Operačný program
Efektívna
verejná správa

Európska únia
Európsky sociálny fond

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

## Výstup č. 1.1.3

# Štandardizácia pre bezpečnosť a ochranu údajov

Zmluva o dielo č. 445/2022

***Projekt:***

**Zlepšenie využívania údajov vo verejnej správe**

***ITMS kód projektu:***

**314011S979**

Tento projekt je podporený z Európskeho sociálneho fondu.

# Document review and approval

## Revision history

| Version | Author | Date | Revision |
|---|---|---|---|
| 0.1 | Bošanská<br>Bárdy<br>Vančo | 16.3.2023 | |
| 0.2 | Bošanská<br>Bárdy<br>Vančo | 14.4.2023 | |
| | | | |
| | | | |
| | | | |
| | | | |

## This document has been reviewed by

| | Reviewer | Date reviewed |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

## This document has been approved by

| | Subject matter experts<br>Name | Signature | Date reviewed |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

# Obsah

# 1 Úvod a zhrnutie

## 1.1 Účel a použitie výstupu

**Detailný výstup č. 1.1.3: Štandardizácia pre bezpečnosť a ochranu údajov vznikol ako aktualizácia dostupných výstupov v téme bezpečnosti a ochrany údajov.**

Dokument bol pripravený v rámci projektu „Zlepšenie využívania údajov vo verejnej správe“. Tento projekt má ambíciu transformovať fungovanie inštitúcií verejnej správy tak, aby dokázali maximálne efektívne spravovať a zdieľať údaje, využívať údaje pre lepšie rozhodovanie na základe faktov a dôkazov, pre zlepšenie efektivity a adresnosti služieb na základe lepšieho využívania dát.

Projekt Zlepšenie využívania údajov vo verejnej správe realizuje Dátová kancelária verejnej správy ako špeciálna jednotka Ministerstva investícii, regionálneho rozvoja a informatizácie (ďalej aj MIRRI).

### 1.1.1 Aktualizácia štandardov pre zabezpečenie bezpečnosti údajov

Štandardy, ktoré adresujú zabezpečenie údajov spadajú do kategórií:

- Šifrovanie údajov: Šifrovanie je proces, ktorým sa údaje zašifrujú tak, aby boli pre neoprávnené osoby nečitateľné.
- Autentifikácia: Autentifikácia je proces, ktorým sa overuje, či je osoba, ktorá sa snaží pristupovať k údajom, oprávnená.
- Zálohovanie údajov: Zálohovanie údajov je proces, ktorým sa vytvárajú kópie údajov, aby sa zabezpečilo, že ak sa údaje stratia alebo poškodia, môžu byť obnovené.
- Kontrola prístupu: Kontrola prístupu je proces, ktorým sa zabezpečí, že len oprávnené osoby majú prístup k údajom.
- Zabezpečenie siete: Zabezpečenie siete je proces, ktorým sa zabezpečí, že údaje sú chránené pred neoprávneným prístupom z vonku.
- Monitorovanie: Monitorovanie je proces, ktorým sa sleduje, čo sa deje s údajmi, aby sa zistilo, či sú vystavené neoprávnenému prístupu alebo poškodeniu.

### 1.1.2 Aktualizácia štandardov pre zabezpečenie ochrany osobných údajov

Z pohľadu zvýšenia ochrany osobných údajov v prostredí eGovernmentu navrhujeme štandardy pre koncept manažmentu osobných údajov:

- End-to-end šifrovanie datasetov, ktoré možno dešifrovať len vtedy, ak je používateľ prítomný, teda ak riešenie pre manažment osobných údajov používa.
- Správa súhlasov na základe štandardu Verifiable Credentials.

Tieto štandardy by mali byť implementované v rámci riešenia MOU.







Tento projekt je podporený z Európskeho sociálneho fondu.

## 1.2 Metodika realizácie výstupu

Prvým krokom analýzy je analýza pokrytia jednotlivých tém v rámci bezpečnosti a ochrany údajov vo verejnej správe z pohľadu pokrytia platnými reguláciami a potrebnými štandardami:

- GDPR ( z angl. General Data Protection Regulation) a zákon o ochrane osobných údajov,
- Zákon o informačných technológiach vo verejnej správe,
- Zákon o kybernetickej bezpečnosti.

Pre identifikované medzery sú vybrané vhodné štandardy, ktorými by sa mohli informačné systémy verejnej správy riadiť (navrhujeme zaviesť najmä End-to-end šifrovanie datasetov a štandardizovať správu súhlasov).

Následne navrhujeme odporúčania, akým spôsobom aplikovať vybrané štandardy do praxe formou zoznamu opatrení, ktoré je vhodné aplikovať pre projekty z programu Manažment údajov. Zámerom je vytvoriť prehľadný „checklist“ a na jedno miesto zoskupiť odkazy na príslušné metodiky a návody.







Tento projekt je podporený z Európskeho sociálneho fondu.

# 2 Koncept pre zabezpečenie bezpečnosti údajov a ochrany osobných údajov

## 2.1 Teoretické východiská

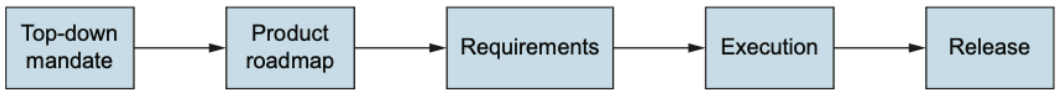
### Bezpečnosť a ochrana údajov sú náročné

Aj pre úspešné súkromné spoločnosti, ktoré disponujú vynikajúcimi inžiniermi, je ochrana súkromia náročná. Majú zručnosti, ktoré vedú k úžasným produktom a rastúcim ziskom - prečo nedokážu naplánovať aj úspech v oblasti ochrany súkromia? Tieto otázky sa kladú v reálnych situáciách, keď spoločnosti bez zlého úmyslu a s preukázateľne úspešnými produktmi urobili vážne chyby v oblasti ochrany súkromia. Tieto ťažkosti súvisia s aktuálnymi trendmi vo vývoji softvéru, ako vysvetlíme ďalej v tejto kapitole.

Výsledky ochrany súkromia súvisia s konkrétnymi rozhodnutiami o údajoch, ktoré organizácia prijíma. Konkrétne ide o tieto rozhodnutia:

- Aké údaje zbierať,
- Ako k nim získať prístup,
- S kým ich zdieľať,
- Čo robiť s poznatkami, ktoré nám údaje prinášajú,
- Ako vhodne riadiť riziká.

Kedysi bol vývoj procesu lineárny a predvídateľný, ako ukazuje Obrázok 1~~Obrázok 1~~, a bol v podstate riadený zhora nadol. Smernice sa tiež vydávali zhora nadol a inžinieri ich plnili.




**Obrázok 1: Tradičný vývoj softvéru – lineárny a predvídateľný proces**

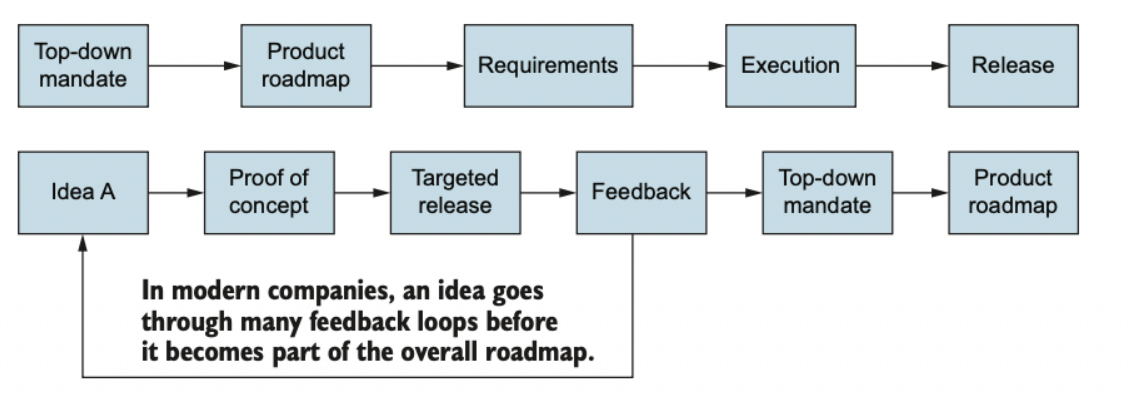
Ako ukazuje Obrázok 1~~Obrázok 1~~, misia organizácie určila jej plán produktov. Plán určil konkrétne požiadavky na produkty a služby a inžinierske tímy plnili túto misiu. Produkt bol potom pripravený na vydanie. Výhodou tohto modelu bolo, že bol predvídateľný a opakovateľný. Nevýhodou bolo, že ste mohli investovať veľa prostriedkov a času do vytvorenia produktu a potom ste museli čakať na spätnú väzbu v podobe prijatia alebo odmietnutia zo strany používateľov.

Neskôr sa proces vývoja stal viac inovatívnym, neregulovaným a nepredvídateľným, ako ukazuje Obrázok 2~~Obrázok 2~~.






Tento projekt je podporený z Európskeho sociálneho fondu.




**Obrázok 2: Moderný dynamický inovačný proces; nepretržitý cyklus spätnej väzby a nových iterácií**

Začiatkom roka 2010, keď sa začali presadzovať trendy ako agilný vývoj a scrum, sa vyvíjali aj inžinierske inovácie. Organizácie mohli stále dodržiavať model vývoja zhora nadol, ale popri tom mohli tímy a inžinieri experimentovať s nápadmi a inovovať po častiach.

Ako vidno v hornom riadku obrázka (Obrázok 2~~Obrázok 2~~), moderné organizácie by mohli vytvárať produkty v tradičnom duchu, kedy by produkt mohol presadzovať vrcholový manažér. Jeho vízia by sa premietla do plánu a špecializované tímy by ju mohli poslušne realizovať. Avšak súčasne môže tím inžinierov skúmať nový nápad, ktorý môže, ale nemusí súvisieť so známou oblasťou expertízy organizácie. Táto inovácia sa často uskutočňuje po častiach, pričom sa postupne uvoľňujú malé časti produktu, aby sa získala spätná väzba, prípadne aby sa vygenerovali nové investície. Pri takýchto projektoch sa často nedodržiavajú typické procesy týkajúce sa nakladania s údajmi a aktívami. Druhý riadok na obrázku (Obrázok 2~~Obrázok 2~~) znázorňuje tento model.

Vzhľadom na tlak na rýchle dodanie produktov, zvýšenie angažovanosti a pružnú realizáciu programov sa čoraz viac presadzuje druhý model. Táto dynamika bráni vedúcim pracovníkom a ich technickým lídrom dohliadať na všetky menšie rozhodnutia, ktoré vedú k nejakému konkrétnemu stavu. A ďalej komplikuje úlohu centralizovaných inžinierov pre bezpečnosť údajov a ochranu súkromia, pretože ich plány musia zohľadňovať dôsledky týchto rozhodnutí vo viacerých disciplínach v čase.

## Čo sa očakáva od bezpečnosti údajov a ochrany súkromia v praxi

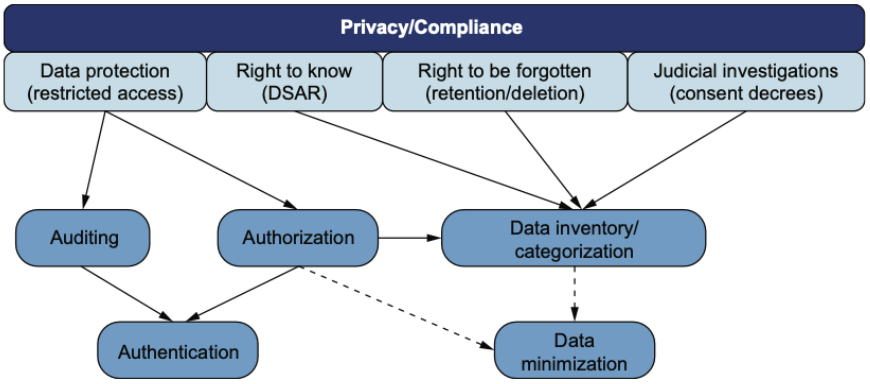
Bezpečnosť a ochrana údajov vyplýva predovšetkým z predpisov a osvedčených postupov v odvetví. Obrázok 3~~Obrázok 3~~ poukazuje na štyri kľúčové očakávania v oblasti ochrany osobných údajov:

1 **Ochrana údajov** - Používatelia a regulačné orgány očakávajú, že údaje zákazníkov sa budú chrániť.
2 **Právo na informácie** - od organizácii sa očakáva, že poskytnú kópie údajov o zákazníkoch na požiadanie. Konkrétne ide o žiadosti o prístup k údajom dotknutých subjektov („Data Subject Access Request (DSAR)“).
3 **Právo byť zabudnutý** - toto právo umožňuje používateľom požiadať o vymazanie svojich údajov.
4 **Evidencia a archivácia** – organizácie musia riadiť, aké údaje zhromažďujú a uchovávať ich z dôvodov dodržiavania právnych predpisov.






Tento projekt je podporený z Európskeho sociálneho fondu.




**Obrázok 3: Štyri kľúčové očakávania v oblasti bezpečnosti údajov a ochrany súkromia a s nimi spojené riešenia**

Tieto abstraktné požiadavky sa premietajú do konkrétnych úloh v oblasti ochrany súkromia a technických kontrol:

- **Minimalizácia údajov**, kedy sa zhromažďuje len to, čo je skutočné potrebné
- **Autentifikácia**, ktorá zahŕňa overenie totožnosti zamestnancov a používateľov, ktorí pristupujú k údajom,
- **Autorizácia**, ktorá mapuje záujemcov o prístup k systému alebo údajom na štruktúru oprávnení a politiku,
- **Inventarizácia a kategorizácia údajov**, ktorá si vyžaduje vytvorenie dátového katalógu údajov organizácie,
- **Audity**, ktorými sa overuje, či sa kontroly ochrany osobných údajov týkajúce sa vymazávania, uchovávania, atď. presadzujú v praxi.

Ako ukazuje Obrázok 3~~Obrázok 3~~, je práca inžinierov v oblasti ochrany súkromia multi-odborová a vyžaduje si zosúladenie. GDPR vyžaduje ešte plnenie dodatočných úloh a technických kontrol na splnenie nasledujúcich cieľov v oblasti bezpečnosti a ochrany údajov, ktorým sa budeme komplexnejšie venovať v kapitole 2.4:

- Dostupnosť,
- Integrita (riešené aj v dokumente 1.1.8 Štandardizácia dôveryhodných údajov),
- Dôvernosť (riešené aj v dokumente 1.1.5 Štandardizácia anonymizácie údajov),
- Nespojiteľnosť (riešené aj v dokumente 1.1.5 Štandardizácia anonymizácie údajov),
- Transparentnosť,
- Intervencia,
- Súčinnosť a spolupráca.

### Presadzovanie dátových politík v rôznych systémoch

Inžinieri pre bezpečnosť a ochranu osobných údajov musia uplatniť svoje nástroje v rôznych systémoch, ktoré existujú v rámci organizácie. Tabuľka 1~~Tabuľka 1~~ ukazuje, ako






Tento projekt je podporený z Európskeho sociálneho fondu.

môže takéto prostredie vyzerať. Tabuľka 1~~Tabuľka 1~~ uvádza príklady druhov systémov, v ktorých sa údaje môžu nachádzať.

### Tabuľka 1: Rôzne typy systémov plniace rôzne účely pri uchovávaní údajov

| Systém | Účel |
|---|---|
| Úložiská dát pre offline analýzu, napríklad v rámci Konsolidovanej analytickej vrstvy | Neštruktúrované dátové jazerá („data lakes“) ako napríklad Hadoop, Hive, BigQuery alebo dátové sklady, napríklad od spoločnosti Oracle |
| Prevádzkové databázy | Prevádzkové údaje, ktoré sa vymieňajú v rámci transakcií v reálnom čase a žijú v štruktúrovaných a neštruktúrovaných databázach ako MySQL, Elasticsearch (odvodené údaje), MongoDB a podobne. |
| Cloudové úložiská | Napríklad úložiská vo vládnom cloude na diskovom poli alebo vo verejnom cloude v Amazone AWS ako S3 „buckets“ |

## Technológie a nástroje na ochranu súkromia: možnosti a voľby

V prostredí verejnej správy treba uvažovať o štandardoch, opatreniach a nástrojoch na ochranu súkromia v troch tematických skupinách (Tabuľka 2~~Tabuľka 2~~):

1 **Vedieť** - Vedieť, kde sa dajú nájsť a lokalizovať citlivé údaje (V dokumente 1.1.2 Štandardizácia pre modelovanie údajov).
2 **Redukovať** – Redukovať objem exponovaných údajov, pričom sa minimalizuje „styčná plocha“ so súkromím používateľov prostredníctvom zastretia a vymazania. (V dokumente 1.1.5 Štandardizácia anonymizácie údajov).
3 **Chrániť** - chrániť tam, kde sa presadzuje riadenie prístupu k údajom (V tomto dokumente).

V prípade nákupu alebo vytvárania nástrojov, ktoré majú spĺňať štandardy pre bezpečnosť a ochranu údajov, je potrebné, aby boli jasne zodpovedané otázky čo konkrétne majú tieto nástroje riešiť a ako by zvažované nástroje alebo prístupy k tomuto riešeniu vo verejnej správe fungovali. Následne musí byť urobená táto kritická voľba: vytvoria sa nástroje na ochranu súkromia vo vlastnej réžii (alebo na mieru cez dodávateľa), alebo sa kúpia hotové riešenia tretích strán, ktoré môžu siahať od komplexných platforiem na ochranu súkromia až po užšie zamerané riešenia? Tento dokument ponúkne prehľad typov nástrojov, ktoré implementujú techniky bezpečnosti a ochrany údajov, ktoré by stálo za to zvážiť v prostredí verejnej správy alebo sa nimi inšpirovať. V dokumente 1.1.2 Štandardizácia pre modelovanie údajov sa venujeme nástrojom na katalogizáciu, kategorizáciu a klasifikáciu údajov a na priraďovanie a evidenciu politík k nim.

### Tabuľka 2: Rámec pre uvažovanie o štandardoch, opatreniach a nástrojoch pre ochranu údajov

| Vedieť | Redukovať | Chrániť |
|---|---|---|
| **Inventarizácia a katalóg** | **Minimalizácia údajov** | **Riadenie prístupov** |
| Kde sa údaje nachádzajú? | Zbierajte menej údajov | Autentifikácia |
| O aký typ údajov ide? (Napríklad kategória citlivosti údajov) | Zastrite alebo anonymizujte údaje | Autorizácia |
| Kto a prečo ich zbiera alebo používa? | Vymažte údaje, pokiaľ ich už netreba | |






Tento projekt je podporený z Európskeho sociálneho fondu.

## 2.2 Kategorizácia a klasifikácia údajov

Údaje, pri ktorých treba aplikovať osobitné politiky správy aktív, pretože sú zásadné pre fungovanie organizácie, ochranu jej kľúčových znalostí, zákazníkov, partnerov ako aj povesti, sa nazývajú citlivé. Základná kategorizácia citlivých údajov rozlišuje dve úrovne:

1 **zverejniteľné údaje (Z)** – údaje, ktorých zverejnenie neohrozuje fungovanie verejnej správy a jej systémov, a preto ich je možné kedykoľvek zverejniť.
2 **nezverejniteľné údaje (NZ)** – údaje, ktoré nie je vhodné zverejniť v žiadnom prípade, pretože zverejnenie nesie riziko okamžitého alebo neskoršieho pokusu o narušenie informačnej bezpečnosti. Pre nezverejniteľné údaje môže existovať podmienka, za splnenia ktorej sa stanú zverejniteľnými.

V dokumente 1.1.5 Štandardizácia anonymizácie údajov pod nezverejniteľnými údajmi rozumieme len osobné údaje a venujeme sa v ňom ich ochrane prostredníctvom anonymizácie a pseudonymizácie. V tom dokumente je vysvetlená aj dôležitosť kategorizácie a klasifikácie a je tam vytvorená kategorizácia a klasifikácia pre osobné údaje. V tomto dokumente sa zaoberáme nezverejniteľnými údajmi v širšom kontexte.

Nezverejniteľné údaje, či už osobné alebo iné, odporúčame deliť do nasledujúcich podkategórií (Tabuľka 3~~Tabuľka 3~~).

### Tabuľka 3: Podkategórie nezverejniteľných údajov (NZ)

| Kategória | Definícia |
|---|---|
| Vyhradené | Osobné alebo iné údaje, ktoré podliehajú najprísnejším požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko pre organizáciu a zákazníkov v prípade nesprávnej manipulácie. |
| Dôverné | Osobné alebo iné údaje, ktoré podliehajú prísnym požiadavkám na spracovanie vzhľadom na ich citlivosť a riziko v prípade nesprávneho zaobchádzania. |
| Interné | Údaje, ktoré sú zamestnancom a prípadným tretím stranám k dispozícii na základe zmluvy/dohody o (zachovaní) mlčanlivosti výlučne v dôsledku ich zamestnania v organizácii alebo prebiehajúceho projektu či poskytovania služby a ktoré nie sú kategorizované ako dôverné alebo obmedzené. |

Na základe priradenej úrovne k nezverejniteľným údajom sa aplikuje príslušná politika správy aktív. Politike správy aktív predchádza identifikácia aktív, ktorá je súčasťou bezpečnostného projektu podľa platnej metodiky a jeho bezpečnostnej dokumentácie vzhľadom na legislatívne požiadavky zákona č. 95/2019 Z.z. a jeho vykonávacích predpisov pre potreby informačného systému verejnej správy.






Tento projekt je podporený z Európskeho sociálneho fondu.

## 2.3 Princípy bezpečnosti údajov

### 2.3.1 Bezpečnosť údajov pri uchovávaní („at rest“)

Princípy bezpečnosť údajov treba zaviesť do rôznych systémov pre uchovávanie – viď Tabuľka 1~~Tabuľka 1~~. Ide predovšetkým o nasledujúce:

- Šifrovať údaje pri uchovávaní („at rest“) neprelomiteľným algoritmom, ideálne takým, ktorý obstojí aj v postkvantovej dobe.
- Minimalizovať počet ľudí, ktorý majú k údajom prístup a mať zavedené procesy na odoberanie prístupov, ako aj na proaktívne sledovanie, kto prístupy potrebuje a aj skutočne využíva.
- Nastavená politika po uplynutí vopred definovaného obdobia uchovávania.

### 2.3.2 Bezpečnosť údajov pri prenose

Ide o scenár, kedy údaje opúšťajú pôvodné agendové systémy a dostanú sa do systémov alebo rúk príjemcov. V tejto oblasti dochádza k zaujímavému prekrývaniu bezpečnosti údajov a ochrany súkromia. Ak by niekto zachytil údaje počas ich prenosu medzi dvoma systémami, toto porušenie bezpečnosti by takmer nevyhnutne viedlo k narušeniu súkromia, napríklad zneužitím osobných údajov. Znížiť vplyv tohto narušenia súkromia možno použitím pseudonymizačných techník na údaje pred ich prenosom, popísaných v kapitole 6.1 dokumentu 1.1.5 Štandardizácia anonymizácie údajov, ale treba tiež znížiť pravdepodobnosť zachytenia týchto údajov aj použitím špecifických kontrolných mechanizmov. Bezpečnostné stratégie treba navrhnúť v spolupráci s bezpečnostným tímom.Tu dávame k dispozícii základný kontrolný zoznam princípov, ktorý je východiskovým bodom. V prípade najcitlivejších údajov (úroveň „Vyhradené“ a „Dôverné“) zasielaných elektronickým prenosom by mali platiť nasledujúce princípy:

- Údaje musia byť v ideálnom prípade predmetom „end-to-end“ šifrovania pri tranzite na servisnej vrstve so vzájomným TLS, ak je to technicky možné. Ak vzájomné TLS nie je možné, treba použiť bežné SSL/TLS, pretože nešifrované HTTP by mohlo predstavovať bezpečnostné riziko.
- Distribúcia údajov prostredníctvom e-mailu je neprípustná, pretože e-mail je zo svojej podstaty nezabezpečený. Vytvára sa tak viacero kópií údajov, čím sa zväčšuje priestor na útoky, a je oveľa ťažšie kontrolovať a sledovať, kde sa tieto kópie nachádzajú, a vytvárať kontroly prístupu k nim. Okrem toho aj skúsení inžinieri často používajú e-mail na odosielanie citlivých údajov, keď sa ponáhľajú, mysliac si, že to urobia "len raz". Časom sa z týchto inštinktov stanú návyky. Takto sa darí pokusom o phishing - externí útočníci môžu používať e-maily ako vstupný bod do agendových IT systémov a extrahovať citlivé údaje.
- Kontroly ochrany súkromia sa sledujú a prispôsobujú na základe dvoch bodov prenosu pre údaje (napríklad z interného dátového centra do externého dátového centra). Treba použiť techniky šifrovania prispôsobené každému typu prenosu, definovanému výstupným a vstupným bodom.






Tento projekt je podporený z Európskeho sociálneho fondu.

## 2.4 Princípy ochrany osobných údajov

Ochrana osobných údajov z pohľadu ochrany súkromia cez princípy anonymizácie a pseudonymizácie je pokrytá aj v dokumente 1.1.5 Štandardizácia anonymizácie údajov.

Dôsledná ochrana osobných údajov, a teda súkromia osôb, si vyžaduje:

- Zavedenie "kultúry učenia, školenia a dôvery", v rámci ktorej sa môžu úradníci a inžinieri naučiť zaobchádzať s údajmi opatrne a s náležitou starostlivosťou. Inžinieri, interní aj externí, musia byť vyškolení, i) aby nepracovali v silách, ale namiesto toho aby ich činnosť bola založená na princípe interoperability a spolupráce, ii) aby chránili údaje dotknutých osôb a iii) aby ich činnosť bola založená na hľadaní dôvery, a nie na súťaživosti a utajovaní.
- Pochopenie zložitosti implementácie nástrojov na ochranu súkromia vo veľkom meradle, ako aj potrebu, aby technické tímy mali podporu vrcholného vedenia orgánu verejnej moci (organizácie) a rozpočet potrebný na vykonanie práce.
- Schopnosti v organizácii navrhnúť technické riešenia ochrany súkromia a prijímať rozhodnutia založené na údajoch, aby technické tímy mali jasné usmernenie.

