



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti



NCC-SK
SLOVAKIA CYBERSECURITY
COORDINATION CENTRE
 

VZŤAH OCHRANY OSOBNÝCH ÚDAJOV A KYBERNETICKEJ BEZPEČNOSTI

eFocus:

Kybernetická bezpečnosť v meniacich sa podmienkach

Bratislava, 20.09.2023

Ivan Makatura



APLIKOVATEĽNÉ DEFINÍCIE

[čl. 4 ods. 1 GDPR]:

- osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby

[čl. 4 ods. 2 GDPR]:

- spracúvanie je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov,

[čl. 8 ods. 1 Charty základných práv Európskej únie]:

- Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. Ochrana fyzických osôb v súvislosti so spracúvaním osobných údajov patrí medzi základné práva. Súčasťou práva na ochranu súkromia je aj ochrana osobných údajov.

[čl. 5 písm. f) GDPR]:

- osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).

[§ 3 písm. h) zákona č. 69/2018 Z.z.]

- 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



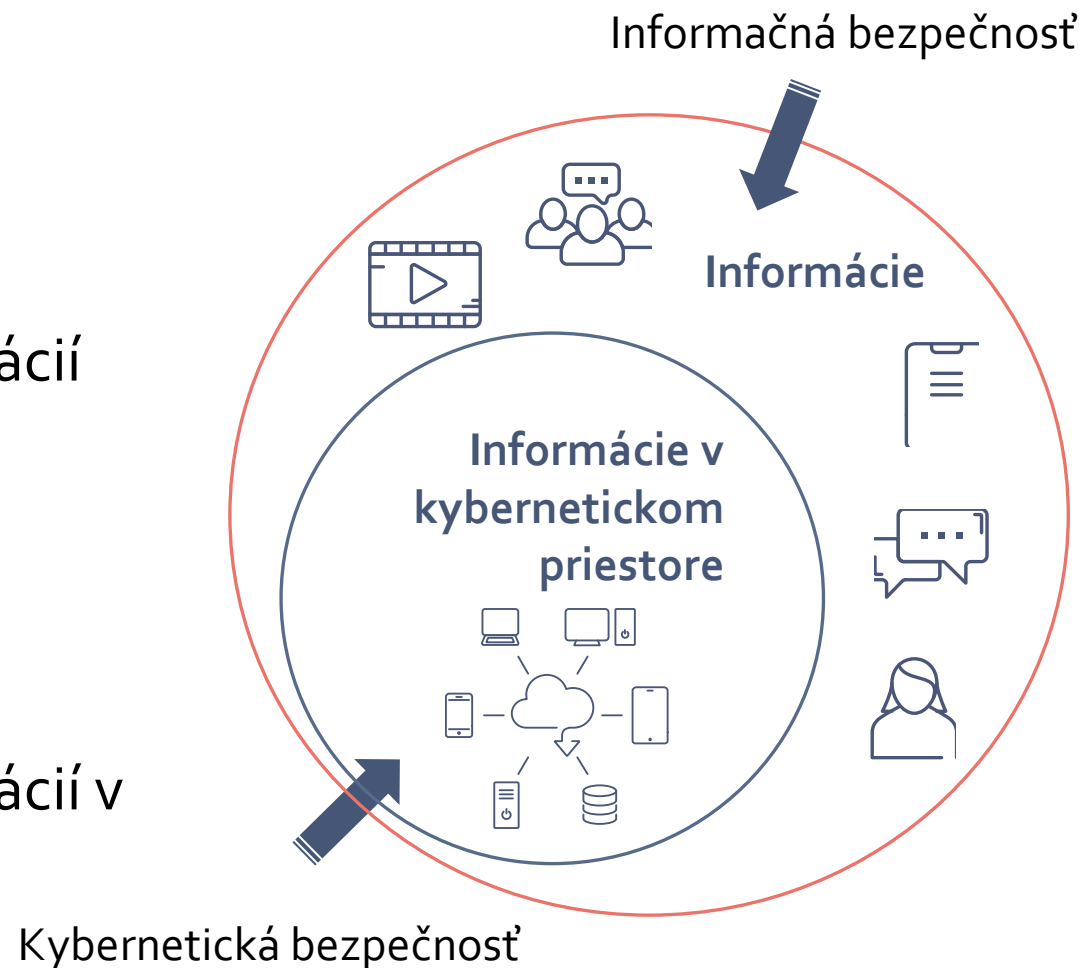
INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

