Centrálny koordinačný orgán

Európska únia

Bezpečnostný manuál pre koncových používateľov a manažérov ITMS2014+

Verzia č. 1.0

Dátum *účinnosti* od: 10.07.2015

CENTRÁLNY KOORDINAČNÝ ORGÁN

Predkladá: Ing. Miloš Hason
riaditeľ odboru ITMS
Dátum:
Podpis:

Schválil: Ing. Alena Sabelová, PhD.
generálna riaditeľka SCKO
Dátum:
Podpis:

OBSAH

1 Úvod

1.1 Ciele

Cieľom dokumentu je definovať základné bezpečnostné pravidlá pre koncových používateľov, administrátorov CKO/CO/OA, administrátorov RO/SO, administrátorov DC a administrátorov IS.

Všetky bezpečnostné pravidlá sú prijaté s ohľadom na ochranu osobných údajov spracovaných v informačnom systéme osobných údajov ITMS2014+ v súlade so zákonom:

- č. 122/2013 Z. z. o ochrane osobných údajov a
- č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov.

1.2 Základné pojmy a skratky

Termín	Popis
Manažér ITMS2014+ CKO/CO/OA	manažér ITMS2014+ na CKO (ÚV SR) a manažér ITMS2014+ na CO/OA (MF SR).
Manažér ITMS2014+DC	manažér ITMS2014+ v DataCentre zodpovedný za vytváranie, zmenu a rušenie používateľských účtov.
Administrátor IS	databázový, systémový a aplikačný administrátor, zodpovedný za chod aplikácie, udržiavanie databázy, vykonávanie administrátorských zásahov a podporu pri riešení problémov používateľov.
Manažér ITMS2014+ RO/SO	manažér ITMS2014+ na RO/SO (rezorty zapojené do čerpania EŠIF a ich sprostredkovateľské orgány).
Blokovanie OÚ	je dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej ZOOÚ.
CPU	Centrum podpory používateľov v DataCentre
Dotknutá osoba	je každá fyzická osoba, ktorej sa osobné údaje týkajú.
IKT	Informačno-komunikačné technológie

Termín	Popis
Informačný systém osobných údajov (ďalej aj „IS OÚ“)	je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom osobných údajov sa na účely ZOOÚ rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania. Poznámka: IS OÚ je osobitne definovaný pojem na účely ZOOÚ, ktorý nie je možné stotožňovať s pojmom informačný systém používaný v oblasti IT; t.j. IS OÚ nemožno stotožňovať s prostriedkami na spracúvanie osobných údajov (hardvér, softvér), ale pri jeho identifikácii je potrebné upriamiť pozornosť na účel spracúvania osobných údajov. Každý účel spracúvania determinuje samostatný IS OÚ. IS OÚ nemusí byť nevyhnutne automatizovaný, t.j. prevádzkovaný pomocou technických a programových prostriedkov (hardvér, softvér), ale môže existovať len v papierovej (listinnej) forme. Príkladom IS OÚ je napríklad kartotéka, kniha návštev, agenda riadenia ľudských zdrojov.
Koncový používateľ / používateľ	osoby s aktívnym používateľským účtom v systéme ITMS2014+.
Oprávnená osoba	je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, na základe pokynu/poverenia.
Osobné údaje (OÚ)	sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
Poskytovanie OÚ	je odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.
Používateľ ITMS2014+	žiadatelia o prístup a používatelia neverejnej časti ITMS2014+.

Termín	Popis
Prevádzkovateľ	každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná; prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený, alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky (porovnaj § 4 ods. 2 písm. b) ZOOÚ).
Spracúvanie OÚ	je vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
Sprístupňovanie OÚ	je oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
Tretia strana	je každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, sprostredkovateľom alebo oprávnenou osobou.
Účel spracúvania OÚ	je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
ZOOÚ	Zákon č. 122/2013 Z. z. v znení neskorších zmien o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
Zverejňovanie OÚ	je publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovo-komunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

2 Základné princípy a pravidlá spracovania OÚ

Prevádzkovateľom IS OÚ v zmysle ZOOÚ sa rozumie každý orgán definovaný zákonom č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov (najmä CKO, CO, OA, RO a SO).

Táto kapitola sumarizuje princípy a pravidlá ochrany osobných údajov aplikovateľné pre prevádzkovateľov a oprávnené osoby prevádzkovateľov v rámci informačného systému ITMS2014+.

Každé závažné narušenie princípov alebo pravidiel spracovania OÚ môže viesť k disciplinárnemu konaniu, resp. k rozviazaniu pracovného pomeru a/alebo k začatiu priestupkového alebo trestného konania.

2.1 Princípy spracovania OÚ

Primeranosť

Získavať a spracúvať možno len také údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania podľa Zákonom stanovených podmienok so súhlasom dotknutej osoby (s ohľadom na výnimky zo ZOOÚ). OÚ získané osobitne pre viacero rôznych účelov nie je možné združovať.

Transparentnosť

Dotknuté osoby sú informované o účeloch spracúvania ich OÚ, o sprostredkovateľoch spracúvania a o okolnostiach spracúvania zabezpečujúcich bezpečnosť.

Možnosť voľby

Dotknuté osoby majú možnosť namietať proti spracúvaniu OÚ, ktoré je vykonávané nad rámec pôvodného účelu. Pre poskytnutie citlivých údajov tretej osobe na spracúvanie OÚ pre iný ako zamýšľaný účel musí byť daný súhlas dotknutej osoby. Ak sú OÚ spracúvané pre účely priameho marketingu, dotknutá osoba má možnosť namietať proti takémuto spracúvaniu.

