



Základy práva informačných a komunikačných technológií pre KIB

I.

(Vzdelávanie pre zamestnancov verejnej správy v kategórií
používateľov „laik“, „odborný zamestnanec“ a „manažér“
– modul č. 6)

Meno a priezvisko

XX.XX.XXXX



KC KB UPJŠ

<https://cyberawareness.sk/>

The screenshot shows the homepage of the KC KB UPJS website. At the top left, there are logos for KCKB UPJS and CSIRT UPJS. To the right, there is a navigation menu with links for 'O projekte', 'Aktivity', 'Vzdelávanie', and 'Informácia o konaní vzdelávacích aktivít', along with a language selector set to 'EN' and a search icon. The main content area features a dark blue background with a glowing shield and padlock icon on the left. The central text reads 'Vitajte na oficiálnom webovom sídle KC KB na UPJŠ'. Below this, there are logos for the European Union (financed by the NextGenerationEU program) and the Ministry of Investment, Regional Development and Information of the Slovak Republic. At the bottom, there are four blue buttons with icons and text: 'Expertná činnosť' (with a hand holding a pencil), 'Výskum' (with a magnifying glass), 'Vzdelávanie' (with three medals), and 'Spolupráca' (with two hands shaking).



Vzdelávacia aktivita (I.)

- Časový harmonogram
 - 08:30 – 10:00 – 1. blok
 - 10:00 – 11:30 – 2. blok
 - 11:30 – 12:30 – prestávka
 - 12:30 – 14:00 – 3. blok
 - 14:00 – 15:30 – 4. blok

Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	Úvod do kybernetickej a informačnej bezpečnosti (KIB)	6	Online / Prezenčne
Modul č. 2	Kritické myslenie a dezinformácie	8	Online / Prezenčne
Modul č. 3	Sociálne inžinierstvo	8	Online / Prezenčne
Modul č. 4	Bezpečnosť prevádzky a riešenie kybernetických incidentov	8	Online / Prezenčne
Modul č. 5	Digitálna identita a súkromie v online prostredí	6	Online / Prezenčne
Modul č. 6	Základy práva informačných a komunikačných technológií pre KIB I.	8	Online / Prezenčne
Modul č. 7	Základy práva informačných a komunikačných technológií pre KIB II.	8	Online / Prezenčne

Právo informačných technológií (I.)

- súhrn právnych noriem, ktoré upravujú vzájomne nezávislé a vysoko špecializované právne oblasti, ktoré sa neustále rozvíjajú v dôsledku rýchleho vývoja a aplikácie nových technológií v praxi (4. a 5. priemyselná revolúcia)
- sťažený legislatívny proces z dôvodu rýchlosti napredovania IKT
- aplikácia tzv. princípu technologickej neutrality
- právna úprava nie je kodifikovaná, ale je obsiahnutá v rôznych právnych predpisoch z rôznych právnych oblastí, a to nielen na vnútroštátnej úrovni, ale aj na úrovni práva Európskej únie a medzinárodného práva



Právo informačných technológií (II.)

- Princíp technologickej neutrality = snaha zákonodarcu prijať takú právnu úpravu, ktorá je **technologicky neutrálna**, tzn. ktorá sa neobmedzuje na konkrétnu technológiu, ale ktorá je použiteľná na akékoľvek novovznikajúce technológie bez potreby revízie príslušnej legislatívy.
- **Technologická neutralita** - sloboda jednotlivcov a organizácií vybrať si technológiu, ktorá je najviac primeraná a najviac vyhovuje ich potrebám.
- Produkty, služby alebo regulačné rámce, v ktorých sa zohľadňuje zásada technologickej neutrality neukladajú povinnosť používať určitý typ technológie ani nediskriminujú v prospech jej používania:
 - uznanie akéhokoľvek podpisu, ktorý je dostatočne spoľahlivý
 - využitie čohokoľvek, čo môže prispieť k objasneniu veci ako dôkaz
 - označenie akejkoľvek infraštruktúry, ktorej narušenie by malo závažný vplyv na bezpečnosť štátu, ako kritickej infraštruktúry
 - označenie akejkoľvek informácie slúžiacej na identifikáciu subjektu údajov ako osobný údaj,