**Tabuľka 4: Ciele ochrany údajov pokryté jednotlivými článkami GDPR**

| | Ciele ochrany údajov | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Minimalizácia** | **Dostupnosť** | **Integrita** | **Dôvernosť** | **Nespojiteľnosť** | **Transparentnosť** | **Intervencia** | **Súčinnosť, spolupráca** |
| **Články GDPR** | 5 (1) (c), 5 (1) (e), | 5 (1) (e), | 5 (1) (f), | 5 (1) (f), | 5 (1) (c), 5 (1) (e), | 5 (1) (a), | 5 (1) (d), 5 (1) (f), | |
| | | 13, 15, | | | 17, 18, | 13, 14, 15, 19, | 13 (2) (c), 14 (2) (d), 15 (1) (e), 16, 17, 18, | |
| | 25, 28, 29, | 20, 25, | 25, | 25, 28 (3) (b), 29, | 22, 25, | 25, | 20, 21, 22 (3), 25, | |
| | 30, 32, 39 | 32, | 32, 33, 34, 39, | 32, 39, | 32, 33, | 30, 32, 33, 39, | 32, 39, | 31, 39, |
| | | 49, | 49, | 49, | 40 (2) (d), | 40, 42, | | |
| | | | | | 52 | 53, 58, | 59, | 50, 53, |
| | | | | | | 60, 61, 63, | 65, 66, 68, 69, | 60, 61, 62, 67, 68, |
| | | 78, 79, | 78 | 78, | | 74, 78, | 70, 78, | 70, 78, |
| | | 86 | | 83 | | 84, 85, 86, 87, | 83 | |
| | | | | | | 90, 91 | | |

## 2.5 Medzinárodné štandardy pre bezpečnosť údajov

### 2.5.1 Prehľad štandardov ISO/IEC 27000

ISO/IEC normy radu 27000 predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti odvodené od britských štandardov radu BS 7799. Uvedený







Tento projekt je podporený z Európskeho sociálneho fondu.

prehľad obsahuje názvy a označenia jednotlivých noriem spolu s ich stručným opisom. Získať samotné normy alebo viac informácií je možné na webovom sídle Medzinárodnej organizácie pre štandardizáciu ISO.

### Tabuľka 5: Prehľad štandardov ISO/IEC 27000

| Štandard | Popis |
|---|---|
| **ISO/IEC 27000: 2018** | ISO/IEC 27000: 2018 poskytuje prehľad systémov manažérstva informačnej bezpečnosti (SMIB) a základne pojmy a definície bežne používané v štandardoch radu 27000. Je aplikovateľný na všetky typy a veľkosti organizácií (vládne, komerčné, neziskové). |
| **ISO/IEC 27001:2013** | ISO/IEC 27001:2013 špecifikuje požiadavky na vytvorenie, implementáciu, udržiavanie a zlepšovanie SMIB v kontexte organizácie. Tiež obsahuje požiadavky na posudzovanie a narábanie s rizikami informačnej bezpečnosti. Požiadavky tejto normy sú generické a aplikovateľné na všetky organizácie nezávisle na ich type, veľkosti a charaktere. |
| **ISO/IEC 27002:2013** | ISO/IEC 27002:2013 poskytuje pokyny pre štandardy informačnej bezpečnosti organizácie a praktiky riadenia informačnej bezpečnosti vrátane výberu, implementácie a riadenia opatrení berúc do úvahy rizikové prostredia informačnej bezpečnosti organizácie. Je navrhnutý pre organizácie, ktoré zamýšľajú:<br>výber opatrení v rámci procesu implementácie SMIB založeného na ISO/IEC 27001,<br>implementáciu všeobecne akceptovaných opatrení informačnej bezpečnosti,<br><br>vývoj vlastných smerníc pre informačnú bezpečnosť. |
| **ISO/IEC 27003:2017** | SO/IEC 27003:2017 sa zameriava na kritické aspekty úspešného návrhu a implementácie SMIB v súlade s ISO/IEC 27001:2013. Popisuje proces špecifikácie a návrhu SMIB od počiatku až po vytvorenie plánu implementácie. |
| **ISO/IEC 27004:2016** | ISO/IEC 27004:2016 poskytuje návod pre vývoj a používanie metrík a merania pre posúdenie efektivity implementovaného SMIB a opatrení špecifikovaných v ISO/IEC 27001. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27005:2018** | ISO/IEC 27005:2018 poskytuje návod pre riadenie rizík informačnej bezpečnosti. Podporuje všeobecné koncepty špecifikované v ISO/IEC 27001 a je navrhnutý tak, aby podporoval implementáciu informačnej bezpečnosti založenej na riadení rizík. |
| **ISO/IEC 27006:2015** | ISO/IEC 27006:2015 špecifikuje požiadavky a poskytuje návod pre organizácie poskytujúce audit a certifikácie SMIB. Štandard je primárne zameraný na podporu akreditácie organizácií poskytujúcich certifikáciu SMIB. |
| **ISO/IEC 27007: 2020** | ISO/IEC 27007:2017 poskytuje návod a požiadavky pre riadenie programu auditov SMIB, vykonávanie auditov a kompetencie audítorov SMIB. |
| **ISO/IEC TS 27008:2019** | ISO/IEC TS 27008:2019 poskytuje návod na preskúmavanie a posudzovanie implementácie a prevádzky opatrení, vrátane technického súladu opatrení informačnej bezpečnosti. |
| **ISO/IEC 27009:2020** | ISO/IEC 27009:2016 definuje požiadavky na používanie ISO / IEC 27001 v každom špecifickom sektore (oblasť použitia alebo trhový sektor). Vysvetľuje, ako zahrnúť dodatočné požiadavky k požiadavkám v ISO / IEC 27001, ako zdokonaliť niektorú z požiadaviek a ako zahrnúť opatrenia alebo súbory opatrení navyše k ISO / IEC 27001. Táto medzinárodná norma zabezpečuje, že dodatočné alebo vylepšené požiadavky nie sú v rozpore s požiadavkami normy ISO / IEC 27001. Cieľovou skupinou tejto medzinárodnej normy sú subjekty, ktoré vyrábajú odvetvovo špecifické normy, ktoré sa týkajú ISO / IEC 27001. |
| **ISO/IEC 27010:2015** | ISO/IEC 27010:2015 poskytuje návod pre implementáciu riadenia informačnej bezpečnosti v rámci organizácií zdieľajúcich informácie. Je aplikovateľný na všetky formy výmeny a zdieľania citlivých informácií (verejné, súkromné, národné, medzinárodné, v rámci odvetvia, alebo medzi jednotlivými sektormi). |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27011:2016** | ISO/IEC 27011:2016 Cieľom tohto návodu je podporiť implementáciu riadenia informačnej bezpečnosti v telekomunikačných organizáciách. Prijatie tohto štandardu umožní telekomunikačným organizáciám splniť základné požiadavky na dostupnosť, dôvernosť a integritu. |
| **ISO/IEC 27013:2015** | ISO/IEC 27013:2015 poskytuje návod pre integrovanú implementáciu ISO 27001 a ISO 20000-1 pre organizácie, ktoré zamýšľajú:<br>implementovať ISO 27001 po predchádzajúcej implementácií ISO 20000-1 alebo opačne,<br>implementovať súčasne ISO 27001 a ISO 20000-1,<br><br>integrovať existujúce ISO 27001 a ISO 20000-1 manažérske systémy. |
| **ISO/IEC 27014:2013** | ISO/IEC 27014:2013 poskytuje koncepty a princípy strategického riadenia informačnej bezpečnosti (Governance) pomocou ktorých môžu organizácie vyhodnocovať, koordinovať, monitorovať a komunikovať aktivity súvisiace s informačnou bezpečnosťou. |
| **ISO/IEC TR 27016:2014** | ISO/IEC TR 27016:2014 poskytuje návod pre organizácie pre tvorbu rozhodnutí o ochrane informácií a pochopenie ekonomických dôsledkov týchto rozhodnutí v kontexte konkurenčných požiadaviek na zdroje. |
| **ISO/IEC 27017:2015** | ISO/IEC 27017:2015 je kódexom postupov, ktorý poskytuje dodatočné odporúčania na implementáciu opatrení informačnej bezpečnosti nad rámec toho, čo je uvedené v ISO / IEC 27002, v kontexte cloud computingu. Štandard radí zákazníkom cloudových služieb aj poskytovateľom cloudových služieb, pričom v každom oddiely sú uvedené primárne pokyny. |
| **ISO/IEC 27018:2019** | ISO/IEC 27018:2014 ustanovuje všeobecne prijaté ciele riadenia, opatrenia a návod pre implementáciu opatrení na ochranu osobných údajov (Personally Identifiable Information) v súlade s princípmi ochrany súkromia v ISO/IEC 29100 pre verejné cloudy. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27019:2017** | ISO/IEC TR 27019:2017 poskytuje návod založený na ISO/IEC 27002 na aplikáciu riadenia informačnej bezpečnosti na riadiace a kontrolné systémy používané v energetickom priemysle. |
| **ISO/IEC 27021:2017** | ISO/IEC 27021:2017 sa týka spôsobilostí požadovaných alebo očakávaných od odborníkov, ktorí riadia ISMS v súlade s normami ISO / IEC 27001, 27002, 27005 a 27007.Norma nešpecifikuje systém osobnej certifikácie alebo kvalifikácie ako taký, ale v skutočnosti slúži ako referencia pre orgány, ktoré takéto systémy prevádzkujú. Norma nezahŕňa spôsobilosť audítora. |
| **ISO/IEC TR 27023:2015** | ISO/IEC 27023:2015 mapuje alebo porovnáva vydania z roku 2013 podľa noriem ISO / IEC 27001 a ISO / IEC 27002 s predchádzajúcimi vydaniami, pričom uvádza, kde sa pôvodná sekcia skončila. |
| **ISO/IEC 27031:2011** | ISO/IEC 27031:2011 popisuje koncepty a princípy pripravenosti IKT na kontinuitu činností a poskytuje rámec metód a procesov pre identifikáciu a špecifikáciu všetkých aspektov (kritérií výkonnosti, návrhu a implementácie) pre zlepšovanie pripravenosti IKT organizácie na zaistenie kontinuity činností. |
| **ISO/IEC 27032:2012** | ISO/IEC 27032:2012 poskytuje návod pre zlepšovanie stavu kybernetickej bezpečnosti popisujúc špecifické aspekty tejto aktivity a jej závislosti na ostatných oblastiach bezpečnosti, ako napr.:<br>informačná bezpečnosť,<br>sieťová bezpečnosť,<br>bezpečnosť internetu,<br><br>ochrana kritickej informačnej infraštruktúry (CIIP). |
| **ISO/IEC 27033-1:2015** | ISO/IEC 27033-1:2015 poskytuje prehľad sieťovej bezpečnosti a súvisiacich definícií. |
| **ISO/IEC 27033-2:2012** | ISO/IEC 27033-2:2012 poskytuje návod pre plánovanie, návrh, implementáciu a dokumentovanie sieťovej bezpečnosti v organizácii. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27033-3:2010** | ISO/IEC 27033-3:2010 popisuje hrozby, techniky návrhu a problémy súvisiace s opatreniami súvisiacimi s referenčnými sieťovými scenármi. Pre každý scenár poskytuje detailný návod pre narábanie s bezpečnostnými hrozbami, technikami návrhu opatrení a opatreniami na minimalizáciu súvisiacich rizík. |
| **ISO/IEC 27033-4:2014** | ISO/IEC 27033-4:2014 poskytuje návod pre zabezpečenie komunikácie medzi sieťami použitím bezpečnostných brán (firewall, aplikačný firewall, IPS) v súlade s dokumentovanou politikou informačnej bezpečnosti. |
| **ISO/IEC 27033-5:2013** | ISO/IEC 27033-5:2013 poskytuje návod pre výber, implementáciu a monitorovanie technických opatrení potrebných na zaistenie sieťovej bezpečnosti využitím pripojení virtuálnej súkromnej siete (VPN) na prepojenie sietí a pripojenie vzdialených používateľov do týchto sietí. |
| **ISO/IEC 27033-6:2016** | ISO/IEC 27033-6:2016 popisuje hrozby, bezpečnostné požiadavky, bezpečnostné opatrenia a spôsoby návrhu bezdrôtových sietí. Je relevantná pre všetkých pracovníkov, ktorí sa podieľajú na podrobnom plánovaní, navrhovaní a implementácii bezpečnosti bezdrôtových sietí (napríklad sieťoví architekti a dizajnéri, správcovia sietí a pracovníci pre bezpečnosť siete). |
| **ISO/IEC 27034-1:2011** | ISO/IEC 27034-1:2011 poskytuje organizáciám pomoc pri integrovaní bezpečnosti do procesov na riadenie aplikácií. Poskytuje prehľad aplikačnej bezpečnosti, oboznamuje s definíciami, konceptmi, princípmi a procesmi súvisiacimi s aplikačnou bezpečnosťou. |
| **ISO/IEC 27034-2:2015** | ISO/IEC 27034-2:2015 vysvetľuje štruktúru, vzťahy a vzájomné závislosti medzi procesmi v organizačnom normatívnom rámci (ONF) – súbor politík, postupov, rolí a nástrojov súvisiacich s bezpečnosťou aplikácií. Cieľom normy je usmerňovať organizácie pri navrhovaní, implementácii, prevádzke a audite ich ONF. |
| **ISO/IEC 27034-3:2018** | ISO/IEC 27034-3:2018 opisuje proces riadenia bezpečnosti aplikácií, t. j. celkový proces riadenia bezpečnosti pre každú konkrétnu aplikáciu používanú organizáciou. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27034-5:2017** | ISO/IEC 27034-5:2017 definuje dátovú štruktúru Application Security Control (ASC), ktorá poskytuje požiadavky, popisy, grafické reprezentácie a XML schémy pre dátový model. Schéma XML založená na norme ISO / TS 15000: Elektronický obchodný eXtensible Markup Language ebXML, je určený ako štandardný formát výmeny pre ASC. |
| **ISO/IEC 27034-5-1:2018** | ISO/IEC 27034-5-1:2018 schémy XML implementujú minimálny súbor požiadaviek na informácie a základné atribúty ASC a aktivity a úlohy referenčného modelu životného cyklu aplikácie Security Security z časti 5. |
| **ISO/IEC 27034-6:2016** | ISO/IEC 27034-6:2016 poskytuje príklady, ako by mohli byť vyvinuté a zdokumentované bezpečnostné opatrenia aplikácií (ASC), ktoré definujú, ako sa má v priebehu vývoja softvéru riešiť bezpečnosť informácií. |
| **ISO/IEC 27034-7:2018** | ISO/IEC 27034-7:2018 sa týka rámca poskytujúceho záruku potrebnú na zabezpečenie dôvery v bezpečnostných opatreniach počítačového programu, napríklad keď sa jeden program spolieha na iný (napr. systém správy databáz, obslužný program, operačný systém alebo sprievodný program) na vykonávanie kritických bezpečnostných funkcií (ako napríklad autentifikácia užívateľa, riadenie logického prístupu alebo kryptografia), alebo keď organizácia aktualizuje alebo opravuje dôveryhodný program. |
| **ISO/IEC 27035-1:2016** | ISO/IEC 27035-1: 2016 načrtáva koncepcie a zásady, na ktorých sa zakladá riadenie incidentov v oblasti bezpečnosti informácií, a zavádza zostávajúcu časť / normy. Popisuje proces riadenia incidentov informačnej bezpečnosti, ktorý sa skladá z piatich fáz a hovorí, ako zlepšiť riadenie incidentov. |
| **ISO/IEC 27035-2:2016** | ISO/IEC 27035-2:2016 sa týka uistenia, že organizácia je skutočne pripravená primerane reagovať na incidenty v oblasti bezpečnosti informácií, ktoré sa ešte môžu vyskytnúť. Rieši rétorickú otázku „Sme pripravení reagovať na incident?“, a podporuje učenie sa z incidentov s cieľom zlepšiť veci do budúcnosti. Zahŕňa fázy plánu a prípravy a poučenia z procesu, ktorý je stanovený v časti 1 – začiatok a koniec. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27036-1:2014** | ISO/IEC 27036-1:2014 poskytuje pomoc organizáciám pri zabezpečení ich informácií a informačných systémov v kontexte vzťahov s dodávateľmi. |
| **ISO/IEC 27036-2:2014** | ISO/IEC 27036-2:2014 špecifikuje základné požiadavky informačnej bezpečnosti na definovanie, implementovanie, prevádzku, monitorovanie, preskúmavanie, udržiavanie a zlepšovanie vzťahov s dodávateľmi a nadobúdateľmi. |
| **ISO/IEC 27036-3:2013** | ISO/IEC 27036-3:2013 poskytuje návod pre dodávateľov a nadobúdateľov prostriedkov IKT na:<br>získanie prehľadu a riadenie rizík informačnej bezpečnosti spôsobených fyzicky rozptýlenými a mnoho vrstvovými dodávateľskými reťazcami,<br>reakciu na riziká vyplývajúce z globálneho dodávateľského reťazca prostriedkov IKT , ktoré môžu mať dopad na organizácie používajúce tieto prostriedky IKT,<br>integráciu procesov informačnej bezpečnosti do životného cyklu informačných systémov a softvéru. |
| **ISO/IEC 27036-4:2016** | ISO/IEC 27036-4:2016ponúka poradenstvo v oblasti informačnej bezpečnosti pre dodávateľov a zákazníkov cloudových služieb. |
| **ISO/IEC 27037:2012** | ISO/IEC 27037:2012 poskytuje návod pre špecifické aktivity pri narábaní s digitálnymi dôkazmi, ktorými sú identifikácia, zber, získanie a uchovávanie potenciálnych digitálnych dôkazov, ktoré môžu mať dôkaznú hodnotu. |
| **ISO/IEC 27038:2014** | ISO/IEC 27038:2014 špecifikuje techniky vykonávania digitálnej redakcie elektronických dokumentov. Tiež špecifikuje požiadavky na softvérové nástroje používané pri odstraňovaní citlivých informácií zo zverejňovaných elektronických dokumentov a metódy testovania bezpečného odstraňovania týchto informácií. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27039:2015** | ISO/IEC 27039:2015 poskytuje pokyny na pomoc organizáciám pri príprave na zavedenie systémov detekcie a/alebo prevencie prienikov (IDPS). Týka sa najmä výberu, zavádzania a prevádzky IDPS. Poskytuje tiež základné informácie, z ktorých sú tieto usmernenia odvodené. |
| **ISO/IEC 27040:2015** | Cieľom ISO/IEC 27040:2015 je pomôcť organizáciám pri plánovaní, návrhu, dokumentovaní a implementácií bezpečnosti úložných médií a pri určovaní a ošetrovaní súvisiacich rizík informačnej bezpečnosti. Rozsah zahŕňa bezpečnosť zariadení a médií, bezpečnosť riadiacich činností súvisiacich so zariadeniami a médiami, aplikáciami / službami a koncovými používateľmi, ako aj bezpečnosť informácií prenášaných cez komunikačné prepojenia spojené s ukladaním. Norma popisuje riziká spojené s ukladaním údajov a opatrenia na zmiernenie týchto rizík. |
| **ISO/IEC 27041:2015** | ISO/IEC 27041:2015 poskytuje usmernenie o mechanizmoch na zabezpečenie toho, aby metódy a postupy používané pri vyšetrovaní incidentov informačnej bezpečnosti boli „vhodné na daný účel“. Zahŕňa osvedčené postupy pri definovaní požiadaviek, opisovaní metód a poskytovaní dôkazov, že implementácia metód môže preukázať, že spĺňajú požiadavky. |
| **ISO/IEC 27042:2015** | Štandard ISO/IEC 27042:2015 ponúka návod na proces analýzy a interpretácie digitálnych dôkazov, čo je samozrejme len časť forenzného procesu. Stanovuje všeobecný rámec zahŕňajúci osvedčené postupy v tejto oblasti. |
| **ISO/IEC 27043:2015** | ISO/IEC 27043:2015 poskytuje usmernenia založené na idealizovaných modeloch pre všeobecné procesy vyšetrovania incidentov naprieč rôznymi scenármi zahŕňajúce digitálne dôkazy. Patria sem procesy od prípravy pred incidentom až po vrátenie , ako aj všetky všeobecné odporúčania a upozornenia na takéto procesy. |
| **ISO/IEC 27050-1:2019** | ISO/IEC 27050-1:2016 poskytuje prehľad o eDiscovery; definuje pojmy, koncepty, procesy atď., ako napríklad elektronicky uložené informácie; zavádza a definuje rozsah a kontext tejto viacdielnej normy. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO/IEC 27050-2:2018** | ISO/IEC 27050-2:2018 vedenie manažmentu pri identifikácii a spracovaní informačných rizík súvisiacich s eDiscovery, napr. stanovením a uplatňovaním politík súvisiacich s eDiscovery a dodržiavaním príslušných (väčšinou právnych) povinností a očakávaní. |
| **ISO/IEC 27050-3:2017** | ISO/IEC 27050-3:2017identifikuje požiadavky a ponúka usmernenie k identifikácii elektronicky uložených informácií (ESI) a ich uchovávaniu, zberu, spracovaniu, preskúmavaniu, analýze a tvorbe. |
| **ISO/IEC 270102:2019** | Štandard ISO/IEC 270102:2019 poskytuje pokyny pri zvažovaní nákupu kybernetického poistenia, ako možnosť zníženia dopadu kybernetického incidentu v rámci systému riadenia rizík informačnej bezpečnosti organizácie. Je použiteľná pre organizácie všetkých typov, veľkostí a charakteru, aby pomohol pri plánovaní a kúpe kybernetického poistenia. |
| **ISO/IEC TR 270103:2018** | ISO/IEC 27034-3:2018 poskytuje informácie o tom, prečo je dôležitý rámec pre riziká, priority, flexibilitu, zameranie na výsledky a komunikačný rámec pre kybernetickú bezpečnosť. Potom opisuje ciele silného rámca kybernetickej bezpečnosti a zahŕňa mapovanie existujúcich noriem, ktoré možno použiť na dosiahnutie týchto cieľov. |
| **ISO/IEC 27551** | ISO/IEC 27550:2019 poskytuje usmernenia k ochrane súkromia, je určené na pomoc organizáciám pri integrácií najnovších postupov, v oblasti ochrany súkromia, do procesov a systémov. Opisuje vzťah medzi súkromným inžinierstvom a inými inžinierskymi hľadiskami. Opisuje aj riadenie znalostí, riadenie rizika, analýza požiadaviek a návrh architektúry pri ochrane súkromia. |
| **ISO/IEC 27701:2019** | ISO 27701:2019 špecifikuje požiadavky a poskytuje návod na zriadenie, implementáciu, údržbu a neustále zlepšovanie systému riadenia informácií o ochrane súkromia (PIMS) vo forme rozšírenia noriem ISO/IEC 27001 a ISO/IEC 27002 na správu súkromia v organizácií. |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Štandard | Popis |
|---|---|
| **ISO 27799:2016** | ISO 27799:2016 poskytuje návod a podporu pri interpretácii a implementácii ISO 27002 do zdravotníckych organizácií. |







Tento projekt je podporený z Európskeho sociálneho fondu.

# 3 Posúdenie požiadaviek na aplikáciu štandardu v rámci verejnej správy

## 3.1 Regulácia bezpečnosti údajov a ochrany osobných údajov

### 3.1.1 Prehľad relevantnej legislatívy

Regulácia bezpečnosti údajov a ochrany údajov je realizovaná najmä nasledovnými právnymi predpismi:

- Nariadenie 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 - z angl. General Data Protection Regulation, ďalej aj ako "**Nariadenie**" alebo "**GDPR**)
- zákon č. 18/2018 Z.z. o ochrane osobných údajov o ochrane osobných údajov (ďalej aj ako "**Zákon**" alebo "**zákon o ochrane osobných údajov**"),
- Zákon číslo 95/2019 Z. z. o informačných technológiach vo verejnej správe (ďalej aj ako "**zákon o informačných technológiách vo verejenej správe**"),
- Zákon číslo 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej aj ako "**zákon o kybernetickej bezpečnosti**").

#### *3.1.1.1 GDPR a Zákon*

##### *Predmet úpravy a ciele*

Cieľom GDPR je stanoviť jednotné zásady a pravidlá ochrany osobných údajov pre jednotlivé členské štáty Európskej únie. Zároveň nariadenie zabezpečuje voľný tok osobných údajov a vymedzuje hranice spracúvania osobných údajov. Poskytuje legislatívne útočisko pre všetky fyzické osoby v oblasti ochrany ich osobných údajov a uplatňovania svojich základných práv a slobôd v medziach ochrany osobných údajov. Vznikom GDPR sa zabránilo rozdielom, ktoré by mohli vznikať pri ochrane osobných údajov fyzických osôb v rámci celej EÚ.

Hlavným cieľom vzniku a prijatia GDPR bolo zabezpečenie konzistentnej a vysokej úrovne ochrany fyzických osôb a odstránenie prekážok v tokoch osobných údajov v rámci EÚ. Tento cieľ vychádza z predpokladu, že úroveň ochrany práv a slobôd fyzických osôb pri spracúvaní osobných údajov by mala byť vo všetkých členských štátoch rovnaká, a že v rámci celej EÚ by malo byť zabezpečené konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv a slobôd fyzických osôb pri spracúvaní osobných údajov.

GDPR zároveň poskytuje členským krajinám priestor pre zachovanie alebo prijatie vnútroštátnych predpisov spresňujúcich uplatňovanie pravidiel stanovených týmto všeobecným nariadením, ako aj svojich vnútroštátnych pravidiel vrátane pravidiel spracúvania osobitných kategórií osobných údajov, označovaných aj ako citlivé údaje). Tieto úlohy v slovenskom právnom poriadku plní zákon o ochrane osobných údajov, ktorý spresňuje úpravu práv, povinností a zodpovednosti pri spracúvaní osobných






Tento projekt je podporený z Európskeho sociálneho fondu.