Cezhraničný tok

V rámci úradu môžu byť OÚ prenášané mimo krajiny, v ktorej boli získané, vrátane krajín mimo EÚ, len na základe legitímneho dôvodu a v súlade s aplikovateľnou legislatívou. V týchto prípadoch sú implementované primerané bezpečnostné opatrenia a podľa potreby získaný dodatočný súhlas dotknutých osôb respektíve Úradu na ochranu OÚ (ďalej len „Úrad“), ak prenos OÚ smeruje do krajín nezabezpečujúcich primeranú ochranu OÚ.

2.2 Pravidlá spracovania OÚ

Každý kto spracúva osobné údaje v systéme ITMS2014+ sa riadi a dodržiava zásady ochrany osobných údajov, chráni osobné údaje pred možným zneužitím, poškodením alebo stratou a bráni prípadnému úniku osobných údajov.

2.2.1 Spracúvanie osobných údajov

Spracúvať osobné údaje môže len oprávnená osoba a len v rozsahu pridelených oprávnení. V rámci vykonávanej činnosti zodpovedá za dodržiavanie pravidiel

spracúvania osobných údajov určených týmto predpisom ako aj ostatnými predpismi vydanými CKO alebo prevádzkovateľom, ktorý oprávnenú osobu poveril.

Spracúvať možno len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania: „poskytovanie príspevku z európskych štrukturálnych a investičných fondov, kontrola a súvisiace činnosti“ (porovnaj § 47 ods. 1 zákona č. 292/2014 Z. z.).

2.2.2 Súhlas dotknutej osoby

Osobné údaje je možné spracúvať iba so súhlasom dotknutej osoby s výnimkou situácií uvedených nižšie.

Bez súhlasu dotknutej osoby je možné spracúvať osobné údaje len v prípadoch, ak:

- spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo na zavedenie predzmluvných vzťahov alebo opatrení na žiadosť dotknutej osoby,
- sa osobné údaje spracúvajú na základe osobitného zákona (napríklad v zmysle § 47 zákona č. 292/2014 Z. z.), ktorý ustanovuje zoznam osobných údajov, účel ich spracúvania a okruh dotknutých osôb,
- spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ktorá nemá spôsobilosť na právne úkony alebo je fyzicky nespôsobilá na vydanie súhlasu, a ak nemožno získať súhlas jej zákonného zástupcu,
- predmetom spracúvania sú výlučne titul, meno, priezvisko a adresa dotknutej osoby bez možnosti priradiť k nim ďalšie osobné údaje a ich využitie je určené výhradne pre potreby prevádzkovateľa v poštovom styku s dotknutou osobou a na evidenciu týchto údajov,
- spracúvajú sa už zverejnené osobné údaje, ktoré boli zverejnené v súlade so zákonom; v týchto prípadoch treba osobné údaje náležite označiť, a súčasne treba vedieť preukázať kde boli zákonne zverejnené,
- spracúvanie osobných údajov je nevyhnutné na splnenie dôležitej úlohy realizovanej vo verejnom záujme, alebo spracúvanie osobných údajov je nevyhnutné na ochranu zákonných práv a právom chránených záujmov prevádzkovateľa alebo tretej strany za predpokladu, že pri takomto spracúvaní osobných údajov Úrad a tretia strana rešpektuje základné práva a slobody dotknutej osoby, a svojím konaním neoprávnene nezasahuje do práva na ochranu jej osobnosti a súkromia.

2.2.3 Získavanie osobných údajov

Osobné údaje je možné od dotknutej osoby získavať iba spôsobom a postupom schváleným prevádzkovateľom a v súlade s jeho internými predpismi. Spravidla sú osobné údaje získavané prostredníctvom formulárov webovej aplikácie ITMS2014+.

Na požiadanie dotknutej osoby je oprávnená osoba zabezpečujúca získavanie osobných údajov povinná preukázať príslušnosť k prevádzkovateľovi.

Pri získavaní a spracúvaní osobných údajov dotknutých osôb sú osoby oprávnené spracúvať osobné údaje povinné dodržiavať nasledovné pravidlá:

- zabezpečiť dodržiavanie diskrétnosti v mieste získavania osobných údajov,
- zabezpečiť, aby do písomností, ktoré obsahujú osobné údaje, nemali možnosť nahliadnuť osoby, ktoré nie sú oprávnené spracúvať osobné údaje,
- overiť správnosť osobných údajov v súlade s definovanými pracovnými postupmi,
- telefonický prenos osobných údajov minimalizovať iba na nevyhnutné prípady a v minimálnom rozsahu,
- osoby oprávnené spracúvať osobné údaje nesmú získavať osobné údaje dotknutých osôb pod zámienkou iného účelu alebo inej činnosti.

2.2.4 Kopírovanie/skenovanie úradných dokladov

Kopírovanie/skenovanie úradných dokladov je možné iba po splnení niektorej z nižšie uvedených podmienok, iba s písomným súhlasom dotknutej osoby, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby (napríklad v zmysle § 47 ods. 6 zákona č. 292/2014 Z. z.).

