UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE INÝCH REGULÁCIÍ

Meno a priezvisko

XX.XX.XXXX

OBSAH

1) Kybernetická bezpečnosť v kontexte iných regulácií – všeobecne
2) Ochrana osobných údajov
3) Ochrana súkromia v elektronických komunikáciách
4) Regulácia platobných služieb vo finančnom sektore
5) Elektronické služby verejnej správy a elektronické podpisovanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE INÝCH REGULÁCIÍ

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE INÝCH REGULÁCIÍ

- právna úprava kybernetickej bezpečnosti nie je „osamotená“
- úzke prepojenie s reguláciou iných, súvisiacich oblastí, najmä:
  a) ochrana osobných údajov
  b) ochrana súkromia v elektronických komunikáciách
  c) regulácia platobných služieb vo finančnom sektore
  d) elektronické služby verejnej správy a elektronické podpisovanie

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ A OCHRANA OSOBNÝCH ÚDAJOV

OCHRANA OSOBNÝCH ÚDAJOV AKO ZÁKLADNÉ PRÁVO KAŽDÉHO

- **Článok 8 Charty základných práv EÚ:**
  1. *Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.*
  2. *Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.*
  3. *Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.*
- **Článok 19 ods. 3 Ústavy Slovenskej republiky:** *Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.*

PRÁVNA ÚPRAVA

Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.4.2016 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov a o zrušení Smernice 95/46/ES (všeobecné nariadenie o ochrane osobných údajov)

PRÁVNA ÚPRAVA

Zákon č. 428/2002 Z. z. o ochrane osobných údajov

Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

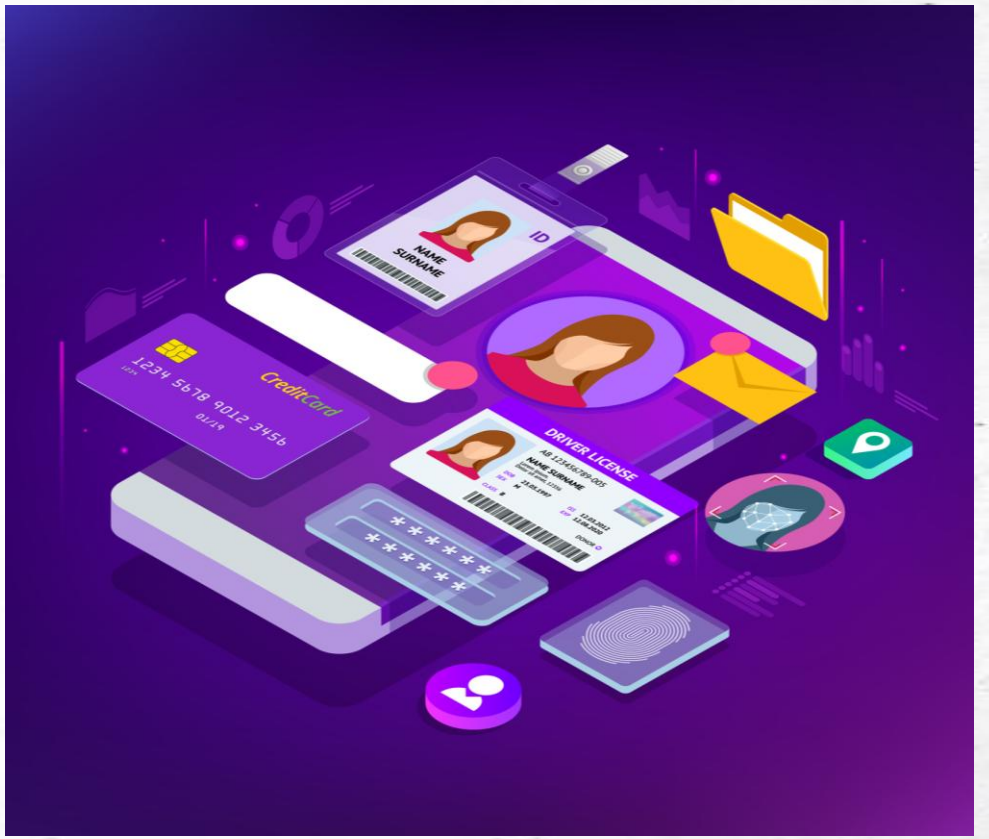
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

PÔSOBNOSŤ GDPR

- Čl. 2 ods. 1: Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.
  - Čl. 4 ods. 6: „informačný systém“ je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe;

ROZSAH OCHRANY

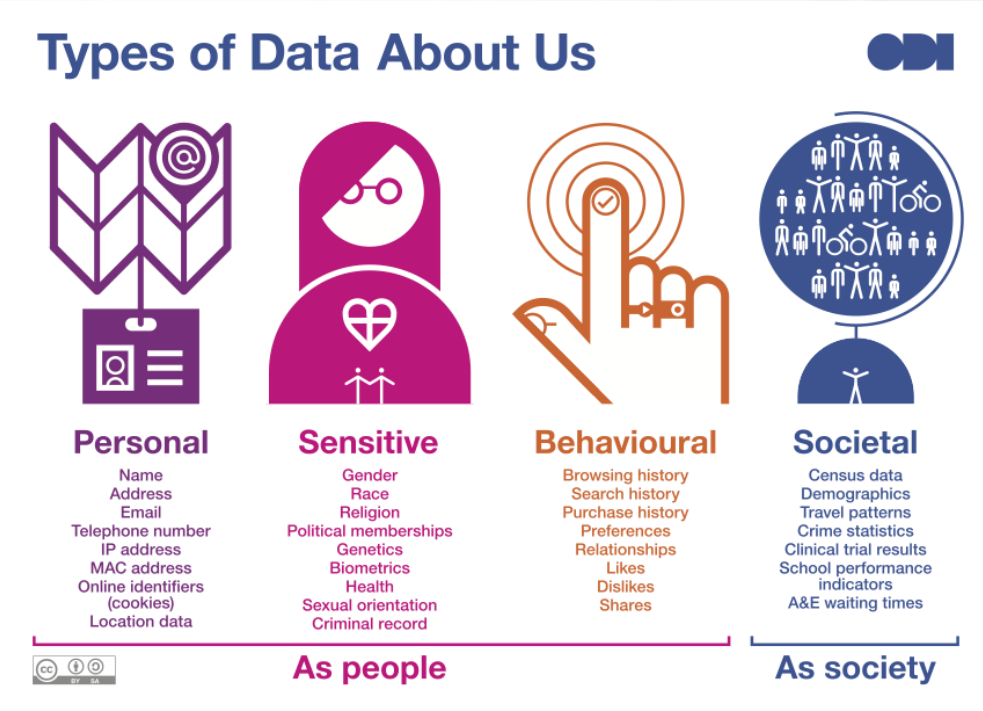
- článok 4 ods. 1 GDPR: „**osobné údaje sú akékoľvek údaje týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby**“
- rozlišujeme:
  - **a)** **identifikovanú osobu –** jednoznačne vieme určiť, o koho ide, na základe určitého údaju;
  - **b)** **identifikovateľnú osobu –** osoba, ktorú **možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor**, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, **alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre** fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu **identitu tejto fyzickej osoby**



ROZSAH OCHRANY

- potrebné vziať do úvahy všetky prostriedky, pri ktorých existuje **primeraná pravdepodobnosť, že ich možno využiť na priamu alebo nepriamu identifikáciu fyzickej osoby**
- na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali **zohľadniť všetky objektívne faktory, ako sú:**

  →**náklady a čas potrebný na identifikáciu** so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na **technologický vývoj**



ROZSAH OCHRANY

Osobitné kategórie osobných údajov

- Čl. 9 ods. 1 GDPR: **Zakazuje sa** spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

ROZSAH OCHRANY

- základné právo na ochranu osobných údajov patrí **výlučne fyzickým osobám, a to bez ohľadu na ich štátnu príslušnosť alebo miesto bydliska, ak sa nachádzajú v EÚ**
- **ochrana sa neposkytuje právnickým osobám,** napr. vo vzťahu k podnikom a ich obchodnému menu, právnej forme a kontaktným údajom
- ochrana sa neposkytuje ani osobným údajom zosnulých osôb