údajov fyzických osôb, bližšie špecifikuje ochranu práv fyzických osôb pred neoprávneným spracúvaním ich osobných údajov a zároveň ustanovuje postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len ako „Úrad“ alebo „Úrad na ochranu osobných údajov“).

### *Pôsobnosť GDPR a zákona o ochrane osobných údajov*

GDPR a Zákon o ochrane osobných údajov sa vzťahujú na spracúvanie osobných údajov vykonávané:

- úplne alebo čiastočne automatizovanými prostriedkami a aj
- inými prostriedkami, ak tieto údaje tvoria alebo majú tvoriť súčasť informačného systému,
- nevzťahujú sa napríklad na osobné údaje, ktoré sú spracúvané fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti, Slovenskou informačnou službou, Vojenským spravodajstvom, alebo Národným bezpečnostným úradom Slovenskej republiky, ani na osobné údaje zosnulých osôb.

Zákon sa vzťahuje na spracúvanie osobných údajov:

- v rámci činnosti prevádzkovateľa alebo sprostredkovateľa, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt je na území Slovenskej republiky, a to bez ohľadu na to, či sa spracúvanie osobných údajov vykonáva na území Slovenskej republiky alebo mimo územia Slovenskej republiky,
- v rámci činnosti prevádzkovateľa alebo sprostredkovateľa, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt nie je na území Slovenskej republiky, ale je v mieste, kde sa na základe medzinárodného práva verejného uplatňuje právny poriadok Slovenskej republiky,
- dotknutej osoby, ktorá sa nachádza na území Slovenskej republiky, prevádzkovateľom alebo sprostredkovateľom, ktorého sídlo, miesto podnikania, organizačná zložka, prevádzkareň alebo trvalý pobyt nie je v členskom štáte, pričom spracúvanie osobných údajov súvisí s ponukou tovaru alebo služieb tejto dotknutej osobe na území Slovenskej republiky bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba alebo nie, alebo so sledovaním jej správania na území Slovenskej republiky.

Zákon o ochrane osobných údajov garantuje voľných pohyb osobných údajov medzi Slovenskou republikou a členskými štátmi EÚ, pričom Slovenská republika neobmedzí ani nezakáže prenos osobných údajov z dôvodu ochrany základných práv a fyzických osôb, najmä ich práva na súkromie.

Na spracúvanie osobných údajov inštitúciami, orgánmi, úradmi a agentúrami EÚ sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES.







Tento projekt je podporený z Európskeho sociálneho fondu.

## *Vysvetlenie vybraných pojmov*

**Spracúvanie osobných údajov -** spracovateľská operácia s osobnými údajmi, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

**Dotknutá osoba -** každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

**Osobný údaj -** všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.

**Prevádzkovateľ -** každý, kto vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene.

**Sprostredkovateľ -** každý, kto spracúva osobné údaje v mene prevádzkovateľa.

**Príjemca -** každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy.

**Tretia strana -** každý, kto nie je dotknutou osobou, prevádzkovateľom, sprostredkovateľom alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

**Informačný systém -** 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 základe alebo geografickom základe.

**Profilovanie -** automatizované spracúvanie osobných údajov, na základe ktorého dochádza k vyhodnocovaniu alebo vyhodnoteniu určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

**Pseudonymizácia -** spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií.

**Logovanie –** záznam o tom, aké činnosti prebiehali alebo prebiehajú v automatizovanom informačnom systéme.

**Šifrovanie -** transformácia osobných údajov spôsobom, vďaka ktorému je opätovné spracúvanie možné napríklad len po zadaní kľúču alebo hesla.

**Online identifikátor -** najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, a ktoré sa v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.







Tento projekt je podporený z Európskeho sociálneho fondu.

## *Osobné údaje*

GDPR stanovuje, aké informácie majú byť považované za osobné údaje, pričom ide o **všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby**. To znamená, že osobnými údajmi sú všetky informácie alebo útržky informácií, ktoré po spojení môžu byť priradené ku konkrétnej osobe alebo môžu viesť k identifikácii konkrétnej osoby.

Za osobné údaje sú považované aj **pseudonymizované osobné údaje**, teda osobné údaje ktoré boli odidentifikované alebo zašifrované, ale je možné ich použiť na opätovnú identifikáciu konkrétnej osoby, na základe čoho aj takéto osobné údaje patria pod ochranu GDPR.

Osobné údaje, ktoré boli **anonymizované** takým spôsobom, že jednotlivca viac nemožno identifikovať, sa viac nepovažujú za osobné údaje. Na to, aby údaje boli skutočne anonymizované, musí byť anonymizácia nezvratná.

GDPR chráni osobné údaje **bez ohľadu na technológiu použitú na spracovanie týchto údajov**. Sú teda technologicky neutrálne a pokiaľ sú údaje organizované podľa vopred vymedzených kritérií (napr. v abecednom poradí), tak sa uplatňujú na automatizované aj manuálne spracovanie. Nezáleží ani na tom, ako sa údaje ukladajú – či už v systéme IT, v bezpečnostnom kamerovom systéme alebo na papieri. Vo všetkých prípadoch osobné údaje podliehajú požiadavkám na ochranu definovaným v GDPR.

**Príklady osobných údajov:**

- meno a priezvisko
- domáca adresa
- e-mailová adresa, napr. *priezvisko@podnik.com*
- číslo preukazu totožnosti
- lokalizačné údaje (napr. funkcia lokalizačných údajov na mobilnom telefóne)*
- adresa internetového protokolu (IP)
- ID súboru cookie
- reklamný identifikátor na vašom telefóne
- údaje, ktoré uchováva nemocnica alebo lekár, napr. to môže byť symbol, ktorý jedinečne identifikuje osobu

V niektorých prípadoch existujú osobitné odvetvové právne predpisy, ktorými sa napr. riadi používanie lokalizačných údajov alebo používanie súborov cookies – smernica o súkromí a elektronických komunikáciách [smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 z 27. októbra 2004.

Príklady údajov, ktoré sa nepovažujú za osobné údaje:

- registračné číslo spoločnosti
- e-mailová adresa, napr. *info@podnik.com*
- anonymizované údaje







Tento projekt je podporený z Európskeho sociálneho fondu.

**Osobitné kategórie osobných údajov (citlivé údaje):**

Osobitné kategórie osobných údajov sú typy osobných údajov, ktorých spracúvanie je nariadením vo všeobecnosti zakázané a smú sa spracúvať iba na základe osobitných výnimiek, ktoré GDPR stanovuje v článku 9 ods. 2. Napríklad ak bol udelený výslovný súhlas alebo je spracúvanie potrebné z dôvodov významného verejného záujmu na základe práva EÚ alebo vnútroštátneho práva. Sú to údaje o:

- rasovom alebo etnickom pôvode
- sexuálnej orientácii
- politických názoroch
- náboženských alebo filozofických presvedčeniach
- členstve v odborových organizáciách
- genetických, biometrických alebo zdravotných informáciách

Ďalšou samostatnou kategóriou osobných údajov citlivej povahy podľa čl. 10 GDPR, sú napríklad údaje uznaní viny za trestné činy a priestupky, ktoré sa môžu spracúvať len pod kontrolou orgánov verejnej moci, alebo ak je to povolené právom EÚ alebo vnútroštátnym právom.

Právny základ a účel spracúvania osobných údajovOsobné údaje môžu byť spracúvané len na základe:

- **zákona alebo medzinárodnej zmluvy**, ak zákon alebo medzinárodná zmluva prijímateľovi osobných údajov alebo prevádzkovateľovi udelí právo určité osobné údaje spracúvať
- **súhlasu dotknutej osoby** so spracúvaním osobných údajov, ktorá udelí takýto súhlas osobe alebo osobám, ktoré budú jeho osobné údaje spracúvať, a to na konkrétny účel
- **zmluvy**, ak je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba

Osobné údaje môžu byť tiež spracúvané, ak je spracúvanie nevyhnutné na:

- ochranu života, zdravia alebo majetku
- splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi
- účel oprávnených záujmov prevádzkovateľa alebo tretej strany (tento právny základ nemôže byť uplatnený orgánmi verejnej moci pri plnení ich úloh).

Forma súhlasu

Súhlas musí byť poskytnutý jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním osobných údajov, ktoré sa jej týkajú, a to napríklad

- písomným vyhlásením,
- vyhlásením prostredníctvom elektronických prostriedkov (označením políčka na webe) alebo







Tento projekt je podporený z Európskeho sociálneho fondu.

- ústnym vyhlásením.

Zo súhlasu musí byť zrejmé, že dotknutá osoba súhlasí s navrhovaným spracúvaním jej osobných údajov. Mlčanie, vopred označené políčka alebo nečinnosť sa nepovažujú za súhlas so spracúvaním.

Náležitosti súhlasu

Ak je spracúvanie založené na súhlase dotknutej osoby, **prevádzkovateľ by mal vedieť preukázať**, že dotknutá osoba vyjadrila súhlas so spracúvaním, a že dotknutá osoba si je vedomá, že dáva súhlas a **v akom rozsahu ho udeľuje**.

Dotknutá osoba by si mala byť vedomá identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov. Ak sa spracúvanie vykonáva na viaceré účely, súhlas by sa mal udeliť na všetky tieto účely.

Súhlas sa nepovažuje za poskytnutý slobodne, ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov.

**Dotknutá osoba musí mať možnosť súhlas kedykoľvek odvolať, a to v rovnakej forme v akej súhlas udelila**.

Zlučiteľnosť účelov

Spracúvanie osobných údajov na iné účely ako na účely, na ktoré boli osobné údaje pôvodne získané, by malo byť umožnené len vtedy, ak je toto spracúvanie zlučiteľné s účelmi, na ktoré boli osobné údaje pôvodne získané. V takom prípade sa nevyžaduje žiadny iný samostatný právny základ, než je právny základ, ktorý umožňoval získavanie osobných údajov.

S cieľom zistiť, či je účel ďalšieho spracúvania v súlade s účelom, na ktorý boli osobné údaje pôvodne získané, by mal prevádzkovateľ po splnení všetkých požiadaviek zákonnosti pôvodného spracúvania zohľadniť okrem iného akékoľvek prepojenie medzi týmito účelmi a účelmi zamýšľaného ďalšieho spracúvania; kontext, v ktorom sa osobné údaje získali, najmä primerané očakávania dotknutých osôb vyplývajúce z ich vzťahu k prevádzkovateľovi, pokiaľ ide o ich ďalšie použitie; povahu osobných údajov; následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby; a existenciu primeraných záruk v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania.

Ak dotknutá osoba udelila súhlas alebo sa spracúvanie zakladá na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti, najmä na ochranu dôležitých verejných záujmov, mal by mať prevádzkovateľ možnosť osobné údaje ďalej spracúvať bez ohľadu na zlučiteľnosť účelov.

V každom prípade by sa malo zabezpečiť uplatnenie zásad stanovených GDPR a Zákonom, najmä povinnosti informovať dotknutú osobu o týchto iných účeloch a o jej právach vrátane práva namietať.

Oznámenie možných trestných činov alebo ohrozenia verejnej bezpečnosti prevádzkovateľom a poskytnutie relevantných osobných údajov v jednotlivých prípadoch alebo viacerých prípadoch týkajúcich sa toho istého trestného činu alebo ohrozenia verejnej bezpečnosti príslušnému orgánu by sa malo považovať za oprávnený záujem, ktorý sleduje prevádzkovateľ. Takéto poskytnutie v oprávnenom záujme






Tento projekt je podporený z Európskeho sociálneho fondu.

prevádzkovateľa alebo ďalšie spracúvanie osobných údajov by sa však malo zakázať, ak toto spracúvanie nie je v súlade s právnou, profesijnou alebo inou záväznou povinnosťou mlčanlivosti.

### *Zásady spracovúnia osobných údajov*

Všetky osoby, ktoré spracúvajú osobné údaje sú povinné dodržiavať pri spracúvaní nasledujúce zásady definované GDPR a Zákonom:

Zásada zákonnosti

Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby. To znamená, že osobné údaje je možné spracúvať len na právnych základoch stanovených zákonom. Pri spracúvaní osobných údajov je nevyhnutné riadiť sa ustanoveniami, povinnosťami a pravidlami uvedenými v Zákone alebo GDPR a prísne sledovať, či spôsob spracúvania osobných údajov nezasahuje nad mieru stanovenú Zákonom alebo GDPR do práv dotknutých osôb alebo nenarúša ich oprávnené záujmy.

Zásada obmedzenia účelu

Účel stanovený napríklad prevádzkovateľom nesmie byť vymedzený len všeobecne, účel musí byť určený konkrétne a výslovne uvedený napríklad v súhlase a v podmienkach ochrany osobných údajov viažucich sa na spracúvanie. Účel pre ktorý sa osobné údaje spracúvajú musí byť tiež , teda prevádzkovaľ musí mať v prvom rade právo osobné údaje na takýto účel spracúvať. Osobné údaje sa navyše nesmú spracúvať spôsobom, ktorý nie je zlučiteľný s účelom. Ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, je povolené, ak je v súlade s osobitným predpisom.

Zásada minimalizácie osobných údajov

Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú. Je potrebné zabezpečiť, aby sa na daný účel spracúvali len tie osobné údaje, ktorých spracúvanie je nevyhnutné pre dosiahnutie tohto účelu. Napríklad, ak údaj o veku dotknutej osoby nie je potrebné spracúvať pre dosiahnutie zamýšľaného účelu spracúvania, nesmie byť tento údaj spracúvávaný. To znamená, že nesmie dochádzať k tomu, aby boli spracúvávané akékoľvek údaje navyše, bez vopred stanoveného účelu ich využitia.

Zásada správnosti

Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované. Pre dosiahnutie tohto cieľa je potrebné vytvoriť nástroje, ktoré umožnia kontrolu správnosti a vykonanie aktualizácie údajov, ktoré prestali byť aktuálne. Je nevyhnutné tiež prijať primerané a účinné opatrenia, vďaka ktorým sa osobné údaje nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Zásada minimalizácie uchovávania

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 aj dlhšie, teda aj po uplynutí času






Tento projekt je podporený z Európskeho sociálneho fondu.

určeného pre dosiahnutie účelu spracúvania, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu, a to pri súčasnom zabezpečení primeraneych záruk na ochranu práv dotknutej osoby.

Zásada integrity a dôvernosti

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. Osoby, ktorá oprávnene disponuje osobnými údajmi, ich nesmie odovzdať bez súhlasu dotknutej osoby žiadnej ďalšej osobe a musí ich dostatočne chrániť pred akýmikoľvek negatívnymi vplyvmi.

Zásada zodpovednosti

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. Dotknutá osoba udeľuje súhlas a odozvdáva svoje osobné údaje prevádzkovateľovi a ten je zodpovedný voči dotknutej osobe za to, akým spôsobom sa s údajmi nakladá, či spracúvanie osobných údajov prebieha podľa vyššie uvedených zásad a na základe toho zodpovedá aj za prípadnú škodu, ktorá dotknutej osobe môže v súvislosti so spracúvaním jej osobných údajov vzniknúť.

### *Práva dotknutých osôb*

Podľa GDPR by sa mali stanoviť postupy, ktoré by dotknutej osobe uľahčili uplatnenie jej práv a ktoré by zahŕňali mechanizmy na vyžiadanie si a prípadné získanie bezplatného prístupu k osobným údajom a ich bezplatnú opravu alebo vymazanie, a na uplatnenie práva namietať. Prevádzkovateľ by mal tiež poskytnúť možnosť, aby sa žiadosti mohli podávať elektronicky, najmä ak sa osobné údaje spracúvajú elektronickými prostriedkami. Prevádzkovateľ by mal byť povinný odpovedať na žiadosti dotknutej osoby bez zbytočného odkladu a najneskôr do jedného mesiaca a uviesť dôvody v prípade, ak nemá v úmysle vyhovieť takejto žiadosti.

Právo na poskytnutie informácií

Zásady spravodlivého a transparentného spracúvania si vyžadujú, aby dotknutá osoba bola informovaná o:

- existencii spracovateľskej operácie a jej účeloch
- kontaktných a identifikačných údajoch prevádzkovateľa, zodpovednej osoby a príjemcu
- prípadnom prenose osobných údajov a dobe uchovávania
- právach dotknutej osoby vrátane práva na odvolanie súhlasu
- tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, či je dotknutáa osoba povinná poskytnúť osobné údaje
- existencii automatizovaného individuálneho rozhodovania vrátane profilovania.






Tento projekt je podporený z Európskeho sociálneho fondu.

Prevádzkovateľ by mal dotknutej osobe poskytnúť všetky informácie, ktoré sú potrebné na zaručenie spravodlivého a transparentného spracúvania, pričom sa zohľadnia konkrétne okolnosti a kontext, v ktorom sa osobné údaje spracúvajú.

Ak sa osobné údaje získavajú od dotknutej osoby, dotknutá osoba by mala byť informovaná aj o tom, či je povinná osobné údaje poskytnúť, a o následkoch v prípade, že tieto údaje neposkytne. Tieto informácie možno poskytnúť v kombinácii so štandardizovanými ikonami s cieľom poskytnúť dobre viditeľným, zrozumiteľným a čitateľným spôsobom zmysluplný prehľad zamýšľaného spracúvania. Ak sú ikony uvedené v elektronickej podobe, mali by byť strojovo čitateľné.

Informácie súvisiace so spracúvaním osobných údajov týkajúcich sa dotknutej osoby by sa mali dotknutej osobe poskytnúť v čase získavania osobných údajov od dotknutej osoby, alebo ak sa osobné údaje získali z iného zdroja, v primeranej lehote v závislosti od okolností prípadu.

Ak možno osobné údaje legitímne poskytnúť inému príjemcovi, dotknutá osoba by mala byť informovaná o tom, kedy boli osobné údaje prvýkrát poskytnuté tomuto príjemcovi.

Ak má prevádzkovateľ v úmysle spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané, mal by dotknutej osobe pred takýmto ďalším spracúvaním poskytnúť informácie o tomto inom účele a ďalšie potrebné informácie. Ak sa z dôvodu použitia viacerých zdrojov nemohol dotknutej osobe poskytnúť pôvod osobných údajov, mala by sa poskytnúť všeobecná informácia.

Nie je však potrebné uložiť povinnosť poskytovať informácie, ak dotknutá osoba už informácie má, ak zaznamenanie alebo poskytnutie osobných údajov je výslovne stanovené zákonom, alebo ak sa poskytnutie informácií dotknutej osobe ukáže ako nemožné alebo by si vyžiadalo vynaloženie neprimeraného úsilia. Posledná situácia by mohla byť najmä spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely. V tejto súvislosti by sa mal zohľadniť počet dotknutých osôb, vek údajov a všetky prijaté primerané záruky.

Právo na prístup k osobným údajom

Dotknutá osoba by mala mať právo na prístup k osobným údajom, ktoré boli o nej získané, a uvedené právo aj jednoducho a v primeraných intervaloch uplatňovať, aby si bola vedomá zákonnosti spracúvania a mohla si ju overiť. Prevádzkovateľ by mal teda zabezpečiť nástroje, prostredníctvom ktorých bude mať dotknutá osoba prístup k svojim údajom, ako aj k informýciám o:

- účele spracúvania osobných údajov
- kategórii spracúvaných osobných údajov
- identifikácii príjemcu alebo o kategórii príjemcu
- dobe uchovávania osobných údajov
- právach dotknutej osoby
- zdroji osobných údajov, ak boli osobné údaje získané od inéj osoby
- existencii automatizovaného individuálneho rozhodnovania vrátane prfilovania
- o primeraných zárukách týkajúcich sa prípadného prenosu osobných údajov.







Tento projekt je podporený z Európskeho sociálneho fondu.

Za opakované poskytnutie osobných údajov, ktoré spracúva, môže prevádzkovateľ žiadať od dotknutej osoby **zaplatenie primeraného poplatku**, ktorý zodpovedá nákladom na takéto posktnutie.

Prevádzkovateľ by mal poskytnúť prístup k osobným údajom na diaľku, prostredníctvom bezpečného spôsobu, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom.

Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií, môže požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka.

Právo na prístup k osobným údajom by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru. Výsledkom zohľadnenia týchto prvkov by však nemalo byť odmietnutie poskytnutia akýchkoľvek informácií dotknutej osobe.

Právo na opravu osobných údajov

Dotknutá osoba má právo na opravu osobných údajov, ktoré sa jej týkajú. To znamená, že prevádzkovateľ má na požiadanie dotknutej osoby bez zbytočného odkladu **zabezpečiť**:

- opravu
- doplnenie, alebo
- aktualizáciu nesprávnych, neúplnych alebo neaktuálnych osobných údajov tejto dotknutej osoby.

Právo na výmaz odobných údajov

Toto právo dotknutej osoby sa nazýva aj „**právo na zabudnutie**“. Dotknutá osoba má možnosť využiť toto právo, ak uchovávanie takýchto údajov porušuje GDPR alebo právo EÚ alebo právne predpisy platné a účinné na území Slovenskej republiky.

Dotknutá osoba má najmä právo na to, aby jej osobné údaje boli bez zbytočného odkladu vymazané a prestali sa spracúvať, a to ak:

- osobné údaje už nie sú potrebné v súvislosti s účelmi, na ktoré boli získané alebo inak spracúvané
- ide o spracúvanie osobných údajov nevyhnutné pre splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci prevádzkovateľom, alebo ide o spracúvanie nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany a dotknutá osoba odvolala svoj súhlas alebo namieta voči spracúvaniu osobných údajov, ktoré sa jej týkajú
- dotknutá osoba namieta spracúvanie osobných údajov a neprevažujú dôvody,
- je dôvodom pre vymazanie splnenie povinnosti podľa zákona alebo medzinárodnej zmluvy
- sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti, alebo
- spracúvanie jej osobných údajov nie je v súlade s GDPR alebo Zákonom z iných dôvodov.






Tento projekt je podporený z Európskeho sociálneho fondu.

Právo na zabudnutie sa môže realizovať, napríklad keď dotknutá osoba dala súhlas ako dieťa, pričom si nebola plne vedomá rizík spojených so spracúvaním, a neskôr sa táto osoba rozhodne, že chce svoje osobné údaje z internetu odstrániť. Dotknutá osoba má možnosť uplatniť uvedené právo bez ohľadu na skutočnosť, že už nie je dieťa.

Ďalšie uchovávanie osobných údajov je zákonné v prípadoch, keď je potrebné na uplatnenie slobody prejavu a práva na informácie, na plnenie zákonnej povinnosti, na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, z dôvodov verejného záujmu v oblasti verejného zdravia, na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely, alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Prevádzkovateľ, ktorý osobné údaje zverejnil, je povinný prijať primerané kroky, so zohľadnením dostupnej technológie a prostriedkov, ktoré má prevádzkovateľ k dispozícii, vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí spracúvajú osobné údaje, o žiadosti dotknutej osobyn a požiadať týchto prevádzkovateľov, ktorí takéto osobné údaje spracúvajú, o **vymazaní všetkých odkazov na tieto osobné údaje alebo kópií či replík týchto osobných údajov**.

Právo na obmedzenie spracúvania

Dotknutá osoba má právo, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak:

- dotknutá osoba namieta správnosť osobných údajov
- spracúvanie osobných údajov je nezákonné
- prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
- dotknutá osoba namieta spracúvanie osobných údajov, pričom ide o spracúvanie osobných údajov nevyhnutné pre splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci prevádzkovateľom, alebo ide o spracúvanie nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany, a oprávnené dôvody na strane prevádzkovateľa neprevažujú nad oprávnenými dôvodmi dotknutej osoby.

Metódy na obmedzenie spracúvania osobných údajov môžu zahŕňať:

- **dočasné presunutie** vybraných údajov do iného systému spracúvania
- **zamedzenie prístupu** používateľov k vybraným osobným údajom alebo
- **dočasné odstránenie** zverejnených údajov z webového sídla.

V automatizovaných informačných systémoch by sa obmedzenie spracúvania malo zabezpečiť technickými prostriedkami takým spôsobom, aby osobné údaje neboli predmetom ďalších spracovateľských operácií a nebolo možné ich meniť. **Skutočnosť, že spracúvanie osobných údajov je obmedzené, by sa v systéme mala jasne vyznačiť**.

Ak sa spracúvanie osobných údajov obmedzilo, okrem uchovávania môže osobné údaje prevádzkovateľ spracúvať len so súhlasom dotknutej osoby alebo na účel uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.







Tento projekt je podporený z Európskeho sociálneho fondu.

**Dotknutú osobu je prevádzkovateľ povinný informovať pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené**.

Právo na prenosnosť osobných údajov

S cieľom ďalej posilniť kontrolu nad svojimi vlastnými údajmi má dotknutá osoba v prípade, že sa spracúvanie osobných údajov vykonáva automatizovanými prostriedkami:

- **právo získať** osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, a to v štruktúrovanom, bežne používanom strojovo čitateľnom a interoperabilnom formáte a
- **právo preniesť** ich k ďalšiemu prevádzkovateľovi.

Prevádzkovatelia by teda mali vyvinúť interoperabilné formáty, ktoré reálne umožnia prenosnosť údajov. Keď je to technicky možné, mala by mať dotknutá osoba právo na prenos osobných údajov priamo od jedného prevádzkovateľa k druhému.

Právo na prenosnosť údajov sa môže uplatniť, ak

- dotknutá osoba poskytla osobné údaje **na základe svojho súhlasu** alebo
- je spracúvanie **potrebné na plnenie zmluvy**.