Ak je to nevyhnutné, za získanie písomného súhlasu dotknutých osôb s kopírovaním/skenovaním úradného dokladu zodpovedá oprávnená osoba. Súhlas dotknutej osoby nesmie byť podmieňovaný hrozbou odmietnutia zmluvného vzťahu, služby, tovaru alebo povinnosti ustanovenej právnym prepisom.

Pri získavaní osobných údajov kopírovaním/skenovaním úradných dokladov je nevyhnutné zabezpečiť, aby boli získavané osobné údaje len v rozsahu zlučiteľnom s účelom spracúvania (to znamená, že všetky nepotrebné osobné údaje musia byť pred kopírovaním/skenovaním prekryté alebo po kopírovaní musí byť zabezpečené ich vymazanie/začiernenie tak, aby neboli čitateľné).

2.2.5 Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov

Zverejňovanie osobných údajov spracúvaných prevádzkovateľom je zakázané s výnimkou, ak je zverejňovanie osobných údajov vykonané v súlade s ustanoveniami zákona, ktorý ukladá povinnosť prevádzkovateľovi na ich zverejnenie (napríklad § 47 ods. 5 alebo § 48 ods. 1 zákona č. 292/2014 Z. z.).

Poskytovanie a sprístupňovanie osobných údajov tretím stranám môže byť realizované len na základe písomnej zmluvy alebo platného právneho predpisu (napríklad § 47 ods. 5 zákona č. 292/2014 Z. z.).

Poskytovanie alebo sprístupňovanie osobných údajov na základe osobitných zákonov musí byť vykonané v súlade s ustanoveniami príslušného zákona, resp. s požiadavkami organizácií, ktoré sú poverené spracúvaním osobných údajov (napr. Sociálna poisťovňa, miestne príslušný Daňový úrad, zdravotná poisťovňa a pod.).

2.2.6 Spracovanie osobných údajov sprostredkovateľom

Spracúvanie osobných údajov v mene prevádzkovateľa môže zabezpečovať aj sprostredkovateľ za podmienky, že:

- so sprostredkovateľom bude uzatvorená písomná zmluva alebo písomné poverenie v súlade so ZOOÚ,
- prevádzkovateľ zabezpečí, aby poverenie sprostredkovateľa spracúvaním osobných údajov bolo oznámené dotknutým osobám pri najbližšom kontakte s nimi, najneskôr však do troch mesiacov od poverenia sprostredkovateľa,
- sprostredkovateľ poskytuje záruky, pokiaľ ide o opatrenia v oblasti technickej, organizačnej a personálnej bezpečnosti a nie je dôvod domnievať sa, že poverením sprostredkovateľa dôjde k ohrozeniu práv a právom chránených záujmov dotknutých osôb.

Dohľad pri výbere sprostredkovateľa a vypracovanie návrhu zmluvy alebo písomného poverenia zabezpečí štatutár prevádzkovateľa, alebo ním poverený zamestnanec (napr. zodpovedná osoba za dohľad nad ochranou osobných údajov).

Každá zmluva, v ktorej je súčasťou plnenia aj spracúvanie osobných údajov inou zmluvnou stranou, musí byť pred podpisom odsúhlasená štatutárom prevádzkovateľa alebo ním splnomocnenou osobou (napr. zabezpečenie technickej prevádzky informačného systému obsahujúceho osobné údaje).

V prípade poverenia prevádzkovateľa spracúvaním osobných údajov v mene iného prevádzkovateľa sa ustanovenia tejto podkapitoly použijú v primeranom rozsahu. Prevádzkovateľ nesmie spracúvať osobné údaje v mene iného prevádzkovateľa, ak na takéto spracúvanie osobných údajov nebol poverený prostredníctvom písomnej zmluvy.

Prevádzkovatelia sú povinní s každým sprostredkovateľom uzatvoriť zmluvu ešte pred začatím spracúvania osobných údajov týmto sprostredkovateľom (najneskôr v deň začatia spracúvania) v súlade s požiadavkami ZOOÚ (porovnaj § 8 ods. 4 zákona č. 122/2013 Z. z. v znení neskorších zmien).

Zákonné náležitosti písomnej zmluvy medzi prevádzkovateľom a sprostredkovateľom sú nasledovné:

- údaje o zmluvných stranách ("identifikačné údaje"),
- titul, meno, priezvisko, dátum narodenia a adresu trvalého pobytu, ak ide o fyzickú osobu,
- názov, právnu formu, adresu sídla a identifikačné číslo, ak ide o právnickú osobu,
- obchodné meno, adresu miesta podnikania a identifikačné číslo, ak ide o fyzickú osobu – podnikateľa,
- deň, od ktorého je sprostredkovateľ oprávnený začať so spracúvaním osobných údajov v mene prevádzkovateľa,
- účel spracúvania osobných údajov,
- názov informačného systému,
- zoznam OÚ, ktoré sa budú spracúvať; zoznam OÚ možno nahradiť rozsahom osobných údajov podľa § 10 ods. 4,
- okruh dotknutých osôb,
- podmienky spracúvania osobných údajov vrátane zoznamu povolených operácií s osobnými údajmi,

- vyhlásenie prevádzkovateľa, že pri výbere sprostredkovateľa postupoval podľa odseku 2 prvej vety,
- súhlas prevádzkovateľa na spracúvanie OÚ sprostredkovateľom prostredníctvom inej osoby (ods. 5),
- dobu, na ktorú sa zmluva uzatvára,
- dátum uzatvorenia zmluvy a podpisy zmluvných strán.

