Základná škola, Na bielenisku č. 2, 902 01 Pezinok, IČO: 36 062 162

Posúdenie vplyvu na ochranu osobných údajov („PIA“)

Spracované na základe Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 (ďalej len „nariadenie GDPR“), zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) a vyhlášky Úradu na ochranu osobných údajov č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

PIA IS pedagogická dokumentácia

Číslo výtlačku	Počet listov	Miesto	Dátum	Posudzovateľ	Validátor
1	23	Pezinok	25.5.2018		

Informácie PIA

PIA
IS pedagogická dokumentácia

Autor
PROENERGY, s. r. o.

Posudzovateľ
Základná škola

Validátor
zodpovedná osoba

Dátum vytvorenia
25/05/2018

Meno zodpovednej osoby
Ing. Dominik Bartko

Stanovisko Zodpovednej osoby
Bez výhrad

Získanie názorov dotknutých osôb
Neboli požadované názory dotknutých osôb

Dôvod, prečo neboli požadované názory dotknutých osôb
Spracúvanie sa vykonáva vo verejnom záujme podľa príslušných osobitných predpisov.

Prílohy

Bez príloh

1. Kontext

1.1 Prehľad

Ktoré spracúvanie sa posudzuje?

Spracovanie a vedenie osobných údajov v rámci pedagogickej dokumentácie a ich poskytovanie do centrálneho registra sa vykonáva podľa zákona č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov (ďalej len „školský zákon“) v súlade s čl. 6 ods. 1 písm. c) nariadenia GDPR.

Účelom spracúvania osobných údajov je vedenie pedagogickej dokumentácie a poskytovanie osobných údajov dotknutých osôb do centrálneho registra podľa školského zákona.

Aké sú zodpovednosti spojené so spracúvaním?

Za spracúvanie osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ. Prevádzkovateľ preveril sprostredkovateľa o zabezpečovaní primeraných záruk pri spracúvaní osobných údajov a uzatvoril s ním zmluvu podľa čl. 28 nariadenia GDPR. Predmetom zmluvy je poskytovanie **IT služieb**, pri výkone ktorých bude dochádzať k spracúvaniu osobných údajov v nevyhnutnom rozsahu pre dané úkony.

Existujú platné normy pre spracúvanie?

Prevádzkovateľ nedisponuje kódexom správania, ani certifikátom.

Hodnotenie: Prijaté

1.2 Osobné údaje, procesy a podporné aktíva

Aké osobné údaje spracúvate?

Dotknuté osoby: uchádzači, žiaci, poslucháči a deti prevádzkovateľa, ich zákonní zástupcovia.

Rozsah spracúvaných osobných údajov: bežné a citlivé osobné údaje podľa školského zákona, nasledovne:

- podľa § 63 ods. 6 školského zákona na prihláške na vzdelávanie sa vyžadujú tieto osobné údaje:

a) meno a priezvisko, rodné číslo, vyučovací jazyk, štátne občianstvo, potvrdenie o zdravotnej spôsobilosti žiaka, výchovno-vzdelávacie výsledky žiaka na základnej škole,

b) meno a priezvisko, adresa a telefónny kontakt zákonných zástupcov.

- podľa § 11 ods. 6 školského zákona školy alebo školské zariadenia majú právo získavať a spracúvať osobné údaje:

a) o deťoch a žiakoch v rozsahu

1. meno a priezvisko,

2. dátum a miesto narodenia,

3. adresa trvalého pobytu alebo adresa miesta, kde sa dieťa alebo žiak obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu,

4. rodné číslo,

5. štátna príslušnosť,

6. národnosť,

7. fyzického zdravia a duševného zdravia,

8. mentálnej úrovne vrátane výsledkov pedagogicko-psychologickej a špeciálnopedagogickej diagnostiky,

b) o identifikácii zákonných zástupcov dieťaťa alebo žiaka v rozsahu

1. meno a priezvisko a adresa trvalého pobytu,

2. adresa miesta, kde sa zákonný zástupca obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu a kontakt na účely komunikácie.

- podľa § 157 ods. 3 školského zákona škola poskytuje do centrálneho registra tieto osobné údaje:

a) ak ide o dieťa, žiaka alebo poslucháča:

1. titul, meno a priezvisko, rodné priezvisko,

2. dátum, miesto, okres a štát narodenia,

3. dátum a miesto úmrtia alebo údaj o vyhlásení za mŕtveho alebo zrušení vyhlásenia za mŕtveho,

4. rodné číslo,

5. pohlavie,

6. národnosť,

7. štátne občianstvo,

8. spôsobilosť na právne úkony,

9. rodinný stav,

10. adresa bydliska a druh pobytu,

11. zákaz pobytu,

12. kontakt na účely komunikácie,

13. adresa bydliska, z ktorého dochádza do školy,

14. skutočnosti podľa § 144 ods. 7 písm. d) školského zákona, (t.j. informácie o zdravotnej spôsobilosti dieťaťa, zdravotných problémoch alebo iných závažných skutočnostiach, ktoré by mohli mať vplyv na priebeh výchovy a vzdelávania),