SPRACÚVANIE OSOBNÝCH ÚDAJOV

- **spracúvanie osobných údajov** je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;
- **Rozhodnutie SD EÚ vo veci C-101/01 Göta hovrätt (Švédsko) vs. Bodil Lindqvist**
  - operácia, ktorou sa odkazuje na internetovej stránke na rôzne osoby a ktorou sa tieto osoby identifikujú buď prostredníctvom ich mena, alebo iným spôsobom, napríklad prostredníctvom ich telefónneho čísla alebo informácií o ich pracovných podmienkach a o ich záľubách, predstavuje úplne alebo čiastočne **automatizované spracovanie osobných údajov**
  - údaj o tom, že si určitá osoba poranila nohu a je čiastočne práceneschopná, je osobným údajom
- **Najvyšší súd SR sp. Zn. 1 Sžo 410/2009 -** prevádzkovateľ sa nemôže z povinnosti zlikvidovať osobné údaje po splnení účelu spracovania vyviniť poukázaním na skutočnosť, že osobné údaje nie je možné zlikvidovať z dôvodu chýbajúcich technických kapacít prevádzkovateľa

POVINNÝ SUBJEKT

- **prevádzkovateľ** = fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý **sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov**; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu
- **sprostredkovateľ** = fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý **spracúva osobné údaje v mene prevádzkovateľa**

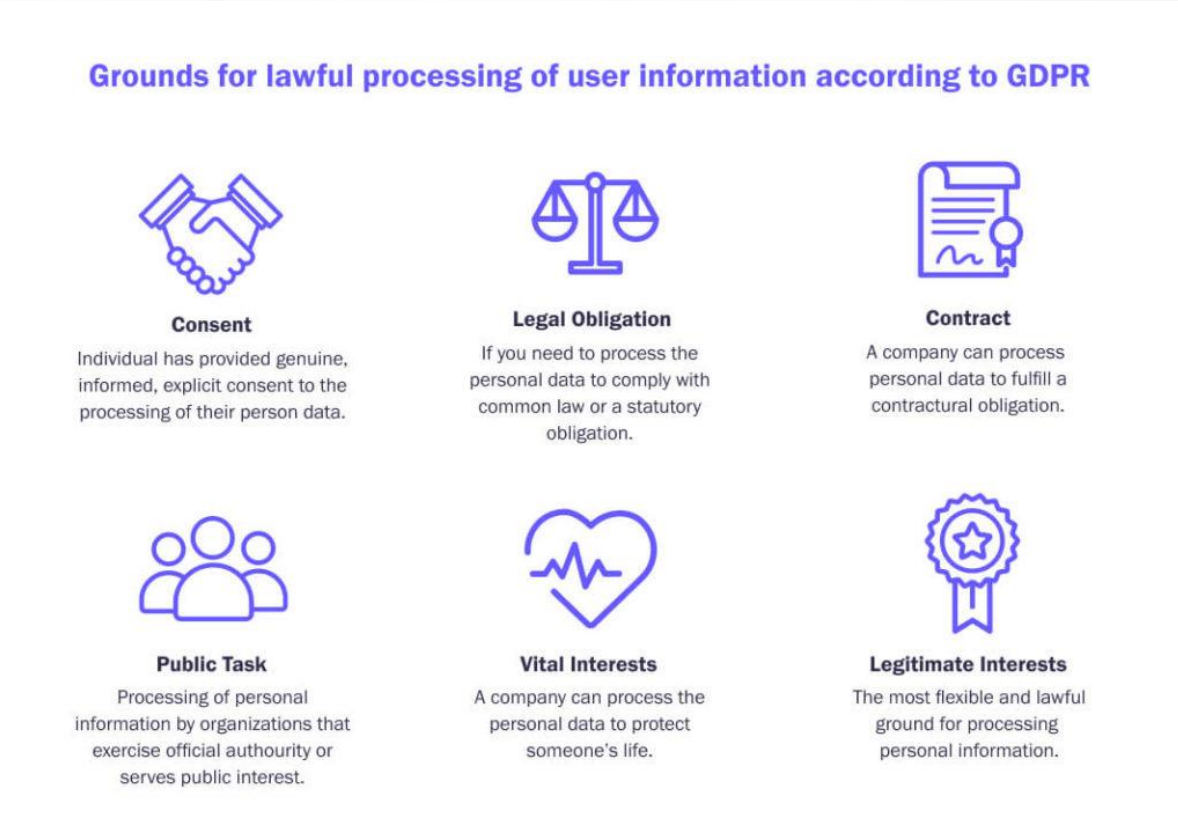
ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

1) Zásada zákonnosti
2) Zásada transparentnosti
3) Zásada obmedzenia účelu
4) Zásada minimalizácie osobných údajov
5) Zásada správnosti
6) Zásada minimalizácie uchovávania
7) Zásada integrity a dôvernosti
8) Zásada zodpovednosti

ZÁSADA ZÁKONNOSTI

§ 6: Osobné údaje možno spracúvať len **zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.**

- zákonnosť je daná, ak je spracúvanie založené na niektorom **z taxatívne vymedzených právnych základov (§ 13 ods. 1 ZOOÚ)**



ZÁSADA ZÁKONNOSTI – PRÍKLADY PORUŠENÍ

- uverejňovanie na webovom sídle prevádzkovateľa (v ozname Rozhodnutie Inšpektorátu práce BA o uložení pokuty) mena, priezviska a dátumu narodenia dotknutej osoby bez právneho základu (00841/2020-Os-15)
- uverejňovanie na svojom webovom sídle v dokumentoch Uznesenie zo zasadnutia obecného zastupiteľstva a Zápisnica zo zasadnutia obecného zastupiteľstva OÚ, a to dátumov narodenia dotknutých osôb bez právneho základu (01363/2020-Os-8)
- v registračnom formulári za člena Baťa klubu vyjadruje dotknutá osoba jedným svojím súhlasom na účel "marketing a komunikácia" zároveň súhlas aj so spracúvaním svojich OÚ v rozsahu uvedenom v dokumente "Zásady spracovania OÚ", čo nemožno považovať za slobodne poskytnutý súhlas dotknutej osoby, uvedené zistenie sa vzťahuje aj na vyjadrenie súhlasu v tomto registračnom formulári na účel členstva v Baťa klube v čase kontroly a na účel "Profilovanie" (00006/2021-Os-2)
- používaním emailovej schránky dotknutej osoby v období po ukončení pracovného pomeru dotknutej osoby bez právneho základu (00009/2020-Os-11)

ZÁSADA TRANSPARENTNOSTI

- Čl. 5 ods. 1 písm. a) GDPR: „Osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo **a transparentne vo vzťahu k dotknutej osobe** („zákonnosť, spravodlivosť a **transparentnosť**)
- Čl. 12 ods. 1 GDPR: Prevádzkovateľ prijme vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky informácie uvedené v článkoch 13 a 14 a všetky oznámenia podľa článkov 15 až 22 a článku 34, ktoré sa týkajú spracúvania, a to v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a to najmä v prípade informácií určených osobitne dieťaťu. Informácie sa poskytujú písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami. Ak o to požiadala dotknutá osoba, informácie sa môžu poskytnúť ústne za predpokladu, že sa preukázala totožnosť dotknutej osoby iným spôsobom.