2.2.7 Cezhraničný prenos osobných údajov

Pred uskutočnením cezhraničného prenosu osobných údajov je každý iniciátor prenosu povinný nechať odsúhlasiť podmienky cezhraničného prenosu štatutárovi prevádzkovateľa alebo ním poverenej osobe.

2.2.8 Kvalita spracúvania osobných údajov

Všetky osoby, ktoré vykonávajú spracúvanie osobných údajov sú povinné spracúvať iba správne (presné a aktuálne) osobné údaje. Osobný údaj sa považuje za správny, kým sa nepreukáže opak.

Nesprávne a neúplné osobné údaje musia byť blokované a bez zbytočného odkladu opravené alebo doplnené. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, musia byť zreteľne označené a bez zbytočného odkladu zlikvidované. Všetky tieto kroky oprávnené osoby konzultujú s osobou poverenou dohľadom nad spracovaním osobných údajov alebo administrátorom RO/SO.

Oprávnená osoba súčasne zaistí, aby informácie o zablokovaní, oprave, doplnení alebo likvidácii osobných údajov boli bez zbytočného odkladu odovzdané všetkým príjemcom.

2.2.9 Likvidácia osobných údajov

Osobné údaje je možné spracúvať iba po dobu, pokiaľ pretrváva účel ich spracovania. Po tejto dobe je každá oprávnená osoba povinná tieto osobné údaje bezodkladne zlikvidovať. Doby uchovávania jednotlivých údajov definujú interné riadiace akty prevádzkovateľa (napr. registratúrny plán), respektíve všeobecne záväzné právne predpisy.

Osobné údaje sa nezlikvidujú iba v prípadoch, ak osobitný zákon ustanovuje lehotu, ktorá neumožňuje osobné údaje zlikvidovať.

Ak nie sú inými internými predpismi prevádzkovateľa definované prísnejšie pravidlá na likvidáciu, musia byť osobné údaje likvidované minimálne vymazaním (prepísaním) alebo fyzickým zničením informačného média prekračujúcim možnosť obnovy informačného obsahu.

Pred odovzdaním pamäťových médií alebo zariadení obsahujúcich pamäťové médiá na údržbu, servis alebo výmenu externému subjektu, musí byť vykonaná identifikácia, či sa na pamäťovom médiu nenachádzajú osobné údaje. V prípade, ak sa na disku osobné údaje nachádzajú, musí byť pred odovzdaním média externému subjektu zabezpečená

bezpečná likvidácia osobných údajov z média alebo musí byť externému subjektu odovzdané zariadenie bez takéhoto média.

Každá osoba oprávnená spracúvať osobné údaje je povinná bezodkladne zlikvidovať tie osobné údaje, na ktoré dotknutá osoba uplatnila uznanú námietku v zmysle § 28 ZOOÚ. Požiadavku na likvidáciu osobných údajov je oprávnený zadať generálny riaditeľ, alebo ním poverený zamestnanec.

2.2.10 Poučenie oprávnených osôb

Štatutár prevádzkovateľa, alebo ním poverená osoba, zodpovedá za oboznámenie dotknutých osôb s právami a povinnosťami ustanovenými ZOOÚ, so zodpovednosťami za ich porušenie a s rozsahom oprávnení, popisom povolených činností a podmienkami spracúvania osobných údajov v podmienkach prevádzkovateľa.

Oprávnené osoby musia byť poučené v zmysle ZOOÚ a poverené na výkon činnosti ešte pred uskutočnením prvej operácie. Oprávnené osoby potvrdia vykonanie poučenia vlastnoručným podpisom na zázname: „Poučenie oprávnených osôb“ (formulár je možné nájsť na webovom sídle Úradu na ochranu osobných údajov).

V primeranom rozsahu musia byť s obsahom tohto bezpečnostného manuálu oboznámení aj zamestnanci externých subjektov, ktorí majú prístup k IS OÚ ITMS2014+. Oboznámenie týchto osôb a zmluvné zabezpečenie dodržiavania tejto smernice zaistia zamestnanci úradu, ktorí spoluprácu s externými subjektmi realizujú.

2.2.11 Ochrana práv dotknutých osôb

Na základe písomnej žiadosti má dotknutá osoba právo vyžadovať:

- potvrdenie, či sú alebo nie sú osobné údaje o nej spracúvané,
- informácie o zdroji, z ktorého boli získané jej osobné údaje na spracúvanie,
- zoznam jej osobných údajov, ktoré sú predmetom spracúvania,
- opravu alebo likvidáciu svojich nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
- likvidáciu jej osobných údajov, ktorých účel spracúvania sa skončil; ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže požiadať o ich vrátenie,
- likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona,
- blokovanie jej osobných údajov z dôvodu odvolania súhlasu pred uplynutím času jeho platnosti, ak úrad spracúva osobné údaje na základe súhlasu dotknutej osoby.

