede ohlášení dozorovému úřadu a oznámení subjektům údajů, (bez zbytečného odkladu).

7) Dále pověřenec pro ochranu osobních údajů společně s dalšími odpovědnými zaměstnanci vypracuje návrh a přijme prvotní možná nápravná opatření ke snížení dopadů na práva subjektů údajů nebo k eliminaci příčiny porušení bezpečnosti osobních údajů.

8) Připraví a zpracuje hlášení v souladu s čl. 33 odst. 3 písm. a) až d) nebo s čl. 33 odst. 3 písm. b) až d) GDPR, vždy podle úrovně vyhodnoceného rizika, které po schválení pověřeným zástupcem z vedení GJAK odešle příslušným subjektům (dozorovému úřadu, případně subjektům údajů).

9) Pověřenec pro ochranu osobních údajů v součinnosti s odpovědnými vedoucími zaměstnanci po odeslání hlášení provede:

   a) další vyšetřování incidentu na základě návrhů uvedených v hlášení dozorovému úřadu,

   b) vypracuje návrh na přijetí dalších nápravných opatření,

   c) kontrolu účinnosti přijatých opatření.

10) Pověřenec pro ochranu osobních údajů společně s dalšími odpovědnými zaměstnanci zpracovává dokumentaci týkající se porušení zabezpečení osobních údajů. Dokumentace musí obsahovat:

   a) veškeré skutečnosti, které se týkají příslušného porušení, včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů,

b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů

c) pravděpodobné dopady, důsledky porušení, a

d) přijatá nápravná opatření, včetně opatření ke zmírnění následků porušení.

11) Dokumentace o porušení zabezpečení osobních údajů musí dozorovému úřadu umožnit ověření souladu s GDPR.

Uherský Brod: 25. 5. 2018

RNDr. Jaroslav Krpal

ředitel GJAK