Európska právna úprava

- **Dôveryhodné služby a e-government** - elektronická identifikácia, elektronická služba, elektronické schránky
- nariadenie EP a Rady č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (nariadenie eIDAS)
- nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity - rozšírenie funkcionalít národných eID - EU Digital Identity Wallet (EUDIW) alebo tzv. **eWallet**, mobilné vodičské preukazy a vzdelávacie certifikáty
- nariadenie EP 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 - GDPR**)

Tuzemská právna úprava

- zákon č. 305/2013 Z.z. o e-governmente
- zákon č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu
- zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe

Ochrana osobných údajov (I.)

Komu sa poskytuje ochrana?

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

Zdroj: <https://dataprivacymanager.net/processing-personal-data-of-employees/>
22. 8. 2025



Ochrana osobných údajov (II.)

- *akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“), pričom identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby (čl. 4 bod 1 GDPR)*

Demonštratívny výpočet:

titul, meno, priezvisko, dátum narodenia, bydlisko, fotka, e-mailová adresa, kontaktné informácie, číslo bankového účtu, zdravotné informácie, IP adresa (okrem tzv. maskovanej IP adresy a IP adresy pridelennej k sieti využíwanej viacerými používateľmi – napr. internetové kaviarne), súbory cookies, lokalizačné údaje (z mobilného telefónu)

Uvedená definícia osobných údajov nevyžaduje, aby išlo o konkrétnu identitu fyzickej osoby, ale postačuje, aby za splnenia daných podmienok bola osoba identifikovateľná.



Ochrana osobných údajov (III.)

Tri nové kategórie údajov v zmysle GDPR:

- Genetické
- Biometrické
- Údaje o fyzickom alebo duševnom zdraví

Osobnými údajmi nebudú napríklad údaje určujúce právnickú osobu alebo fyzickú osobu podnikateľa, anonymné údaje a pod.

Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality (test proporcionality – napríklad kamerový záznam z miesta činu, ktorý zachytáva tvár útočníka).

Ochrana osobných údajov (IV.)

Príklady osobných údajov

- **odoberanie a ukladanie odlačkov prstov štátnymi orgánmi** (Rozhodnutie SD EÚ vo veci C-291/12 Michael Schwarz vs. Stadt Bochum)
- **záznamy o pracovnom čase** (Rozhodnutie SD EÚ vo veci C-342/12)
- **údaje o výške príjmu** (Rozhodnutie SD EÚ vo veci C-465/00, C-38/01, C-139/01)
- **informácie o dátumoch, volaných telefónnych číslach alebo prijatých hovoroch, ako aj informácie o dĺžke hovoru** (Rozsudok Európskeho súdu pre ľudské práva k sťažnosti č. 5935/02)

Zdroj: <https://www.osobnyudaj.sk/novinka/11-osobny-udaj-podla-gdpr>

22. 8. 2025

Ochrana osobných údajov

7



Ochrana osobných údajov – subjekty (I.)

❑ **Prevádzkovateľ** – fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov.

Nesie zodpovednosť za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov, pričom je povinný tento súlad preukázať na požiadanie Úradu na ochranu osobných údajov.

Zodpovednosť - objektívna

❑ **Dotknutá osoba** - fyzická osoba, ktorej osobné údaje sa spracúvajú

❑ **Sprostredkovateľ** - subjekt, ktorý sa môže, ale zároveň aj nemusí vyskytnúť v konkrétnom reťazci vzťahov pri zabezpečovaní ochrany osobných údajov. Spracúva osobné údaje v mene prevádzkovateľa, ktorý rozhoduje o účele a dôvode spracúvania. Vzťah medzi prevádzkovateľom a sprostredkovateľom – obchodnoprávny (buď sprostredkovateľská zmluva alebo inominátna zmluva o spracúvaní osobných údajov)

Za sprostredkovateľa sa nepovažuje zamestnanec prevádzkovateľa

Ochrana osobných údajov – subjekty (II.)