15. dátum prijatia, študijný odbor, zameranie študijného odboru, učebný odbor alebo zameranie učebného odboru, výchovno-vzdelávací program a forma organizácie výchovy a vzdelávania v škole, školskom zariadení alebo pracovisku praktického vyučovania a údaje o účasti na aktivitách v nich,

16. učebná zmluva podľa osobitného predpisu,

17. zmluva o budúcej pracovnej zmluve podľa osobitného predpisu,

18. dosiahnutý stupeň vzdelania a dosiahnuté výsledky vzdelávania,

19. počet vyučovacích hodín, ktoré neabsolvoval bez ospravedlnenia, a to za každý kalendárny mesiac školského roka.

b) ak ide o zákonného zástupcu dieťaťa, žiaka alebo poslucháča:

1. osobné údaje v rozsahu podľa písmena a) prvého až dvanásteho bodu,

2. dosiahnuté vzdelanie.

Doba spracúvania a uchovávania: Doba uchovávania: Prevádzkovateľ spracúva osobné údaje po dobu nevyhnutnú na splnenie účelu, podľa registratúrneho poriadku v zmysle osobitného predpisu č. 395/2002 Z. z. o archívoch a registratúrach, smernice – Lehoty uloženia a podľa §157 ods. 10 a 11 školského zákona.

Osobné údaje v mene prevádzkovateľa môžu spracúvať poučené oprávnené osoby definované podľa smernice - Rozsah a povolené činnosti pri spracúvaní osobných údajov.

Príjemcovia, ktorým môžu byť osobné údaje poskytnuté sú:

1.oprávnené subjekty podľa školského zákona, nasledovne:

- Ministerstvo školstva, vedy, výskumu a športu SR - Centrálny register,

- zriaďovateľ školy podľa § 158 ods.6 školského zákona,

- orgány štátnej správy v školstve v rozsahu ich pôsobnosti podľa osobitných predpisov,

- iné oprávnené subjekty v zmysle školského zákona.

2. oprávnené subjekty podľa čl. 6 ods. 1 písm. c) nariadenia GDPR (napr. polícia, prokuratúra, súdy a iné);

3. zmluvný partner – sprostredkovateľ.

Ako funguje životný cyklus osobných údajov a procesov?

Prevádzkovateľ získava a zhromažďuje osobné údaje osobne - ústne, písomne, aj elektronickými technickými prostriedkami prostredníctvom svojich oprávnených osôb.

Tieto následne spracúva v papierovej aj elektronickej podobe za účelom spracovania a vedenia pedagogickej dokumentácie v zmysle školského zákona a súvisiacich predpisov podľa §157 ods. 9 školského zákona (zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie, preskupovanie, kombinovanie, obmedzenie, vymazávanie) a tiež zabezpečí ich poskytnutie do centrálneho registra.

Oprávnené osoby prevádzkovateľa môžu spracúvať osobné údaje na základe poučenia podľa schválených oprávnení podľa smernice - Rozsah oprávnení a povolených činností, pracovných zmlúv a interných dokumentov prevádzkovateľa.

Prevádzkovateľ je oprávnený sprístupniť, resp. poskytnúť osobné údaje z informačného systému sprostredkovateľovi podľa platnej sprostredkovateľskej zmluvy.

Prevádzkovateľ je oprávnený sprístupniť, resp. poskytnúť osobné údaje z informačného systému vyššie uvedeným príjemcom, podľa školského zákona a osobitných predpisov.

Poskytnutie osobných údajov (okrem povinného poskytovania podľa školského zákona) sa zaznamenáva prostredníctvom záznamu o vypožičaní/odovzdaní osobných údajov na spracúvanie inému spracovateľovi, alebo na základe iného akceptovateľného dokumentu (žiadosti, výzvy a pod.).

Zálohovanie dát s osobnými údajmi sa vytvára periodicky na externé médium, likvidácia prebieha zabezpečeným spôsobom podľa predpísaných postupov po uplynutí doby uchovávania.

Jednotlivé postupy spracúvania - opatrenia pre zachovanie primeranej úrovne bezpečnosti osobných údajov, sú

zdokumentované v bezpečnostnej analýze rizík, bezpečnostnej politike a bezpečnostnej smernici, ktoré podliehajú periodickej kontrole a podľa potreby sa aktualizujú.

Aké sú podporné aktíva pre osobné údaje?

Hardware a elektronické média - technické prostriedky
Softvér (podľa smernice - Rozsah oprávnení a povolených činností)
Počítačové pripojenia
Ľudia - používatelia, IT administrátor (podľa smernice - Rozsah oprávnení a povolených činností)
Písomnosti - tlačené, písané, kópie dokumentov
Spôsob prenosu písomností - email, pracovný poriadok

Hodnotenie: Prijaté

2. Základné zásady

2.1 Proporcionalita a nevyhnutnosť

Sú procesy špecifikované, explicitné a legitímne?

Spracovanie a vedenie osobných údajov v rámci pedagogickej dokumentácie a ich poskytovanie do centrálneho registra sa vykonáva podľa školského zákona.

Účelom spracúvania osobných údajov je vedenie pedagogickej dokumentácie a poskytovanie osobných údajov dotknutých osôb do centrálneho registra podľa školského zákona.