ZÁSADA TRANSPARENTNOSTI – PRÍKLADY PORUŠENÍ

- prevádzkovateľ uvádza na svojom webovom sídle odkaz na neúčinný právny predpis (pri kamerovom systéme odkazuje na zákon č. 122/2013 Z. Z. o ochrane OÚ) (00921/2022-Os-8)
- v súvislosti s poskytovaním informácií prostredníctvom webového sídla neposkytuje dotknutým osobám informácie o účele a právnom základe spracúvania OÚ, ktorým je poskytovanie zdravotnej starostlivosti ako základnej činnosti zdravotníckeho zariadenia, a že spracúvanie OÚ vyplýva poskytovateľovi zdravotnej starostlivosti z osobitného zákona (01077/2021-Os-7)
- poskytoval dotknutým osobám nesprávne informácie o príjemcovi OÚ podľa čl. 13 ods. 1 písm. e), nakoľko príjemcom podľa čl. 4 ods. 9 GDPR nemôže byť sám prevádzkovateľ (01080/2021-Os-2)
- prevádzkovateľ ad 2) na webovej stránke v súvislosti s odvolaním súhlasu so spracúvaním OÚ dotknutých osôb na účel zasielania obchodných oznámení v súvislosti s uplatňovaním práv dotknutých osôb súvisiacich s účelom zasielania obchodných oznámení odkazovala na nefunkčnú emailovú adresu, čím postupovala voči dotknutým osobám netransparentne (00049/2022-Os-14)

ZÁSADA OBMEDZENIA ÚČELU

§ 7: Osobné údaje sa môžu získavať len **na konkrétne určený, výslovne uvedený a oprávnený účel** a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom[8]) a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa ***§ 78 ods. 8***, sa nepovažuje za nezlučiteľné s pôvodným účelom.

ZÁSADA OBMEDZENIA ÚČELU – PRÍKLADY PORUŠENÍ

- OÚ, ktoré prevádzkovateľ pôvodne získal na základe osobitných práv. predpisov a za zákonom stanoveným účelom, využil aj na účel zverejňovania v občasníku Smolenické noviny, čím prekročil zákonom stanovený účel spracúvania OÚ (01080/2021-Os-2)
- záznam z kamerového systému inštalovaného v Múzeu Bojnice obsahujúci OÚ navrhovateľky (podobizeň a informáciu o jej pohybe v danom čase a priestore) nevyužil výlučne za deklarovaným účelom, ale aj za účelom plnenia kontroly pracovných povinností navrhovateľky (0101/2021-Os-7)
- uskutočnil spracovateľskú operáciu zverejnenia OÚ 16 dotknutých osôb v rozsahu: titul, meno a priezvisko, ktoré pôvodne získal na základe zákona č. 53/1998 Z. z. o hlásení pobytu občanov SR a registri obyvateľov SR z evidencie obyvateľov a tieto využil na účel zverejňovania v obecných novinách a na svojom webovom sídle (00170/2020-Os-9)

ZÁSADA MINIMALIZÁCIE

§ 8: Spracúvané osobné údaje musia byť **primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú**.

- menej je viac!

ZÁSADA MINIMALIZÁCIE – PRÍKLADY PORUŠENÍ

- porušenie zásady minimalizácie vzhľadom na rozsah OÚ, ktoré vyžaduje od dotknutých osôb pri vybavovaní žiadosti na poskytnutie potvrdenia, či o nich OÚ spracúva, resp. pri poskytnutí kópie takýchto OÚ (00090-2021-Os-17)
- porušil zásadu minimalizácie údajov nakoľko spracúval pr. kamier monitorujúcich okolie budov prevádzkovateľa OÚ v neprimerane veľkom rozsahu vzhľadom na stanovený účel spracúvania (00091/2020-Os-5)
- pri vybavovaní žiadosti navrhovateľa vyžadoval na overenie jeho totožnosti údaje, ktoré neboli nevyhnutné na vybavenie žiadosti dotknutej osoby (00093/2022-Os-4)

ZÁSADA MINIMALIZÁCIE UCHOVÁVANIA

§ 10: Osobné údaje musia byť **uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú**; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu[8]) a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa ***§ 78 ods. 8***.

ZÁSADA MINIMALIZÁCIE UCHOVÁVANIA – PRÍKLADY PORUŠENÍ

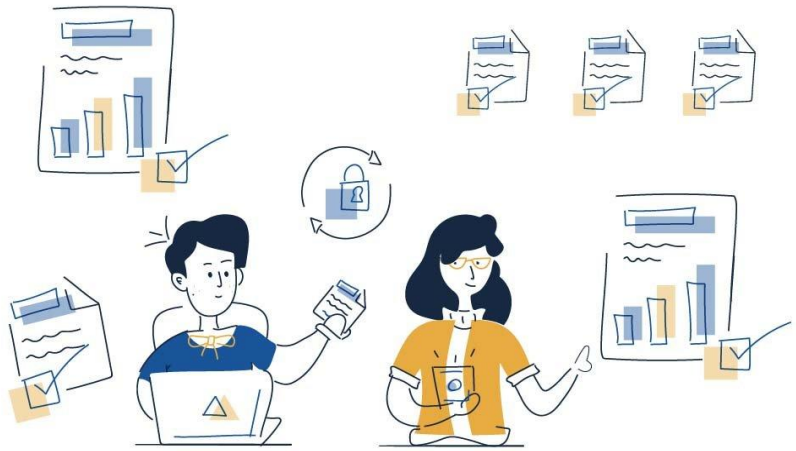
- prevádzkovateľ uchováva záznamy z kamerového systému nad časový rozsah nevyhnutný pre splnenie účelu spracúvania (12-13 dní) (00136/2021-Os-1)
- prevádzkovateľ Úradu nepreukázal nevyhnutnosť spracúvania pracovného emailu navrhovateľa pod dobu 10 mesiacov od skončenia pracovného pomeru s ním (00210/2021-Os-6)
- prevádzkovateľ uchovával poistnú dokumentáciu klientov v elektronickej podobe najmenej 15 rokov od skončenia zmluvného vzťahu s dotknutou osobou, pričom táto nebola nevyhnutná na dosiahnutie takto stanoveného účelu (0570/2022-Os-7)

ZÁSADA SPRÁVNOSTI

§ 9: Spracúvané osobné údaje musia byť **správne a podľa potreby aktualizované**; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

ZÁSADA ZODPOVEDNOSTI

§ 12: Prevádzkovateľ je zodpovedný **za dodržiavanie základných zásad spracúvania osobných údajov,** za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.



ZÁSADA ZODPOVEDNOSTI – PRÍKLADY PORUŠENÍ

- vo vzťahu k spracovateľským operáciám, ktoré súvisia so spracúvaním lokalizačných údajov cca 600 000 dotknutých osôb (účastníkov) nepreukázal vykonanie posúdenia vplyvu na ochranu OÚ podľa čl. 35 GDPR a nepreukázal splnenie povinnosti viesť v záznamoch o spracovateľských činnostiach účel "telefónny zoznam", ktorý mu vyplýva z § 50 ods. 2 písm. c) zákona č. 351/2011 Z. z. o elektronických komunikáciách (00182/2022-Os-9)
- spracúvanie vo veľkom rozsahu osobitnej kategórie OÚ podľa čl. 9 ods. 1 GDPR bez posúdenia vplyvu na ochranu OÚ podľa čl. 35 ods. 3 písm. a) GDPR a bez preukázania prijatia primeraných technických a organizačných opatrení podľa čl. 32 GDPR (00331/2022-Os-14)
- prevádzkovateľ nepreukázal súlad spracúvania so zásadou integrity a dôvernosti v zmysle čl. 5 ods. 1 písm. f) Nariadenia, keď v súvislosti so spracúvaním biometrických údajov nepredložil posúdenie vplyvu na ochranu osobných údajov (00387/2022-Os-3)

ZÁSADA INTEGRITY A DÔVERNOSTI

§ 11: Osobné údaje musia byť spracúvané **spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov** vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.