Toto právo sa teda nemôže uplatňovať, ak je spracúvanie založené na inom právnom základe, než je súhlas alebo zmluva. Z toho vyplýva, že by sa nemalo uplatňovať voči prevádzkovateľom, ktorí spracúvajú osobné údaje pri výkone svojich verejných úloh. Nemalo by sa preto uplatňovať, ak je spracúvanie osobných údajov potrebné na plnenie zákonnej povinnosti, ktorá sa na prevádzkovateľa vzťahuje, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

Ak v rámci určitého súboru osobných údajov sú spracúvané osobné údaje viac ako jednej dotknutuej osoby, **výkon práva na prenosnosť osobných údajov by nemalo negatívne dôsledky pre práva a slobody iných dotknutých osôb**.

Výkonom tohto práva:

- by nemalo byť obmedzené právo dotknutej osoby dosiahnuť vymazanie osobných údajov a obmedzenie spracúvania,
- by nemalo viesť k vymazaniu osobných údajov dotknutej osoby, ktoré poskytla na účely plnenia zmluvy, v takom rozsahu a počas takého obdobia, ako sú tieto osobné údaje potrebné na plnenie danej zmluvy.

Právo namietať

Ak je spracúvanie nevyhnutné

- pre splnenie úlohy realizovanej **vo verejnom záujme** alebo
- **pri výkone verejnej moci** zverenej prevádzkovateľovi, alebo
- **na účely oprávnených záujmov** prevádzkovateľa alebo tretej strany,

má dotknutá osoba právo namietať proti spracúvaniu akýchkoľvek osobných údajov, ktoré sa týkajú jej konkrétnej situácie.







Tento projekt je podporený z Európskeho sociálneho fondu.

Ak chce prevádzkovateľ v spracúvaní osobných údajov tejto dotknutej osoby **napriek jej namietaniu pokračovať, musí preukázať**, že jeho oprávnené záujmy v tejto konkrétnej situácii prevažujú nad záujmami alebo základnými právami a slobodami dotknutej osoby.

Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo namietať proti takému spracúvaniu vrátane profilovania, bez ohľadu na to, či ide o pôvodné alebo ďalšie spracúvanie, a to **kedykoľvek a bezplatne**.

**Dotknutá musí byť na právo namietať výslovne upozornená**, a to

- najneskôr pri prvej komunikácii s ňou
- jasne a zrozumiteľne
- oddelene od akýchkoľvek iných poskytovaných informácií.

Právo nepodliehať rozhodnutiu založenom výlučne na automatizovanom rozhodovaní vrátane profilovania

Dotknutá osoba má právo, aby sa na ňu nevzťahovalo rozhodnutie, ktoré **môže zahŕňať opatrenie**, **hodnotí jej osobné aspekty**, **je založené výlučne na automatizovanom spracúvaní** a **má právne účinky**, ktoré sa dotknutej osoby týkajú alebo ju podobným spôsobom významne ovplyvňujú, ako je napríklad:

- automatické zamietnutie online žiadosti o úver alebo
- elektronické postupy prijímania pracovníkov bez akéhokoľvek ľudského zásahu.

Takéto spracúvanie zahŕňa „profilovanie“ pozostávajúce z akejkoľvek formy automatizovaného spracúvania osobných údajov spočívajúceho v hodnotení osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým na analýzu alebo predvídanie aspektov súvisiacich s:

- výkonnosťou dotknutej osoby v práci
- jej majetkovými pomermi
- zdravím
- osobnými preferenciami alebo záujmami
- spoľahlivosťou alebo správaním
- polohou alebo pohybom

pokiaľ vedie k právnym účinkom, ktoré sa dotknutej osoby týkajú alebo ju podobným spôsobom významne ovplyvňujú.

Rozhodovanie založené na takomto spracúvaní vrátane profilovania je však možné, ak je výslovne povolené právom EÚ alebo právom Slovenskej republiky, ktoré sa vzťahuje na prevádzkovateľa, a to aj na účely:

- monitorovania podvodov a daňových únikov a ich predchádzania, ktoré sa uskutočňuje v súlade s právnym predpismi, normami a odporúčaniami inštitúcií EÚ alebo slovenských orgánov dozoru






Tento projekt je podporený z Európskeho sociálneho fondu.

- zaistenia bezpečnosti a spoľahlivosti služby poskytovanej zo strany prevádzkovateľa,
- uzavretia alebo plnenia zmluvy medzi dotknutou osobou a prevádzkovateľom, alebo ak dotknutá osoba dala svoj výslovný súhlas, a ak je to nevyhnutné.

V každom prípade by takéto spracúvanie malo **podliehať vhodným zárukám**, ktoré by mali zahŕňať určité informácie pre dotknutú osobu a právo na ľudský zásah, vyjadriť svoj názor, dostať vysvetlenie rozhodnutia, ktoré bolo prijaté po takomto posúdení, a napadnúť rozhodnutie. Takéto opatrenie by sa memalo týkať dieťaťa.

S cieľom zabezpečiť spravodlivé a transparentné spracúvanie vo vzťahu k dotknutej osobe a s ohľadom na konkrétne okolnosti a súvislosti spracúvania osobných údajov by mal prevádzkovateľ:

- používať na účely profilovania **primerané matematické alebo štatistické postupy**
- prijať **technické a organizačné opatrenia** vhodné na to, aby sa predovšetkým zabezpečilo, že faktory, ktoré vedú k nesprávnosti osobných údajov, sa opravia a riziko chýb sa minimalizuje
- zabezpečiť osobné údaje tak, aby sa zohľadnili súvisiace potenciálne riziká pre záujmy a práva dotknutej osoby a aby sa okrem iného zabránilo diskriminačným účinkom na fyzické osoby na základe rasového alebo etnického pôvodu, politického názoru, náboženstva alebo presvedčenia, členstva v odborových organizáciách, genetického alebo zdravotného stavu či sexuálnej orientácie, alebo účinkom, ktoré vedú k opatreniam majúcim takéto účinky.

Automatizované rozhodovanie a profilovanie založené na osobitných kategóriách osobných údajov **je možné, ak:**

- sú zavedené **vhodné opatrenia** na zaručenie práv a oprávnených záujmov dotknutej osoby a
- dotknutá osoba udelila **výslovný súhlas** so spracúvaním takýcjto údajov, alebo je spracúvanie nevyhnutné **z dôvodu verejného záujmu** na základe Zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

Toto právo sa neuplatňuje, ak **je spracúvanie**:

- nevyhnutné na uzavretie **zmluvy** alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom,
- vykonané na základe **osobitného predpisu alebo medzinárodnej zmluvy**, ktorou je Slovenská republika viazaná, alebo
- založené na výslovnom **súhlase** dotknutej osoby.

### *Práva a povinnosti prevádzkovateľa*

1. **Prevádzkovateľ je povinný prijať vhodné opatrenia a poskytnúť dotknutej osobe informácie** vyplývajúce z:

- práva na poskytnutie informácií (podľa § 19 a 20 Zákona)






Tento projekt je podporený z Európskeho sociálneho fondu.

- práva na prístup k osobným údajom (podľa § 21 Zákona)
- práva na oznámenie porušenia ochrany osobných údajov (podľa § 41 Zákona),

ktoré sa týkajú spracúvania jej osobných údajov, **v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme**, a to najmä pri informáciách určených osobitne dieťaťu. Informácie je povinný poskytnúť v listinnej podobe alebo elektronickej podobe, spravidla **v rovnakej podobe, v akej bola podaná žiadosť**. Ak o to požiada dotknutá osoba, informácie môže prevádzkovateľ poskytnúť aj **ústne**.

**2. Prevádzkovateľ poskytuje súčinnosť dotknutej osobe pri uplatňovaní jej práv**. Prevádzkovateľ nemôže odmietnuť žiadosť dotknutej osoby pri výkone jej práv, ak nepreukáže, že dotknutú osobu nie je schopný identifikovať.

**3. Prevádzkovateľ je povinný poskytnúť dotknutej osobe informácie o opatreniach**, ktoré sa prijali na základe jej žiadosti jedného mesiaca od doručenia žiadosti. Uvedenú lehotu môže prevádzkovateľ v odôvodnených prípadoch s ohľadom na komplexnosť a počet žiadostí predĺžiť o ďalšie dva mesiace, a to aj opakovane, o čom je povinný ju informovať. Ak dotknutá osoba podala žiadosť v elektronickej podobe, prevádzkovateľ poskytne informácie v elektronickej podobe, ak dotknutá osoba nepožiadala o poskytnutie informácie iným spôsobom.

### *Obmedzenia práv dotknutej osoby*

Prevádzkovateľ alebo sprostredkovateľ môže za podmienok ustanovených osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, obmedziť rozsah povinností a práv dotknutej osoby a zásad spracúvania osobných údajov, ktoré sa týkajú práv dotknutej osoby, ak je také obmedzenie ustanovené s cieľom zaistiť:

- bezpečnosť Slovenskej republiky, obranu Slovenskej republiky, alebo verejný poriadok
- plnenie úloh na účely trestného konania
- iné dôležité ciele všeobecného verejného záujmu Európskej únie alebo Slovenskej republiky, najmä predmet dôležitého hospodárskeho záujmu alebo dôležitého finančného záujmu Európskej únie alebo Slovenskej republiky vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia alebo sociálneho zabezpečenia
- ochranu nezávislosti súdnictva a súdnych konaní
- predchádzanie porušeniu etiky v regulovaných povolaniach alebo regulovaných odborných činnostiach
- monitorovaciu funkciu, kontrolnú funkciu alebo regulačnú funkciu spojenú s výkonom verejnej moci
- ochranu práv dotknutej osoby alebo iných osôb
- uplatnenie právneho nároku
- hospodársku mobilizáciu.






Tento projekt je podporený z Európskeho sociálneho fondu.

Prevádzkovateľ alebo sprostredkovateľ môže obemedziť práva len vtedy, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, ustanovuje aspoň:

- účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov
- kategóriu osobných údajov
- rozsah zavedeného obmedzenia
- záruky zabraňujúce zneužitiu osobných údajov alebo nezákonnému prístupu alebo nezákonnému prenosu
- určenie prevádzkovateľa alebo kategórií prevádzkovateľov
- lehotu uchovávania a uplatniteľné záruky s ohľadom na povahu, rozsah a účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov
- riziká pre práva dotknutej osoby a práva dotknutej osoby na informovanie o obmedzení, ak tým nie je ohrozený účel obmedzenia.

## *Bezpečnosť osobných údajov*

Povinnosti prevádzkovateľa

1. Prevádzkovateľ je povinný prijať vhodné **technické a organizačné opatrenia** na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade so Zákonom.
2. O konkrétnych opatreniach sa prevádzkovateľ rozhodne po **zvážení povahy, rozsahu a účelu** spracúvania osobných údajov a rizík s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby. Uvedené opatrenia je prevádzkovateľ povinný podľa potreby pravidelne aktualizovať.
3. Opatrením je z napríklad zavedenie **primeraných interných postupov a procesov** ochrany osobných údajov zo strany prevádzkovateľa.
4. Prevádzkovateľ je povinný pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov; to neplatí, ak osobné údaje sú súčasťou registratúrneho záznamu.
5. Prevádzkovateľ je povinný zaviesť **štandardnú ochranu osobných údajov**, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie:
   - spracúvania osobných údajov **len na konkrétny účel**
   - **minimalizácie** množstva získaných osobných údajov a rozsahu ich spracúvania
   - doby uchovávania a dostupnosti osobných údajov
   - aby osobné údaje **neboli** bez zásahu fyzickej osoby **prístupné** neobmedzenému počtu fyzických osôb.

Prevádzkovateľ (a sprostredkovateľ) sú povinní prijať so zreteľom na:

- najnovšie poznatky a náklady na vykonanie opatrení
- povahu, rozsah, kontext a účel spracúvania osobných údajov a
- riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb







Tento projekt je podporený z Európskeho sociálneho fondu.

**špecificky navrhnutú ochranu osobných údajov**, ktorá spočíva v primeraných technických a organizačneých opatreniach na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä:

- **pseudonymizáciu a šifrovanie** osobných údajov zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov
- **proces obnovy dostupnosti** osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu
- **proces pravidelného testovania, posudzovania a hodnotenia** účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Pri posudzovaní **primeranej úrovne bezpečnosti** sa prihliada na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä:

- náhodné zničenie alebo nezákonné zničenie
- strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo
- neoprávnený prístup k takýmto osobným údajom.

Povinnosti v súvislosti so sprostredkovateľom

1. Prevádzkovateľ môže poveriť **len sprostredkovateľa, ktorý poskytuje dostatočné záruky** na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky GDPR a Zákona, a aby sa zabezpečila ochrana práv dotknutej osoby. Dostatočné záruky by mali spočívať v odborných znalostiach, spoľahlivosti a zdrojoch na prijatie technických a organizačneých opatrení.
2. Spracúvanie osobných údajov sprostredkovateľom **sa riadi zmluvou** alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi, a v ktorom je ustanovený:
   - predmet spracúvania
   - doba spracúvania
   - povaha a účel spracúvania
   - zoznam alebo rozsah osobných údajov
   - kategórie dotknutých osôb
   - povinnosti a práva sprostredkovateľa a prevádzkovateľa.

Zmluva alebo iný právny úkon musí obsahovať, že sprostredkovateľ je povinný:

- **spracúvať osobné údaje len na základe písomných pokynov prevádzkovateľa**, a to aj vtedy, ak ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii okrem prenosu na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná
- zabezpečiť, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú mlčanlivosť o informáciách, o ktorých sa dozvedeli







Tento projekt je podporený z Európskeho sociálneho fondu.

- **splniť povinnosti na zaistenie bezpečnosti** spracúvaných osobných údajov v zmysle § 39 Zákona (bod 6. vyššie).

**Po ukončení spracúvania** v mene prevádzkovateľa by mal sprostredkovateľ podľa rozhodnutia prevádzkovateľa vrátiť alebo vymazať osobné údaje, pokiaľ podľa práva EÚ alebo Slovenskej republiky, neexistuje požiadavka na uchovanie osobných údajov.

Riziká spracúvania osobných údajov

Spracúvanie osobných údajov môže prebiehať len v rozsahu, v ktorom je zaistená bezpečnosť siete a informačná bezpečnosť. Kľúčovým ukazovateľom je **schopnosť siete alebo informačného systému odolať** poruchám alebo činom, ktoré narušujú dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenesených osobných údajov.

**Bezpečnosť služieb** ponúkaných alebo dostupných prostredníctvom sietí a systémov orgánmi verejnej moci (jednotkami reakcie na núdzové počítačové situácie (CERT), jednotkami pre riešenie počítačových incidentov (CSIRT), poskytovateľmi elektronických komunikačných sietí a služieb a poskytovateľmi bezpečnostných technológií a služieb) **predstavuje oprávnený záujem prevádzkovateľa**, ktorého účelom je:

- **zabránenie neoprávnenému prístupu** k elektronickým komunikačným sieťam a šíreniu škodlivých programových kódov
- **zastavenie útokov** sledujúcich cielené preťaženie serverov („denial of service“) poškodzovanie počítačových a elektronických komunikačných systémov.

Hodnotenie rizika

S cieľom zachovať bezpečnosť a predchádzať spracúvaniu v rozpore s týmto nariadením by prevádzkovateľ alebo sprostredkovateľ mali posúdiť riziká súvisiace so spracúvaním a prijať opatrenia na zmiernenie týchto rizík, ako napríklad šifrovanie. Týmito opatreniami by sa mala zaistiť primeraná úroveň bezpečnosti vrátane dôvernosti.

Pravdepodobnosť a závažnosť rizika pre práva a slobody dotknutých osôb by sa mala stanoviť **v závislosti od povahy, rozsahu, kontextu a účelov spracúvania**. Riziko by sa malo posudzovať na základe objektívneho posúdenia, ktorým sa určí, či spracovateľské operácie obsahujú riziko alebo vysoké riziko.

Hodnotenie rizika pre práva a slobody fyzických osôb by sa malo vykonávať s ohľadom na rôzne stupne pravdepodobnosti a závažnosti negatívneho dopadu spracovateľských operácií.

**Negatívnym dopadom sa myslí ujma na zdraví, majetková alebo iná nemajetková ujma, ktoré sa môžu prejaviť nasledovnými spôsobmi**:

- diskriminácia, krádež totožnosti, poškodenie dobrého mena
- podvod, finančná strata
- strata dôvernosti osobných údajov, neoprávnená reverzná pseudonymizácii
- závažné hospodárske alebo sociálne znevýhodnenie
- pozbavenie práv a slobôd dotknutej osoby alebo zamedzenie kontroly nad osobnými údajmi.






Tento projekt je podporený z Európskeho sociálneho fondu.

Špeciálnu pozornosť pri hodnotení rizika je **potrebné venovať v nasledovnách prípadoch**:

- ak sa spracúvajú osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženstvo alebo filozofické názory a členstvo v odborových organizíciách, a ak sa spracúvajú genetické údaje, údaje týkajúce sa zdravia či údaje týkajúce sa sexuálneho života alebo uznania viny zo spáchania trestného činu a priestupku či súvisiacich bezpečnostných opatrení
- ak sa posudzujú osobné aspekty, najmä ak sa analyzujú alebo predvídajú aspekty týkajúce sa výkonnosti v práci, majetkových pomerov, zdravia, osobných preferencií alebo záujmov, spoľahlivosti alebo správania, polohy alebo pohybu, s cieľom vytvoriť alebo používať osobné profily
- ak sa spracúvajú osobné údaje zraniteľných fyzických osôb, najmä detí
- ak spracúvanie zahŕňa veľké množstvo osobných údajov a má dôsledky na veľký počet dotknutých osôb.

Splnenie povinností a súlad s požiadavkami zákona a GDPR

Splnenie povinnosti prijať primerané opatrenia možno preukázať**:**

- určením zodpovednej osoby
- schváleným kódexom správania
- vydaným alebo obnoveným **certifikátom**
- využitie monitorovacieho subjektu
- z**áznamom spracovateľských operácií**
- posúdením vplyvu
- predchádzajúcou konzultáciou
- systémom pre oznamovanie porušení.

### *Zodpovedná osoba*

Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak

- spracúvanie osobných údajov vykonáva **orgán verejnej moci** alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a **systematické monitorovanie dotknutej osoby vo veľkom rozsahu**
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie **osobitných kategórií osobných údajov vo veľkom rozsahu** alebo spracúvanie osobných údajov týkajúcich sa **uznania viny** za spáchanie trestného činu alebo priestupku vo veľkom rozsahu






Tento projekt je podporený z Európskeho sociálneho fondu.

- ak sa to vyžaduje v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná.

Zodpovedná osoba:

- je vybraná na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa Zákona, môže byť zamestnancom prevádzkovateľa alebo sprostredkovateľa alebo môže plniť úlohy na základe zmluvy
- **poskytuje informácie a porad**enstvo prevádzkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa Zákona, osobitných predpisov alebo medzinárodných zmlúv týkajúcich sa ochrany osobných údajov
- **monitoruje súlad** so Zákonom, osobitnými predpismi alebo medzinárodnými zmluvami týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov
- poskytuje poradenstvo súvisiace s **posúdením vplyvu na ochranu osobných údajov** a monitorovanie jeho vykonávania podľa Zákona
- **spolupracuje s úradom** pri plnení svojich úloh a plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie a podľa potreby aj konzultácie v iných veciach
- náležite **zohľadňuje riziko** spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

### *Kódex správania*

Dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu sprostredkovateľom môže slúžiť ako nástroj na **preukázanie súladu s požiadavkami** Zákona a GDPR pre bezpečnosť spracúvania osobných údajov.

**Prostredníctvom kódexu správania možno prijať interné pravidlá a opatrenia**, ktoré budú spĺňať zásady špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov. Takéto opatrenia by mohli okrem iného pozostávať z:

- minimalizácie spracúvania osobných údajov
- čo najskoršej **pseudonymizácie** osobných údajov
- transparentnosti v súvislosti s funkciami a spracúvaním osobných údajov
- umožnenia dotknutým osobám **monitorovať** spracúvanie údajov.

Združenie zastupujúce kategóriu prevádzkovateľov alebo sprostredkovateľov môže prijať kódex správania, a to najmä na účely spresnenia uplatňovania Zákona, ktorý môže byť **predložený na schválenie Úradu na ochranu osobných údajov** SR. Schválením kódexu správania zo strany úradu nie je dotknutá zodpovednosť prevádzkovateľa alebo zodpovednosť sprostredkovateľa za reálne dodržiavanie Zákona a GDPR.






Tento projekt je podporený z Európskeho sociálneho fondu.

**Európsky výbor pre ochranu údajov** (European Data Protection Board, EDPB), je nezávislý európsky orgán, ktorého činnosť sa sústredí na jednotné uplatňovanie pravidiel ochrany osobných údajov na území celej Európskej únie a spoluprácu medzi dozornými orgánmi. EDPB vydáva všeobecné usmernenia (guidelines), odporúčania (recommendations) a príklady najlepšej praxe (best practice) s cieľom vyjasňovať pravidlá, povinnosti, práva a podmienky vyplývajúce z GDPR (https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_sk), ktoré môžu byť použité pri vypracuvávaní kdexov správania.

### *Certifikát*

Na preukázanie splnenia povinností v záujme bezpečnosti osobných údajov môže prevádzkovateľ použiť **certifikát** podľa § 86 Zákona. Vydanie certifikátu, obnovu certifikátu alebo odňatie certifikátu vykonáva subjekt, ktorému bola udelená akreditácia podľa § 88 Zákona alebo Úradu na ochranu osobných údajov SR. Certifikát sa vydáva alebo obnoviuje najviac na obdobie troch rokov.

Úradu na ochranu osobných údajov SR alebo certifikačný subjekt posudzuje súlad spracúvania osobných údajov a existenciu primeraných záruk ochrany osobných údajov prevádzkovateľa alebo sprostredkovateľa na základe **certifikačných kritérií**. Vydaním certifikátu nie je dotknutá zodpovednosť prevádzkovateľa alebo zodpovednosť sprostredkovateľa za dodržiavanie Zákona, ani nie sú dotknuté právomoci úradu podľa tohto zákona.

### *Monitorovací subjekt*

Monitorovanie súladu spracúvania osobných údajov s kódexom správania vykonáva subjekt, ktorý spĺňa kritériá a podmienky na udelenie akreditácie podľa Zákona a bola mu udelená akreditácia Úradom na ochranu osobných údajov SR.

Kódexy správania schválené úradom pre orgány verejnej moci a verejnoprávne inštitúcie nepodliehajú činnosti monitorovacieho subjektu podľa tohto zákona.

Monitorujúcim subjektom môže byť právnická osoba alebo fyzická osoba – podnikateľ, ktorý má vytvorené technické a organizačné podmienky na **vykonávanie monitorovania schváleného kódexu správania**.

Monitorujúci subjekt je oprávnený:

- monitorovať súlad spracúvania osobných údajov
- prijať primerané opatrenia v prípadoch porušenia kódexu správania prevádzkovateľom alebo sprostredkovateľom
- dočasne pozastaviť záväznosť schváleného kódexu správania pre prevádzkovateľa alebo sprostredkovateľa.
- zrušiť záväznosť schváleného kódexu správania pre prevádzkovateľa alebo sprostredkovateľa.







Tento projekt je podporený z Európskeho sociálneho fondu.

## *Záznam o spracovateľských činnostiach*

**Na účely preukázania súladu** spracovávania osobných údajov s GDPR a Zákonom sú prevádzkovateľ alebo sprostredkovateľ povinní **viesť a uchovávať záznamy o spracovateľských činnostiach**, za ktoré sú zodpovední. Prevádzkovateľ a sprostredkovateľ sú povinní spolupracovať s dozorným orgánom a na požiadanie mu **poskytnúť tieto záznamy, aby mohli slúžiť na monitorovanie** týchto spracovateľských činností.

**Tieto povinnosti sa vzťahujú** na prevádzkovateľov a sprostredkovateľov s 250 a viac zamestnancami, ak spracúvanie predstavuje riziko pre ochranu práv dotknutej osoby, ak nie je spracúvanie osobných údajov príležitostné, alebo ak nezahŕňa osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku.

Z**áznam o spracovateľských činnostiach vypracovaný prevádzkovateľom a zástupcom prevádzkovateľa musí obsahovať**:

- identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený, a zodpovednej osoby
- účel spracúvania osobných údajov
- opis kategórií dotknutých osôb a kategórií osobných údajov
- kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii
- označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos
- predpokladané lehoty na vymazanie rôznych kategórií osobných údajov
- všeobecný opis technických a organizačných bezpečnostných opatrení

Sprostredkovateľ a zástupca sprostredkovateľa, je povinný viesť záznam o kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa. Tento záznam musí obsahovať**:**

- identifikačné údaje a kontaktné údaje sprostredkovateľa a prevádzkovateľa, v mene ktorého sprostredkovateľ koná, zástupcu prevádzkovateľa alebo sprostredkovateľa, ak bol poverený, a zodpovednej osoby
- kategórie spracúvania osobných údajov vykonávaného v mene každého prevádzkovateľa
- označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos
- všeobecný opis technických a organizačných bezpečnostných opatrení

Záznamy sa vedú v listinnej podobe alebo elektronickej podobe.






Tento projekt je podporený z Európskeho sociálneho fondu.

## *Posúdenie vplyvu*

V smernici 95/46/ES bola stanovená v**šeobecná povinnosť oznamovať spracúvanie osobných údajov dozorným orgánom**. Uvedená povinnosť spôsobovala administratívnu a finančnú záťaž, a pritom neprispela vždy k zlepšeniu ochrany osobných údajov. Takéto nerozlišujúce všeobecné oznamovacie povinnosti boli **nahradené efektívnejšími povinnosťami, postupmi a mechanizmami zameranými** na tie typy spracovateľských operácií, **ktoré pravdepodobne povedú k vysokému riziku** pre práva a slobody fyzických osôb z dôvodu ich povahy, rozsahu, kontextu a účelu. Napríklad tie**, ktoré používajú nové technológie, alebo tie, ktoré sú nového druhu**.

V takýchto prípadoch by prevádzkovateľ mal **pred spracúvaním vykonať posúdenie vplyvu na ochranu údajov**, aby posúdil osobitnú pravdepodobnosť a závažnosť vysokého rizika, pričom zohľadní povahu, rozsah, kontext a účely spracúvania a zdroje rizika.