Spracúvanie sa vykonáva podľa osobitného predpisu v súlade s čl. 6 ods. 1 písm. c) nariadenia GDPR, spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa.

Prevádzkovateľ spracúva osobné údaje na konkrétne určený, výslovne uvedený a legitímny účel, a tieto osobné údaje ďalej nespracúva na iný účel, ktorý je nezlučiteľný s pôvodným účelom v zmysle čl. 5 ods. 1 písm. b) nariadenia GDPR.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ spracúva osobné údaje v súlade so zásadou obmedzenia účelu podľa čl. 5 ods. 1 písm. b) nariadenia GDPR.

Aké sú právne základy pre zákonné spracúvanie?

v zmysle čl. 6 ods. 1 písm. c) nariadenia GDPR – školský zákon

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ spracúva osobné údaje v súlade so zásadou zákonnosti podľa čl. 5 ods. 1 písm. a) nariadenia GDPR.

Sú zhromaždené osobné údaje primerané, relevantné a obmedzené na to, čo je nevyhnutné vo vzťahu k účelom, pre ktoré sú spracúvané („minimalizácia údajov")?

Prevádzkovateľ spracúva osobné údaje - bežné a citlivé v zmysle školského zákona.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ spracúva osobné údaje v súlade so zásadou minimalizácie údajov podľa čl. 5 ods. 1 písm. c) nariadenia GDPR.

Sú osobné údaje presné a aktuálne?

Prevádzkovateľ má prijaté a zdokumentované opatrenia prostredníctvom interných smerníc tak, aby spracúval osobné údaje správne a podľa potreby aktualizované. Údaje nesprávne bez zbytočného odkladu vymaže, alebo opraví v súlade s požiadavkou čl. 5 ods. 1 písm. d) nariadenia GDPR.

Hodnotenie: Prijaté
Komentár k hodnoteniu:

Prevádzkovateľ spracúva osobné údaje v súlade so zásadou správnosti podľa čl. 5 ods. 1 písm. d) nariadenia GDPR.

Aké je doba uloženia údajov?

Doba uchovávania: Prevádzkovateľ spracúva osobné údaje po dobu nevyhnutnú na splnenie účelu, podľa registratúrneho poriadku v zmysle osobitného predpisu č. 395/2002 Z. z. o archívoch a registratúrach, smernice – Lehoty uloženia a podľa §157 ods. 10 a 11 školského zákona.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ spracúva osobné údaje v súlade so zásadou minimalizácie uchovávania podľa čl. 5 ods. 1 písm. e) nariadenia GDPR.

2.2 Opatrenia na ochranu práv dotknutých osôb

Ako sú dotknuté osoby informované o spracúvaní?

Prevádzkovateľ si plní informačnú povinnosť podľa čl. 13 a 14 nariadenia GDPR pri získavaní osobných údajov tak, aby dotknutá osoba mala možnosť sa s týmito informáciami oboznámiť pred poskytnutím osobných údajov. Prevádzkovateľ zabezpečuje poskytnutie informácie osobne prostredníctvom oprávnených osôb v priestoroch školy pri získavaní osobných údajov, ako aj na nástenkách, či na web stránke.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ zabezpečuje informovanie dotknutých osôb pred získavaním ich osobných údajov podľa čl.13 a 14 nariadenia GDPR.

Ako ste získali súhlas dotknutých osôb?

Súhlas sa nevyžaduje.

Hodnotenie: Prijaté

Ako môžu dotknuté osoby uplatňovať svoje práva na prístup a prenosnosť údajov?

Prevádzkovateľ zabezpečuje vybavovanie žiadostí dotknutých osôb v súvislosti s uplatňovaním ich práv prostredníctvom emailovej adresy, alebo písomne. Za týmto účelom má prevádzkovateľ poverenú zodpovednú osobu podľa čl. 37 nariadenia GDPR.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ zabezpečuje dotknutým osobám výkon ich práva na prístup a prenosnosť údajov podľa čl.15 a 20 nariadenia GDPR.

Ako môžu dotknuté osoby uplatňovať svoje práva na opravu a vymazanie?

Prevádzkovateľ zabezpečuje vybavovanie žiadostí dotknutých osôb v súvislosti s uplatňovaním ich práv prostredníctvom emailovej adresy, alebo písomne. Za týmto účelom má prevádzkovateľ poverenú zodpovednú osobu podľa čl. 37 nariadenia GDPR.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ zabezpečuje dotknutým osobám výkon ich práva na opravu a vymazanie údajov podľa čl. 16 a 17 nariadenia GDPR.

Ako môžu dotknuté osoby uplatňovať svoje práva na obmedzenie spracúvania a namietať spracúvanie?

Prevádzkovateľ zabezpečuje vybavovanie žiadostí dotknutých osôb v súvislosti s uplatňovaním ich práv prostredníctvom emailovej adresy, alebo písomne. Za týmto účelom má prevádzkovateľ poverenú zodpovednú osobu podľa čl. 37 nariadenia GDPR.

Hodnotenie: Prijaté
Komentár k hodnoteniu:
Prevádzkovateľ zabezpečuje dotknutým osobám výkon ich práva na obmedzenie spracúvania a namietať spracúvanie údajov podľa čl. 18 a 21 nariadenia GDPR.