Zodpovedná osoba – osoba poverená prevádzkovateľom na vykonávanie dohľadu nad spracúvaním osobných údajov. Prevádzkovateľ je povinný určiť zodpovednú osobu, ak spĺňa aspoň jednu z nasledovných podmienok:

- 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** – telekomunikačné služby, smart autá, vernostné programy, cielená reklama a pod.
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je **spracúvanie vo veľkom rozsahu** napr. nemocnice

Príjemca - každý, komu sa osobné údaje poskytnú (napr. aj poisťovne, zmluvný partneri prevádzkovateľa na osobitné účely - napr. audítori, advokáti a pod.). Príjemcom nie sú ústredné orgány štátnej správy, ministerstvá, ani samotný Úrad na ochranu osobných údajov nie je príjemcom. Tieto subjekty **sú v pozícií tretích strán**.



Práva dotknutých osôb (I.)

- Právo na prístup k údajom
- Právo na opravu
- Právo na vymazanie (právo „na zabudnutie“)
- Právo na obmedzenie spracúvania
- Právo na prenosnosť údajov
- Právo namietiť
- Právo na to, aby sa na dotknutú osobu nevzťahovalo automatizované individuálne rozhodovanie vrátane profilovania
- Právo odvolať súhlas
- Právo podať návrh na začatie konania o ochrane osobných údajov



Práva dotknutých osôb (II.)

Príklad 1: prevádzkovateľ informačného systému OÚ nevyhovel žiadosti navrhovateľa ako dotknutej osoby vo veci uplatnenia si **práva na prístup k jeho OÚ v lehote 1 mesiaca** od jej doručenia (obchodná spoločnosť, 10.000€)

Príklad 2: nevybavenie žiadosti dotknutej osoby v lehote 1 mesiaca od doručenia žiadosti (poskytnutie **informácie o tom, či spoločnosť disponuje fotokópiou občianskeho preukazu**) (obchodná spoločnosť, 1.000€)

Príklad 3: nevybavenie žiadosti dotknutej osoby v lehote 1 mesiaca od jej doručenia (štátny orgán, 700€) povinnosť v lehote 10 dní od právoplatnosti rozhodnutia **priebežne sledovať pracovné emaily vrátane spamov**, aby včas zaznamenal uplatnenie práva dotknutých osôb a vybavoval ich bezodkladne, najneskôr do 1 mesiaca od doručenia žiadosti dotknutej osoby

Zásady ochrany osobných údajov (I.)

- zásada zákonnosti
- zásada obmedzenia účelu
- zásada minimalizácie osobných údajov
- zásada správnosti
- zásada minimalizácie uchovávania
- zásada integrity a dôvernosti
- zásada zodpovednosti



Zásady ochrany osobných údajov (II.)

Spracúvanie osobných údajov je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:

1

SÚHLAS

- dotknutá osoba (napr. pacient) vyjadrila súhlas so spracúvaním svojich osobných údajov
- napr. posielanie marketingových správ od poskytovateľa zdravotnej starostlivosti



2

PLNENIE ZMLUVY

- spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy
- napr. pracovnoprávne vzťahy

3

ZÁKONNÁ POVINNOSŤ

- spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;
- napr. zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podľa ktorého sa súhlas dotknutej osoby (pacienta) na spracúvanie, poskytovanie a sprístupňovanie údajov zo zdravotnej dokumentácie za podmienok ustanovených týmto zákonom nevyžaduje

4

ŽIVOTNE DÔLEŽITÝ ZÁUJEM

- spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby
- napr. spracúvanie osobných údajov obetí alebo účastníkov dopravnej nehody
- napr. spracúvanie osobných údajov je nevyhnutné na humanitárne účely

5

VEREJNÝ ZÁUJEM

- spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi
- napr. samotné poskytovanie zdravotnej starostlivosti

6

OPRÁVNENÝ ZÁUJEM

- spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana
- napr. prevádzka kamerového systému v priestoroch poskytovateľa zdravotnej starostlivosti



Zásady ochrany osobných údajov (III.)