P**osúdenie vplyvu by malo zahŕňať najmä:**

- plánované opatrenia
- záruky a mechanizmy na zmiernenie daného rizika, na zabezpečenie ochrany osobných údajov a na preukázanie súladu s GDPR a Zákonom.

Posúdenie **vplyvu sa vykoná:**

- **ak spracovateľské operácie povedú k vysokému riziku** pre práva a slobody fyzických osôb, prevádzkovateľ by mal byť zodpovedný za vykonanie posúdenia vplyvu na ochranu údajov s cieľom zhodnotiť najmä pôvod, povahu, osobitosť a závažnosť tohto rizika. Výsledok posúdenia by sa mal zohľadniť pri stanovení primeraných opatrení, ktoré sa majú prijať s cieľom preukázať, že spracúvanie osobných údajov je v súlade s týmto nariadením.
- **najmä pri spracovateľských operáciách veľkého rozsahu**, ktorých cieľom je spracúvať značný objem osobných údajov na regionálnej, vnútroštátnej alebo nadnárodnej úrovni, ktoré by mohli ovplyvniť veľký počet dotknutých osôb
- ak sa vo veľkom rozsahu využíva nová technológia
- ak je pre dotknuté osoby náročnejšie uplatniť svoje vlastné práva
- ak sa osobné údaje spracúvajú s cieľom prijímať rozhodnutia, ktoré sa prijímajú po akomkoľvek systematickom a rozsiahlom zhodnotení osobných aspektov súvisiacich s fyzickými osobami na základe profilovania týchto údajov alebo v nadväznosti na spracúvanie osobitných kategórií osobných údajov, biometrických údajov alebo údajov o uznaní viny za trestné činy a priestupky či súvisiacich bezpečnostných opatreniach
- **v prípade monitorovania verejne prístupných miest vo veľkom rozsahu**, najmä ak sa používajú optické elektronické zariadenia, alebo v prípade akýchkoľvek iných operácií, ak sa príslušný dozorný orgán domnieva, že spracúvanie pravdepodobne povedie k vysokému riziku pre práva a slobody dotknutých osôb, najmä preto, lebo tieto operácie bránia dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu, alebo preto, že sa systematicky vykonávajú vo veľkom rozsahu.

Spoločné posúdenie vplyvu







Tento projekt je podporený z Európskeho sociálneho fondu.

Existujú okolnosti, za ktorých môže byť **vhodné a hospodárne**, aby sa predmet posúdenia vplyvu na ochranu údajov nevzťahoval len na jeden projekt, ale bol širší, napríklad ak orgány verejnej moci alebo verejnoprávne subjekty zamýšľajú vytvoriť spoločnú aplikáciu či spracovateľskú platformu alebo ak niekoľko prevádzkovateľov zamýšľa zaviesť spoločnú aplikáciu či spracovateľské prostredie v rámci odvetvia alebo segmentu priemyslu alebo na široko rozvetvenú horizontálnu činnosť.

Vykonanie posúdennia vplyvu

Prevádzkovateľ je povinný počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená.

Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä

- **systematický opis** plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ
- **posúdenie nutnosti a primeranosti** spracovateľských operácií vo vzťahu k účelu
- **posúdenie rizika** pre práva dotknutej osoby
- **opatrenia na elimináciu rizík** vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

Pri posudzovaní dosahu spracovateľských operácií vykonávaných prevádzkovateľom alebo sprostredkovateľom Úrad na ochranu osobných údajov SR zohľadňuje, či prevádzkovateľ alebo sprostredkovateľ postupuje v súlade so schváleným kódexom správania.

Na zabezpečenie súladu so zákonom musí byť spracovateľská operácia vo vzťahu k účelu spracúvania osobných údajov nevyhnutná a primeraná.

- Nevyhnutnosť spracovateľskej operácie sa preukazuje jej posúdením vo vzťahu k požadovanému účelu spracúvania osobných údajov.
- Primeranosť spracovateľskej operácie sa preukazuje posúdením jej povahy, rozsahu a kontextu, ktorý musí zodpovedať účelu spracúvania osobných údajov.

Pri posúdení nevyhnutnosti a primeranosti spracovateľskej operácie sa zohľadní a odôvodní každé opatrenie prijaté na dosiahnutie súladu so zákonom, najmä uplatnenie zásady zákonnosti, obmedzenia účelu, minimalizácie osobných údajov, správnosti, minimalizácie uchovávania, integrity a dôvernosti, dodržiavanie postupov na uplatňovanie práv dotknutých osôb, dodržiavanie postupov na zabezpečenie zákonného spracúvania osobných údajov sprostredkovateľom, primerané záruky súvisiace s prenosom osobných údajov do tretej krajiny alebo medzinárodnej organizácii, primerané technické a organizačné opatrenia a **názory dotknutých osôb alebo organizácií zastupujúcich záujmy dotknutých osôb** na spracúvanie osobných údajov.

**Posúdenie rizika** pre práva fyzickej osoby prevádzkovateľ vykonáva z pohľadu dopadov na fyzickú osobu, pričom zohľadňuje najmä riziko súvisiace s

- náhodným alebo nezákonným poškodením, zničením, stratou, zmenou







Tento projekt je podporený z Európskeho sociálneho fondu.

- neoprávneným prístupom
- poskytnutím alebo zverejnením osobných údajov
- iným neprípustným spôsobom spracúvania.

V rámci tohto posúdenia musí identifikovať:

- hrozby a pravdepodobnosť ich výskytu
- zraniteľnosti zneužiteľné hrozbami
- riziká a pravdepodobnosť ich výskytu a závažnosť,

V rámci tohto posúdenia musí zhodnotiť:

- mieru dopadu na práva fyzickej osoby v dôsledku straty integrity, dôvernosti a dostupnosti údajov a
- vysoké riziko pre práva fyzickej osoby, ak neprijme opatrenia na zmiernenie rizika.

Predchádzajúca konzultácia

Ak sa na základe posúdenia vplyvu na ochranu údajov ukáže, že **spracovateľské operácie zahŕňajú vysoké riziko, ktoré**

- **prevádzkovateľ nemôže zmierniť** primeranými opatreniami, pokiaľ ide o najnovšie technológie a náklady na vykonanie opatrení, mala by sa pred spracúvaním uskutočniť konzultácia s dozorným orgánom
- na základe vykonaného posúdenia vyplyvu **nie je možné zmierniť bez prijatia primeraných opatrení**.

Vysoké riziko môže vyplývať**:**

- z typu spracúvania a
- rozsahu frekvencie spracúvania,

v dôsledku ktorých môže tiež vzniknúť škoda alebo zásah do práv a slobôd fyzickej osoby.

Priebeh konzultácie

Súčasťou konzultačného procesu je **predloženie výsledku posúdenia vplyvu** na ochranu údajov, ktoré sa vykonalo v súvislosti s daným spracúvaním, Úradu na ochranu osobných údajov SR, a to najmä opatrení určených na zmiernenie rizika pre práva a slobody fyzických osôb.

Ak Úrad na ochranu osobných údajov SR zistí, že plánované spracúvanie osobných údajov bude v rozpore s**o Zákonom**, najmä ak

- prevádzkovateľ nedostatočne identifikoval riziko alebo
- zmiernil riziko,

úrad do ôsmich týždňov od prijatia žiadosti o konzultáciu poskytne prevádzkovateľovi, prípadne aj sprostredkovateľovi, písomné poradenstvo.







Tento projekt je podporený z Európskeho sociálneho fondu.

Oznámenie porušenia

Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu, ako je napríklad:

- strata kontroly nad svojimi osobnými údajmi alebo obmedzenie práv týchto osôb
- diskriminácia
- krádež totožnosti alebo podvod
- finančná strata
- neoprávnená reverzná pseudonymizácia
- poškodenie dobrého mena
- strata dôvernosti osobných
- akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby.

Prevádzkovateľ je povinný ihneď, ako sa dozvie, že došlo k porušeniu ochrany osobných údajov, **bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov, toto porušenie oznámiť Úradu na ochranu osobných údajov** s výnimkou prípadov, keď vie prevádzkovateľ v súlade so zásadou zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

Oznámenie porušenia ochrany osobných údajov musí obsahovať najmä:

- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch
- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií
- opis pravdepodobných následkov porušenia ochrany osobných údajov
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

#### *3.1.1.2 Zákon o informačných technológiach vo verejnej správe*

Všeobecná právna úprava obsahujúca:

- organizáciu správy informačných technológií verejnej správy
- práva a povinnosti orgánu vedenia a orgánov riadenia
- základné požiadavky kladené na informačné techniológie vo verejnej správe a na ich správu

je uvedená v **zákone o informačných technológiáach vo verejenej správe**. Cieľom tohto zákona je najmä vytvorenie štruktúry vhodnej pre zvyšovanie informatizácie,

rozdelenie kompetencií orgánov verejnej správy a vytvorenie nástrojov pre ich vykonávanie v tejto oblasti.

Kľúčovou zmenou oproti pôvodnej právnej úprave je zakotvenie Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky ako orgánu vedenia, výsledkom čoho je posun ministerstva v oblasti informatízácie od koordinačnej role do riadiacej role.

Zákon o informačných technológiách vo verejnej správe tiež stanovuje konkrétne požiadavky týkajúce sa bezpečnosti informačných technologií v rámci plánovania, organizácie, obstarávania, implementácie, prevádzky, servisu, podpory, monitoringu a hodnotenia, ako aj osobitné opatrenia na úseky bezpečnosti informačných technológií verejnej správy.

Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností a citlivých informácií. Tieto oblasti reguluje napríklad zákon o ochrane utajovaných skutočností alebo zákon o kritickej infraštruktúre. Na informačné technológie verejnej správy sa vzťahuje aj osobitný predpis, zákon o kybernetickej bezpečnosti.

### *Vysvetlenie vybraných pojmov*

**Informačná technológia** je prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.

**Informačný systém** je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

**Informačnou technológiou verejnej správy** je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

**Informačný systém** verejnej správy je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

**Správca** je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa, pričom ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.

**Prevádzkovateľ** je na účely tohto zákona správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba, ktorý vykonáva činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis; pričom ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu.






Tento projekt je podporený z Európskeho sociálneho fondu.

**informačná činnosť** je získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov.

**Infraštruktúra** je technologicko-komunikačné prostredie zabezpečujúce implementáciu a prevádzkovanie informačných systémov verejnej správy, poskytovanie a rozvoj elektronických služieb verejnej správy.

**Služba verejnej správy** je výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis.

**Elektronická služba verejnej správy** je elektronická komunikácia s orgánom riadenia pri vybavovaní podania, oznámenia, pri prístupe k informáciám a ich poskytovaní alebo pri účasti verejnosti na správe verejných vecí.

**Služba vo verejnom záujme** je výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah ustanovuje osobitný predpis.

**Verejná služba** je činnosť orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis a ktorej výsledok možno použiť pri výkone služby verejnej správy a služby vo verejnom záujme.

**Úsek verejnej správy** je vecná oblasť, v ktorej právomoci, práva a povinnosti orgánu riadenia, ako aj spôsob ich výkonu ustanovuje osobitný predpis a ktorá obsahuje najmenej dve agendy verejnej správy.

**Agenda verejnej správy** je ucelený súhrn činností na konkrétnom úseku verejnej správy, ktoré vrátane spôsobu ich výkonu ustanovuje osobitný predpis.

Definície a obsah ďalších pojmov určuje zákon o informačných technológiách vo verejnej správe v § 2 a § 3.

### *Správa informačných technológií vo verejnej správe*

Postavenie a zodpovednosť orgánov správy infromačných technológií

**Správu informačných technológií verejnej správy**, ktoré podporujú služby verejnej správy, služby vo verejnom záujme alebo verejné služby, **vykonávajú**:

- **orgán vedenia**, ktorým je Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
- orgány riadenia, ktorými sú
  - ministerstvá a ostatné ústrednyé orgány štátnej správy, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a podobne
  - obce a vyššiie územné celky
  - Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Najvyššieho správneho súdu Slovenskej republiky, Kancelária Súdnej rady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad






Tento projekt je podporený z Európskeho sociálneho fondu.

komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu

- právnické osoby v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia
- komory regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom
- iné osoby okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov
- záujmové združenia právnických osôb, DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.

Základné povinnosti v správe informačných technológií verejnej správy, ktoré sú orgán vedenia a orgány riadenia povinné plniť:

- dodržiavať princípy transparentnosti, proporcionality, hospodárnosti a efektívnosti
- zabezpečiť, aby vynaložené náklady na informačné technológie musia byť primerané ich kvalite
- prednostne využívať už existujúce informačné technológie, ak to nie je v rozpore s inými povinnosťami, a ak to umožňujú technické možnosti a bezpečnostné požiadavky
- dbať na vytvorenie integrovaného prostredia informačných technológií verejnej správy
- postupovať pri tvorbe, zmene alebo pri zabezpečovaní kontinuity prevádzky informačných technológií v súlade s časovým aspektom identifikovaných potrieb koncových užívateľov alebo s nadobudnutím účinnosti všeobecne záväzných právnych predpisov
- využívať podnety a poznatky odbornej verejnosti a prihliadať na spoločenské potreby používateľov služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb.

Špecifické úlohy a nástroje orgánu vedenia

Orgán vedenia je povinný najmä:

- monitorovať výkon riadenia v správe informačných technológií verejnej správy
- vyhodnocovať informácie získané z monitorovania, kontroly a z iných podnetov na účely identifikácie rizík a nedostatkov
- vydávať metodické usmernenia, usmerňovať a koordinovať orgány riadenia na účely jednotného spôsobu výkonu riadenia
- vypracúva, aktualizuje a predkladá vláde Slovenskej republiky národnú koncepciu
- určuje koncepciu štátnej politiky jednotného digitálneho trhu






Tento projekt je podporený z Európskeho sociálneho fondu.

- koordinuje budovanie informačných technológií verejnej správy vrátane ich uvádzania do prevádzky a rozhoduje o využívaní finančných zdrojov na ich budovanie a rozvoj v rozsahu ustanovenom zákonom
- určuje centrálnu architektúru budovania a rozvoja informačných technológií verejnej správy a referenčnú architektúru budovania a rozvoja informačných technológií verejnej správy
- vydáva štandardy a výkladové stanoviská.

Ministerstvo investícií je **ako orgán riadenia** správcom:

- integrovanej infraštruktúry
- centrálneho metainformačného systému verejnej správy
- nadrezortného informačného systému verejnej správy na úseku verejnej správy ministerstva investícií.

**Národná koncepcia** je hlavným nástrojom ministerstva investícií pre stanovenie strategických cieľov, priorít, opatrení, programov, organizačných, technických a technologických nástrojov, ktorých účelom je na celoštátnej úrovni **určiť centrálnu architektúru, referenčnú architektúru a definovať politiku, regulačné a iné nástroje** a konkrétny plán úloh a zdrojov s cieľom budovania riadnej a efektívnej úrovne informatizácie vo verejnej správe.

Špecifické úlohy a nástroje orgánu riadenia

Orgán riadenia, ktorý je správcom informačných technológií zodpovedným za vytváranie, správu a rozvoj informačnej technoloógie verejnej správy, je v prvom rade povinný **poskytovať orgánu vedenia súčinnosť** potrebnú na riadny výkon vedenia v správe informačných technológií verejnej správy a poskytovať mu prostredníctvom elektronickej služby verejnej správy údaje o informačných technológiách verejnej správy na účely štatistických analýz.

Orgán riadenia vypracúva vnútorné predpisy na účely plánovania, organizácie, obstarávania, implementácie, prevádzky, servisu, podpory, monitoringu, hodnotenia a bezpečnosti informačných technológií verejnej správy, pri ktorých vychádza:

- zo **všeobecne akceptovaných štandardov riadenia** informačných technológií, ktoré vychádzajú z uznaných technických noriem a
- metodických usmernení orgánu vedenia.

Hlavná povinnosť orgánu riadenia:

- zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných technológií verejnej správy, ktorých je správcom, vrátane organizačného, odborného a technického zabezpečenia a zabezpečenia proti zneužitiu, a to v súlade so zákonom o informačných technológiách vo verejnej správe, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a **národnou koncepciou**.

**Koncepcia rozvoja** informačných technológií verejnej správy je dokument vypracovaný orgánom riadenia pre informačné technológie verejnej správy, ktorých je správcom, definujúci ciele, organizačné, technické a technologické nástroje, architektúru informačných technológií verejnej správy a plánovanie jednotlivých aktivít, najmä **s**

**cieľom riadneho a včasného naplnenia požiadaviek národnej koncepcie** a strategických priorít informatizácie verejnej správy.

### *Bezpečnosť informačných technológií vo verejnej správe*

Správca, ktorý je prevádzkovateľom základnej služby, povinný:

- prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe **v závislosti od klasifikácie informácií a kategorizácie** sietí a informačných systémov
- prijímať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe s cieľom dosiahnuť **vyššiu úroveň bezpečnosti**.

Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

Správca je na úseku plánovania a organizácie informačných technológií verejnej správy povinný:

- nastaviť systém riadenia a určiť stratégiu rozvoja a riadenia
- zabezpečiť riadenie správy architektúry, nastaviť organizačnú štruktúru, procesy a nástroje potrebné na riadenie
- zabezpečiť riadenie kľúčových zdrojov, ktorými sú ľudské zdroje, finančné prostriedky alebo zdroje poskytované inými osobami
- riadiť nastavenie zmluvných vzťahov pre poskytovanie služieb
- zabezpečiť riadenie kvality, rizík a bezpečnosti.

**V rámci zaistenia riadenia bezpečnosti** je správca povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý:

- určí ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti **vo forme bezpečnostnej dokumentácie** schválených procesov riadenia bezpečnosti informačných technológií verejnej správy
- zriadi **riadiacu, výkonnú a kontrolnú zložku** systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené
- zabezpečí a zdokumentuje identifikovanie aktív a riadenie rizík, najmä vo forme **bezpečnostnej dokumentácie** vrátane bezpečnostného projektu
- určí a zavedie bezpečnostné opatrenia na procesnej, organizačnej a na technickej úrovni
- určí **prostriedky a zdroje** na zabezpečenie implementácie, riadneho fungovania a kontroly bezpečnostných opatrení, vrátane postupov riešenia bezpečnostných incidentov.

**Správca prostredníctvom riadiacej zložky systému riadenia bezpečnosti zabezpečuje** prerokovanie a schválenie bezpečnostnej stratégie kybernetickej bezpečnosti a strategických opatrení týkajúcich sa bezpečnosti informačných technológií verejnej správy, informácií o zaznamenaných závažných kybernetických bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného






Tento projekt je podporený z Európskeho sociálneho fondu.

výskytu, návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov kybernetickej bezpečnosti informačných technológií verejnej správy.

**Správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje** vypracovanie a aktualizáciu bezpečnostnej dokumentácie upravujúcej systém riadenia bezpečnosti, preskúmanie stavu kybernetickej bezpečnosti informačných technológií verejnej správy najmenej jedenkrát do roka a informovanie riadiacej zložky o výsledkoch preskúmania, realizáciu bezpečnostných opatrení, plánovanie, koordináciu a vyhodnocovanie činností súvisiacich s riadením bezpečnostných rizík v oblasti bezpečnosti informačných technológií verejnej správy, koordináciu riešenia bezpečnostných incidentov, organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií verejnej správy.

**Správca prostredníctvom kontrolnej zložky systému riadenia bezpečnosti zabezpečuje** nezávislú kontrolu dodržiavania povinností v oblasti bezpečnosti informačných technológií verejnej správy, hodnotenie súladu stavu bezpečnosti s požiadavkami všeobecne záväzných právnych predpisov.

**Správca pri plánovaní vytvorenia alebo nadobudnutia informačného systému verejnej správy** dodržiava bezpečnostnú stratégiu kybernetickej bezpečnosti, určí osobu zodpovednú za bezpečnosť informačného systému verejnej správy, identifikuje riziká prostredia, v ktorom bude informačný systém verejnej správy prevádzkovaný.

Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie

Správca je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný:

- zabezpečiť riadenie projektov
- identifikovať požiadavky na informačné technológie verejnej správy a podmienky ich zabezpečenia
- zabezpečiť riadenie dostupnosti a kapacity zdrojov a zmien na organizačnej a procesnej úrovni
- zabezpečiť riadenie aktív a konfigurácií.

Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy

- určí **bezpečnostné požiadavky** na informačný systém verejnej správy vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania informačného systému verejnej správy
- zabezpečí pre tento systém vypracovanie **bezpečnostnej dokumentácie** vrátane bezpečnostného projektu

**Dodávateľ informačného** systému verejnej správy pre vývoj tohto systému je povinný

- zabezpečiť **bezpečné vývojové prostredie, dokumentáciu vývoja a testovania** vrátane používateľskej dokumentácie a administrátorskej dokumentácie
- dodržiavať **mlčanlivosť o** dodávanom informačnom systéme verejnej správy







Tento projekt je podporený z Európskeho sociálneho fondu.

- doplniť bezpečnostné požiadavky a predložiť správcovi **návrh bezpečnostných opatrení** na naplnenie týchto bezpečnostných požiadaviek
- preukázateľne odstrániť alebo **znemožniť neoprávnený prístup** do tohto systému a k údajom, ktoré obsahuje.

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

Správca je na úseku prevádzky, servisu a podpory informačných technológií verejnej správy povinný

- nastaviť a zabezpečiť riadenie prevádzky
- zabezpečiť riadenie kontinuity prevádzky
- zabezpečiť riadenie služieb bezpečnosti prevádzky.

**V rámci zabezpečenia riadenia služieb bezpečnosti prevádzky správca zabezpečuje** zavedenie informačného systému verejnej správy do prevádzky, prevádzku informačného systému verejnej správy, vyradenie informačného systému verejnej správy z prevádzky.

**V rámci zabezpečenia zavedenia informačného systému verejnej správy do prevádzky správca** overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek pred zavedením do prevádzky a nezavedie do prevádzky informačný systém verejnej správy, ktorý tieto požiadavky nespĺňa, vykoná bezpečnostné testovanie informačného systému verejnej správy, ktorý má rozhranie s verejnou sieťou internet a ktorý spracúva osobitné kategórie osobných údajov podľa osobitného predpisu alebo informácie klasifikované z hľadiska dôvernosti ako chránené alebo prísne chránené podľa osobitného predpisu.

**V rámci zabezpečenia prevádzky informačného systému verejnej správy správca** zabezpečí pre informačný systém verejnej správy, určenie a pravidelné aktualizovanie bezpečnostnej dokumentácie, dodržiavanie bezpečnostných opatrení, v závislosti od zaradenia informačného systému verejnej správy z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov, aktualizuje bezpečnostný projekt pre tento systém vypracovaný, zavedie jednotný systém riadenia informačnej bezpečnosti pre všetky informačné systémy, ktoré sú v jeho správe, zabezpečí riadenie konfigurácie informačného systému verejnej správy a jeho častí, určí bezpečnostne závažné operácie, ktorými sa rozumejú najmä správa prístupov a prístupových údajov, ukladanie záznamov o systémových udalostiach, realizácia bezpečného oddelenia vnútornej časti systému a siete od vonkajšej časti, a zavedie dokumentovanie postupov pre tieto operácie, zabezpečí nepretržitý monitoring informačného systému verejnej správy, zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch určených najmä s ohľadom na dôležitosť informačného systému verejnej správy a na minulé zistenia bezpečnostných auditov a pri zistení závažných bezpečnostných nedostatkov prepracuje bezpečnostný projekt a naň nadväzujúce dokumenty.

**V rámci vyradenia informačného systému verejnej správy z prevádzky správca** vypracuje plán vyradenia informačného systému verejnej správy z prevádzky, ktorý obsahuje najmä uchovanie informácií vyraďovaného informačného systému verejnej správy, ktoré sú potrebné pre funkčnosť iného informačného systému, spoľahlivé odstránenie informácií z pamäťových médií vyraďovaného informačného systému verejnej správy, postup vyraďovania programových prostriedkov a technických

prostriedkov informačného systému verejnej správy, zabezpečí, aby nedošlo ku strate alebo k úniku informácií a k narušeniu práv priemyselného vlastníctva a duševného vlastníctva.

Bezpečnosť informačných technológií verejnej správy v oblasti monitoringu a hodnotenia

Správca je na úseku monitoringu a hodnotenia informačných technológií verejnej správy povinný

- **pravidelne monitorovať** informačné technológie verejnej správy a systém kontroly
- **zabezpečiť súlad** prevádzky s podmienkami ustanovenými všeobecne záväznými právnymi predpismi.

V oblasti monitoringu a hodnotenia je správca vo vzťahu k informačným technológiám v jeho správe povinný prijímať a vykonávať bezpečnostné opatrenia pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov podľa osobitného predpisu.

Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

**Bezpečnostný projekt** informačného systému verejnej správy sa vypracúva v súlade s osobitným predpisom a tvorí súčasť bezpečnostnej dokumentácie. Pri vypracúvaní bezpečnostného projektu správca vychádza z:

- bezpečnostnej stratégie kybernetickej bezpečnosti a bezpečnostných politík
- všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem
- metodických usmernení orgánu vedenia.

Správca vypracuje bezpečnostný projekt pre informačný systém verejnej správy, ktorý pri narušení bezpečnosti môže spôsobiť závažný kybernetický bezpečnostný incident.

**Orgán riadenia a rozpočtová organizácia a príspevková organizácia** v jeho zriaďovateľskej pôsobnosti sú povinní vo vzťahu k informačným technológiám verejnej správy (ak sú zaradení do registra prevádzkovateľov základných služieb) nahlasovať kybernetický bezpečnostný incident, poskytnúť orgánu vedenia súčinnosť a spoluprácu, zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív, určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

**Orgán vedenia vo vzťahu k informačným technológiám verejnej správy** môže na žiadosť orgánu riadenia vykonávať činnosti na účely predchádzania, riešenia a odstraňovania kybernetického bezpečnostného incidentu a hodnotenia zraniteľnosti, zbiera, spracúva a vyhodnocuje systémové informácie na účely predchádzania kybernetickým bezpečnostným incidentom, ich riešenia a obnovenia kybernetickej bezpečnosti, vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií poskytovaných prostredníctvom siete internet alebo prostredníctvom

Govnetu, môže na žiadosť orgánu riadenia za tento orgán riadenia vykonať bezpečnostný audit alebo preň vykonať hodnotenie zraniteľnosti.