Sú povinnosti sprostredkovateľov jasne identifikované a riadené zmluvou?

Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou podľa čl. 28 nariadenia GDPR. Účelom zmluvy je poskytovanie IT služieb pre prevádzkovateľa, v rámci ktorých bude dochádzať k spracúvaniu osobných údajov v nevyhnutnom rozsahu. Zmluva popisuje zodpovednosti sprostredkovateľa v rámci zadefinovaného trvania zmluvy, rozsahu, účelu, pokynov pre spracovanie a ďalšie požiadavky podľa nariadenia. Sprostredkovateľ sa súčasne zaručil, že poskytuje dostatočné záruky pri spracúvaní osobných údajov.

Hodnotenie: Prijaté

V prípade prenosu osobných údajov mimo Európsku úniu sú údaje dostatočne chránené?

Prenos sa nevykonáva.

Hodnotenie: Prijaté

3. Riziká

3.1 Plánované alebo súčasné opatrenia

Anonymizácia

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Oddelenie osobných údajov

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Logické riadenie prístupu

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Vysledovateľnosť (logging)

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Archivácia

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Bezpečnosť písomností

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Minimalizácia množstva osobných údajov

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Operačná bezpečnosť

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Kontrola škodlivého softvéru

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Manažment pracovných staníc

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Bezpečnosť webovej stránky

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Zálohy

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Údržba

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Spracovanie zmlúv

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Sieťová bezpečnosť

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Kontrola fyzického prístupu

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Monitoring sieťových aktivít

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Bezpečnosť hardwaru

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Vyhýbanie sa zdrojom rizika

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Ochrana proti iným ako ľudským zdrojom rizika

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Organizácia

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Politika

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Manažment bezpečnostných rizík

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Integrácia ochrany súkromia v projektoch

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Manažment porušení ochrany osobných údajov

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica, smernica o vyšetrovaní bezpečnostných incidentov

Hodnotenie: Prijaté

Personálny manažment

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Vzťahy s tretími stranami

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Kontrolná činnosť

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

Šifrovanie

Opatrenie sa vykonáva podľa prijatých interných dokumentov - analýza rizík, bezpečnostná politika, bezpečnostná smernica

Hodnotenie: Prijaté

3.2 Nelegitímny prístup k osobným údajom

Aké by mohli byť hlavné dopady na dotknuté osoby, ak by k takému riziku došlo?

Ujma na zdraví, majetková a nemajetková ujma, diskriminácia, krádež totožnosti, podvod, finančná strata, poškodenie dobrého mena, strata dôvernosti, neoprávnená reverzná pseudonymizácia, pozbavenie práv a slobôd a pod.

V dôsledku zváženia závažnosti rizika, sa odhadujú nasledovné možné dopady:

Stupeň závažnosti	Všeobecný popis dopadu na dotknuté osoby (priamy a nepriamy)	Možný fyzický dopad na dotknuté osoby	Možný materiálny dopad na dotknuté osoby	Možný morálny dopad na dotknuté osoby
3. Významný	Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami	- Vážne fyzické zdravotné problémy, ktoré spôsobujú dlhodobú ujmu (napríklad zhoršenie zdravia kvôli nevhodnej starostlivosti, alebo z dôvodu prehliadania kontraindikácií) - zmena fyzickej integrity napríklad napadnutie, nehoda doma, v práci atď.	-nevykompenzované odcudzenie peňazí - dlhodobé finančné ťažkosti (napríklad nutnosť vziať si pôžičku) - cielené, jedinečné a neopakovateľné, stratené príležitosti (napr. úver na bývanie, odmietnutie štúdia, stáže alebo zamestnania, zákaz skúšok) - zákaz držby bankových účtov - škody na majetku - Strata bývania - Strata zamestnania - Separácia alebo rozvod - finančná strata ako dôsledok podvodu (napríklad v dôsledku phishing pokusov) - zabránenie cudziny - Strata údajov o zákazníkoch	- Vážne psychologické zdravotné problémy (napr. depresie, fóbie) - Pocit narušenia súkromia s nezvratným poškodením - Pocit zraniteľnosti po predvolaní na súd - Pocit porušenia základných práv (napr. diskriminácia, sloboda prejavu) - obeť vydierania -kyberšikana a obťažovanie

Aké sú hlavné hrozby, ktoré by mohli viesť k riziku?