[ISO/IEC 27032, čl. 2.33]

- Informačná bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií

[ISO/IEC 27032, čl. 4.20]

- Kybernetická bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore





CIELE OCHRANY - ATRIBÚTY BEZPEČNOSTI

- **Dôvernosť (Confidentiality)** - záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
- **Dostupnosť (Availability)** - záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná
- **Integrita (Integrity)** - záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené
- **Nepopierateľnosť (Non- repudiation)** - záruka že pôvodca údajov nemôže neskôr poprieť svoju identitu ani účasť na spracúvaní týchto údajov
- **Zodpovednosť (Accountability)** – záruka, že aktivitu entity pri spracúvaní údajov možno určiť jedinečným spôsobom



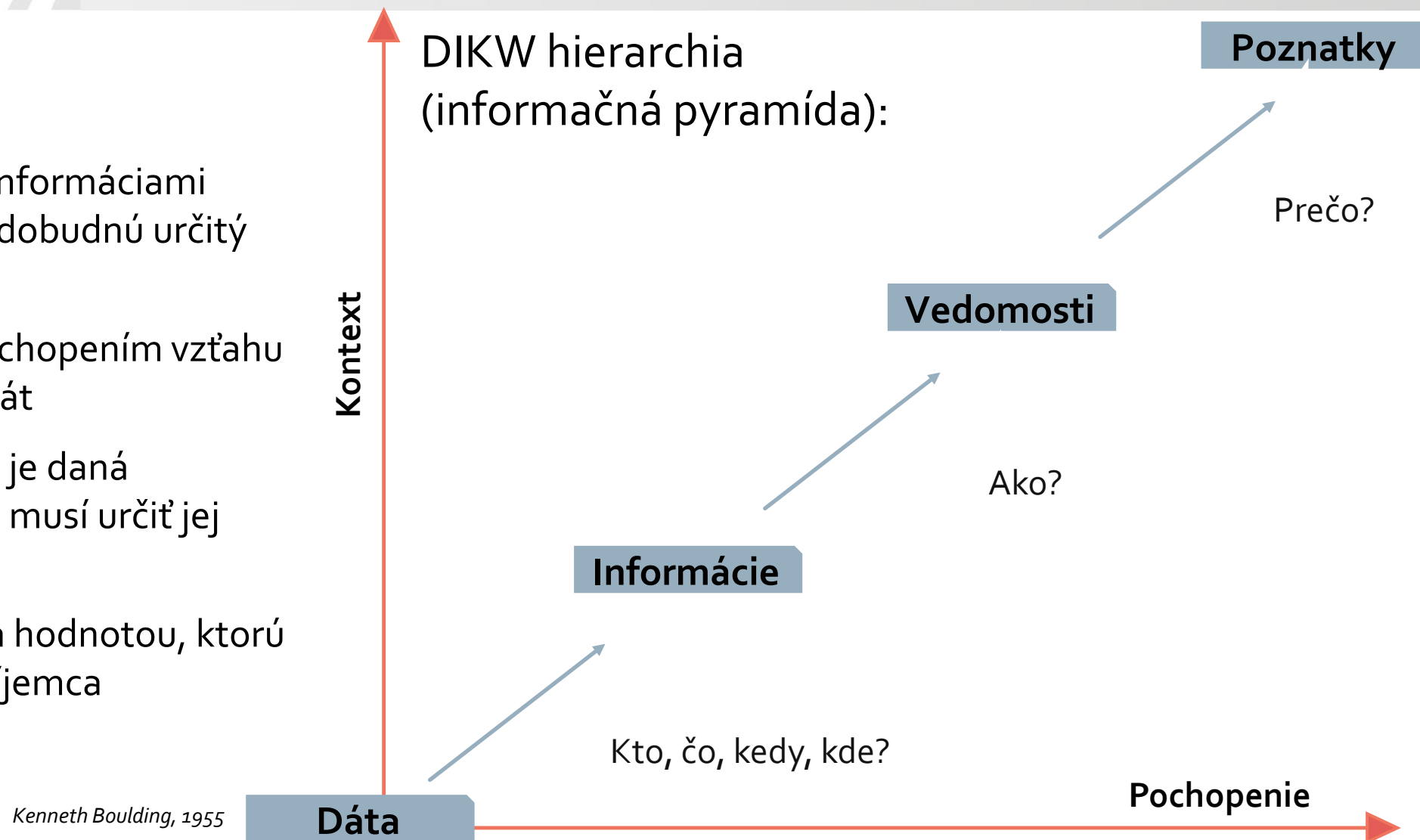
ČO ZNAMENÁ „BEZPEČNOSŤ“?