Súhlas

- **definícia:** akýkoľvek **slobodne daný, konkrétny, informovaný a jednoznačný** prejav vôle dotknutej osoby, ktorá formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracovaním osobných údajov, ktoré sa jej týka
- potrebné vymedziť **konkrétny účel/y spracovania**
- **nemá ísť o primárny dôvod na dosiahnutie zákonnosti spracovania**
- odvolanie súhlasu má byť **také jednoduché ako jeho poskytnutie** (čl. 7 (3) GDPR)
- **Príklad 1:** prevádzkovateľ v dokumente vstupného formulára nezískal od dotknutej osoby (navrhovateľky) súhlas so zasielaním obchodných ponúk formou jednoznačného potvrdzujúceho úkonu a slobodne, nakoľko tento súhlas bol v okienku formulára vopred prednastavený a prevádzkovateľ udelením súhlasu podmieňoval ďalšiu komunikáciu navrhovateľky ... (obchodná spoločnosť, 1.100€)



Zásady ochrany osobných údajov (IV.)

Zásada zákonnosti:

Príklad 1: používaním **emailovej schránky** dotknutej osoby v období **po ukončení pracovného pomeru** dotknutej osoby bez právneho základu (obec, 500€)

Príklad 2: prevádzkovateľ nepreukázal Úradu primeraný právny základ **spracúvania pracovnej emailovej adresy navrhovateľa po ukončení** pracovného pomeru s ním, nakoľko sa v zmysle čl. 6 ods. 1 písm. f) GDPR porovnávaním jednotlivých práv dotknutých osôb s jeho oprávneným záujmom vôbec nezaoberal

Príklad 3: ... uverejňovanie na webovom sídle prevádzkovateľa (v ozname Rozhodnutie Inšpektorátu práce BA o uložení pokuty) mena, priezviska a dátumu narodenia dotknutej osoby bez právneho základu (obec, 2.000€)



Zásady ochrany osobných údajov (V.)

Zásada minimalizácie osobných údajov

- osobné údaje musia byť primerané, relevantné a **obmedzené na rozsah**, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú
- **Príklad 1:** v prípade kamier je monitorovaný aj priestor nad rámec nevyhnutný na dosiahnutie účelu monitorovania (okolité rodinné domy a záhrady) – (obec, 700€)
- **Príklad 2:** pri telefonickom rozhovore realizovanom z telefónneho čísla ... prevádzkovateľ na účel vybavenia žiadosti o overenie dostupnosti služieb na adrese trvalého bydliska vyžadoval od potenciálneho klienta (navrhovateľa) jeho rodné číslo, ktorého získavanie nebolo nevyhnutné na dosiahnutie daného účelu spracúvania (obchodná spoločnosť, 1.200€)

Porušenie ochrany osobných údajov

Tri typy porušení ochrany osobných údajov:

- porušenie dôvernosti - neoprávnené alebo náhodné zverejnenie alebo sprístupnenie osobných údajov (napr. zaslanie e-mailu s citlivými osobnými údajmi nesprávnemu adresátovi),
- porušenie dostupnosti údajov - náhodná alebo neoprávnená strata prístupu k alebo zničenie osobných údajov (napr. výmaz osobných údajov, či už náhodný alebo neoprávnený)
- porušenie integrity - neoprávnené alebo náhodné pozmenenie osobných údajov (napr. manipulácia s dátami spôsobená hackermi)

Prípadová štúdia

Záchranná zdravotná služba (ZZS) prijíma tiesňové volania, vysiela posádky na zásahy a zabezpečuje prevoz pacientov do zdravotníckych zariadení. V rámci tejto činnosti je nevyhnutné spracúvať osobné údaje pacientov aj iných osôb, aby bolo možné účinne poskytnúť zdravotnú starostlivosť.