Na základe písomnej žiadosti má dotknutá osoba ďalej právo vyžadovať informácie o spracúvaní osobných údajov v informačnom systéme v rozsahu:

- identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol vymenovaný,
- identifikačné údaje sprostredkovateľa; to neplatí, ak prevádzkovateľ pri získavaní osobných údajov nepostupuje podľa § 8 ZOOÚ,

- účel spracúvania osobných údajov,
- zoznam osobných údajov alebo rozsah osobných údajov,
- doplňujúce informácie, ktoré sú s ohľadom na všetky okolnosti a podmienky spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov najmä v nasledujúcom rozsahu:

poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje; ak prevádzkovateľ získava osobné údaje dotknutej osoby na základe súhlasu dotknutej osoby, oznámi jej aj čas platnosti súhlasu, a ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z priamo vykonateľného právne záväzného aktu Európskej únie, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo zo zákona, Úrad oznámi dotknutej osobe právny základ, ktorý jej túto povinnosť ukladá, a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,

tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté,

okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,

formu zverejnenia, ak majú byť osobné údaje zverejnené,

tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov.

Informácie uvedené vyššie sú poskytované dotknutej osobe bezplatne (resp. za úhradu, ktorej výška nesmie prekročiť náklady spojené so zhotovením kópií, so zadovážením technických nosičov a s odoslaním informácií dotknutej osobe) najneskôr do 30 dní odo dňa prijatia písomnej žiadosti.

Dotknutá osoba na základe písomnej žiadosti má právo namietať voči:

- spracúvaniu jej osobných údajov, o ktorých predpokladá, že sú alebo budú spracúvané na účely priameho marketingu bez jej súhlasu, a žiadať ich likvidáciu,
- využívaniu osobných údajov v rozsahu titul, meno, priezvisko a adresa dotknutej osoby na účely priameho marketingu v poštovom styku,
- poskytovaniu osobných údajov v rozsahu titul, meno, priezvisko a adresa dotknutej osoby na účely priameho marketingu.

Uplatnenie práv dotknutých osôb vyplývajúcich zo ZOOÚ zabezpečuje zamestnanec poverený štatutárom prevádzkovateľa.

2.2.12 Incidenty týkajúce sa spracovania OÚ

Oprávnené osoby sú povinné informovať svojho priameho nadriadeného, resp. zodpovednú osobu alebo bezpečnostného zamestananca, ak zistia porušenie alebo nedodržanie princípov ochrany OÚ.

3 Základné princípy a pravidlá informačnej bezpečnosti

Táto kapitola sumarizuje princípy a pravidlá informačnej bezpečnosti aplikovateľné pre koncových používateľov, administrátorov IS a manažérov ITMS2014+, platné pre prostredie ITMS2014+.

Každé závažné narušenie princípov alebo pravidiel informačnej bezpečnosti (napr. úmyselné porušenie) môže viesť k disciplinárnemu konaniu a/alebo k začatiu priestupkového alebo trestného konania.

3.1 Princípy informačnej bezpečnosti

V tejto podkapitole sú uvedené všeobecne záväzné princípy informačnej bezpečnosti.

Dôvernosť

Pri spracúvaní dát v IS ITMS2014+ sú povinní tí, ktorí prichádzajú s nimi do styku, zachovávať o týchto údajoch mlčanlivosť. Údaje môžu zverejniť, poskytnúť a sprístupniť iba v súlade s internými predpismi, resp. po schválení prevádzkovateľom. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania dát a platí aj po zániku oprávnenia k prístupu k údajom. Zároveň sú aplikované primerané bezpečnostné opatrenia proti náhodnému, resp. úmyselnému neautorizovanému prístupu k údajom.

Integrita

Údaje sú počas celého životného cyklu uchovávané podľa okolností aktuálne, presne a konzistentne a sú chránené pred neautorizovanou alebo náhodnou zmenou. Sú aplikované primerané bezpečnostné opatrenia proti náhodnému, resp. úmyselnému narušeniu alebo modifikácii dát.

Dostupnosť

Používatelia s primeranými prístupovými právami majú prístup k údajom spracúvaných v ITMS2014+ v zmysle interných predpisov. Sú aplikované primerané bezpečnostné opatrenia proti náhodnej, resp. úmyselnej strate alebo zničeniu dát.

Nepopierateľnosť

Všetky úkony používateľov musia byť primerane zaznamenávané, aby bolo spätne dohľadateľné kto a kedy zmeny vykonal. Činnosť používateľov v IS je zaznamenávaná prostredníctvom auditných záznamov (logov) a vo vybraných prípadoch aj elektronickým podpisom, prípadne časovou pečiatkou. Použitie elektronického podpisu a časovej pečiatky vyplýva buď priamo z požiadaviek legislatívy (napr. zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov), alebo je to nevyhnutné pre zaručenie právnych následkov spojených s úkonom používateľa v ITMS2014+.

Minimálne právomoci

Rozsah prístupu k údajom musí byť v každom okamihu obmedzený na minimálnu možnú a zároveň plne postačujúcu mieru nevyhnutnú pre plnenie pracovných povinností používateľa.

Oddelenie právomocí

Špecifické role v matici prístupových práv (napr. audit a prevádzka) nesmú byť vzájomne kombinované, aby sa zamedzilo možnému vzniku konfliktu záujmov.

3.2 Pravidlá informačnej bezpečnosti

Používateľ sa riadi a dodržiava zásady bezpečnosti pri práci s informačným systémom, chráni informačný systém proti možným útokom, ktoré môžu narušiť jeho funkčnosť a bráni prípadnému úniku dôverných informácií.

Nasledujúce pravidlá sú záväzné najmä pre koncových používateľov, administrátorov IS a manažérov ITMS2014+.

3.2.1 Riadenie prístupových práv

Táto oblasť je v zodpovednosti manažérov ITMS2014+ DC a je podrobne upravená interným predpisom Datacentra: Manuál pre prístupové práva do ITMS2014+, vrátane procesu riadenia prístupových práv ako aj princípom oddelenia právomocí a procesom previerky prístupových práv.