ZÁSADA INTEGRITY A DÔVERNOSTI – PRÍKLADY PORUŠENÍ

- nedôsledná anonymizácia OÚ obsiahnutých v zmluve, v dôsledku čoho došlo k zverejneniu OÚ v rozsahu meno, priezvisko, adresa, dátum narodenia, rodné číslo a úradne overený podpis (00136/2022-Os-7)
- sprostredkovateľ zaslal email obsahujúci OÚ dotknutej osoby v rozsahu meno, priezvisko, dátum narodenia, adresa, telefónne číslo a číslo poistnej zmluvy mobilného zariadenia na emailovú adresu bez toho, aby boli uvedené OÚ v rámci zaslaného emailu zabezpečené heslom, čím bez právneho základu sprístupnil OÚ inej osobe (00268/2022-Os-5)
- prevádzkovateľ pri likvidácii OÚ dotknutých osôb na listinných dokumentoch (napr. fotokópie zmlúv o pôžičke, úradné doklady ako občiansky preukaz, rodný list, cestovný pas) pri rušení jeho predajne a odvoze odpadu do zberného dvora došlo k neoprávnenému spracúvaniu a prístupu, čím bola porušená bezpečnosť spracúvania OÚ (00320/2019-Os-19)
- OÚ dotknutých osôb - zamestnancov prevádzkovateľa (identifikačné a kontaktné pracovné údaje, najmä meno, priezvisko, email, telefónne číslo prípadne pracovná pozícia) boli v dôsledku kybernetického útoku cez phishingový email neoprávnene sprístupnené tretej osobe, ktorá následne rozposlala phishingový email na 4500 emailov interných zamestnancov (00742/2020-Os-5)

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

Čl. 32 GDPR: Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

a) pseudonymizáciu a šifrovanie osobných údajov;

b) schopnosť zabezpečiť trvalú **dôvernosť, integritu, dostupnosť a odolnosť** systémov spracúvania a služieb;

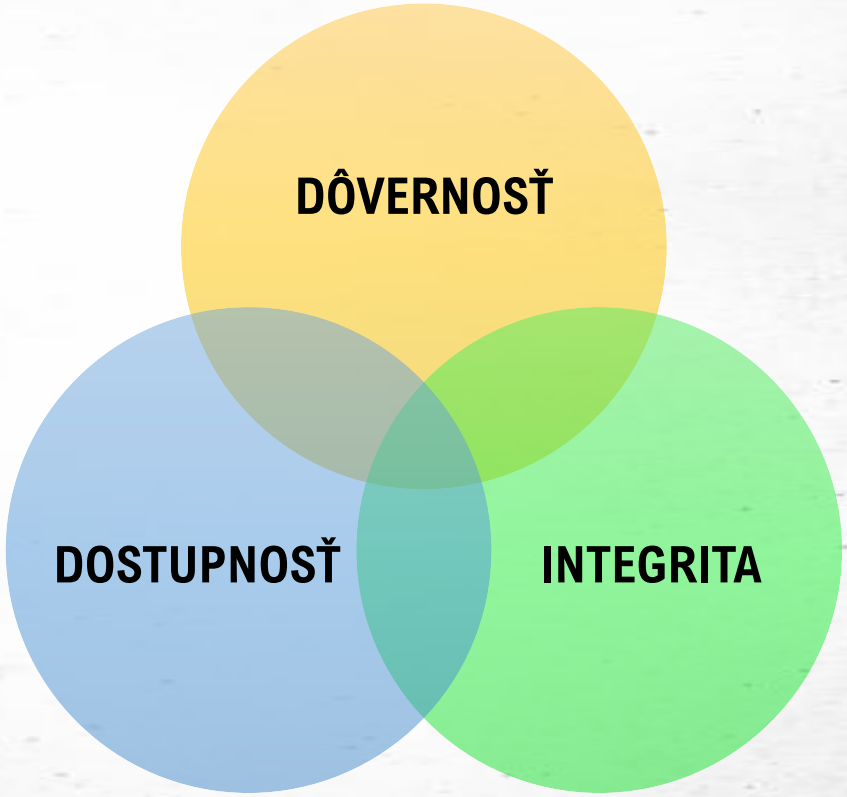
c) schopnosť včas **obnoviť dostupnosť osobných údajov** a prístup k nim v prípade fyzického alebo technického incidentu;

d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

Informačná bezpečnosť:

- **Dôvernosť -** informácie prístupné len osobám, ktoré určíme
- **Integrita -** informácie sú úplné a neboli nevedomky upravované
- **Dostupnosť -** informácie prístupné na požiadanie týchto osôb v tom čase



BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

- prevádzkovateľ je zodpovedný za dodržanie zásad a musí vedieť tento **súlad preukázať** („zodpovednosť“) (čl. 5 ods. 2 GDPR)
- s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme **vhodné technické a organizačné opatrenia**, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením (čl. 24 ods. 1 GDPR)
- v prípade porušenia ochrany osobných údajov **prevádzkovateľ bez zbytočného odkladu** a podľa možnosti najneskôr **do 72 hodín** po tom, čo sa o tejto skutočnosti dozvedel, oznámi **porušenie ochrany osobných údajov** dozornému orgánu ... Dotknutej osobe (čl. 33 ods. 1 a čl. 34 ods. 1 GDPR)

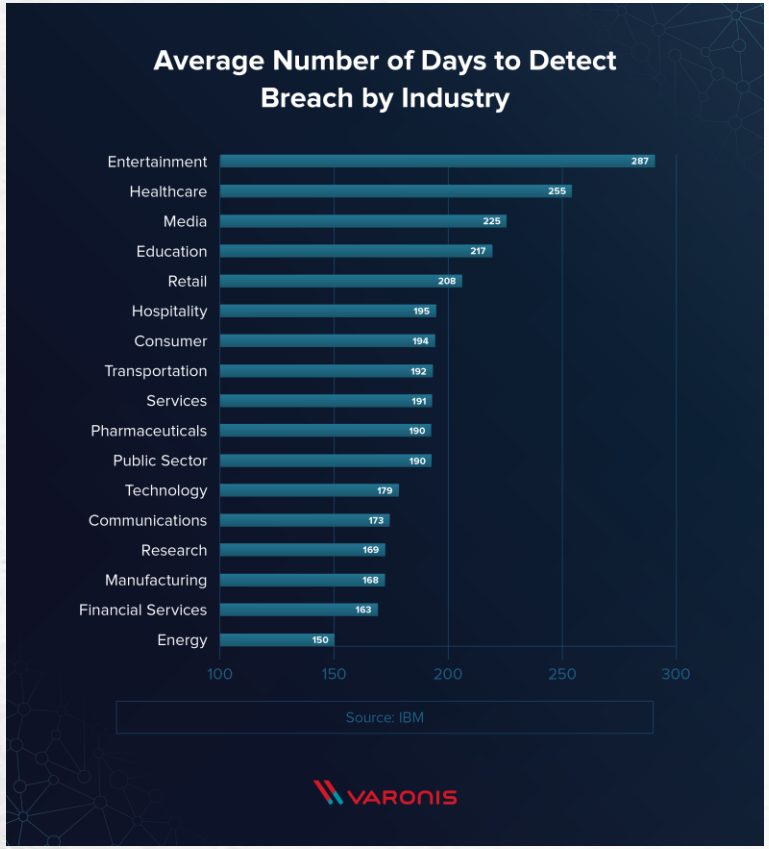
BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

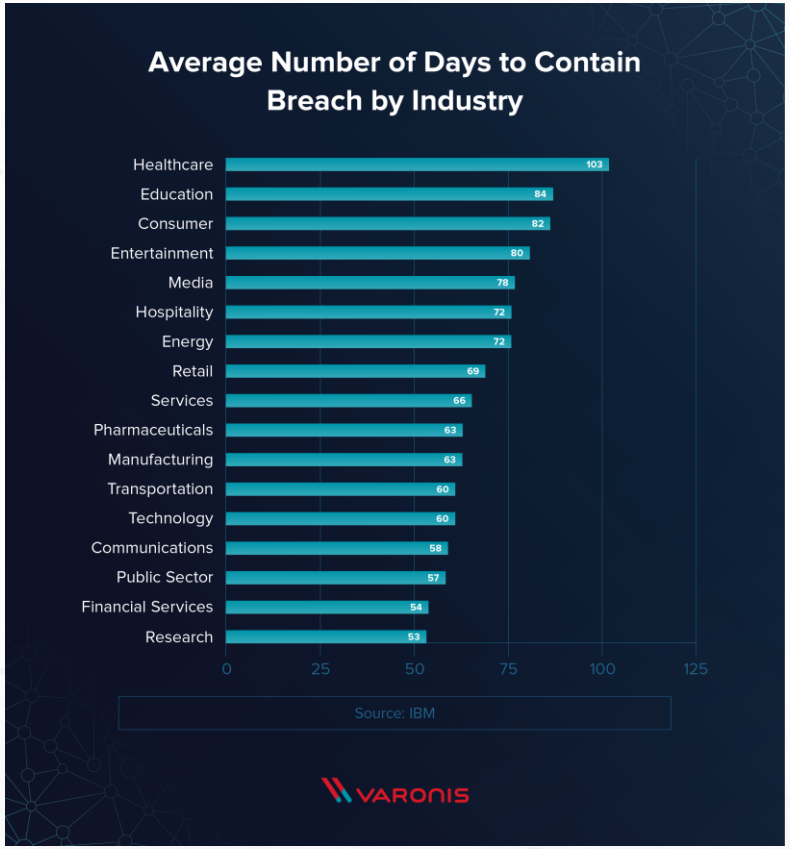
- Čl. 4 ods. 12 GDPR: „porušenie ochrany osobných údajov“ je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