- Pojem bezpečnosť pôvodne pochádza z latinského „securitas“, čo znamenalo bezstarostnosť, bezpečnosť, istotu, pokoj, ochranu a zabezpečenie
- Najvyššia miera nebezpečenstva alebo hrozby, ktorú spoločnosť v určitej oblasti života pripúšťa
- Všeobecný význam výrazu „bezpečnosť“: **stav, v ktorom je chránený život, zdravie, prostredie či majetok (vrátane informačného majetku)**
- Možné interpretácie pojmu informačná bezpečnosť:
 - **Interdisciplinárna oblasť**, ktorá sa zaoberá skúmaním zraniteľností a hrozieb a/alebo vývojom metód a mechanizmov ochrany dát a informácií, ošetrovaním hrozieb a riadením a rizík, ktoré pôsobia na informačné aktíva
 - **Súbor procesov** a činností zameraných na dosiahnutie požadovanej úrovne ochrany informačných aktív
 - **Stav systému**, kedy sú dostatočne ošetrené známe riziká vyplývajúce z hrozieb pôsobiacich na informačné aktíva



DÁTA VS. INFORMÁCIE

- Dáta (údaje) sa informáciami stanú, až keď nadobudnú určitý význam
- Informácia je pochopením vzťahu medzi časťami dát
- Cena informácie je daná hodnotou, ktorú musí určiť jej vlastník
- Cena dát je daná hodnotou, ktorú musí určiť ich príjemca





DÁTA VS. INFORMÁCIE





POŽIADAVKY NA BEZPEČNOSŤ PODĽA GDPR

[Čl. 24 GDPR: Bezpečnosť spracúvania]

1. S ohľadom na:

- povahu (spracúvania),
- rozsah (spracúvania),
- kontext a účely spracúvania,
- ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb

prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením.

Uvedené opatrenia sa podľa potreby

- preskúmajú a
- aktualizujú.

audit

Patch mgmt., Configuration mgmt., Release mgmt.

2. Ak je to primerané vzhľadom na spracovateľské činnosti, opatrenia uvedené v odseku 1 zahŕňajú **zavedenie primeraných politík** ochrany údajov zo strany prevádzkovateľa.



POŽIADAVKY NA BEZPEČNOSŤ PODĽA GDPR

[Čl. 32 GDPR: Bezpečnosť spracúvania]

1. Prevádzkovateľ a sprostredkovateľ prijímú...

primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

- a) pseudonymizáciu a šifrovanie osobných údajov;
- b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
- d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Jediný konkrétny typ opatrenia

Vyššie uvedené požiadavky na bezpečnostné opatrenia sú iba generické, veľmi všeobecné



POŽIADAVKY NA BEZPEČNOSŤ PODĽA GDPR

[Čl. 32 GDPR: Bezpečnosť spracúvania]

2. Pri posudzovaní primeranej úrovne bezpečnosti **sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie**, a to najmä v dôsledku:

- náhodného alebo nezákonného zničenia

[integrita, dostupnosť]

- straty

[integrita, dostupnosť]

- zmeny

[integrita]

- neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú

[dôvernosť]

- alebo neoprávneného prístupu k takýmto údajom

[dôvernosť, nepopierateľnosť, zodpovednosť]



DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

Opatrenia podľa § 20 (1) Zákona 69/2018 Z.z. sú:

- **Úlohy, procesy, roly a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

V zmysle § 19 (1) Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať:

- **Všeobecné bezpečnostné opatrenia** najmenej v rozsahu podľa §20
- **Sektorové bezpečnostné opatrenia**, ak sú prijaté