V prípade straty, resp. zneužitia alebo podozrenia zo zneužitia bezpečnostných prvkov je používateľ povinný bezodkladne informovať o tejto skutočnosti na telefónnom čísle 0850 123 344 alebo elektronicky na adrese cpu@datacentrum.sk, a následne písomne na adresu Datacentrum, Cintorínska 5, 814 88 Bratislava.

3.2.2 Politika hesiel

Všetci používatelia musia dodržiavať nasledovné pravidlá politiky hesiel:

- heslá musia udržiavať v tajnosti;
- heslá nesmú byť zaznamenávané (napr. na papieri, v súboroch alebo v prenosných zariadeniach), s výnimkou ich bezpečného uloženia a v prípade, ak bol spôsob ich uloženia schválený;
- heslá sa musia zmeniť v prípade akéhokoľvek náznaku možného kompromitovania systému alebo hesla;
- heslo musí byť kvalitné, a to tak, aby:
  - bolo dobre zapamätateľné;
  - heslo musí byť zložené z malých a veľkých písmen, číslic a špeciálneho znaku (nealfanumerického);
  - heslo má mať minimálnu dĺžku 8 (osem) znakov, ak ide o bežný používateľský účet a 10 (desať) znakov, ak ide o privilegovaný účet;
  - nebolo založené na informáciách vzťahujúcich sa k osobe, ktoré môže ktokoľvek ďalší ľahko uhádnuť alebo získať, napríklad mená, telefónne čísla, dátumy narodenia a pod.;
  - nebolo zraniteľné pri použití slovníkových útokov (nemalo by sa skladať zo slov vyskytujúcich sa v slovníkoch);
  - neobsahovalo po sebe idúce rovnaké znaky a neobsahovalo iba číselné alebo iba písmenové skupiny.
- používatelia musia meniť heslá v pravidelných intervaloch alebo na základe počtu prihlásení (heslá pre privilegovaný prístup by sa mali meniť častejšie ako pre

štandardný používateľský prístup), vyhýbať sa opakovanému používaniu alebo opakovaniu starých hesiel;

- používatelia musia zmeniť dočasné heslá pri prvom prihlásení;
- používatelia nebudú zahŕňať heslá do žiadneho automatizovaného prihlasovacieho procesu, napríklad uloženie do makra alebo funkčné klávesy;
- používatelia nesmú zdieľať osobné používateľské heslá;
- používatelia nebudú používať rovnaké heslá pre súkromné a pracovné účely;
- používatelia sa môžu prihlasovať do informačného systému len pod svojím prístupovým menom (loginom).

3.2.3 Politika čistej obrazovky

Používateľ je povinný odhlásiť sa z informačného systému pri prerušení alebo ukončení práce, resp. je povinný uzamknúť svoj počítač (napr. pred opustením pracoviska).

3.2.4 Spracovanie údajov

Používatelia (žiadatelia a prijímatelia) v zmysle § 49 ods. 3 zákona č. 292/2014 Z. z. zodpovedajú za aktuálnosť, pravdivosť, úplnosť a správnosť nimi vložených údajov do ITMS2014+.

Používateľ je povinný kontrolovať údaje, ktoré vkladá do informačného systému. Kontrolované majú byť transakčné vstupy, vlastné dáta (napr. mená a adresy, telefónne čísla) a číselníky (napr. mestá, mestské časti). V prípade, ak zistí chybu v údajoch vložených do systému, pokiaľ je to možné, údaje zaktualizuje alebo o chybe informuje relevantné osoby (napr. CKO).

Používateľ nesmie bez primeraného dôvodu z IS sťahovať citlivé dáta (napr. osobné údaje) a ukladať ich na lokálnu pracovnú stanicu, ani ich posielať nechráneným kanálom (napr. email) alebo poskytovať/sprístupnovať tretím stranám.

3.2.5 Antivírová ochrana

Používateľ je povinný používať na svojej lokálnej stanici aktualizovaný antivírusový systém a nesmie ho bezdôvodne vypínať ani inak znefunkčniť.

Používateľ musí pristupovať k mailovým správam s obozretnosťou; neotvárať neznáme prílohy alebo prílohy od neznámych odosielateľov a nespúšťať internetové odkazy z emailových správ, ale odkaz manuálne skopírovať do prehliadača.

V prípade podozrenia na vírovú infekciu je povinný bezodkladne kontaktovať svojho správcu IT.

3.2.6 Riešenie incidentov a porúch

Používatelia informačného systému sú povinní zaznamenať a hlásiť akékoľvek bezpečnostné incidenty a slabiny, alebo podozrenia na bezpečnostné incidenty a slabiny v systémoch alebo službách.

Ak používateľ identifikuje akékoľvek problémy, poruchy alebo odchýlky od štandardnej prevádzky, je povinný bezodkladne o týchto problémoch informovať svojho správcu IT alebo CPU.

Niektoré príklady bezpečnostných udalostí a incidentov sú:

- strata služby, zariadenia alebo vybavenia;
- chybné fungovanie alebo preťaženie systému;
- ľudské chyby,
- nesúlad s politikami alebo smernicami;
- porušenie opatrení fyzickej bezpečnosti;
- nekontrolované zmeny systému;
- chybné fungovanie technického a programového vybavenia;
- porušenie prístupu.