Podporné aktíva	Činnosť	Hrozby
Hardware	Neprimerané použitie	Použitie USB flash diskov; ktoré nie sú vhodné vzhľadom na citlivosť informácií; použitie; alebo preprava citlivého hardwaru na osobné účely a pod.
Hardware	Špionáž	Sledovanie obrazovky bez vedomia osoby vo vlaku; fotografovanie obrazovky; geolokalizácia hardvéru; diaľková detekcia elektromagnetických signálov atď.
Hardware	Strata	Krádež laptopu z hotelovej izby; krádež profesionálneho mobilného telefónu; získanie vyhodeného harwarového úložného zariadenia; strata elektronického úložného zariadenia
Hardware	Modifikácia	Sledovanie prostredníctvom keylogger-u; odstránenie hardwarových komponentov; pripojenie zariadení (napríklad USB flash diskov) na spustenie operačného systému alebo na získanie dát atď.
Hardware	Strata	Slabé dohody o likvidácii alebo údržbe môžu viesť k neoprávnenému prístupu k osobným údajom
Software	Neprimerané použitie	Vymazanie údajov; používanie falšovaného alebo kopírovaného softvéru; chyby operátora, ktoré odstraňujú údaje atď.; skenovanie obsahu; nezákonné krížové odkazovanie na údaje; zvýšenie právomocí; zmazanie používateľských ciest; posielanie nevyžiadanej pošty prostredníctvom e-mailového programu; zneužitie funkcií siete atď.
Software	Špionáž	Skenovanie sieťových adries a portov; zhromažďovanie konfiguračných údajov; analýza zdrojových kódov s cieľom nájsť využiteľné nedostatky; testovanie toho, ako databázy reagujú na škodlivé dopyty atď.
Software	Špionáž	Skenovanie sieťových adries a portov; útoky na zraniteľnosti v počúvaní, analýze, reportovaní alebo sprostredkovaní portov a služieb.
Software	Modifikácia	Sledovanie prostredníctvom keylogger-u; infikovanie škodlivým softvérom; inštalácia nástroja vzdialenej správy; nahradenie komponentov atď.
Počítačové pripojenia	Špionáž	Zablokovanie prenosu prostredníctvom siete Ethernet, získavanie údajov odosielaných prostredníctvom siete Wi-Fi, atď
Osoby	Neprimerané použitie	Vplyv (phishing, sociálne inžinierstvo, úplatkárstvo atď.), Tlak (vydieranie, psychické obťažovanie atď.)
Osoby	Špionáž	Neúmyselné zverejnenie informácií počas rozhovoru; používanie odpočúvacích zariadení na stretnutiach atď.
Osoby	Strata	Zamestnanecké pytliactvo; zmeny priradenia; prevzatie kontroly nad celou organizáciou alebo jej časti atď.
Písomnosti	Špionáž	Odpozeranie, fotokopírovanie, fotografovanie, atď.
Písomnosti	Strata	Krádež spisov z kancelárií; krádež z poštových schránok; znovuzískanie vyhodených dokumentov atď.
Prenos písomností	Špionáž	Odpozeranie podpisových kníh v obehu; rozmnožovanie dokumentov v obehu atď.

Aké sú zdroje rizika?

Interné ľudské zdroje	Zamestnanci, osoby v obdobnom pracovnoprávnom vzťahu, osoby na študentskej praxi
Externé ľudské zdroje	Príjemcovia, oprávnené tretie strany, poskytovatelia služieb, hackery, návštevy, bývalý zamestnanci, klienti, aktivisti, konkurencia, odborové organizácie, médiá, mimovládne organizácie, zločinecké organizácie, organizácie pod kontrolou iného štátu, teroristické organizácie, neďaleká priemyselná činnosť
Iné ako ľudské zdroje	Škodlivý kód neznámeho pôvodu (vírusy, červy, a pod.), prírodné katastrofy, epidémie, horľavé, korózne, alebo výbušné materiály, voda (vodné potrubia, kanalizácia)

Ktoré z identifikovaných opatrení prispievajú k riešeniu rizika?

Opatrenia podľa kapitoly 3.1

Ako odhadujete závažnosť rizika, hlavne podľa možných dopadov a plánovaných opatrení?

3. Významné:

Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami.

V prípade nelegitímneho prístupu k osobným údajom sa odhadujú významné negatívne vplyvy na dotknutú osobu. Je to najmä z dôvodu systematického spracúvania citlivých osobných údajov týkajúcich sa zdravia, mentálnej úrovne, národnosti a iných citlivých údajov zraniteľných osôb (detí). Zo spracúvania môžu vyplynúť rozhodnutia s právnymi účinkami, alebo rozhodnutia s podobne závažnými účinkami pre dotknutú osobu.

Ako odhadujete pravdepodobnosť rizika, hlavne ak ide o hrozby, zdroje rizika a plánované opatrenia?

1. Zanedbateľná:

Uskutočnenie hrozby využitím vlastností podporných aktív sa javí ako nemožné pre vybrané zdroje rizík

Prevádzkovateľ je v súlade s požiadavkami novej legislatívy, identifikované hrozby by mali byť u prevádzkovateľa dostatočne pokryté, za predpokladu dodržiavania prijatých bezpečnostných opatrení. Pravdepodobnosť vzniku nelegitímneho prístupu k osobným údajom sa javí ako zanedbateľná, avšak úplná eliminácia nežiaducich udalostí nie je možná.

Hodnotenie: Prijaté

3.3 Neželaná modifikácia osobných údajov

Aké by mohli byť hlavné dopady na dotknuté osoby, ak by k takému riziku došlo?