- **Ktoré incidenty je potrebné oznámiť?**
  - porušenie ochrany osobných údajov (personal data breach)
  - porušenie bezpečnosti
- **Kto musí oznamovať?**
  - každý prevádzkovateľ a sprostredkovateľ
- **Komu je potrebné incident oznámiť?**
  - Úradu na ochranu osobných údajov
  - dotknutým osobám (niektoré prípady)
- **Do kedy je potrebné incident oznámiť?**
  - **bez zbytočného odkladu**, resp. **do 72 hodín**

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV





BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

Štandardný vzhľad | Lineárne zobrazenie
Mapa stránok | RSS | Kontakt

Slovenčina English

Domov | Úrad | Legislatíva a judikatúra | Práva dotknutých osôb | Schengenský priestor | Prenos osobných údajov | Sme členom | Metodiky a FAQ
Formuláre, vzory

Domov » Formulár pre prevádzkovateľa na nahlasovanie bezpečnostných incidentov v zmysle Čl. 33 Nariadenia (EÚ)2016/679 a § 40 zákona č. 18/2018 Z. z

Formulár pre prevádzkovateľa na nahlasovanie bezpečnostných incidentov v zmysle Čl. 33 Nariadenia (EÚ)2016/679 a § 40 zákona č. 18/2018 Z. z

Verzia pre tlač

Formulár je určený pre prevádzkovateľov, ktorí sú povinní v zmysle čl. 33 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) ako aj § 40 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z. (ďalej len „zákon“) bezodkladne oznámiť Úradu na ochranu osobných údajov SR (ďalej len „úrad“), ako dozornému orgánu v oblasti ochrany a spracúvania osobných údajov porušenie ochrany osobných údajov, ktoré môže mať za následok riziko pre práva a slobody fyzických osôb.

Úvod — Náhľad — Dokončiť

Oznámenie o porušení ochrany osobných údajov

Upozornenie: Ak máte podozrenie, že došlo alebo dochádza k porušeniu Vašich práv pri spracúvaní Vašich osobných údajov alebo došlo k porušeniu zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 18/2018 Z. z.“) alebo nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27.04.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „nariadenie“), postupujte v zmysle informácií zverejnených TU.

1. Identifikácia oznamovateľa bezpečnostného incidentu:

Názov prevádzkovateľa (fyzická/právnická osoba), ktorého sa týka oznámenie o porušení ochrany osobných údajov:

*

Adresa / sídlo:

Deň | Mesiac | Rok

hodina: **minúta:**

Hour : 00

Uveďte, ako prevádzkovateľ zistil, že došlo k porušeniu ochrany osobných údajov, resp. akým spôsobom sa prevádzkovateľ o porušení ochrany osobných údajov dozvedel (uveďte aj napr. situáciu, ak porušenie ochrany osobných údajov identifikovala dotknutá osoba, resp. iná osoba, sprostredkovateľ, atď.):

*

4. Opis porušenia ochrany osobných údajov:

V zmysle Čl. 4 ods. 12 Nariadenia je porušenie ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

V tejto časti čo najpresnejšie opíšte situáciu (incident). **Odporúčame opis porušenia ochrany osobných údajov poskytnúť minimálne v intenciách nižšie uvedených bodov.**

- Uveďte, kto incident spôsobil, resp. čo malo vplyv na vznik incidentu. Prečo a ako došlo k vzniku incidentu.
- Uveďte, či došlo k narušeniu dôvernosti osobných údajov, tzn. či nastala situácia, že k osobným údajom má prístup strana, ktorá nemá legitímne oprávnenie pre prístup k týmto údajom, príp. či došlo k neoprávnenému prístupu k zariadeniam, prostredníctvom ktorých sú tieto osobné údaje prenášané, spracúvané, uchovávané.
- Uveďte, či došlo k narušeniu integrity, tzn. či došlo k neoprávnenej zmene, úprave osobných údajov. Aký nepriaznivý vplyv môže mať táto zmena, úprava pre dotknuté osoby.
- Uveďte, či došlo k narušeniu dostupnosti osobných údajov, tzn. či došlo napr. k nezákonnému zničeniu, vymazaniu, strate osobných údajov a údaje nie sú dostupné. Zároveň uveďte, či strata dostupnosti osobných údajov je trvalá alebo dočasná, či je možná obnova týchto osobných údajov a za akých podmienok. Uveďte, či prevádzkovateľ disponuje napr. zálohou na obnovu údajov atď..
- Uveďte, či incident má vplyv napr. na poskytnutie služby prevádzkovateľa voči dotknutým osobám. Uveďte, aké údaje boli odhalené o dotknutých osobách. Čo tieto údaje odhaľujú o dotknutých osobách. Aká ujma môže odhalením týchto údajov vzniknúť dotknutým osobám.
- Uveďte, či predmetný incident vznikol v dôsledku nedodržania zavedených opatrení u prevádzkovateľa, a kto tieto opatrenia nedodržal. Zároveň opíšte, akým spôsobom boli tieto opatrenia prijaté u prevádzkovateľa a dátum ich prijatia. Uveďte, či osoba, ktorá spôsobila incident bola oboznámená s pokynmi prevádzkovateľa. Uveďte akou formou prebieha oboznámenie osôb s pokynmi prevádzkovateľa pre spracúvanie osobných údajov.
- Ak incident spôsobil napr. zamestnanec uveďte, či bol tento zamestnanec oboznámený s pokynmi prevádzkovateľa, ktoré má uplatňovať pri spracúvaní osobných údajov.
- Uveďte, aký nepriaznivý dopad má tento incident na práva a slobody dotknutých osôb.
- Uveďte ďalšie informácie viažuce sa k incidentu, ktoré považujete za relevantné na objasnenie príčin vzniku incidentu, v dôsledku ktorého bola porušená ochrana osobných údajov dotknutých osôb.

Popíšte: *

5. Kategória osobných údajov:

Uveďte kategóriu osobných údajov (osobné údaje, osobitná kategória osobných údajov), ktorých sa predmetné porušenie ochrany osobných údajov týka.

Označte, prípadne doplňte, ktorých osobných údajov sa porušenie ochrany osobných údajov týka:

ÚRAD NA OCHRANU
OSOBNÝCH ÚDAJOV
SLOVENSKEJ REPUBLIKY

Univerzita Pavla Jozefa Šafárika v Košiciach
Šrobárova 2
041 80 Košice
IČO: 00397768

Váš list číslo / zo dňa	Naše číslo	Vybavuje / linka	Bratislava
	007669/2022 DB62/2022	02/0911430818	18.10.2022

Vec
Porušenie ochrany osobných údajov - žiadosť o súčinnosť

Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad") bolo dňa 04.07.2022 doručené oznámenie o porušení ochrany osobných údajov DB 62/2022 v zmysle článku 33 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „Nariadenie") prevádzkovateľom Univerzita Pavla Jozefa Šafárika v Košiciach, Šrobárova 2, 041 80 Košice, IČO: 00397768 (ďalej len „prevádzkovateľ").