3.2.7 Povedomie o informačnej bezpečnosti

Používateľ je povinný oboznamovať sa s bezpečnostnými princípmi a pravidlami ITMS2014+ a zúčastňovať sa školení koncových používateľov v oblasti informačnej bezpečnosti.

Používateľ je povinný zúčastňovať sa školení v oblasti informačnej bezpečnosti (o možnostiach sa môže informovať u svojho správcu IT). Používateľ si má udržiavať primerané povedomie o informačnej bezpečnosti a potenciálnych hrozbách. Používateľ by mal poznať:

- aktuálne odporúčania pre kvalitu hesiel (napr. odporúčanú minimálnu dĺžku hesla a komplexitu hesla, odporúčania ohľadom používania fráz miesto tradičných hesiel a pod.),
- aktuálne pravidlá informačnej bezpečnosti platné v jeho oranizácii,
- možné negatívne dopady vyplývajúce z úniku a prezradenia citlivých údajov,
- najčastejšie hrozby spojené s používaním sociálnych sietí (napr. Facebook),
- najčastejšie hrozby v oblasti škodlivého softvéru,
- najčastejšie scenáre sociálneho inžinierstva (napr. nevyžiadané maily/telefonáty požadujúce zadanie autentifikačných prostriedkov, podvodné webstránky navodzujúce dojem legitímnosti),
- stav aktualizácií operačného systému, internetového prehliadača, antivírového softvéru a ďalších kľúčových prvkov (napr. JAVA) lokálnej pracovnej stanice používateľa,
- komu a ako nahlasovať podozrenia na porušenie informačnej bezpečnosti.

3.2.8 Aktualizácia používateľských údajov

Každý používateľ je povinný bez zbytočného odkladu aktualizovať údaje vo svojom používateľskom účte.

3.3 Vybrané pravidlá informačnej bezpečnosti pre administrátorov IS

Nasledujúce pravidlá sú záväzné len pre administrátorov IS.

3.3.1 Riadenie prevádzkových záznamov

V systéme ITMS2014+ sa musia vytvárať prevádzkové záznamy s cieľom:

- spojiť udalosti v systéme ITMS2014+ s konaním používateľov a administrátorov IS;
- rekonštruovať udalosti v chronologickom slede;
- detegovať potenciálny prienik do systému;
- monitorovať systémové kapacity a prevádzkové parametre.

Za celý životný cyklus (nastavenie, monitorovanie, vyhodnocovanie, zálohovanie a likvidáciu) prevádzkových záznamov sú zodpovední administrátori IS. Rovnako sú zodpovední aj za nastavenie a konsolidovanie časových informácií (prostredníctvom NTP protokolu) naprieč infraštruktúrou ITMS2014+.

Prevádzkové záznamy musia byť chránené pred náhodnou alebo úmyselnou zmenou a pred zničením. Prístup k prevádzkovým záznamom musí byť obmedzený len pre administrátorov IS a ďalšie relevantné role (napr. audítor, vlastník systému a pod).

Pri nastavení rozsahu prevádzkových záznamov, ako aj doby ich archivácie, je potrebné okrem bezpečnostných požiadaviek prihliadať aj na dostupné kapacity monitorovacieho systému.Všetky systémy vytvárajúce prevádzkové záznamy musia mať primeranú diskovú kapacitu pre uchovávanie záznamov. Vhodné je, aby médium uchovávajúce záznamy neumožňovalo zmenu údajov, ale iba zápis a čítanie.

Prevádzkové záznamy musia byť pravidelne vyhodnocované (aspoň raz mesačne). Na vyhodnocovanie sa môže použiť automatizovaný nástroj (napr. SIEM). Takýto systém by mal vytvárať varovania v prípade neštandardných udalostí.

Prevádzkové záznamy musia byť taktiež pravidelne zálohované do geograficky odlišnej lokality a primerane dlho archivované.

Administrátori IS musia zabezpečiť, že v prípade krátkodobého špičkového zaťaženia systému nedôjde k prerušeniu tvorby záznamov.

Príklady prevádzkových záznamov a štandardizovaného formátu prevádzkových záznamov

Prevádzkové záznamy by mali zahŕňať transakcie alebo udalosti, ako napríklad:

- neúspešné prihlásenia,
- prihlásenia mimo bežného pracovného času (napr. 07:00 – 19:00),
- zamknutie účtov po presiahnutí povoleného počtu pokusov o prihlásenie,
- neobvyklú sieťovú aktivitu (skenovanie siete, prenos neobvykle veľkého objemu dát apod.),
- zmeny konfigurácie mimo bežnej údržby a bez formálneho záznamu,

- prístupy používateľov,
- eskalácia prístupových práv,
- neautorizované použitie zdrojov,
- neprivilegovaný prístup k súborom,
- prístup k samotným prevádzkovým záznamom,
- neobvyklé čerpanie systémových prostriedkov (napr. pamäť, CPU),
- vytvorenie/spustenie novej služby (procesu) v operačnom systéme,
- pokles kapacity systémových prostriedkov pod kritickú hranicu (napr. diskový priestor, pamäte a pod.),
- zlyhanie systémových procesov,
- vznik systémových chýb,
- atď.

Každý log by mal byť generovaný v štandardizovanom formáte (napr. podľa iniciatívy CEE) a mal by obsahovať:

- dátum a časovú počiatku,
- zdrojovú adresu alebo službu alebo ID používateľa (subjekt),
- cieľovú adresu alebo názov služby prípadne zdroja (objekt),
- ďalšie doplňujúce charakteristiky paketu alebo transakcie alebo udalosti.