- 1. Ktoré osobné údaje pacientov spracúva záchranná služba počas zásahu?**
- 2. Ktoré z týchto údajov patria medzi osobitné kategórie osobných údajov podľa GDPR?**
- 3. Na akých právnych základoch je založené spracúvanie osobných a zdravotných údajov v tejto situácii?**
- 4. Prečo sa v urgentnom prípade nespolieha na súhlas pacienta?**
- 5. Ktoré údaje sú pre zásah skutočne nevyhnutné a ktoré by bolo nadbytočné zaznamenávať?**
- 6. Ako by mala záchranná služba postupovať, ak pacient odmietne uviesť svoje osobné údaje?**
- 7. Aké riziká pre ochranu osobných údajov vyplývajú z činnosti záchranej služby?**
- 8. Navrhňte minimálne dve technické a dve organizačné opatrenia na ich zníženie.**
- 9. Komu môže záchranná služba poskytovať získané údaje a za akých podmienok?**
- 10. Je možné poskytnúť informácie o zásahu médiám alebo tretím osobám? Prečo áno/nie?**
- 11. Ako dlho je možné uchovávať záznamy o zásahu a aké predpisy to upravujú?**
- 12. Čo sa má urobiť s údajmi po uplynutí tejto lehoty?**

Prípadová štúdia

1. Ktoré osobné údaje pacientov spracúva záchranná služba počas zásahu?

meno, priezvisko, rodné číslo/dátum narodenia, adresa, telefónne číslo, zdravotné údaje (anamnéza, diagnóza, zásah, podané lieky), údaje o zásahu (miesto, čas, okolnosti).

2. Ktoré z týchto údajov patria medzi osobitné kategórie osobných údajov podľa GDPR?

(čl. 9 GDPR): zdravotné údaje (stav pacienta, anamnéza, diagnóza, liečba).

3. Na akých právnych základoch je založené spracúvanie osobných a zdravotných údajov v tejto situácii?

Čl. 6 ods. 1 písm. c) GDPR – plnenie zákonnej povinnosti (zákon o zdravotnej starostlivosti, zákon o ZZS)

Čl. 6 ods. 1 písm. e) GDPR – plnenie úlohy vo verejnom záujme.

Čl. 9 ods. 2 písm. h) GDPR – spracúvanie osobitných kategórií údajov na účely poskytovania zdravotnej starostlivosti.

4. Prečo sa v urgentnom prípade nespolieha na súhlas pacienta?

V urgentných situáciách nie je možné čakať na súhlas, navyše poskytovanie zdravotnej starostlivosti je zákonná povinnosť

Prípadová štúdia

5. Ktoré údaje sú pre zásah skutočne nevyhnutné a ktoré by bolo nadbytočné zaznamenávať? (zásada minimalizácie)

Nevyhnutné údaje: identifikácia pacienta, zdravotné údaje potrebné na zásah, miesto a čas zásahu.
Nadbytočné: zisťovanie pracovného postavenia, sociálnych pomerov, rodinných vzťahov

6. Ako by mala záchranná služba postupovať, ak pacient odmietne uviesť svoje osobné údaje?

Ak pacient odmietne poskytnúť údaje, je záchranná služba oprávnená zaznamenať minimálne údaje potrebné na poskytnutie starostlivosti a identifikáciu pacienta (ak je to možné).

7. Aké riziká pre ochranu osobných údajov vyplývajú z činnosti záchrannej služby?

Únik zdravotných údajov, neoprávnený prístup (napr. zamestnanec, ktorý nemá oprávnenie), nesprávne zadanie údajov, neautorizované poskytovanie údajov tretím stranám

8. Navrhnite minimálne dve technické a dve organizačné opatrenia na ich zníženie.

Technické opatrenia: šifrovanie prenosu dát medzi operátorom a posádkou, prístup do systému iba s dvojfaktorovým overením.