#### 3.1.1.3 *Zákon o kybernetickej bezpečnosti*

***Právny rámec a ciele úpravy kybernetickej bezpečnosti***

Osobitným zákonom regulujúcim aktivity a vzťahy vznikajúce v oblasti kybernetickej bezpečnosti upravuje **zákon o kybernetickej bezpečnosti**. Predmetom tohto zákona je:

- organizácia, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti
- národnú stratégiu kybernetickej bezpečnosti
- jednotný informačný systém kybernetickej bezpečnosti
- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov – **CSIRT** a ich akreditáciu
- postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby
- bezpečnostné opatrenia
- **systém zabezpečenia** kybernetickej bezpečnosti
- **kontrolu** nad dodržiavaním tohto zákona a audit.

Zákon o kybernetickej bezpečnosti ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, ale nevzťahuje sa na:

- požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností
- osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu
- ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov
- požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu, a ani na platobné systémy a na systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov
- požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu
- osobitné predpisy (napríklad nariadenie o elektronickej identifikácii a dôveryhodnýych službách pre elektronické transakcie na vnútornom trhu alebo zákon o chrane súkromia pred neoprávneným použitím informačno-technických prostriedkov).

## *Vysvetlenie vybraných pojmov*

**Sieť** je elektronická komunikačná sieť.

**Informačný systém** je funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov.

**Kybernetický priestor** je globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.

**Kontinuita** znamená strategickaú a taktickaú schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni.

**Dôvernosť** je záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom.

**Dostupnosť** znamená záruku, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná.

**Integrita** je záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

**Kybernetická bezpečnosť** je stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.

**Riziko** je miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami.

**Hrozba** je každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť.

**Kybernetický bezpečnostný incident** je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

- strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému
- obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby
- vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
- ohrozenie bezpečnosti informácií.
- **Základna služba** je služba, ktorá je zaradená v zozname základných služieb a závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore







Tento projekt je podporený z Európskeho sociálneho fondu.

alebo podsektore podľa prílohy č. 1 zákona o kybernetickej bezpečnosti, alebo je prvkom kritickej infraštruktúry.

- **Prevádzkovateľ** základnej služby je orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu základnú službu.
- **Digitálna služba** je služba, ktorej druh je uvedený prílohe č. 2 zákona o kybernetickej bezpečnosti.
- **Poskytovateľ** digitálnej služby je právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur.
- **Riešenie kybernetického bezpečnostného incidentu** zahŕňa všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

### *Pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti*

Pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva

- Národný bezpečnostný úrad Sloevenskej republiky
- Ústredné orgány, teda Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky a Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „ústredný orgán“)
- Iné orgány štátnej správy, teda ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti.

Národný bezpečnostný úrad

V zmysle zákona o kybernetickej beepečnosti úrad najmä:

- určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore, určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia a vypracúva **národnú stratégiu kybernetickej bezpečnosti** a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi
- je národným **kontaktným miestom pre kybernetickú bezpečnosť** pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy
- spravuje a prevádzkuje jednotný informačný **systém kybernetickej bezpečnosti**, systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike zabezpečuje a zodpovedá za







Tento projekt je podporený z Európskeho sociálneho fondu.

koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni

- rieši **kybernetické bezpečnostné incidenty**, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie, zasiela včasné varovania, prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom
- spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a **jednotkami CSIRT**, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona, akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT
- je vnútroštátnym orgánom pre **certifikáciu kybernetickej bezpečnosti** a orgánom posudzovania zhody podľa osobitného predpisu
- vykonáva **kontrolu**, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt, vykonáva **audit** alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby.

Ústredné orgány

Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa zákona o kybernetickej bezpečnosti, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že najmä:

- plní úlohy jednotky **CSIRT**
- poskytuje úradu požadovanú **súčinnosť a informácie** získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti
- **spolupracuje** s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona
- buduje **bezpečnostné povedomie, koordinovanú spoluprácu** na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje **bezpečnostné opatrenia** a politiku správania sa v kybernetickom priestore
- **základnú službu a prevádzkovateľa** základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb.

Iné orgány štátnej správy

Na účely zaistenia kontinuity a riadenia rizík súvisiacich so zabezpečením sietí a informačných systémov, ktoré nie sú základnou službou a procesu riešenia kybernetických bezpečnostných incidentov, iný orgán štátnej správy **prijíma a dodržiava vhodné a primerané bezpečnostné opatrenia**.







Tento projekt je podporený z Európskeho sociálneho fondu.

### *Nástroje orgánov kybernetickej bezpečnosti*

Medzi strategické nástroje orgánov pôsobiacich v oblasti kybernetickej bezpečnosti patria najmä národná jednotka CSIRT, národná stratégia kybernetickej bezpečnosti, jednotný informačný systém kybernetickej bezpečnosti, vládna jednotka CSIRT.

Národná jednotka CSIRT

Národné centrum kybernetickej bezpečnosti je organizačnou zložkou Národného bezpečnostného úradu, ktorá má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku, ktorá musí spĺňať podmienky akreditácie a plniť úlohy jednotky CSIRT podľa zákona o kybernetickej bezpečnosti.

Národná jednotka CSIRT plní úlohu ústredného orgánu

Národná stratégia kybernetickej bezpečnosti

Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán ako konkrétny plán čiastkových úloh a zdrojov.

Národná stratégia kybernetickej bezpečnosti obsahuje najmä:

- ciele, priority a rámec riadenia na dosiahnutie týchto cieľov a priorít vrátane úloh a zodpovedností orgánov verejnej moci a ďalších relevantných subjektov
- identifikáciu opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným sektorom a súkromným sektorom
- popis bezpečnostného prostredia.

Jednotný informačný systém kybernetickej bezpečnosti

Jednotný informačný systém kybernetickej bezpečnosti je informačný systém, ktorého správcom a prevádzkovateľom je úrad a ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT.

Jednotný informačný systém kybernetickej bezpečnosti je určený aj na spracovanie a vyhodnocovanie údajov a informácií o stave kybernetickej bezpečnosti a slúži pri krízovom plánovaní v čase mieru, riadení štátu v krízových situáciách mimo času vojny a vojnového stavu, ako aj na potrebné činnosti v čase vojny alebo vojnového stavu.

Jednotný informačný systém kybernetickej bezpečnosti obsahuje:

- komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov, ktorý zaisťuje systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch a
- centrálny systém včasného varovania, ktorý zaisťuje včasnú výmenu informácií o hrozbách, kybernetických bezpečnostných incidentoch a rizikách s nimi spojených.

Vládna jednotka CSIRT







Tento projekt je podporený z Európskeho sociálneho fondu.

Vládna jednotka CSIRT v pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky plní úlohy v podsektore informačné systémy verejnej správy.

Úlohy jednotky CSIRT

Jednotka CSIRT zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.

- **Preventívne služby** sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov, a to:
  - vytváraním bezpečnostného povedomia a výcvikom
  - spoluprácou s ostatnými jednotkami CSIRT,
  - monitorovaním a evidenciou kybernetických bezpečnostných incidentov
  - pripojením na jednotný informačný systém kybernetickej bezpečnosti, poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti
  - prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.
- **Reaktívne služby** sa zameriavajú na riešenie kybernetických bezpečnostných incidentov, a to najmä prostredníctvom:
  - výstrahy a varovania, detekcie kybernetických bezpečnostných incidentov
  - analýzy kybernetických bezpečnostných incidentov,
  - odozvy, ohraničenia, riešenia a nápravy následkov kybernetických bezpečnostných incidentov
  - asistenciou pri riešení kybernetického bezpečnostného incidentu na mieste
  - reakciou na kybernetický bezpečnostný incident a podporou reakcií na kybernetické bezpečnostné incidenty
  - koordináciou reakcií na kybernetické bezpečnostné incidenty, návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

### *Bezpečnostné opatrenia pre zaistenie kybernetickej bezpečnosti*

Bezpečnostnými opatreniami na účely tohto zákona sú **úlohy, procesy, role a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom **predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv** kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby.







Tento projekt je podporený z Európskeho sociálneho fondu.

**Klasifikácia informácií** a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť:

- organizácie kybernetickej bezpečnosti a informačnej bezpečnosti
- riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti
- personálnej bezpečnosti
- riadenia prístupov
- riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami
- bezpečnosti pri prevádzke informačných systémov a sietí, hodnotenia zraniteľností a bezpečnostných aktualizácií
- ochrany proti škodlivému kódu
- sieťovej a komunikačnej bezpečnosti
- akvizície, vývoja a údržby informačných sietí a informačných systémov
- zaznamenávania udalostí a monitorovania
- fyzickej bezpečnosti a bezpečnosti prostredia
- riešenia kybernetických bezpečnostných incidentov
- kryptografických opatrení, kontinuity prevádzky, auditu, riadenia súladu a kontrolných činností.

Bezpečnostné opatrenia musia zahŕňať minimálne:

- určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly kybernetickej bezpečnosti
- detekciu kybernetických bezpečnostných incidentov
- evidenciu kybernetických bezpečnostných incidentov
- postupy riešenia a riešenie kybernetických bezpečnostných incidentov
- určenie kontaktnej osoby pre prijímanie a evidenciu hlásení
- pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

**Bezpečnostné opatrenia sa prijímajú a realizujú na základe** analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

- plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách
- možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy

- analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany
- analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií
- informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky.
- Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

## 3.2 Prehľad požiadaviek na aplikáciu štandardov v rámci verejnej správy

### 3.2.1 Kontrolný zoznam

#### *3.2.1.1 Súvislosti medzi právnymi predpismi*

Regulácie, ktoré riešia tému bezpečnosti a ochrany osobných údajov sa častočne prekrývajú, pričom každá sleduje svoje špecifické ciele.

Zákon o informačných technológiách vo verejnej správe je zameraný na klasickú aplikáciu princípov informačnej bezpečnosti v doméne verejnej správy.

Zákon o kybernetickej bezpečnosti sa snaží pokryť tému kybernetických hrozieb adresovaním poznania, že orientácia na formálne kroky a postupy často nestačí minimalizovať hrozby z neustále sa vyvíjajúceho digitálneho priestoru. Je preto potrebné zamerať sa na kontinuálne riešenie úloh a na dostatočné pokrytie technologickej vrstvy bezpečnosti.

GDPR z pohľadu bezpečnosti rieši jedno konkrétne aktívum – osobné údaje. Nastavuje teda rámec pre aplikáciu princípov informačnej a kybernetickej bezpečnosti na ochranu osobných údajov. Okrem toho rieši ďalšie otázky týkajúce sa spracovania osobných údajov, ako sú právny základ spracovanie údajov, informačné povinnosti a podobne.

Prehľad tém, ktoré adresujú jednotlivé regulácie a ich vyhlášky sú v nasledujúcej tabuľke.

**Tabuľka 6: Prehľad regulácie ktorá rieši ochranu a bezpečnosť údajov**

| Téma | GDPR/Zákon o ochrane osobných údajov | Zákon o informačných technológiách verejnej správy | Zákon o kybernetickej bezpečnosti |
|---|---|---|---|
| **Ochrana údajov/informácií** | ✓ | ✓ | ✓ |
| **Zásady ochrany údajov** | ✓ | | ✓ |
| **Klasifikácia informácií** | ✓ | | ✓ |
| **Regulácia prístupu k údajom** | ✓ | ✓ | ✓ |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | GDPR/Zákon o ochrane osobných údajov | Zákon o informačných technológiách verejnej správy | Zákon o kybernetickej bezpečnosti |
|---|---|---|---|
| Právny základ a účel spracúvania údajov | ✓ | | |
| Špecifické práva fyzických/dotknutých osôb | ✓ | | |
| Povinnosti prevádzkovateľov pri spracúvaní údajov | ✓ | ✓ | ✓ |
| Regulácia informačných systémov (IS) | ✓ | ✓ | ✓ |
| Národné stratégie/koncepcie rozvoja IS | | ✓ | ✓ |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku IS | ✓ | ✓ | ✓ |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | ✓ | ✓ | ✓ |
| Bezpečnosť IS a kybernetická bezpečnosť | ✓ | ✓ | ✓ |
| Bezpečnostné štandardy a nástroje | ✓ | ✓ | ✓ |
| Audity a kontrolné činnosti | ✓ | ✓ | ✓ |
| Riešenie bezpečnostných incidentov | | ✓ | ✓ |

### 3.2.1.2 *Prehľad požiadaviek a povinností*

Kontrolný zoznam požiadaviek a povinností vznikol agregáciu náležitostí z jednotlivých regulácií. Je orientovaný podľa tém, tak, aby bolo možné jednoducho vyhodnotiť, či bola požiadavka alebo povinnosť splnená. Tento kontrolný zoznam je možné použiť pri návrhu bezpečnostných politík pre nový informačný systém verejnej správy, pri aktualizácii alebo pri audite existujúceho systému.







Tento projekt je podporený z Európskeho sociálneho fondu.

Tento projekt je podporený z Európskeho sociálneho fondu.

## Tabuľka 7: Kontrolný zoznam požiadaviek a povinností pre bezpečnosť a ochranu údajov v informačnom prostredí verejnej správy

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Ochrana údajov/ informácií | Prijatie vhodných technických a organizačných opatrení na zabezpečenie ochrany, preverovanie trvania účelu spracúvania a riadne vyraďovanie registratúrnych záznamov, schválený kódex správania, certifikát | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §31, §85, §86 | | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Zásady ochrany osobných údajov | Dodržiavanie zásady zákonnosti, obmedzenia účelu, minimalizácie osobných údajov, správnosti, minimalizácie uchovávania, integrity, dôvernosti a zodpovednosti pri každom rozhodnutí spojenom so spracúvaním osobných údajov | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 2 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Klasifikácia informácií | Prijať opatrenia pre zabezpečenie adekvátneho prístupu k rôznym typom osobných údajov (citlivé osobné údaje, osobitné kategórie osobných údajov). | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §6 - §12 | | |
| Klasifikácia informácií | Ak prevádzkovateľ základnej služby disponuje vlastnou klasifikáciou informácií, vykoná sa mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §4, ods. (2) až ods. (4) |
| Regulácia prístupu k údajom | Dodržanie zásady pridelenia najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §16 | | |
| Regulácia prístupu k údajom | Dodržanie zásady oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §4, ods. (2) až ods. (4) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia prístupu k údajom | Identifikácia a evidencie všetkých aktív, od ktorých závisí poskytovanie základnej služby. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §5, písm. b) |
| Regulácia prístupu k údajom | Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §5, písm. c) |
| Regulácia prístupu k údajom | Ukladanie všetkých hesiel v nereverzibilnom formáte vždy, keď je to možné, pričom prípady, kedy to nie je možné musia byť odôvodnené a zdokumentované. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (3) písm. a) |
| Regulácia prístupu k údajom | Práca pod používateľským účtom s priradenou jednoznačnou identitou a heslom bez administrátorských privilégií, používanie administrátorského účtu s názvom s priradenou jednoznačnou identitou a heslom na vykonávanie činností súvisiacich so správou koncovej stanice. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória I, písm. b) | |
| Regulácia prístupu k údajom | Riadenie jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia prístupu k údajom | Prijatie bezpečnostných opatrení zabezpečujúcich ochranu údajov používaných pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1<br><br>Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(4), písm. a) |
| Regulácia prístupu k údajom | Používanie používateľských unikátnych hesiel s dĺžkou minimálne 9 znakov, ktoré je zložené z aspoň jedného veľkého písmena, jedného malého písmena, jedného čísla, jedného znaku a ktoré neobsahuje bežné slovo (napr. meno, prezývky a pod.) alebo jeho obmeny a jeho zmena aspoň raz ročne. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(4) |
| Regulácia prístupu k údajom | Používanie unikátnych hesiel s dĺžkou minimálne 15 znakov pre administrátorov, ktoré je zložené z aspoň jedného veľkého písmena, jedného malého písmena, jedného čísla, jedného znaku a ktoré neobsahuje bežné slovo (napr. meno, prezývky a pod.) alebo jeho obmeny a jeho zmena aspoň raz za 90 dní. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(2) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia prístupu k údajom | Zaznamenávanie zmien v pridelenom prístupe a ich archivácia. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Regulácia prístupu k údajom | Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Regulácia prístupu k údajom | Automatické zaznamenávanie každého prístupu administrátora do informačných technológií verejnej správy a automatické zaznamenávanie prístupu používateľa. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória II, písm. c) | |
| Regulácia prístupu k údajom | Implementácia centrálnej správy identít (IDM). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória II, písm. d) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia prístupu k údajom | Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória II, písm. i) | |
| Regulácia prístupu k údajom | Implementácia, vynucovanie prístupových rolí v informačných technológiách verejnej správy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória III, písm. a) | |
| Regulácia prístupu k údajom | Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov 6 mesiacov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória III, písm. c) | |
| Regulácia prístupu k údajom | Používanie silných autentizačných metód na overenie identity používateľov, ako je viacfaktorová autentizácia pri informačných technológiách verejnej správy, ktoré obsahujú prísne chránené informačné aktíva v zmysle klasifikácie informačných aktív. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória III, písm. d) | |
| Regulácia prístupu k údajom | Zavedenie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória III, písm. e) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia prístupu k údajom | Zavedenie nástroja na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., D. Riadenie prístupov, Kategória III, písm. f) | |
| Regulácia prístupu k údajom | Riadenie prístupu osôb k operačnému systému a jeho službám. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(4), písm. c) |
| Regulácia prístupu k údajom. | Riadenie prístupu osôb k aplikáciám. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(4), písm. c) |
| Regulácia prístupu k údajom | Monitorovanie prístupu a používania informačného systému. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(3), písm. e) |
| Regulácia prístupu k údajom | Riadenie vzdialeného prístupu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(3), písm. f) |
| Regulácia prístupu k údajom | Riadenie a monitorovanie prístupov do informačných technológií verejnej správy vrátane spôsobu a mechanizmu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(3), písm. g) |
| Regulácia prístupu k údajom | Zamedzenie prístupu tretích strán ku všetkým údajom v ITVS, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom len na základe zmluvy tak, aby nebola narušená bezpečnosť ITVS a bezpečnostná politika orgánu riadenia. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §12, ods.(3), písm. h) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Právny základ spracúvania | Dodržiavať podmienku zákonnosti spracúvania a spracúvať osobné údaje na základe zákona, medzinárodnej zmluvy, súhlasu dotknutej osoby alebo pre účely plnenie zmluvy, ochranu života, zdravia alebo majetku, vo verejnom záujme alebo na účel oprávnených záujmov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 4 | |
| Účel spracúvania údajov | Získavať osobné údaje len na konkrétne určený, výslovne uvedený a oprávnený účel a nespracúvať osobné údaje na ďalší účel nezlučiteľný s pôvodným účelom, pre ktorý boli údaje získané. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Práva dotknutých osôb a povinnosti prevádzkovateľov a sprostredkovateľov | Vytvoriť adekvátne procesy pre uplatňovanie a dodržiavanie práv dotknutých osôb (právo na informácie a prístup k osobným údajom, právo na opravu, vymazanie a obmedzenie spracúvania, právo na prenosnosť, právo namietať a práva spojené s automatizovaným individuálnym rozhodovaním), ako aj procesy pre ochranu osobných údajov, záznamy o spracovateľských činnostiach a uplatnenia práva na náhradu škody. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §13 - §18 | | |
| Regulácia informačných systémov a technológií | Kategorizácia sietí a informačných systémov | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §7 | | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Regulácia informačných systémov | Zavedenie povinného minimálneho rozsahu zmluvy s dodávateľom podľa § 20 ods. 2. Zákona 95/2019 Z. z., ktorou sa ustanovujú bezpečnostné podmienky ktoré musí dodávateľ zabezpečiť. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §19 - §29, §31 - §38 | | |
| Národné koncepcie/ stratégie | Postupovať v súlade s národnou stratégiou kybernetickej bezpečnosti, národnou koncepciou informatizácie verejnej správy SR, koncepciou rozvoja informačných technológií verejnej správy, stratégiou rozvoja a vedenia určenou správcom na príslušnom úseku plánovania a organizácie informačných technológií verejnej správy. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §4, ods. (5) až ods. (8) |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zavedenie povinného minimálneho rozsahu zmluvy s treťou stranou podľa § 8 ods. 2 vyhlášky NBÚ č.362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. | | Zákon č. 95/2019 Z. z., §10 a §13 | Zákon č. 69/2018 Z. z., §7 |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zavedenie povinného minimálneho rozsahu zmluvy s dodávateľom podľa § 20 ods. 2. Zákona 95/2019 Z. z., ktorou sa ustanovujú bezpečnostné podmienky ktoré musí dodávateľ zabezpečiť. | | Zákon 95/2019 Z. z., § 20 ods. 2) | Vyhláška NBÚ SR č. 362/2018 Z. z., §8 ods. 2 ) |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti. | | Zákon č. 95/2019 Z. z., §20 ods. 2) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zabezpečenie, aby boli v zmluvách s treťou stranou o poskytovaní služieb súvisiacich s ITVS uvedené bezpečnostné požiadavky na tieto služby. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória I, písm. a ) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. a) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 1 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti) certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 3 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 5 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 6 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 7 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre organizáciu správcu, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. b), ods. 8 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Základným bezpečnostným opatrením pre účasť tretej strany je analýza rizík v súvislosti s ITVS vyplývajúcich z činnosti tretích strán v týchto ITVS, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb a zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích strán v ITVS, aby nebola narušená bezpečnosť ITVS a bezpečnostná politika orgánu riadenia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. c), ods. 1 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zavedenie procesu na vytváranie záložných kópií dôležitých informácií a softvéru. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. c), ods. 2 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. c), ods. 3 | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zabezpečenie vykonania testu obnovy informačných technológií VS a údajov z prevádzkovej zálohy najmenej raz za rok. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. c), ods. 4 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. d) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch: operačné systémy a virtualizačné prostredia, aplikačný softvér, pracovné stanice, sieťové zariadenia vrátane bezpečnostných zariadení, databázové prostredia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. e) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória II, písm. f) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Riadenie bezpečnosti prevádzky siete a IS - riadenie zmien. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória III, písm. c) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zavedenie ochrany pred škodlivým kódom. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória I, písm. a) | |
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky pre akvizíciu, vývoj, implementáciu, údržbu a prevádzku informačných technológií | Zavedenie využívania verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Identifikácia všetkých významných informačných aktív v organizácii správcu a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. c) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Identifikácia a evidencia podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. d) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pre informačné technológie verejnej správy, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. e) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. f) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na - používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD, škodlivé emailové prílohy a odkazy, podozrivé a škodlivé webové stránky a odkazy, externú a internú sieťovú komunikáciu v organizácii správcu vrátane webových sídiel a na prenos súborov z externých sietí. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., J. Akvizícia, vývoj a údržba informačných technológií verejnej správy, Kategória II, písm. g) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Používanie len aktuálneho a legálneho softvéru, ktorý je povolený príslušnými internými predpismi orgánu riadenia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória I, písm. a) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie ochrany informačných technológií verejnej správy pred škodlivým kódom najmenej v rozsahu kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách verejnej správy | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. c) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. f) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. j), ods. 1, 2, 3, 4 a 5 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie ochrany pred nevyžiadanou elektronickou poštou. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. k) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §11, písm. a) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §11, písm. e) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie hardeningu pracovných staníc a pravidelné preverovanie jeho účinnosti a aktuálnosti raz ročne. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., F. Bezpečnosť pri prevádzke informačných systémov a sietí, Kategória II, písm. l) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Riadenie prístupov používateľov k sieťam a IS podľa zásady povolenia minimálneho prístupu nutného len pre realizovanie úlohy. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §9, písm. c) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória II, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Na sieťových zariadeniach sa implementuje pravidelná aktualizácia firmvéru. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória II, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementuje sa zmena továrensky nastavených autentifikačných údajov. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (3) písm. b) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami, Kategória III, písm. a) | |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementuje sa vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória I, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie ochrany vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória I, písm. c, ods. 1, 2, 3, 4 a 5 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória I, písm. d) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Nástroj na ochranu integrity sietí a informačných systémov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória II, písm. a), ods. 1 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória II, písm. a), ods. 2 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Správa počítačových sietí je riadená a kontrolovaná. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória II, písm. a), ods. 3 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória II, písm. a), ods. 4 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória II, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória III, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Špecifikované služby informačných systémov alebo sietí musia byť umiestnené vo vyhradených segmentoch siete počítačovej siete. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., H. Ochrana proti škodlivému kódu, Kategória III, písm. b ) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Špecifikované služby informačných systémov alebo sietí musia byť umiestnené vo vyhradených segmentoch siete počítačovej siete. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Ochrana vonkajšieho a interného prostredia, ako aj jednotlivých segmentov, sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. a) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zásada zabezpečujúca že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov (IDS). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. b), ods. 1 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Bezpečnostné opatrenia na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup (napr. bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. b), ods. 2 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. b), ods. 3 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. b), ods. 4 | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória I, písm. c) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. b) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vzdialený prístup do vnútornej siete organizácie správcu musí podliehať autentifikácii a autorizácii, vyžaduje sa použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. b) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie ochrany serverov prostredníctvom lokálnych softvérových firewallov na princípe najnižšieho privilégia pre prichádzajúcu aj odchádzajúcu komunikáciu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vykonanie hardeningu všetkých serverov, sieťových a bezpečnostných prvkov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Identifikácia a evidencia zoznamu všetkých vstupno-výstupných bodov na hranici siete a jeho udržiavanie v aktuálnom stave. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. c) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou (SIEM). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. d) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje (NGFW, WAF). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. e) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie blokovania komunikácie a prevádzky aplikácií cez neautorizované porty. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. f) | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. b) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie systému monitorovania bezpečnosti, ktorý musí byť nakonfigurovaný tak, že bude zaznamenávať a vyhodnocovať aj informácie o sieťových paketoch na hranici siete. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. e) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia systému detekcie prienikov (IDS) alebo systému prevencie prienikov (IPS) na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. g) | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. c) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. f) |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie pravidelného identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. h) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Synchronizácia času všetkých ITVS v sieti s dôveryhodným NTP serverom. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. d) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie prístupu používateľov k Internetu a k službám mimo siete orgánu riadenia cez proxy server a uchovávanie prístupových logov aspoň 4 mesiace. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. i) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS. | Uchovávanie log záznamov o autentifikácii používateľov aspoň 6 mesiacov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. j) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 mesiace. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. k) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 4 mesiace. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. l) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 mesiace. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória II, písm. m) | Vyhláška NBÚ SR č. 362/2018 Z. z.,§10, písm. o) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Konfigurácia maximálneho počtu aktívnych MAC adries na potrebný počet (maximálne 3) pre klientske porty na prístupových switchoch. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | V organizácii správcu sa implementuje technológia detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1<br><br>Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. g) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy2) správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. h) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. i) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia druhého sieťového firewallu od iného výrobcu tak, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. j) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia Web Application Firewallu (WAF) na všetkých verejne dostupných a kritických webových aplikáciách. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. k) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia manažmentu logov. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. l) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | V prípade používania bezdrôtových sietí (WIFI) ich umiestnenie do segmentu bez prístupu k aktívam klasifikovaným ako C3 alebo I3. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. m) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Synchronizácia času všetkých ITVS v sieti s interným NTP serverom. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10, písm. n) |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zaistenie vysokej dostupnosti ITVS kategórie A3 pomocou redundancie a load balancingu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §10 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby orgánu riadenia. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Konfigurácia a izolovanie klientskych portov na prístupových switchoch tak, aby pracovné stanice spolu nemohli priamo komunikovať(technológia PVLAN). Táto požiadavka nahrádza požiadavku zo Z2-FI) o maximálnom počte MAC adries. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie prístupu používateľov k Internetu a k službám mimo siete orgánu riadenia cez proxy server a uchovávanie prístupových logov aspoň 6 mesiacov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 mesiace. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 mesiacov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 mesiacov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória III, písm. a) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória III, písm. b) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä elektronických dokumentov a technológií v nasledujúcich riadkoch. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., I. Sieťová a komunikačná bezpečnosť, Kategória III, písm. c) | |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Šifrovanie dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Šifrovanie emailovej komunikácie prostredníctvom PGP alebo S/MIME. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Šifrovanie komunikačných kanálov na výmenu nešifrovaných dát. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Šifrovanie centrálnych úložísk. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Šifrovanie záloh. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Podpora elektronického podpisovania emailovej komunikácie. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Podpora asymetrického šifrovania emailovej komunikácie. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia šifrovania diskov na pracovných staniciach a serveroch metódou full disk encryption. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Implementácia manažmentu kryptografických kľúčov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Zavedenie pravidla a postupu určenia cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pravidlo a postup určenia cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Pravidlo a postup testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Požiadavky na dôvernosť, integritu, dostupnosť a kontinuitu IS | Vypracovanie plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória I, písm. a) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnosť IS a kybernetická bezpečnosť | Zabezpečenie preskúmania a identifikácie bezpečnostných rizík v počiatočných fázach procesu riadenia projektov v organizácii správcu a určenie adekvátnych opatrení na zníženie každého identifikovaného rizika na prijateľnú úroveň. Definovanie osoby zodpovednej za kybernetickú a informačnú bezpečnosť v projektovom tíme. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. a) | |
| Bezpečnosť IS a kybernetická bezpečnosť | Zabezpečenie vypracovania bezpečnostného projektu informačného systému verejnej správy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b, ods. 1 | |
| Bezpečnosť IS a kybernetická bezpečnosť | Za účelom stanovenia primeranej úrovne bezpečnosti je potrebné vykonať analýzu rizík s návrhom ich riadenia, ktoré predstavuje spracúvanie osobných údajov a vypracovať návrh technických opatrení na zaistenie úrovne bezpečnosti primeranej identifikovaným rizikám zo spracúvania osobných údajov a ich zapracovanie do dizajnu riešenia, resp. architektúry. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b), ods. 2 | |
| Bezpečnosť IS a kybernetická bezpečnosť | V rámci prípravnej fázy projektu, fázy analýzy a dizajnu riešenia, je potrebné vykonať posúdenie vplyvu na ochranu osobných údajov. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, § 42<br><br>Nariadenie (EU) 2016/679, článok 35 | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b), ods. 3 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnosť IS a kybernetická bezpečnosť | Návrh a prijatie bezpečnostných opatrení pre riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b), ods. 4 | |
| Bezpečnosť IS a kybernetická bezpečnosť | Vykonávanie analýzy rizík a vyhodnocovanie súladu implementovaných opatrení s touto vyhláškou najmenej raz ročne. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b), ods. 5 | |
| Bezpečnosť IS a kybernetická bezpečnosť | Identifikácia zraniteľností. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., N. Kryptografické opatrenia, Kategória II, písm. b), ods. 6 | |
| Bezpečnosť IS a kybernetická bezpečnosť | Identifikácia úmyselných hrozieb pre všetky úmyselné aktivity zamerané na aktíva. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnosť IS a kybernetická bezpečnosť | Identifikácia náhodných hrozieb pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Bezpečnosť IS a kybernetická bezpečnosť | Identifikácia hrozieb spôsobených vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Bezpečnosť IS a kybernetická bezpečnosť | Identifikácia a analýza rizík s ohľadom na aktívum. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Bezpečnosť IS a kybernetická bezpečnosť | Evidencia implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §17, ods.(2), písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnosť IS a kybernetická bezpečnosť | Evidencia bezpečnostných opatrení ktoré nie sú implementované spolu s uvedením odôvodnením. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §17, ods.(2), písm. d) |
| Bezpečnosť IS a kybernetická bezpečnosť | Analýza funkčného dopadu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §17, ods.(2), písm. e) |
| Bezpečnosť IS a kybernetická bezpečnosť | Ustanovenie plánu rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §17, ods.(2), písm. f) |
| Bezpečnosť IS a kybernetická bezpečnosť | Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §17, ods.(2), písm. g) |
| Bezpečnosť IS a kybernetická bezpečnosť | Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória III, písm. h) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnosť IS a kybernetická bezpečnosť | Poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória III, písm. i. Obsah a štruktúra projektu je v Prílohe č. 3 k vyhláške č. 179/2020 Z. z | |
| Bezpečnosť IS a kybernetická bezpečnosť | Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, § 31, §32, § 39 | | |
| Bezpečnostné štandardy a nástroje | Nastavenie automatickej aktualizácie operačného systému a aplikácií. | Zákon č. 18/2018 Z. z. o ochrane osobných údajov, §42 | | |
| Bezpečnostné štandardy a nástroje | Zavedenie pravidelného zisťovania a riešenia efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória I, písm. a, ods. 1 | |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Nástroj určený na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória I, písm. a, ods. 2 | |
| Bezpečnostné štandardy a nástroje | Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti, Kategória III, písm. b) | |
| Bezpečnostné štandardy a nástroje | Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (6) písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (10) písm. a) |
| Bezpečnostné štandardy a nástroje | Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (10) písm. b) |
| Bezpečnostné štandardy a nástroje | Po implementácii aktualizácie sa aktualizovaný prvok informačných technológií verejnej správy verifikuje, najmä jeho správna funkcionalita. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (10) písm. c) |
| Bezpečnostné štandardy a nástroje | Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (6) písm. c) |
| Bezpečnostné štandardy a nástroje | Zaznamenávanie úspešných a neúspešných autentifikačných udalostí. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (6) písm. e) |
| Bezpečnostné štandardy a nástroje | Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (6) písm. e) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Pre každý prvok informačných technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §6, ods. (6) písm. f) |
| Bezpečnostné štandardy a nástroje | Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej úspešné a neúspešné autorizačné udalosti a tiež udalosti uvedené v nasledujúcich riadkoch. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z. , C. Personálna bezpečnosť, Kategória I, písm. a) | Vyhláška NBÚ SR č. 362/2018 Z. z., §7, písm. b) |
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami). | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., C. Personálna bezpečnosť, Kategória I, písm. b) | Vyhláška NBÚ SR č. 362/2018 Z. z.,§7, písm. d) |
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa úspešné a neúspešné prístupy k log súborom. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., C. Personálna bezpečnosť, Kategória II, písm. a) | |
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa úspešné a neúspešné prístupy k systémovým zdrojom. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., C. Personálna bezpečnosť, Kategória II, písm. e) ods. 2 | |