Ujma na zdraví, majetková a nemajetková ujma, diskriminácia, krádež totožnosti, podvod, finančná strata, poškodenie dobrého mena, strata dôvernosti, neoprávnená reverzná pseudonymizácia, pozbavenie práv a slobôd

V dôsledku zváženia závažnosti rizika, sa odhadujú nasledovné možné dopady:

Stupeň závažnosti	Všeobecný popis dopadu na dotknuté osoby (priamy a nepriamy)	Možný fyzický dopad na dotknuté osoby	Možný materiálny dopad na dotknuté osoby	Možný morálny dopad na dotknuté osoby
3. Významný	Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami	- Vážne fyzické zdravotné problémy, ktoré spôsobujú dlhodobú ujmu (napríklad zhoršenie zdravia kvôli nevhodnej starostlivosti, alebo z dôvodu prehliadania kontraindikácií) - zmena fyzickej integrity (napríklad napadnutie, nehoda doma, v práci, atď.)	- nevykompenzované odcudzenie peňazí - dlhodobé finančné ťažkosti (napríklad nutnosť vziať si pôžičku) - cielené, jedinečné a neopakovateľné, stratené príležitosti (napr. úver na bývanie, odmietnutie štúdia, stáže alebo zamestnania, zákaz skúšok) - zákaz držby bankových účtov - škody na majetku	- Vážne psychologické zdravotné problémy (napr. depresie, fóbie) - Pocit narušenia súkromia s nezvratným poškodením - Pocit zraniteľnosti po predvolaní na súd - Pocit porušenia základných práv (napr. diskriminácia, sloboda prejavu) - obeť vydierania - kyberšikana a

			- Strata bývania - Strata zamestnania - Separácia alebo rozvod - finančná strata ako dôsledok podvodu (napríklad po phishing pokusoch) - zabránenie cudziny - Strata údajov o zákazníkoch	obťažovanie

Aké sú hlavné hrozby, ktoré by mohli viesť k riziku?

Podporné aktíva	**Činnosť**	**Hrozby**
Hardware	Modifikácia	Pridanie nekompatibilného hardvéru spôsobujúceho poruchy; odstránenie prvkov nevyhnutných pre správnu prevádzku aplikácie, atď.
Software	Neprimerané použitie	Nežiaduce zmeny údajov v databázach; vymazanie súborov potrebných na správne fungovanie softvéru; chyby operátora, ktoré upravujú údaje, atď.
Software	Modifikácia	Chyby počas aktualizácií, konfigurácie alebo údržby; infikovanie škodlivým softvérom; výmena komponentov, atď.
Počítačové pripojenia	Modifikácia	Útok upravujúci alebo pridávajúci údaje do sieťovej prevádzky, opakovaný útok (preposlanie zachytených dát, atď.)
Osoby	Neprimerané použitie	Ovplyvnenie (klebety, dezinformácia, atď.)
Osoby	Preťaženie	Vysoká pracovná záťaž, stres alebo negatívne zmeny pracovných podmienok; pridelenie zamestnancov na úlohy, ktoré presahujú ich schopnosti; slabé využívanie zručností, atď.
Písomnosti	Modifikácia	Zmeny údajov v spise; nahradenie originálu falšovaním, atď.
Prenos písomností	Modifikácia	Zmeny v obežníku bez vedomia autora; výmena jednej podpisovej knihy za inú; odoslanie viacerých konfliktných dokumentov, atď.

Aké sú zdroje rizika?

Interné ľudské zdroje	zamestnanci, osoby v obdobnom pracovnoprávnom vzťahu, osoby na študentskej praxi
Externé ľudské zdroje	príjemcovia, oprávnené tretie strany, poskytovatelia služieb, hackeri, návštevy, bývalí zamestnanci, klienti, aktivisti, konkurencia, odborové organizácie, médiá, mimovládne organizácie, zločinecké organizácie, organizácie pod kontrolou iného štátu, teroristické organizácie, neďaleká priemyselná činnosť
Iné ako ľudské zdroje	škodlivý kód neznámeho pôvodu (vírusy, červy, a pod.), prírodné katastrofy, epidémie, horľavé, korózne, alebo výbušné materiály, voda (vodné potrubia, kanalizácia)

Ktoré z identifikovaných opatrení prispievajú k riešeniu rizika?

Opatrenia podľa kapitoly 3.1

Ako odhadujete závažnosť rizika, hlavne podľa možných dopadov a plánovaných opatrení?

3. Významné:

Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami.

V prípade neželanej modifikácie osobných údajov sa odhadujú významné negatívne vplyvy na dotknutú osobu. Je to najmä z dôvodu systematického spracúvania citlivých osobných údajov týkajúcich sa zdravia, mentálnej

úrovne, národnosti a iných citlivých údajov zraniteľných osôb (detí). Zo spracúvania môžu vyplynúť rozhodnutia s právnymi účinkami, alebo rozhodnutia s podobne závažnými účinkami pre dotknutú osobu.

Ako odhadujete pravdepodobnosť rizika, hlavne ak ide o hrozby, zdroje rizika a plánované opatrenia?

1. Zanedbateľná:

Uskutočnenie hrozby využitím vlastností podporných aktív sa javí ako nemožné pre vybrané zdroje rizík

Prevádzkovateľ je v súlade s požiadavkami novej legislatívy, identifikované hrozby by mali byť u prevádzkovateľa dostatočne pokryté, za predpokladu dodržiavania prijatých bezpečnostných opatrení. Pravdepodobnosť vzniku nelegitímneho prístupu k osobným údajom sa javí ako zanedbateľná, avšak úplná eliminácia nežiaducich udalostí nie je možná.