Organizačné opatrenia: pravidelné školenia zamestnancov o GDPR, prísne logovanie prístupov k údajom, smernice o spracovaní údajov a povinná mlčanlivosť zdravotníkov.

Prípadová štúdia

9. Komu môže záchranná služba poskytovať získané údaje a za akých podmienok?

nemocnice a iné zdravotnícke zariadenia, zdravotné poisťovne (na účely preplácania výkonov), orgány verejnej moci ak to vyžaduje zákon

10. Je možné poskytnúť informácie o zásahu médiám alebo tretím osobám? Prečo áno/nie?

Médiám a tretím osobám: zásadne nie. Údaje sú chránené a zverejňovať ich možno len vo výnimočných prípadoch stanovených zákonom (napr. anonymizované štatistiky)

11. Ako dlho je možné uchovávať záznamy o zásahu a aké predpisy to upravujú? (minimalizácia uchovávaní údajov)

Lehoty: zdravotná dokumentácia sa uchováva podľa zákona o zdravotnej starostlivosti (napr. 20 rokov od posledného poskytnutia zdravotnej starostlivosti – ak ide o všeobecného lekára, pri úmrtí pacienta 20 rokov od úmrtia - § 22 ods. 2 zákona o zdravotnej starostlivosti)

12. Čo sa má urobiť s údajmi po uplynutí tejto lehoty?

údaje musia byť zlikvidované (bezpečné vymazanie alebo anonymizácia).

IP adresa ako osobný údaj (I.)

- *jedinečný číselný identifikátor, ktorého účelom je identifikácia zariadenia pripojeného v určitej sieti*

tvorí sekvencia 4 čísiel, z ktorých jej jednotlivé zložky slúžia na identifikáciu:

- konkrétnej siete, na ktorej sa zariadenie nachádza (tzv. network ID)
- konkrétneho zariadenia v predmetnej sieti (tzv. host ID)

tvoria čísla v rozsahu od 0-255 (za účelom prevodu do binárnej formy), napr. 121.345.678.12

Rozlišujeme:

- statické IP adresy** – IP adresa je pridelená výlučne jednému konkrétnemu zariadeniu, pričom nedochádza k jej zmene pri jednotlivých pripojeniach
- dynamické IP adresy** – sú automaticky pridelené po pripojení sa do siete rôznym zariadeniam, pričom je však spravidla zo záznamov poskytovateľa pripojenia zrejmé, ktorému zariadeniu bola pridelená konkrétna IP adresa v konkrétnom čase

IP adresa ako osobný údaj (II.)

IP Address



192.168.1.1



Cookies ako osobný údaj (I.)

- *malé textové súbory, ktoré na koncové zariadenie používateľa (akékoľvek zariadenie, ktoré používateľ používa) ukladá server navštívenej internetovej stránky, a to za účelom získania a následného prenosu požadovanej informácie späť na tento server*

Z hľadiska doby pôsobenia možno rozlišovať:

- tzv. session cookies** - pôsobia voči používateľovi výlučne po dobu jeho návštevy konkrétnej internetovej stránky, pričom nie sú dlhodobo ukladané v používateľovom zariadení - napr. funkciu nákupného košíka
- tzv. persistent cookies** - pôsobia voči používateľovi aj nad rámec jeho návštevy konkrétnej internetovej stránky, a to až do uplynutia vopred stanovenej doby - využívané napr. za účelom optimalizácie a prispôsobenia konkrétnej stránky preferenciám používateľa (voľbou jazyka stránky, veľkosti písma a pod.)

Problematické - žiadny vnútroštátny, ako ani európsky predpis nelimituje maximálnu dobu pôsobenia skúmaných cookies, čo môže negatívne ovplyvniť najmä súkromie používateľa.

Cookies ako osobný údaj (II.)



Cookies ako osobný údaj (III.)