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zaznamenáva sa vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., C. Personálna bezpečnosť, Kategória II, písm. d) | |
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa zmeny v prístupových oprávneniach. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória I, písm. a) | |
| Bezpečnostné štandardy a nástroje | Zaznamenáva sa aktivácia a deaktivácia bezpečnostných mechanizmov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. a | Vyhláška NBÚ SR č. 362/2018 Z. z., §9, písm. b) |
| Bezpečnostné štandardy a nástroje | Zaznamenáva sa spustenie a zastavenie procesov. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §9, písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. e) | |
| Bezpečnostné štandardy a nástroje | Zaznamenáva sa spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. f) | |
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa významné aktivity v sieťovej komunikácii. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. i) | |
| Bezpečnostné štandardy a nástroje | Zaznamenáva sa požiadavka na autentizačné služby vrátane označenia požadujúcej entity. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. j) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zaznamenávajú sa IP adresy pridelené prostredníctvom služby DHCP. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória II, písm. k) | |
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti (ak je k dispozícii) čas a dátum udalosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., G. Hodnotenie zraniteľností a bezpečnostné aktualizácie, Kategória III, písm. b) | |
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti identifikáciu používateľa. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória I, písm. a) | |
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti identifikáciu zariadenia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. a) | Vyhláška NBÚ SR č. 362/2018 Z. z., §11, písm. h) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti informáciu týkajúcu sa udalosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. b) | |
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti indikáciu úspešnosti, alebo zlyhania operácie. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 1 | |
| Bezpečnostné štandardy a nástroje | Záznamy v log súboroch obsahujú ku každej udalosti pri sieťových službách zdrojovú IP adresa, cieľovú IP adresa, protokol, zdrojový port, cieľový port. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 2 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 3 | |
| Bezpečnostné štandardy a nástroje | Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 4 | |
| Bezpečnostné štandardy a nástroje | Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 5 | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. c) |






Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 6 | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. c) |
| Bezpečnostné štandardy a nástroje | Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 7 | |
| Bezpečnostné štandardy a nástroje | Monitorovanie služieb prístupných do externých sietí. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 8 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Monitorovanie kritických interných serverov a služieb. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 9 | |
| Bezpečnostné štandardy a nástroje | Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov vytvárajúcom prevádzkové záznamy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 10 | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. d) |
| Bezpečnostné štandardy a nástroje | Zaznamenávať v prevádzkových záznamoch aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c, ods. 11 | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(1), písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zaznamenávať v prevádzkových záznamoch iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 12 | |
| Bezpečnostné štandardy a nástroje | Zaznamenávať v prevádzkových záznamoch detegované podozrivé alebo škodlivé aktivity. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. c), ods. 13 | |
| Bezpečnostné štandardy a nástroje | Zaznamenávať v prevádzkových záznamoch informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 1 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zabezpečenie čitateľnosti prevádzkových záznamov (auditných a logovacích súborov) výlučne osobami povereným ich analýzou. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 2 | |
| Bezpečnostné štandardy a nástroje | Zamedzenie možnosti prepísania alebo vymazania prevádzkových záznamov. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 3 | |
| Bezpečnostné štandardy a nástroje | Záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému presmerovať prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 4 | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Uloženie a archivácia prevádzkových záznamov po dobu zodpovedajúcu kategórii informačného systému. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 5 | |
| Bezpečnostné štandardy a nástroje | Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. d), ods. 6 | |
| Bezpečnostné štandardy a nástroje | Zabezpečenie, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť ITVS umiestnený v tomto zabezpečenom priestore. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória II, písm. h) | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Umiestnenie informačných technológií verejnej správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória III, písm. b) | |
| Bezpečnostné štandardy a nástroje | Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória III, písm. f) | |
| Bezpečnostné štandardy a nástroje | Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., K. Zaznamenávanie udalostí a monitorovanie, Kategória III, písm. g) | |
| Bezpečnostné štandardy a nástroje | Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(1), písm. b) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zaistenie prístupu k serverovým a sieťovým komponentom iba oprávneným osobám napr. pomocou uzamykateľných serverových skríň. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(1), písm. c) |
| Bezpečnostné štandardy a nástroje | Vedenie sieťovej kabeláže iba v priestoroch pod kontrolou orgánu riadenia alebo použitie šifrovania dát. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. a) |
| Bezpečnostné štandardy a nástroje | Stanovenie parametrov pre ITVS, ktoré definujú maximálnu prípustnú dobu výpadku ITVS a vytvorenie a zavedenie opatrení, ktoré sú zamerané na riešenie obnovy prevádzky v prípade výpadku ITVS. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. b) |
| Bezpečnostné štandardy a nástroje | Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. e) |
| Bezpečnostné štandardy a nástroje | Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(2), písm. f) |
| Bezpečnostné štandardy a nástroje | Zabezpečenie budovy strážnou službou s kontrolou vstupov, ktorá je schopná byť na mieste incidentu do 3 minút od spustenia poplachu. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(3), písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Umiestnenie serverových a sieťových komponentov do miestností opatrených certifikovanými bezpečnostnými dverami, tehlovými alebo betónovými dverami bez okien, alebo do miestností s nerozbitnými nepriehľadnými sklami s detektormi rozbitia. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(3), písm. b) |
| Bezpečnostné štandardy a nástroje | Zaistenie miestností alebo serverových skríň, v ktorých sú umiestnené serverové a sieťové komponenty senzormi teploty, vlhkosti, dymu, úniku vody, prachu, detektormi pohybu a vibrácií. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(3), písm. c) |
| Bezpečnostné štandardy a nástroje | Vyvedenie všetkých elektronických zabezpečovacích prostriedkov podľa písm. c) do agregačných bodov s možnosťou zasielania varovaní a notifikácií do centrálneho monitorovacieho systému s možnosťou varovania, automatizovanej akcie na základe vopred nastavaných prahových hodnôt a možnosťou analýzy a reportovania. | | | Vyhláška NBÚ SR č. 362/2018 Z. z., §15, ods.(3), písm. d) |
| Bezpečnostné štandardy a nástroje | Umožnenie prístupu tretích strán do priestorov orgánu riadenia len v sprievode interného zamestnanca. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória I, písm. a | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. a) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Bezpečnostné štandardy a nástroje | Zabezpečenie vstupu na pracovisko prostredníctvom prístupových tokenov, ukladanie a zálohovanie záznamov o vstupoch aspoň 6 mesiacov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1<br><br>Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. c) |
| Audity a kontrolné činnosti | Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa osobitného predpisu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória II, písm. a | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. a) |
| Audity a kontrolné činnosti | Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória II, písm. b | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. b) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Audity a kontrolné činnosti | Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória II, písm. c | |
| Audity a kontrolné činnosti | Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória II, písm. e) | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. e) |
| Audity a kontrolné činnosti | Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Riešenie bezpečnostných incidentov | V organizácii správcu sa určí kontaktné miesto a spôsob hlásenia kybernetických bezpečnostných incidentov podľa § 23 ods. 3 písm. a) a ods. 4 zákona. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |
| Riešenie bezpečnostných incidentov | V organizácii správcu je na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1<br><br>Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. e) |
| Riešenie bezpečnostných incidentov | Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória III, písm. a) | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. e) |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Téma | Požiadavka / povinnosť | Ochrana osobných údajov | Informačné technológie VS | Kybernetická bezpečnosť |
|---|---|---|---|---|
| Riešenie bezpečnostných incidentov | Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy. | | Príloha č. 2 k vyhláške č. 179/2020 Z. z., L. Fyzická bezpečnosť a bezpečnosť prostredia, Kategória III, písm. b | Vyhláška NBÚ SR č. 362/2018 Z. z., §16, ods.(1), písm. f) |
| Riešenie bezpečnostných incidentov | Súčasťou evidencie kybernetických bezpečnostných incidentov sa na zabezpečenie dôkazu alebo dôkazného prostriedku evidujú aj informácie identifikujúce kybernetický bezpečnostný incident ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia. | | | Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia dokumentu 2.1 |







Tento projekt je podporený z Európskeho sociálneho fondu.

### 3.2.2 Zlepšenie bezpečnosti a ochrany údajov

V nasledujúcej kapitole vysvetľujeme systémový pohľad, ako je možné komplexne zlepšiť bezpečnosť a ochranu údajov nad rámec kontrolného zoznamu a platných regulácií. Je potrebné modernizovať a nastaviť biznis procesy v organizácii tak, aby sa maximálne využil potenciál údajov a zároveň ostala zachovaná vysoká miera ochrany údajov. Hoci sa môže zdať, že ide o protichodnú požiadavku, práve moderné nástroje a technológie, ako je MOU sú navrhnuté tak, aby túto situáciu dokázali vyriešiť. Nasleduje teda zoznam požiadaviek na technológie a IT nástroje.

#### *3.2.2.1 Požiadavky na biznis procesy*

- Zostavený režim kontroly prístupu na ochranu údajov bez vytvárania zbytočnej a kontraproduktívnej byrokracie. Takýto systém prepojí prístup k údajom s legitímnymi potrebami a zavedie kontrolné mechanizmy, ktoré zabránia ich zneužitiu.
- Zosúladenie uchovávania a vymazávania údajov s oprávnenými agendovými potrebami a ochranou súkromia: To znamená, že organizácia nebude uchovávať údaje spôsobom, ktorý zneužíva dôveru osôb a ponecháva tieto údaje zraniteľné voči narušeniu alebo exfiltrácii.
- Nastavenie zdieľania údajov s tretími stranami spôsobom, ktorý chráni súkromie: napríklad pomocou techník akou je šifrovanie, ako aj agregovaním a/alebo anonymizáciou, aby nebolo možné identifikovať jednotlivých používateľov.
- Spustené iniciatívy na minimalizáciu údajov s cieľom znížiť počet kópií citlivých údajov v systémoch.
- Vybudované porozumenie v organizácii o rozdieloch medzi bezpečnosťou a ochranou osobných údajov.
- Vytvorenie programu ochrany osobných údajov, ktorý sa bude šíriť celou verejnou správou a ktorý vybuduje odborné znalosti na operacionalizáciu a automatizáciu ochrany súkromia vo veľkom rozsahu. Keď sa tento program začína, treba investovať dostatok času na vybudovanie skúseností. Postupom času však tento program bude ťažiť zo synergií s bezpečnosťou, vybudovanou dátovou platformou a s tímami dátovej vedy. Táto efektívnosť pomôže riadiť náklady a zabrániť výkyvom, ktoré škodia predvídateľnosti organizácie.
  - Meranie vplyvu techník, ako je napríklad pseudonymizácia údajov, na súkromie, aby ste mohli kvalifikovať zníženie rizika, keď sa program ochrany osobných údajov vyvíja.
  - Vykonávanie preskúmania ochrany osobných údajov („privacy reviews“), aby ste mohli posúdiť produkty a služby z právneho pohľadu a pohľadu súladu s reguláciami, ako aj z technického pohľadu.
- Existujúca klasifikácia údajov na základe rizika ohrozenia súkromia.
- Vytvorený dátový katalóg údajov s vložením tejto klasifikácie.
- Mapovanie kontrol a techník ochrany súkromia a bezpečnosti údajov na GDPR, ďalšie zákony, usmernenia a zmluvné povinnosti.







Tento projekt je podporený z Európskeho sociálneho fondu.

### 3.2.2.2 Požiadavky na technológie a nástroje

- Podpora nasledujúcich politík po uplynutí vopred definovaného obdobia uchovávania údajov, pričom je potrebné automatizovať predovšetkým vymazávanie a obfuskáciu:
  - Okamžité vymazanie - Úplné vymazanie používateľa na žiadosť alebo z akéhokoľvek dôvodu na požiadanie,
  - Vymazanie neaktívneho používateľa - vymazanie údajov používateľa, ak bol používateľ neaktívny určité stanovené časové obdobie,
  - Obfuskácia údajov - oddelenie obsahu od používateľa, napríklad prostredníctvom čiastočnej anonymizácie, ktorej sa podrobne venujeme v dokumente 1.1.5 Štandardizácia anonymizácie údajov,
  - Zachovanie - zachovanie údajov len na konkrétny prípad použitia, napríklad zašifrovanie údajov, ku ktorým má prístup po uplynutí doby uchovávania len právny tím,
  - Archivácia - presun údajov do archivačného systému na definované obdobie alebo do definovanej udalosti v budúcnosti.
- Riadenie rizík ochrany súkromia pomocou správu identít a prístupu (IAM) a pomocou kontrol a auditov prístupov.
- Nástroje na zber a správu používateľských súhlasov („consents“).
- Manažovanie prístupu k údajom **pomocou šifrovania** (detailné techniky šifrovania sú popísané v dokumente 1.1.5 Štandardizácia anonymizácie údajov):
  - Identifikovaná potrebná úroveň šifrovania (úroveň aplikácie, v režime uchovávania („at rest“), počas prenosu): To si bude vyžadovať zosúladenie medzi tímami pre bezpečnosť, uchovávanie, dátovú platformu a analytiku.
  - Vybudované systémy správy kľúčov („Key Management Systems (KMS)“) na správu dešifrovacích kľúčov, aby prístup bolo možné udeliť alebo odobrať pomocou automatizácie na veľkej škále.
  - Nakonfigurované systémy na uchovávanie údajov, dátové systémy a agendové systémy na získavanie kľúčov zo systému KMS pre prístup k údajom. Týmto spôsobom môžu inžinieri pre ochranu súkromia zabezpečiť, aby sa ich technické kontroly nemapovali na jednotlivých inžinierov a ich rozmary, ale na systémy a údaje.
  - Nakonfigurované biznis udalosti a udalosti životného cyklu údajov na vykonávanie politík pre šifrovanie a dešifrovanie príslušných údajov.
  - Vytvorené nemeniteľné logy o prístupe vrátane aktéra, cieľa a vrátených údajov. Užitočné vedia byť aj logy, ktoré ukazujú, kto získal prístup k akým údajom, s akým kľúčom na dešifrovanie, a čo sa s údajmi po prístupe vykonalo.
- Minimalizácia zberu údajov budovaním zdieľaných úložísk a využívaním Centrálnej integračnej platformy.
- Presadzovanie technických na širokej škále je možné len pomocou **automatizácie a konfigurácie politík**. V nasledujúcich krokoch je načrtnuté, ako by takýto pracovný postup mohol vyzerať:






Tento projekt je podporený z Európskeho sociálneho fondu.

- Nastavenie politík pre identifikáciu príslušných súborov údajov, po ktorej údaje v rámci organizácie možno identifikovať na základe ich rizika ohrozenia súkromia.
- Rozšírenie nástrojov dátovej platformy o pripojenie k udalostiam životného cyklu údajov, aby sa politiky dali vynútiť na údajoch, ktoré prúdia v celej infraštruktúre.
- Zavádzanie integrácií s úložiskom, údajmi a nástrojmi pre extrakciu, transformáciu a načítanie (ETL) na „vysielanie“ udalostí životného cyklu pri zmene údajov, aby sa politiky nakoniec spustili a vynútili. To je veľmi dôležité, pretože keď sa stav údajov mení, je potrebné prispôsobiť aj politiky, ktoré sa na ne vzťahujú.
- Spustenie vykonávania politík na archiváciu, vymazanie a/alebo šifrovanie príslušných údajov. Predstavuje to posledný krok zabezpečovania toho, aby sa nástroje na ochranu osobných údajov mohli na údaje použiť vo vhodnom čase.

Tieto kroky budú závisieť od identifikácie systémov, v ktorých sa údaje ukladajú, od klasifikácie údajov na základe rizika (aby sa citlivejšie údaje šifrovali) a od označovania údajov (aby sa mohli presadzovať politiky týkajúce sa šifrovania). Klasifikáciou údajov sa zaoberáme aj v dokumente 1.1.5 Štandardizácia anonymizácie údajov, a označovaním v dokumente 1.1.2 Štandardizácia pre modelovanie údajov.







Tento projekt je podporený z Európskeho sociálneho fondu.

# 4 Príklady dobrej praxe aplikácie štandardu

Ochrana osobných údajov v projekte Manažment osobných údajov si vyžaduje aplikáciu nasledovných štandardov:

- End-to-end šifrovanie datasetov, ktoré možno dešifrovať len vtedy, ak je používateľ prítomný, teda ak riešenie pre manažment osobných údajov používa.
- Správa súhlasov na základe štandardu Verifiable Credentials.

## 4.1 Manažment identít a prístupov v Centrálnej integračnej platforme

Centrálna integračná platforma používa na správu identít a prístupu („Identity and Access Management (IAM)“) Keycloak. Ide o softvérové riešenie s otvoreným zdrojovým kódom napísané v jazyku Java, ktoré umožňuje jednotné prihlásenie („Single Sign On“ cez IdP) prostredníctvom správy identít a prístupu. Ponúka širokú škálu integrácií založených na protokoloch ako SAML, OpenID Connect a OAuth2. Vďaka týmto vlastnostiam je Keycloak skutočne flexibilný aj spoľahlivý. Keycloak má zabudovanú podporu na pripojenie k existujúcim serverom LDAP alebo Active Directory. Ak sa nachádzajú používatelia v iných úložiskách, napríklad v relačnej databáze, dá sa implementovať aj vlastný poskytovateľ. Prostredníctvom administrátorskej konzoly môžu správcovia centrálne spravovať všetky aspekty servera Keycloak. Môžu povoliť a zakázať rôzne funkcie. Môžu konfigurovať sprostredkovanie identity a federáciu používateľov. Môžu vytvárať a spravovať aplikácie a služby a definovať autorizačné politiky s veľkou mierou detailu. Môžu tiež spravovať používateľov vrátane oprávnení a povolených „sessions“.