3.3.2 Riadenie incidentov

Incidentom je udalosť, ktorá má alebo potenciálne môže mať negatívny dopad na prevádzku IS ITMS2014+. Administrátori IS v spolupráci s manažérom bezpečnosti sú zodpovední za monitorovanie, analýzu a riešenie incidentov. Preverené musia byť všetky podozrenia na incident.

Fázy riešenia bezpečnostných incidentov:

- kategorizácia identifikovaných alebo nahlásených udalostí,
- detekcia potenciálnych incidentov v prostredí IS ITMS2014+,
- návrh riešenia, odstránenie incidentu a obnova bežnej prevádzky,
- podrobná analýza incidentu a návrh opatrení.

Všetky incidenty musia byť evidované. Evidencia zahŕňa dátum a čas zistenia incidentu, jeho popis, eskaláciu, aktuálny stav a dátum zmeny stavov, riešenie a vyhodnotenie incidentu a návrh opatrení, ako aj dátum a čas uzavretia incidentu. Riadenie incidentov by malo byť podporené automatizovaným nástrojom (napr. Service desk). Každý incident musí mať priradeného vlastníka.

Rovnako musia byť všetky incidenty klasifikované podľa veľkosti možného negatívneho dopadu, respektíve rizík spojených s incidentom na škále:

- nezávažný – negatívny dopad na ITMS2014+ a údaje v ňom uložené (je zanedbateľný),
- závažný – negatívny dopad má významný vplyv na funkčnosť IS alebo dostupnosť, dôvernosť alebo integritu údajov v ňom,
- kritický – negatívny dopad môže spôsobiť úplnú nedostupnosť IS alebo kompromitáciu údajov v IS (prezradenie/zmenu/stratu dát).

Základnú podporu pre používateľov Centrum podpory užívateľov. V prípade ak nedokážu príčinu incidentu a jeho následky odstrániť v primeranom čase, musia incident bezodkladne eskalovať na príslušného administrátora (databázový, systémový alebo aplikačný) alebo poskytovateľa podpory IS.

V prípade opakovania incidentu musí byť preklasifikovaný na problém a musí byť prešetrená príčina jeho opakovaného vzniku; ak je to nevyhnutné v spolupráci s poskytovateľom podpory alebo relevantným dodávateľom. Rovnako musí byť priradené vlastníctvo problému.

Minimálne raz za rok by malo dôjsť k revízii postupu identifikácie incidentov v informačnom systéme a jeho okolí, predovšetkým v prípade nízkeho počtu identifikovaných incidentov respektíve ak všetky incidenty sú klasifikované ako nezávažné.

Administrátori IS by mali pravidelne vyhodnocovať štatistické informácia ako napríklad:

- celkový počet incidentov a problémov (z toho otvorených a uzatvorených),
- progres v riešení incidentov a problémov,
- eskalované incidenty a pod.

Príklady incidentov, ich realizácie a prejavov v IKT prostredí

Príkladom incidentu je:

- neúspešný pokus o prihlásenie sa do systému (zvlášť opakovaný),
- preniknutie útočníka do systému,
- odopretie služby (anglicky Denial of service, DoS), prípadne špeciálny typ distribuovaného odopretia služby, kedy je útok realizovaný z mnohých IP adries (Distributed DoS, DDoS),
- prítomnosť škodlivého kódu,
- poškodenie IKT prírodným živlom,
- zahltenie lokálnej siete nesprávne nakonfigurovaným sieťovým zariadením,
- zlyhanie aplikácie kvôli chybe v kóde aplikácie,
- poškodenie/krádež komponentov IKT.

Príklady spôsobu realizácie útoku zahŕňajú:

- napadnutie samotnej aplikácie a zneužitie jej zraniteľností,

- použitie techník sociálneho inžinierstva, alebo nainštalovania škodlivého kódu na konkrétne pracovné stanice (odchytávanie stlačených kláves, odpočúvanie, snímanie obrazu) kvôli získaniu cenných informácií,
- priame zneužitie privilegovaného prístupu iných používateľov systému, operátorov, alebo administrátorov IS,
- použitie slovníkových útokov na slabé heslá v informačnom systéme a následná eskalácia privilégií,
- násilné činy vlámania, vydierania a krádeže pre získanie prístupu k inkriminovanému systému, alebo jeho dátam.

Príklady prejavu incidentov v IKT prostredí sú nasledovné:

- úplnou nefunkčnosťou systému – hardvérový komponent, alebo informačný systém nereaguje, alebo nie je prístupný,
- zmeneným obsahom webovej stránky – pôvodný obsah webovej stránky bol zmenený kvôli chybe v systéme, alebo úmyselne prepísaný útočníkom,
- neobvyklou sieťovou aktivitou – dajú sa pozorovať určité anomálie oproti štandardnej prevádzke, nezodpovedajúca frekvencia činností používateľov, alebo podozrivé druhy činností,
- neobvyklou záťažou systému – veľké preťaženia systému, ktoré vedú k odopretiu dostupnosti služby,
- podozrivými záznamami – ak prevádzkové záznamy nie sú konzistentné so skutočným správaním systému, nedá sa vylúčiť riziko, že systém je skompromitovaný a útočník tieto záznamy pozmenil.