Podľa Čl. 4 ods. 12 Nariadenia „**porušenie ochrany osobných údajov**" je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

Podľa Čl. 5 ods. 1 Nariadenia osobné údaje musia byť:

a) **spracúvané zákonným spôsobom, spravodlivo a transparentne** vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť");
b) **získavané na konkrétne určené, výslovne uvedené a legitímne účely** a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu");
c) **primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely**, na ktoré sa spracúvajú („minimalizácia údajov");
d) **správne a podľa potreby aktualizované**; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť");
e) **uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú**; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávania");
f) **spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo**

V nadväznosti na vyššie uvedené oznámenie o porušení ochrany osobných údajov úrad na základe § 109 zákona č. 18/2018 Z. z. žiada prevádzkovateľa o súčinnosť vo veci poskytnutia informácií k spracúvaniu osobných údajov, ktoré sú dotknuté incidentom uvedeným v oznámení o porušení ochrany osobných údajov DB 62/2022. Vo Vašej odpovedi žiadame, poskytnúť úradu vyjadrenia prípadne dokumentáciu k nižšie uvedeným bodom:

1. Predložte úradu správu z prešetrovania uvedeného incidentu (dokumentáciu z vyšetrovania celého bezpečnostného incidentu)
2. Bola vykonaná forézna analýza/bezpečnostný audit? Doručte dôkaz.
3. Popísať technológiu na ktorej boli osobné údaje spracovávané (operačný systém (ďalej len „OS"), aplikácie, databázový systém, bezpečnostná infraštruktúra a pod.), vrátane verzie predmetných informačných technológií ku dňu incidentu.
4. V kontexte incidentu preukážte úradu, **aké konkrétne opatrenia boli u prevádzkovateľa prijaté pred vznikom incidentu** na uplatnenie zásady spracúvania osobných údajov v zmysle čl. 5 ods. 1 písm. f) Nariadenia, tzn. preukážte aké opatrenia prijal prevádzkovateľ, aby osobné údaje boli spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, aby osobné údaje boli chránené pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. V zmysle tohto bodu doručte (elektronickou formou) najmä::
   i. bezpečnostné smernice, smernice na ochranu osobných údajov a pod.
   ii. Aké bezpečnostné nástroje boli ku dňu incidentu implementované? – doručte názov technológie vrátane jej verzie ku dňu incidentu. napr. firewall, IPS, SIEM a pod.
   iii. Ako je aplikovaný systém manažmentu záplat (patch management) v danom informačnom systéme? Ak áno doručte príslušný predpis, číslo poslednej verzie záplaty pred incidentom napr. formou logu, screenshotu.
   iv. Je vykonávaná detekcia zraniteľností, penetračné testy? Ak, áno v akej periodicite. Doručte dôkaz.
   v. Je vykonávaný systém záloh? Ak áno, doručte dôkaz o vykonávaní záloh (napr. zálohovací predpis, screenshot zo zálohovacieho softvéru a pod.).
   vi. Je aplikovaný systém na detekciu pred škodlivým kódom? Ak áno, tak aký druh a verzia v čase vzniku incidentu? Doručte dôkaz.
   vii. Sú databázy s osobnými údajmi šifrované? Ak áno, tak akým algoritmom?
   viii. Doručte dôkaz o aplikovaní implementovaných opatrení.
5. Určiť riziko či viedol daný bezpečnostný incident k vysokému riziku pre práva a slobody fyzických osôb.
6. Informovať úrad či boli vykonané opatrenia v zmysle čl. 34 Nariadenia ak bola preukázaná existencia vysokého rizika.
7. Oznámili ste uvedený incident aj orgánom činným v trestnom konaní?
8. Mal bezpečnostný incident do dnešného dňa aj iné negatívne dopady (zneužitie osobných údajov) pre dotknuté osoby?
9. Popíšte úradu, aké konkrétne opatrenia prevádzkovateľ **zaviedol po vzniku incidentu**, aby sa incident neopakoval. Preukážte úradu Vaše tvrdenie.

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

- **Príklad 1:** Prevádzkovateľ prostredníctvom **dvoch hromadných mailov** sprístupnil bez právneho základu OÚ 372 študentov x. ročníka v rozsahu: meno, priezvisko, emailová adresa, výsledok testu, údaje týkajúce sa zaradenia do študijných krúžkov (údaje boli sprístupnené študentom a všetkým zamestnancom fakulty) a osobné údaje 217 študentov x. ročníka v rozsahu: meno, priezvisko, všeobecne použiteľný identifikátor (rodné číslo), údaje týkajúce sa zaradenia do študijných krúžkov (údaje boli sprístupnené študentom a všetkým zamestnancom fakulty) (vysoká škola, 900€). Prevádzkovateľ prijal opatrenia - preškolenie zamestnanca.
- **Príklad 2:** Sprostredkovateľ zaslal email obsahujúci OÚ dotknutej osoby v rozsahu meno, priezvisko, dátum narodenia, adresa, telefónne číslo a číslo poistnej zmluvy mobilného zariadenia na **emailovú adresu** bez toho, aby boli uvedené OÚ v rámci zaslaného emailu **zabezpečené heslom**, čím bez právneho základu sprístupnil OÚ inej osobe (ISP, 700€)
- **Príklad 3:** Zverejnenie rodných čísiel 186 uchádzačov o štúdium (škola, 700€). Novou právnou úpravou ochrany OÚ sa všeobecne použiteľný identifikátor - RČ FO nezaraďuje medzi tzv. osobitné kategórie OÚ, ale naďalej sa na spracúvanie RČ vzťahuje osobitný režim podľa § 78 ods. 4 ZOOU.

BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

Sankcia od ÚOOU

- Počet rozhodnutí: 180
- Priemerná: 1.750 €
- Minimálna: 100 €
- Maximálna: 50.000 €

PRIŤAŽUJÚCE OKOLNOSTI podľa § 106 ods. 1 ZOOU										
Povaha a závažnosť porušenia	Prevádzkovateľ už porušil GDPR	Počet dotknutých osôb alebo ich povaha	Spôsob, akým sa úrad o porušení dozvedel	Trvanie porušenia	K splneniu povinnosti došlo neskôr / nedošlo vôbec	Prevádzkovateľ neprijal primerané technické a organizačné opatrenia	Porušením mohol prevádzkovateľ získať finančný prospech	Osobitná povaha prevádzkovateľa	Zistené porušenie môže mať/malo na dotknutú osobu výrazne negatívny dopad	Osobitná kategória OÚ, ktorých sa porušenie týkalo (napr. RČ, osobitné kategórie OÚ)
169	23	65	86	50	17	2	1	2	2	28

POĽAHČUJÚCE OKOLNOSTI podľa § 106 ods. 1 ZOOU													
V konaní nebolo zistené, že dotknutá osoba v dôsledku porušenia utrpela konkrétnu škodu, majetkovú či nemajetkovú ujmu a neboli zistené škodlivé následky, ktoré by priamo zasiahli dotknutú osobu alebo ohrozili jej súkromný alebo rodinný život (vyššia miera negatívnych dôsledkov nepreukázaná)	Nedbanlivostný charakter porušenia (prevádzkovateľ neporušil GDPR úmyselne či s vedomím, že porušením spôsobí škodu)	Prevádzkovateľ porušením nezískal finančný alebo nefinančný prospech	Bežné OÚ, tzn. nejde o porušenie práv k osobitným kategóriám OÚ	Nižší počet dotknutých osôb	Spolupráca prevádzkovateľa s úradom	Iniciatíva prevádzovateľa pri (dodatočnej) náprave zisteného porušenia	Vo vzťahu k prevádzkovateľovi úrad doposiaľ nekonštatoval porušenie ochrany OÚ	Porušenie nebolo opakované / k porušeniu došlo jednorazovo	Prevádzkovateľ mal prijaté alebo prijal bezpečnostné opatrenia na zamedzenie kodlivých následkov incidentu a na zabránenie jeho opakovania	Konanie / porušenie prevádzkovateľa netrvalo dlhší čas	Spôsob, akým sa úrad o porušení dozvedel	Povaha prevádzkovateľa	Prevádzkovateľa nepochybne priamo zasiahli opatrenia zavedené v súvislosti s pandémiou COVID-19
107	113	105	96	71	33	51	107	49	7	21	11	9	27