Hodnotenie: Prijaté

3.4 Strata osobných údajov

Aké by mohli byť hlavné dopady na dotknuté osoby, ak by k takému riziku došlo?

Ujma na zdraví, majetková a nemajetková ujma, diskriminácia, krádež totožnosti, podvod, finančná strata, poškodenie dobrého mena, strata dôvernosti, neoprávnená reverzná pseudonymizácia, pozbavenie práv a slobôd.

V dôsledku zváženia závažnosti rizika, sa odhadujú nasledovné možné dopady:

Stupeň závažnosti	Všeobecný popis dopadu na dotknuté osoby (priamy a nepriamy)	Možný fyzický dopad na dotknuté osoby	Možný materiálny dopad na dotknuté osoby	Možný morálny dopad na dotknuté osoby
3. Významný	Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami	- Vážne fyzické zdravotné problémy, ktoré spôsobujú dlhodobú ujmu (napríklad zhoršenie zdravia kvôli nevhodnej starostlivosti, alebo z dôvodu prehliadania kontraindikácií) - zmena fyzickej integrity (napríklad napadnutie, nehoda doma, v práci, atď.)	- nevykompenzované odcudzenie peňazí - dlhodobé finančné ťažkosti (napríklad nutnosť vziať si pôžičku) - cielené, jedinečné a neopakovateľné, stratené príležitosti (napr. úver na bývanie, odmietnutie štúdia, stáže alebo zamestnania, zákaz skúšok) - zákaz držby bankových účtov - škody na majetku - Strata bývania - Strata zamestnania - Separácia alebo rozvod - finančná strata, ako dôsledok podvodu (napríklad po phishing pokusoch) - zabránenie cudziny - Strata údajov o	- Vážne psychologické zdravotné problémy (napr. depresie, fóbie) - Pocit narušenia súkromia s nezvratným poškodením - Pocit zraniteľnosti po predvolaní na súd - Pocit porušenia základných práv (napr. diskriminácia, sloboda prejavu) - obeť vydierania - kyberšikana a obťažovanie

			zákazníkoch	

Aké sú hlavné hrozby, ktoré by mohli viesť k riziku?

Podporné aktíva	Činnosť	Hrozby
Hardware	Neprimerané použitie	Uchovávanie osobných spisov; osobné použitie, atď.
Hardware	Poškodenie	Záplavy; požiar; vandalizmus; poškodenie z prirodzeného opotrebenia; porucha pamäťového zariadenia, atď.
Hardware	Strata	Krádež laptopu alebo mobilného telefónu; vyhodenie zariadenia alebo hardvéru atď.
Hardware	Modifikácia	Pridanie nekompatibilného hardvéru spôsobujúceho poruchy; odstránenie komponentov nevyhnutných pre správnu prevádzku systému, atď.
Hardware	Preťaženie	Úložná jednotka je plná; výpadok prúdu; preťaženie spracovateľskej kapacity; prehrievanie; nadmerné teploty, atď.
Software	Neprimerané použitie	Vymazanie údajov; používanie falšovaného alebo kopírovaného softvéru; chyby operátora, ktoré odstraňujú údaje, atď.; skenovanie obsahu; nezákonné krížové odkazovanie na údaje; zvýšenie právomocí; zmazanie používateľských ciest; posielanie nevyžiadanej pošty prostredníctvom emailového programu; zneužitie funkcií siete, atď.
Software	Poškodenie	Vymazanie bežiaceho spustiteľného alebo zdrojového kódu; logická bomba, atď.
Software	Strata	Neobnovenie licencie na softvér používaný na prístup k údajom, atď.
Software	Modifikácia	Uchovávanie osobných spisov; osobné použitie, atď.
Software	Preťaženie	Prekročenie veľkosti databázy; vkladanie údajov mimo normálneho rozsahu hodnôt, atď.
Počítačové pripojenia	Poškodenie	Preseknutie káblov, slabý wifi signál, atď.
Počítačové pripojenia	Strata	Krádež medených káblov, atď.
Počítačové pripojenia	Preťaženie	Zneužitie šírky pásma, neoprávnené sťahovanie, strata pripojenia na internet, atď.
Osoby	Poškodenie	Pracovný úraz; choroba z povolania; iné zranenie alebo choroba; smrť; neurologické, psychologické alebo psychické ochorenie, atď.
Osoby	Strata	Preloženie; skončenie pracovnej zmluvy, alebo prepustenie; prevzatie kontroly nad celou organizáciou alebo jej časťou, atď.
Osoby	Preťaženie	Vysoká pracovná záťaž, stres alebo negatívne zmeny pracovných podmienok; pridelenie zamestnancov na úlohy, ktoré presahujú ich schopnosti; slabé využívanie zručností, atď.
Písomnosti	Opotrebenie	Starnutie archívnych dokumentov, spálenie dokumentov počas požiaru, atď.
Písomnosti	Strata	Krádež dokumentov; strata dokumentov počas premiestňovania; vyhodenie, atď.
Písomnosti	Preťaženie	Postupné vymazávanie časom; úmyselné vymazanie častí dokumentu, atď.
Prenos písomností	Poškodenie	Ukončenie pracovného postupu v nadväznosti na reorganizáciu; doručenie pošty zastavené štrajkom, atď.
Prenos písomností	Strata	Eliminácia procesu v nadväznosti na reorganizáciu, atď.
Prenos písomností	Modifikácia	Zmena spôsobu odosielania pošty; reorganizácia kanálov na prenos písomností; zmena pracovného jazyka, atď.
Prenos písomností	Preťaženie	Preťaženie pošty; nadmerné overovacie procesy, atď.