OPATRENIA VO VZŤAHU K PROCESU RIADENIA RIZÍK

- **Existujúce opatrenia** (z angl. Existing controls)
 - opatrenia inherentne zabudované už v čase návrhu resp. implementácie systému

- **Rozšírené (tiež „vylepšené“) opatrenia** (z angl. Enhanced controls)
 - aplikované na implementovaný systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému; typicky ich navrhuje manažér kybernetickej bezpečnosti, alebo jeho tím

- **Dodatočné opatrenia** (z angl. Additional, Complementary controls)
 - odporúča ich zvyčajne interný, alebo externý audítor v záverečnej správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu



GENERICKÉ ROZDELENIE OPATRENÍ

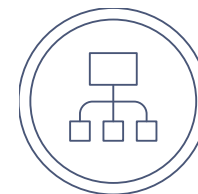
■ TECHNICKÉ OPATRENIA

- opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy



■ ORGANIZAČNÉ OPATRENIA

- opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie



- **PERSONÁLNE OPATRENIA** - podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov



**Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych technických a organizačných opatrení**



OPATRENIA PODĽA ISO/IEC 27002:2022

Nová verzia normy STN ISO/IEC 27002:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022) zavádza nové rozdelenie opatrení.

- Opatrenia sa rozdeľujú z pohľadu toho, kedy a akým spôsobom opatrenie modifikuje riziko v kontexte výskytu incidentu:
 - **preventívne** (#preventive) – opatrenia, ktoré majú zabrániť vzniku bezpečnostných incidentov,
 - **detektívne** (#detective) – opatrenia, ktoré majú nastať v prípade výskytu incidentu a slúžia na zistenie jeho príčin,
 - **nápravné** (#corrective) – opatrenia, ktoré majú nastať po výskyte incidentu a slúžia na zotavenie systému alebo organizácie z incidentu.



AKÉ OPATRENIA IMPLEMENTOVAŤ PRE OOÚ?

- Nie je možné riadiť sa požiadavkami GDPR na bezpečnostné opatrenia - sú iba generické, všeobecné
- Podľa vyhlášky ÚOOÚ SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov prevádzkovateľ pri prijímaní opatrení na zmiernenie rizík pre práva fyzickej osoby postupuje v primeranom rozsahu podľa prílohy
 - uvedené sú iba hlavné kategórie opatrení, heslovite
 - metrika a spôsob overovania nie sú navrhnuté
- Pri konkretizácii technických a organizačných opatrení pre ochranu osobných údajov je možné vychádzať z princípu **analogia legis**:
 - Pokiaľ zákon nejakú problematiku neupravuje, môže odkázať na podobné (analogické) použitie inej normy na daný prípad
- Analogické právne predpisy:
 - **vyhláška NBÚ č. 362/2018 Z. z.** ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
 - **vyhláška ÚPVII č. 179/2020 Z. z.** ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
 - **STN ISO/IEC 27002:2023** Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022)