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ A OCHRANA SÚKROMIA V ELEKTRONICKÝCH KOMUNIKÁCIÁCH

PRÁVNA ÚPRAVA

- Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) – tzv. **ePrivacy Directive**
  - Čl. 1 ods. 1: Táto smernica harmonizuje ustanovenia členských štátov požadované na zabezpečenie primeranej úrovne ochrany základných práv a slobôd a najmä práva na súkromie, z hľadiska spracovávania osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronického komunikačného zariadenia a služieb v spoločenstve.
  - *lex specialis* k všeobecnej úprave v GDPR ⇨ špecifikácia pravidiel pre spracúvanie osobných údajov v telekomunikačnom sektore
- **Zákon č. 452/2021 Z. z. o elektronických komunikáciách**

PREDMET PRÁVNEJ ÚPRAVY

- právna úprava sa vzťahuje na spracúvanie osobných údajov v súvislosti **s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v EÚ** vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu
- definícia **elektronickej komunikačnej služby** - § 3 ods. 17 ZEK - „Služba je služba obvykle poskytovaná za odplatu prostredníctvom sietí, ktorá zahŕňa službu prístupu k internetu, interpersonálnu komunikačnú službu alebo služby pozostávajúce úplne alebo prevažne z prenosu signálov, napríklad prenosové služby používané na poskytovanie služieb komunikácie stroj-stroj (M2M) a na rozhlasové a televízne vysielanie. Službou nie je poskytovanie obsahu alebo vykonávanie redakčnej kontroly obsahu prenášaného pomocou sietí a služieb.“

POVAHA ÚDAJOV

- aké typy údajov sa bežne v rámci elektronických komunikačných služieb spracúvajú?
  a) **údaje týkajúce sa obsahu prenášaných správ, ktoré** sú striktne dôverné a môže sa k nim pristúpiť iba za veľmi limitovaných podmienok
  b) **prevádzkové údaje** (traffic data)
  c) **lokalizačné údaje**
    - prevádzkové a lokalizačné údaje možno súhrnne označiť pojmom metadáta
- ePrivacy smernica obsahuje aj špecifickú úpravu týkajúcu sa informácií v koncovom zariadení užívateľa (cookies) a nevyžiadanej elektronickej pošty (spamu)

BEZPEČNOSŤ

- § 108 ods. 1 ZEK: **Siete a zariadenia sa zriaďujú a prevádzkujú tak, aby sa predchádzalo škodlivému rušeniu.**
- § 108 ods.3 ZEK: Ak dôjde k škodlivému rušeniu alebo k rušeniu, ktoré bráni prevádzke zariadenia v súlade s jeho určením, podnik alebo užívateľ zariadenia, ktoré spôsobuje rušenie, je **povinný bezodkladne urobiť účinné opatrenia alebo ukončiť prevádzkovanie zariadenia**. Ak to nie je možné alebo ak je hospodárnejšie, alebo účelnejšie urobiť opatrenia na rušenom zariadení, urobí ich podnik alebo užívateľ zariadenia, ktoré spôsobuje rušenie. Náklady na odstránenie rušenia uhrádza podnik alebo užívateľ, ktorého zariadenie spôsobuje rušenie.

BEZPEČNOSŤ

- § 3 písm. f) ZEK: **bezpečnostným incidentom** je udalosť, ktorá má reálny nepriaznivý účinok na bezpečnosť sietí alebo služieb
- § 111 ods. 3 ZEK: Podnik je ďalej oprávnený spracúvať prevádzkové údaje a lokalizačné údaje v nevyhnutnom rozsahu aj bez súhlasu užívateľa na účely: (...) d) prevencie a odhaľovania bezpečnostných incidentov a protiprávnych konaní

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ A REGULÁCIA PLATOBNÝCH SLUŽIEB VO FINANČNOM SEKTORE

PRÁVNA ÚPRAVA

- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES
- **Zákon č. 492/2009 Z. z. o platobných službách**

PLATOBNÉ SLUŽBY

- § 2 ods. 1 zákona o platobných službách: **Platobnou službou sa rozumie:**
  a) vklad finančných prostriedkov v hotovosti na platobný účet a vykonávanie všetkých úkonov súvisiacich s vedením platobného účtu
  b) výber finančných prostriedkov v hotovosti z platobného účtu a vykonávanie všetkých úkonov súvisiacich s vedením platobného účtu
  c) vykonávanie platobných operácií vrátane prevodu finančných prostriedkov z platobného účtu alebo na platobný účet vedený u poskytovateľa platobných služieb
  d) vykonávanie platobných operácií z úveru poskytnutého používateľovi platobných služieb
  e) vydávanie platobného prostriedku alebo prijímanie platobných operácií
  f) poukazovanie peňazí
  g) platobná iniciačná služba
  h) služba informovania o platobnom účte

POSKYTOVATEĽ PLATOBNÝCH SLUŽIEB

- § 2 ods. 3 zákona o platobných službách: **Poskytovateľom platobných služieb sa rozumie:**
  a) banka, zahraničná banka alebo pobočka zahraničnej banky, ktorá má v bankovom povolení uvedené aj poskytovanie platobných služieb a zúčtovanie
  b) inštitúcia elektronických peňazí podľa § 81 ods. 1, zahraničná inštitúcia elektronických peňazí alebo pobočka zahraničnej inštitúcie elektronických peňazí
  c) poštový podnik, ak je podľa osobitného zákona oprávnený poskytovať platobné služby
  d) platobná inštitúcia podľa § 63, zahraničná platobná inštitúcia alebo pobočka zahraničnej platobnej inštitúcie
  e) Národná banka Slovenska alebo Európska centrálna banka, ak nekonajú ako menový orgán alebo ak nejde o činnosti, ktoré sa týkajú zabezpečovania verejných potrieb, a ak poskytujú platobné služby okrem § 38 ods. 3 až 6 a § 44b až 44f
  f) Štátna pokladnica, Exportno-importná banka Slovenskej republiky, miestne orgány štátnej správy, obce a vyššie územné celky, ak sú podľa osobitného zákona oprávnené poskytovať platobné služby a ak nejde o činnosti, ktoré sa týkajú zabezpečovania verejných potrieb
  g) poskytovateľ platobných služieb v obmedzenom rozsahu podľa § 79a
  h) poskytovateľ služieb informovania o platobnom účte podľa § 79b

AUTENTIFIKÁCIA

- § 2 ods. 17 zákona o platobných službách: **Autentifikáciou** sa na účely tohto zákona rozumie postup, ktorý umožňuje poskytovateľovi platobných služieb **overiť totožnosť používateľa platobných služieb alebo oprávnenosť použitia platobného prostriedku** vrátane použitia personalizovaných bezpečnostných prvkov používateľa platobných služieb.
- § 2 ods. 48 zákona o platobných službách: **Silnou autentifikáciou** používateľa platobných služieb sa na účely tohto zákona rozumie **autentifikácia na základe použitia dvoch prvkov alebo viacerých prvkov**, ktorými sú vedomosť, vlastníctvo a charakteristické znaky používateľa platobných služieb, pričom vedomosťou je to, čo vie len používateľ platobných služieb, vlastníctvom je to, čo vlastní alebo drží len používateľ platobných služieb a charakteristické znaky špecifikujú používateľa platobných služieb. Tieto prvky sú od seba nezávislé a vytvorené takým spôsobom, že narušenie jedného prvku nenaruší spoľahlivosť ostatných prvkov a ani dôvernosť autentifikačných údajov.