Aké sú zdroje rizika?

Interné ľudské zdroje	zamestnanci, osoby v obdobnom pracovnoprávnom vzťahu, osoby na študentskej praxi
Externé ľudské zdroje	príjemcovia, oprávnené tretie strany, poskytovatelia služieb, hackeri, návštevy, bývalí zamestnanci, klienti, aktivisti, konkurencia, odborové organizácie, médiá, mimovládne organizácie, zločinecké organizácie, organizácie pod

	kontrolou iného štátu, teroristické organizácie, neďaleká priemyselná činnosť
Iné, ako ľudské zdroje	škodlivý kód neznámeho pôvodu (vírusy, červy, a pod.), prírodné katastrofy, epidémie, horľavé, korózne, alebo výbušné materiály, voda (vodné potrubia, kanalizácia)

Ktoré z identifikovaných opatrení prispievajú k riešeniu rizika?

Opatrenia podľa kapitoly 3.1

Ako odhadujete závažnosť rizika, hlavne podľa možných dopadov a plánovaných opatrení?

3. Významné:

Dotknuté osoby sa môžu stretnúť s významnými dôsledkami, ktoré by mali byť schopné prekonať, aj keď s vážnymi ťažkosťami.

V prípade straty osobných údajov sa odhadujú významné negatívne vplyvy na dotknutú osobu. Je to najmä z dôvodu systematického spracúvania citlivých osobných údajov týkajúcich sa zdravia, mentálnej úrovne, národnosti a iných citlivých údajov zraniteľných osôb (detí). Zo spracúvania môžu vyplynúť rozhodnutia s právnymi účinkami, alebo rozhodnutia s podobne závažnými účinkami pre dotknutú osobu.

Ako odhadujete pravdepodobnosť rizika, hlavne ak ide o hrozby, zdroje rizika a plánované opatrenia?

1. Zanedbateľná:

Uskutočnenie hrozby využitím vlastností podporných aktív sa javí ako nemožné pre vybrané zdroje rizík

Prevádzkovateľ je v súlade s požiadavkami novej legislatívy, identifikované hrozby by mali byť u prevádzkovateľa dostatočne pokryté, za predpokladu dodržiavania prijatých bezpečnostných opatrení. Pravdepodobnosť vzniku nelegitímneho prístupu k osobným údajom sa javí ako zanedbateľná, avšak úplná eliminácia nežiaducich udalostí nie je možná.

Hodnotenie: Prijaté

4. Akčný plán

Prehľad

Základné zásady	Nápravné opatrenia	Prijateľné opatrenia
Účely		X
Právne základy		X
Primeranosť osobných údajov		X
Správnosť osobných údajov		X
Minimalizácia uchovávania		X
Informovanosť dotknutých osôb		X
Získanie súhlasu		X
Právo na prístup a prenosnosť		X
Právo na opravu a vymazanie		X
Právo na obmedzenie spracúvania a namietať spracúvanie		X
Poverenie sprostredkovateľa		X
Prenos osobných údajov		X

Plánované alebo súčasné opatrenia	Nápravné opatrenia	Prijateľné opatrenia
Anonymizácia		X
Oddelenie osobných údajov		X
Logické riadenie prístupu		X
Vysledovateľnosť (logging)		X
Archivácia		X
Bezpečnosť písomností		X
Minimalizácia množstva osobných údajov		X
Operačná bezpečnosť		X
Kontrola škodlivého softvéru		X
Manažment pracovných staníc		X
Bezpečnosť webovej stránky		X
Zálohy		X
Údržba		X
Spracovanie zmlúv		X
Sieťová bezpečnosť		X
Kontrola fyzického prístupu		X
Monitoring sieťových aktivít		X
Bezpečnosť hardwaru		X
Vyhýbanie sa zdrojom rizika		X
Ochrana proti iným ako ľudským zdrojom rizika		X
Organizácia		X
Politika		X
Manažment bezpečnostných rizík		X
Integrácia ochrany súkromia v projektoch		X
Manažment porušení ochrany osobných údajov		X
Personálny manažment		X
Vzťahy s tretími stranami		X
Kontrolná činnosť		X
Šifrovanie		X

Riziká	Nápravné opatrenia	Prijateľné opatrenia
Nelegitímny prístup k osobným údajom		X
Neželaná modifikácia osobných údajov		X
Strata osobných údajov		X

Základné zásady

Nebol zaznamenaný žiadny akčný plán.

Plánované alebo súčasné opatrenia

Nebol zaznamenaný žiadny akčný plán.

Riziká

Nebol zaznamenaný žiadny akčný plán.

5. Mapovanie rizík

Vizualizácia umožňuje porovnať umiestnenie rizík pred a po prijatí nápravných opatrení.