Keycloak sa ale dá využiť aj v inom scenári ako na prístup k údajom v Centrálnej integračnej platforme. Zoberme si scenár, v ktorom máme starší systém v kombinácii s ekosystémom nových služieb; tento starší systém má zase na starosti autentifikáciu a autorizáciu používateľov. Ako teda môžeme pokračovať v používaní tejto služby bez toho, aby sme museli všetkých používateľov migrovať do systému Keycloak? Na zjednodušenie tohto druhu integrácie zavádza riešenie Keycloak spomínaný koncept vlastných poskytovateľov.

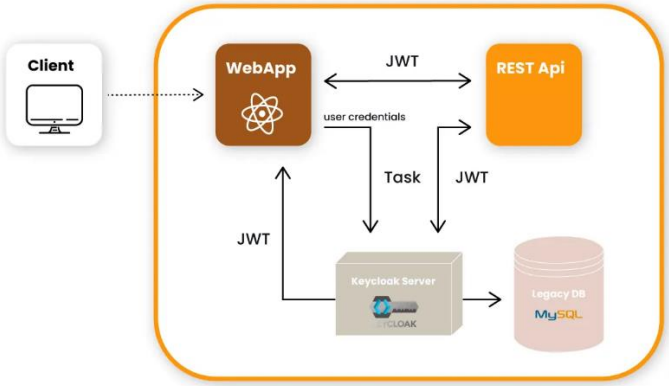
### Keycloak a vlastní poskytovatelia

Vlastný poskytovateľ je súbor .jar, ktorý obsahuje jednu alebo viac implementácií rozhrania poskytovateľa služieb („Service Provider Interface (SPI)“). Pre každú funkcionalitu, akou je napríklad prihlasovanie, autentifikácia alebo autorizácia, existuje SPI. Budeme teda môcť poskytnúť implementácie týchto služieb, ktoré bude systém používať, ako keby boli jeho vlastné. Vo fáze spúšťania Keycloak vyhľadá všetkých dostupných poskytovateľov prostredníctvom dedikovaného mechanizmu. Nasledujúci príklad (Obrázok 4~~Obrázok 4~~) ukazuje implementáciu SPIs.






Tento projekt je podporený z Európskeho sociálneho fondu.




**Obrázok 4: Ukážka implementácie vlastného poskytovateľa cez SPI[1]**

## 4.2 Bezpečnosť údajov v dátových cloudoch

### Platformy pre bezpečnosť údajov

Tieto platformové riešenia poskytujú komplexné nástroje na vymazávanie údajov, export, správu súhlasov, obfuskáciu, zdieľanie a katalogizáciu údajov:

- **Inventarizácia a katalogizácia údajov** – nástroje v tejto oblasti slúžia na objavovanie („discovery“) a indexovanie údajov vo veľkej škále. Pomáhajú zmapovať citlivé a osobné údaje, metadáta a dokumenty pomocou vzorcov zo strojového učenia a dátovej „lineage“.
- **Analýza klastrov** - Na základe vytvoreného katalógu údajov dokážu takéto riešenia poskytnúť prehľad o tom, ktoré dátové úložiská obsahujú citlivé údaje, aby ste mohli cielene vykonávať politiky na ich odstraňovanie, prípadne na aplikovanie iných postupov bezpečnosti. Táto analýza tiež umožňuje korelovať údaje späť k vlastníkom (aby sa znížila stopa takzvaných „osirelých“ datasetov), čím sa znižuje celkové riziko.
- **Spracovanie údajov** - po vytvorení indexovaného katalógu údajov riešenia ponúkajú centralizovaný pohľad na index údajov dotknutej osoby alebo iného subjektu a prístup k nemu prostredníctvom API. To umožňuje organizácii vymazať údaje alebo ich exportovať, aby vyhovela požiadavkám používateľov na základe zákonov ako je GDPR.
- **Mapovanie súladu s reguláciami** - pre činnosti, ako sú prenosy údajov prostredníctvom partnerských platforiem a iných koncových bodov, je cieľom týchto riešení zmapovať procesy ochrany osobných údajov podľa požiadaviek zákonov, ako je GDPR, a tým urýchliť audit súladu.
- Niektoré riešenia ponúkajú aj:
  - šablóny na automatizáciu preskúmaní ochrany osobných údajov („privacy reviews“),

[1] Zdroj: https://medium.com/flux-it-thoughts/how-to-integrate-enterprise-authentication-with-keycloak-part-1-808ce9608743, Dátum referencie: 27.02.2023







Tento projekt je podporený z Európskeho sociálneho fondu.

- posudzovanie rizík dodávateľov,
- podpora životného cyklu žiadosti o prístup k údajom dotknutej osoby,
- manažment incidentov narušenia bezpečnosti údajov.

Príkladmi takýchto platforiem sú BigID a OneTrust.

### „Bodové“ riešenia bezpečnosti údajov

Pri rôznorodých požiadavkách na bezpečnosť údajov v dátovom cloude nemusí byť najlepším riešením platforma, ale skôr „bodové“ riešenie. Príkladom je nástroj Privicera ktorý ponúka správu zásad riadenia prístupu a šifrovanie údajov na úrovni polí/stĺpcov. Poskytuje „out of the box“ podporu pre ETL a preberanie údajov cez Apache Nifi, Kafka, plugin pre Databricks a Hive a REST APIs pre Snowflake. Je založený na Apache Ranger, ktorý je lídrom pre správu prístupov k údajov v prostredí big data. Je to „open source“ projekt od Apache, tým pádom je v súlade s ostatnými riešeniami ako Apache Spark, Apache Kafka a dátovým katalógom Apache Atlas.

### „Plugin“ riešenia

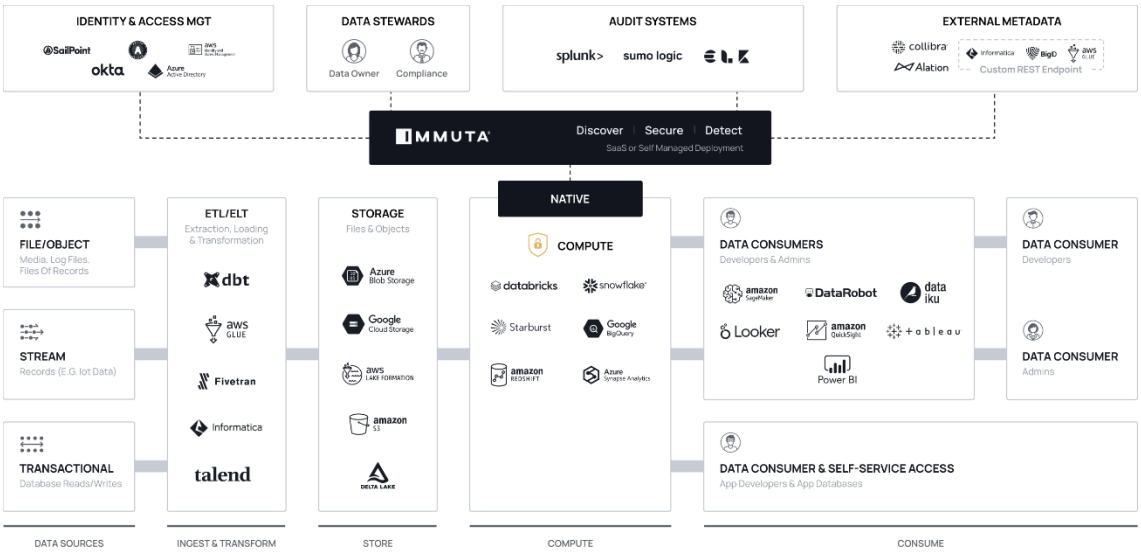
Riešenia vo forme zásuvných modulov – „pluginov“ sa bezproblémovo integrujú s hlavnými platformami dátových cloudov, ako aj s ďalšími nástrojmi na zabezpečenie a správu údajov, ako sú systémy IAM, dátové katalógy a nástroje biznis inteligencie („Business Intelligence (BI)“). Sú tak integrálnou súčasťou moderného dátového zásobníka („data stack“).

Príkladom je riešenie Immuta navrhnuté tak, aby spĺňalo potreby modernej bezpečnosti údajov tým, že ponúka platformu pre prístup k údajom („Data Access Platform“). Táto platforma je navrhnutá tak, aby oddeľovala politiky od výpočtovej techniky, bezproblémovo sa integrovala s moderným dátovým zásobníkom a presadzovala politiky správy aktív s vysokou výkonnosťou. Nasledujúci Obrázok 5~~Obrázok 5~~ znázorňuje ekosystém tohto riešenia, v ktorom je vidno aj všetky kľúčové komponenty dátového zásobníka („data stacku“), ktorému sa podrobnejšie budeme venovať v dokumente 4.2.1 Koncept pre zavádzanie analytického spracovania údajov do praxe.



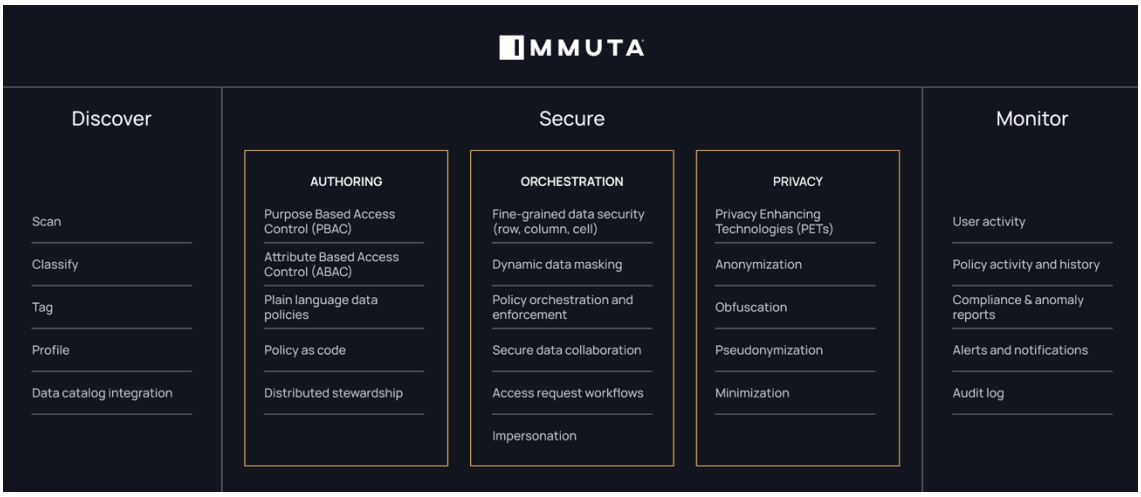



Tento projekt je podporený z Európskeho sociálneho fondu.




**Obrázok 5: Ekosystém zásuvného modulu – "plugin" riešenia Immuta**

Obrázok 6~~Obrázok 6~~ ukazuje komplexnosť takéhoto „plugin" riešenia. Poskytuje možnosti autorizácie, orchestrácie a ochrany osobných údajov. Okrem ústredného piliera pre bezpečnosť („Secure") poskytuje Immuta aj možnosti objavovania („Discover") a monitorovania údajov. Politiky prístupu založené na atribútoch sa vykonávajú priamo pri behu dopytov („query runtime"), pričom prístupy sa automaticky logujú. V rámci ochrany súkromia poskytuje aj funkcionality ako anonymizáciu, obfuskáciu, pseudonymizáciu a minimalizáciu.




**Obrázok 6: Architektúra zásuvného modulu – "plugin" riešenia Immuta**







Tento projekt je podporený z Európskeho sociálneho fondu.

## 4.3 Procesné opatrenia

### 4.3.1 Preverovanie potreby udelených prístupov k údajom

Zamestnanci si často vypýtajú prístupy aj pre istotu, aby ich následne administratívne procesy nebrzdili pri práci. Tým sa samozrejme porušuje princíp bezpečnosti údajov, aby sa minimalizoval počet ľudí, ktorý k nim majú prístup (kapitola 2.3.1).

Skúsenosť spoločnosti Netflix v tejto téme je nasledovná. Tímy pre bezpečnosť a ochranu údajov zaviedli nástroje na kontrolu, či inžinieri a dátoví vedci, ktorí majú prístup k citlivým zašifrovaným údajom, ich stále potrebujú. Rutinne odoberali vzorky údajov a kontrolovali, kedy boli naposledy dešifrované. Často zistili, že zamestnanci si vyžiadali kľúče, ale takmer vôbec alebo vôbec ich nepoužili na prístup k údajom.

V týchto prípadoch tímy vymenili kľúče, aby skontrolovali, či sa technici alebo dátoví vedci budú niekedy stážovať. **V sedemdesiatich piatich percentách** prípadov sa nikdy neozvali. Znamená to, že ľudia si často myslia, že budú potrebovať viac údajov, než skutočné potrebujú, a aj keď ich nepoužívajú, ich možnosť pristupovať k nim predstavuje riziko pre súkromie. Takéto techniky aplikovať interne a aj pri zdieľaní údajov s tretími stranami







Tento projekt je podporený z Európskeho sociálneho fondu.

# 5 Návrh odporúčaní na aplikáciu štandardu

## 5.1 Informačné prostredie verejnej správy

Návrh odporúčaní na aplikáciu štandardu pre informačné prostredie verejnej správy a projekty z programu Manažment údajov definuje zoznam odporúčaní, ktoré je vhodné v rámci projektov implementovať tak, aby bola zabezpečená dôsledná ochrana údajov v predmetných systémoch, najmä z dôrazom na heterogénne integrované informačné prostredie verejnej správy.

### Tabuľka 8: Zoznam odporúčaní

| Opatrenie | Popis | Odkaz |
|---|---|---|
| **Definícia bezpečnostných požiadaviek** | Identifikácia bezpečnostných požiadaviek. Na začiatku každého projektu je nutné zadefinovať bezpečnostné požiadavky, ktoré musia byť naplnene na základe relevantných hrozieb a legislatívnych požiadaviek. Tato aktivita je kľúčová pre správne nasadenie systému | |
| **Vytvorenie bezpečnostnej architektúry informačného systému** | Táto požiadavka smeruje k požiadavke na vytvorenie nie len samotnej architektúre aplikácie alebo IS ale aj vytvoreniu dokumentácie popisujúcej bezpečnostné funkcionality, funkcie a služby v rámci celého systému. Dokumentácia bude obsahovať informácie ako ma byt nastavená infraštruktúra a ako je riešená bezpečnosť v aplikácií samotnej. Napríklad bezpečnosť API, šifrovaná komunikácia, bezpečnosť údajov, ktoré aplikácia spracováva. Bezpečnosť prístupov do aplikácie a jej spravovanie. Akým spôsobom sa budú robiť zálohy a obnova. | |
| **Vytvorenie bezpečnostnej architektúry integrácie** | Musí byt popísaná a dobre navrhnutá architektúra integrácií na externé systémy, ktoré sa budú používať a nie sú súčasťou tohto projektu. | |
| **Definícia diagramu „data flow“** | Data flow diagram je dôležitý hlavne s pohľadu spracovania dát. Ako dáta vstupujú do systému ako sa spracúvajú a menia a ako vystupujú zo systému. Tak isto, čo sa s dátami deje. | |
| **Identifikácia rolí a zodpovedností** | Jasné určenie zodpovedností za jednotlivé úlohy v projekte. Takýmto dokumentom môže byť dokument R&R (Roles and Responsibilities), kde sa definuje jasne, kto je za čo v rámci projektu zodpovedný. | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Opatrenie | Popis | Odkaz |
|---|---|---|
| **Popis a implementácia procesov prevádzky** | Popis procesov prevádzky nasadenia. Pre správne riadenie rizík a bezpečnosti je potrebné vedieť, aké procesy má nasadený prevádzkovateľ plánovaného systému. | |
| **Vytvorenie bezpečnostnej dokumentácie** | Bezpečnostný projekt<br><br>Proces riadenia bezpečnostných incidentov<br><br>Prevádzková dokumentácia<br><br>Špecifikácia procesov prevádzky a nasadenia. | |
| **Bezpečnostný audit zdrojového kódu** | Kontrola zdrojového kódu na chyby a zraniteľnosti. Túto aktivitu berieme, ako samozrejmosť, ale keďže nie je explicitne spomenutá, je nutné spomenúť že je to základná požiadavka na DevSecOps. To znamená zakomponovanie kontroly zdrojového kódu do procesu vývoja riešenia. | |
| **Bezpečnostný audit zdrojového kódu voči licenčným schémam** | Kontrola zdrojového kódu voči licenčným schémam. Táto kontrola je potrebná, pre auditný výkaz, že i keď sa použije open source, tak tento software nie je licencovaný a nespôsobí to objednávateľovi problémy neoprávneného používania. | |
| **Aplikačný audit podľa OWASP** | V rámci tejto požiadavky je potrebné vykonať bezpečnostný asesment aplikácie. Zvolenie správnych frameworkov. | https://owasp.org/ |
| **Analýza systému z pohľadu GDPR a „data privacy“** | Tento proces zahŕňa identifikáciu, ktoré osobné údaje sú spracovávané, ako sú spracovávané a kto má prístup k nim. Analýza tiež zahŕňa posúdenie, či sú všetky požadované postupy a technológie v súlade s GDPR a „data privacy“. Cieľom je zabezpečiť, aby boli osobné údaje spracovávané v súlade s GDPR a „data privacy“ a aby boli chránené pred neoprávneným prístupom. | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Opatrenie | Popis | Odkaz |
|---|---|---|
| **Penetračné testovanie infraštruktúry** | Penetračné testovanie infraštruktúry (angl. Infrastructure Penetration Testing) je proces skúšania zabezpečenia informačnej infraštruktúry organizácie. Tento proces sa používa na identifikovanie, hodnotenie a odstránenie bezpečnostných nedostatkov v informačnej infraštruktúre organizácií. Cieľom penetračného testovania je vystaviť organizáciu potenciálnym bezpečnostným hrozbám a poskytnúť informácie o tom, aké účinné sú jej bezpečnostné opatrenia. Penetračné testovanie sa môže uskutočniť pomocou rôznych techník, ako sú internej a externej penetračné testovanie, sieťové skenovanie a ďalšie. | |
| **Penetračné testovanie nového systému.** | Táto aktivita je potrebná, pre overenie, či daný produkt je dostatočne bezpečný a zodpovedá trhovým štandardom. Tato aktivita zahŕňa aj stres testy aplikácie. Simulovaný DOS útok. | |
| **Penetračné testovanie integrácii na tretie strany** | Penetračné testovanie integrácií. V rámci tejto aktivity, je potrebné skontrolovať, či nový systém nevnáša bezpečnostné rizika do už existujúcich systémov, alebo existujúce systémy nepredstavujú hrozbu pre nový pripadne modernizovaný systém. | |
| **Overenie úrovne zabezpečenia procesov CI/CD** | Kontrola procesu CI/CD pri SDLC. | |
| **Špecifikácia bezpečnostného dohľadu a požiadaviek** | Špecifikácia a integrácia systému do bezpečnostného dohľadu. Keďže sa jedna o kľúčové systémy, ktoré spadajú do kategórie III informačných systémov, je nutne zadefinovať kto a ako bude vykonávať bezpečnostný monitoring. S tým súvisí aj definícia log informácii a určenie prípadov použitia, ktoré budú nastavene na detekciu bezpečnostných udalosti. Tieto je potom potrebné implementovať a integrovať do monitorovacieho riešenia. | |
| **Vytvorenie architektúry a dokumentácie nasadenia bezpečnostného monitoringu** | Tento proces zahŕňa identifikáciu požiadaviek na bezpečnosť, vytvorenie architektúry a dokumentácie pre monitorovanie bezpečnosti a implementáciu monitorovacích nástrojov. Cieľom je zabezpečiť, aby boli všetky systémy a siete chránené pred neoprávneným prístupom a aby boli všetky bezpečnostné incidenty monitorované a riešené. | |
| **Stress testy na aplikáciu.** | Simulovaný DOS alebo DDOS útok. | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Opatrenie | Popis | Odkaz |
|---|---|---|
| **Definícia bezpečnostných štandardov pre tretie strany** | Definícia bezpečnostných štandardov pre tretie strany. Pokiaľ sa na systémy budú napájať tretie strany, je nutne definovať aké bezpečnostné požiadavky mame voči týmto subjektom a čo musia spĺňať. | |
| **DPIA analýza** | DPIA analýza (Data Protection Impact Assessment) je proces, ktorý zahŕňa posúdenie rizík súvisiacich s ochranou osobných údajov. DPIA analýza má nasledujúcu štruktúru:<br>1. Identifikácia procesu spracovania osobných údajov.<br>2. Identifikácia rizík pre ochranu osobných údajov.<br>3. Posúdenie rizík pre ochranu osobných údajov.<br>4. Navrhnutie opatrení na zníženie rizík pre ochranu osobných údajov.<br>5. Implementácia opatrení na zníženie rizík pre ochranu osobných údajov.<br>6. Monitorovanie a revízia opatrení na zníženie rizík pre ochranu osobných údajov. | |
| **Zadefinovanie metodiky Business continuity služby (BCM)** | Metodika Business continuity služby (BCM) je proces, ktorý zahŕňa identifikáciu, plánovanie a implementáciu opatrení na zabezpečenie pokračovania prevádzky v prípade výpadku alebo poškodenia. Tento proces zahŕňa identifikáciu kritických procesov, vytvorenie plánu na obnovenie prevádzky a implementáciu opatrení na zabezpečenie pokračovania podnikania. Cieľom je zabezpečiť, aby boli všetky kritické procesy chránené pred výpadkom alebo poškodením a aby boli všetky procesy obnovené čo najskôr. | |
| **Implementácia procesov DRP (disaster recovery plan)** | Implementácia procesov DRP (disaster recovery plan) zahŕňa vytvorenie plánu na obnovenie prevádzky v prípade poškodenia alebo výpadku. Tento proces zahŕňa identifikáciu kritických procesov, vytvorenie plánu na obnovenie prevádzky a implementáciu opatrení na zabezpečenie obnovenia prevádzky. Cieľom je zabezpečiť, aby boli všetky kritické procesy chránené pred poškodením alebo výpadkom a aby boli všetky procesy obnovené čo najskôr. | |
| **Testovanie procesov DRP** | Realizácia testov. | |
| **Testovanie procesov BCM** | Realizácia testov. | |







Tento projekt je podporený z Európskeho sociálneho fondu.

| Opatrenie | Popis | Odkaz |
|---|---|---|
| **Návrh detailných postupov pre overenie úrovne zabezpečenia systému** | Z pohľadu rozšírenia okruhu poskytovateľov dát, konzumentov dát a používateľov systému návrh detailných postupov pre overenie úrovne zabezpečenia systému minimálne v nasledovných oblastiach :<br>• Autentifikácia<br>• Riadenie používateľských relácií a riadenie prístupu<br>• Eliminácia zlomyseľných vstupov a tvorba bezpečných výstupov<br>• Logovanie<br>• Ochrana dát a šifrovanie<br>• Antivírová ochrana<br>• Bezpečnosť webových služieb<br>• Konfigurácia aplikačného prostredia | |
| **Definovanie a popis fyzickej bezpečnosti pre riešenia** | Proces, ktorý má za cieľ chrániť informačný systém pred fyzickým poškodením alebo zneužitím. Tento proces zahŕňa kontrolu prístupu k informačnému systému, zabezpečenie fyzických zariadení, ako sú počítače, servery, siete a ďalšie, ako aj zabezpečenie údajov a informácií uložených vo fyzických médiách, ako sú diskety, diskety, CD a DVD. Fyzická bezpečnosť informačného systému je dôležitá pre zabezpečenie informácií vo všetkých fázach ich životného cyklu. | |

## 5.2 Dátová kancelária verejnej správy

Dátová kancelária verejnej správy pomáha a asistuje inštitúciám verejnej správy v aplikácií štandardov, ktoré sa týkajú dát. Týka sa to i bezpečnosti a ochrany údajov. V budúcnosti odporúčame nasledujúce činnosti:

- Šírenie najlepšej praxe a skúseností v oblasti ochrany a bezpečnosti údajov (dedikované webové sídlo a organizovanie pracovných skupín).
- Príprava a publikácia manuálov a návodov v oblasti ochrany a bezpečnosti údajov (ako napríklad tento dokument).
- Zabezpečenie a prevádzku technológií pre manažment osobných údajov (systém MOU), ktorý verejným inštitúciám umožňuje implementovať požiadavky GDPR.
- Organizácia školení ako správne aplikovať odporúčania v oblasti bezpečnosti a ochrany údajov.
- Výkon auditov v oblasti ochrany a bezpečnosti údajov na základe kontrolného zoznamu.
- Právne poradenstvo v oblasti ochrany a bezpečnosti údajov.







Tento projekt je podporený z Európskeho sociálneho fondu.

Aby bola Dátová kancelária schopná tieto činnosti realizovať, je potrebné, aby mala dostatočnú kapacitu a vznikol dedikovaný tím aspoň troch expertov na ďalších minimálne 5 rokov. Potrebnými kvalifikáciami pre členov tohto tímu sú: legislatíva v oblasti bezpečnosti a ochrany údajov, technológie pre manažment osobných údajov, prepojené údaje a SOLID, bezpečnosť informačných systémov a kybernetická bezpečnosť.







Tento projekt je podporený z Európskeho sociálneho fondu.

# Chyba! Nenašiel sa

**Contact us**

**Rudolf Sedmina**
**partner**
**Management Consulting**
**E** rsedmina@kpmg.sk

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**www.kpmg.com**





Tento projekt je podporený z Európskeho sociálneho fondu.