HIERARCHIA PRÁVNÝCH A TECHNICKÝCH PREDPISOV

Nariadenia EÚ

Smernice EÚ

Technické normy
EN ISO/IEC

Nariadenia vlády

Zákony NRSR

Vykonávacie právne predpisy

Technické normy
STN EN ISO/IEC



TVRDENIA

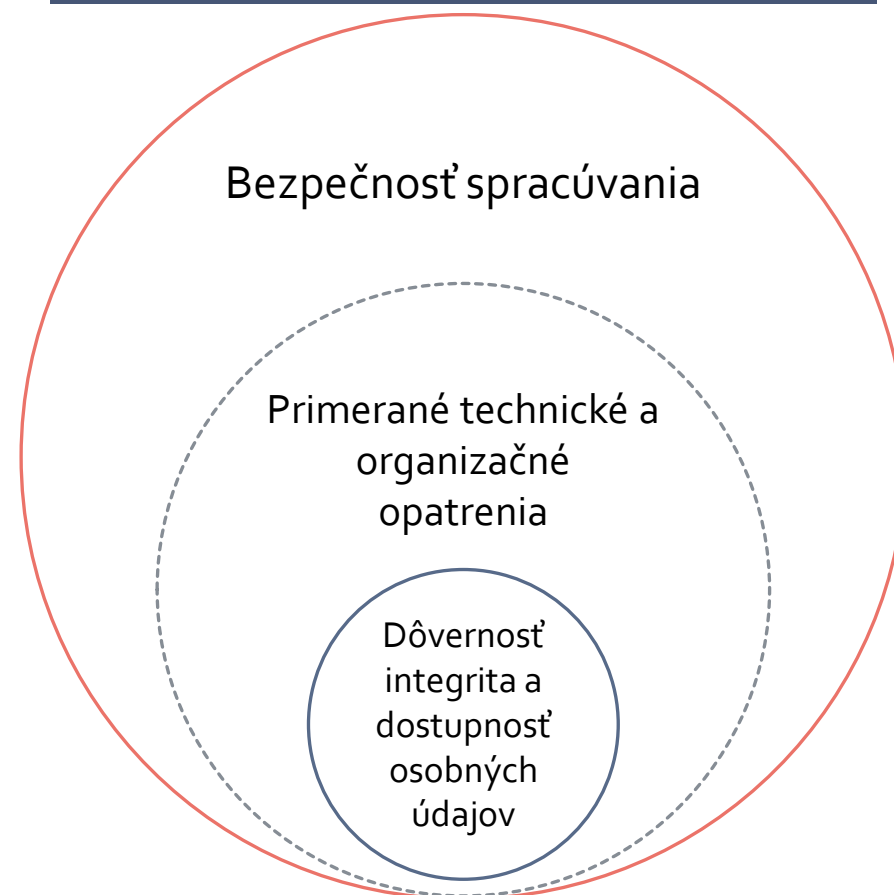
- Spracúvanie je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov ✓
- Dá sa implicitne vyvodzovať, že výrazom „**súbor operácií**“ je myslené „**automatizovaných operácií**“ ✓
- Spracúvanie pomocou automatizovaných prostriedkov = spracúvanie v kybernetickom priestore ✓
- Spracúvanie akýchkoľvek dát (vrátane osobných údajov) prebieha **majoritne v kybernetickom priestore** ✓
- Ciele ochrany údajov a ciele kybernetickej bezpečnosti sú totožné - zachovanie požadovaných bezpečnostných atribútov: **dôvernosť, dostupnosť, integrita**, resp. aj **nepopierateľnosť, zodpovednosť** ✓
- Povinnosť prijať opatrenia vyplýva z rôznych právnych predpisov pre rôzne typy povinných osôb. GDPR v tomto nemá unikát. ✓
 - Prevádzkovateľ a sprostredkovateľ prijímú... **primerané technické a organizačné opatrenia** s cieľom zaistiť úroveň bezpečnosti
 - Prevádzkovateľ základnej služby je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia, ak sú prijaté
- Ochrana súkromia znamená implementovať opatrenia a vykonávať činnosti, ktoré sú takmer totožné s opatreniami a činnosťami súvisiacimi s bezpečnosťou akýchkoľvek iných typov informácií ✓
- GDPR má iba všeobecné požiadavky na bezpečnostné opatrenia ✓
- Pri konkretizácii technických a organizačných opatrení je možné vychádzať z princípu analogia legis ✓



VZŤAH KYBERNETICKEJ BEZPEČNOSTI, OCHRANY ÚDAJOV A PRÁVA NA SÚKROMIE

- Zaručenie základných ľudských práv = vynucovanie práva prostredníctvom právnych predpisov a zmlúv
- Zaručenie **práva** na ochranu súkromia => zaručenie bezpečnosti spracúvania osobných údajov
- Zaručenie **bezpečnosti** spracúvania osobných údajov = prijatie primeraných technických a organizačných opatrení (pre zachovanie dôvernosti, integrity a dostupnosti informácií)
- Informačná bezpečnosť = zachovanie dôvernosti, integrity a dostupnosti informácií
- Kybernetická bezpečnosť = zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore
- **Ochrana osobných údajov $\cong$ Kybernetická bezpečnosť**

Zaručenie práva na ochranu súkromia



Kybernetická bezpečnosť



NCC-SK

SLOVAKIA CYBERSECURITY
COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akémkoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



@CybercenterSk