NAHLASOVANIE INCIDENTOV

- § 28c ods. 1 zákona o platobných službách: Poskytovateľ platobných služieb určí rámec s vhodnými opatreniami na zmiernenie prevádzkového rizika a bezpečnostného rizika a s kontrolným mechanizmom na riadenie týchto rizík, ktoré súvisia s poskytovaním platobných služieb. Poskytovateľ platobných služieb ako súčasť tohto rámca **zavedie a uplatňuje účinné postupy riadenia incidentov** vrátane zisťovania a členenia závažných prevádzkových incidentov a bezpečnostných incidentov (ďalej len „incident“).
- § 28d ods. 1 zákona o platobných službách: Ak ide o incident, poskytovateľ platobných služieb **bezodkladne informuje Národnú banku Slovenska**. Poskytovateľ platobných služieb, ak ide o incident, ktorý má vplyv na finančné záujmy jeho používateľov platobných služieb, **bezodkladne informuje svojich používateľov platobných služieb o incidente a o všetkých opatreniach, ktoré môžu prijať na zmiernenie nepriaznivých účinkov tohto incidentu.**
- § 28d ods. 2 zákona o platobných službách: Národná banka Slovenska po prijatí oznámenia podľa odseku 1 bezodkladne poskytne informácie o incidente Európskemu orgánu dohľadu (Európskemu orgánu pre bankovníctvo) a Európskej centrálnej banke. Národná banka Slovenska po posúdení tohto incidentu Európskym orgánom dohľadu (Európskym orgánom pre bankovníctvo) a Európskou centrálnou bankou informuje **Národný bezpečnostný úrad** alebo iné príslušné národné orgány v Slovenskej republike, ktoré prijmú nevyhnutné opatrenia s cieľom ochrániť bezpečnosť finančného systému.

NAHLASOVANIE INCIDENTOV

- Európska banková asociácia (EBA) vydala usmernenie pre poskytovateľov platobných služieb pre nahlasovanie incidentov, ktoré určuje kritéria na klasifikáciu toho, či ide o závažný bezpečnostný incident alebo nie
  - poskytovatelia platobných služieb vyhodnocujú dve množiny kritérií a to kritéria vysokého dopadu a kritéria nízkeho dopadu
  - na klasifikovanie incidentu ako závažného postačí, ak je splnené aspoň jedno kritérium vysokého dopadu alebo najmenej tri kritéria nízkeho dopadu

Kritérium	Nízky dopad	Vysoký dopad
Ovplyvnené transakcie	viac ako 10 % transakcií v rámci platobnej služby a trvanie incidentu dlhšie ako jednu hodinu alebo transakcie nad výšku 500 000 eur a trvanie incidentu dlhšie ako jednu hodinu	viac ako 25 % transakcií v rámci platobnej služby alebo Transakcie nad výšku 15 000 000 eur
Počet ovplyvnených užívateľov	viac ako 5000 užívateľov a trvanie incidentu dlhšie ako jednu hodinu alebo viac ako 10 % užívateľov a trvanie incidentu dlhšie ako jednu hodinu	viac ako 50 000 užívateľov alebo viac ako 25 % užívateľov
Výpadok služby	viac ako dve hodiny	N/A
Narušenie bezpečnosti siete alebo IT	Áno	N/A
Ekonomický vplyv	N/A	viac ako 0.1 % prvej vrstvy kapitálu, 200 000 eur alebo viac ako 5 000 000 eur
Vysoká úroveň internej eskalácie	Áno	áno a krízový manažment prevádzky
Vplyv na iné platobné služby alebo infraštruktúru	Áno	N/A
Vplyv na reputáciu	Áno	N/A

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ BEZPEČNOSŤ A ELEKTRONICKÁ IDENTIFIKÁCIA

PRÁVNA ÚPRAVA

- NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

PREDMET PRÁVNEJ ÚPRAVY

1) vzájomné uznávanie prostriedkov elektronickej identifikácie fyzických a právnických osôb, ktoré patria do oznámenej schémy elektronickej identifikácie iného členského štátu
2) pravidlá pre dôveryhodné služby, najmä elektronické transakcie
3) právny rámec pre elektronické podpisy, elektronické pečate, elektronické časové pečiatky, elektronické dokumenty, elektronické doručovacie služby pre registrované zásielky a certifikačné služby pre autentifikáciu webových sídiel

NARUŠENIE BEZPEČNOSTI SCHÉMY ELEKTRONICKEJ IDENTIFIKÁCIE

- Čl. 3 bod 4 Nariadenia eIDAS: „**schéma elektronickej identifikácie** je systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie.“
- Čl. 10 Nariadenia eIDAS: **Narušenie bezpečnosti**
    1. Keď sa schéma elektronickej identifikácie oznámená podľa článku 9 ods. 1 alebo autentifikácia uvedená v článku 7 písm. f) naruší alebo čiastočne skompromituje spôsobom, ktorý ovplyvní spoľahlivosť cezhraničnej autentifikácie danej schémy, oznamujúci členský štát danú cezhraničnú autentifikáciu alebo dotknuté skompromitované časti bezodkladne pozastaví alebo zruší a informuje o tom ostatné členské štáty a Komisiu.
    2. Po náprave narušenia alebo skompromitovania uvedeného v odseku 1 oznamujúci členský štát cezhraničnú autentifikáciu opätovne zavedie a bez zbytočného odkladu o tom informuje ostatné členské štáty a Komisiu.
    3. Ak sa narušenie alebo skompromitovanie uvedené v odseku 1 neodstráni v lehote troch mesiacov od pozastavenia alebo zrušenia, oznamujúci členský štát informuje ostatné členské štáty a Komisiu o stiahnutí schémy elektronickej identifikácie.
    4. Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny v zozname uvedenom v článku 9 ods. 2 v *Úradnom vestníku Európskej únie*.

BEZPEČNOSTNÉ POŽIADAVKY UPLATNITEĽNÉ NA POSKYTOVATEĽOV DÔVERYHODNÝCH SLUŽIEB

Čl. 19 ods. 1 Nariadenia eIDAS:

Kvalifikovaní a nekvalifikovaní poskytovatelia dôveryhodných služieb prijmú **vhodné technické a organizačné opatrenia na riadenie rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytujú**. So zreteľom na najnovší technologický vývoj sa uvedenými opatreniami **musí zaistiť úroveň bezpečnosti primeraná stupňu rizika.** Prijmú sa najmä **opatrenia na prevenciu a minimalizáciu vplyvu bezpečnostných incidentov a na oznámenie nepriaznivých účinkov všetkých takýchto incidentov zainteresovaným stranám.**

BEZPEČNOSTNÉ POŽIADAVKY UPLATNITEĽNÉ NA POSKYTOVATEĽOV DÔVERYHODNÝCH SLUŽIEB

Čl. 19 ods. 2 Nariadenia eIDAS:

2. Kvalifikovaní a nekvalifikovaní poskytovatelia dôveryhodných služieb bez zbytočného odkladu, najneskôr však do 24 hodín, odkedy sa dozvedeli o akomkoľvek narušení bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci nej, **oznámia túto skutočnosť orgánu dohľadu** a prípadne iným príslušným orgánom, ako je napríklad vnútroštátny orgán zodpovedný za informačnú bezpečnosť alebo orgán pre ochranu údajov.

Ak môže narušenie bezpečnosti alebo integrity negatívne ovplyvniť **fyzickú alebo právnickú osobu, ktorej sa dôveryhodná služba poskytovala,** poskytovateľ dôveryhodných služieb bez zbytočného odkladu **oznámi** narušenie bezpečnosti alebo integrity aj tejto fyzickej či právnickej osobe.

Ak je to vhodné, a najmä keď sa narušenie bezpečnosti alebo integrity týka dvoch alebo viacerých členských štátov, informovaný orgán dohľadu o veci informuje orgány dohľadu v ostatných dotknutých členských štátoch a **agentúru ENISA.**

Ak informovaný orgán dohľadu usúdi, že zverejnenie narušenia bezpečnosti alebo integrity je vo verejnom záujme, informuje o ňom **verejnosť**, alebo o to požiada poskytovateľa dôveryhodných služieb.

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

laura.rozenfeldova@upjs.sk

https://cyberawareness.sk