Z hľadiska domény, ku ktorej súbory cookies patria, možno rozlišovať:

- ❑ **tzv. first-party cookies** - patria k doméne tej internetovej stránky, ktorú používateľ skutočne navštívil. Účelom tohto typu cookies je zabezpečenie efektívneho fungovania všetkých funkcií predmetnej internetovej stránky, pričom dôsledkom ich zablokovania je často znefunkčnenie a znemožnenie prístupu k tejto stránke. Používanie týchto súborov cookies nie je spravidla v praxi považované za problematické. Príkladom umožňujú napr. automatické prihlásenie sa na konkrétnu stránku.
- ❑ **tzv. third-party cookies** - sú priradené k doméne inej internetovej stránky, akú používateľ skutočne navštívil. Dôvodom pre uvedené je skutočnosť, že v rámci jednej internetovej stránky možno nájsť nielen vlastný obsah tejto stránky, ale aj obsah iných stránok. Typickým príkladom je funkcia „Like Button“ platformy Facebook, ktorú možno nájsť na množstve iných platforiem (online denníky, časopisy), na použitie ktorej sú naviazané osobitné cookies.

Cookies ako osobný údaj (IV.)

Osobitne možno rozlišovať súbory cookies používané na reklamné účely - **tzv. advertising, resp. targeting cookies**, ktoré slúžia na dvojaký účel.

- na jednej strane sa nimi sleduje zlepšenie používateľovej skúsenosti s reklamami, ktoré sú mu na jeho zariadení zobrazované, a to napr. zabránením opakovaného zobrazovania reklám.
- na strane druhej je cieľom zabezpečiť zobrazovanie vhodných reklám používateľom a tak zaručiť propagovanie tovaru a služieb osobám, ktorým sú určené. Na dosiahnutie uvedeného, súbory cookies zbierajú údaje napr. o tom, čo ten-ktorý používateľ na internete vyhľadáva, ako reaguje na konkrétne reklamy, ktorým bol vystavený a pod.



Cookies ako osobný údaj (V.)

Súhlas ako právny základ pre spracovanie osobných údajov

v zmysle § 5 písm. a) zákona č. 18/2018 Z. z. sa súhlasom dotknutej osoby rozumie „*akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov*“

požiadavka jednoznačnosti:

preferuje sa **tzv. opt-in princíp**, tzn. požiadavka aktívneho konania dotknutej osoby pri poskytovaní súhlasu, na rozdiel od **tzv. opt-out princípu**, podľa ktorého možno súhlas udeliť aj pasívnym, konkludentným spôsobom (nevyjadrenie nesúhlasu)

napr. používaním tejto stránky súhlasíte s použitím súborov cookies.

napr. táto internetová stránka používa súbory cookies na zlepšenie funkcií prehliadania. Bližšie informácie o používaní súborov cookies sú dostupné tu. Súhlasíte s ich použitím? ÁNO/NIE

Odvolanie súhlasu

- právo kedykoľvek odvolať už poskytnutý súhlas (§ 14 zákona č. 18/2018 Z. z.)
- povinnosť informovať dotknutú osobu o jej práve odvolať súhlas predtým, ako ho poskytne
- odvolanie súhlasu má byť také jednoduché ako jeho poskytnutie (čl. 7 (3) GDPR)
- právo odvolať súhlas rovnakým spôsobom, akým bol udelený (§ 14 ods. 3 zákona č. 18/2018 Z. z.)

Cookies ako osobný údaj (VI.)

Náležitosti súhlasu (rozsudok SD Z 21.3.2019 VO VECI C-673/17 PLANET 49 proti Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

- požiadavka aktívneho súhlasu** - potreba *indikácie prianí* subjektu + podmienka *jednoznačného udelenia* súhlasu, pričom platí, že nejednoznačnosť možno odstrániť len aktívnym, a nie pasívnym správaním, tzn. **nepostačuje, že používateľovo vyjadrenie súhlasu je vopred naformulované a že používateľ musí aktívne namietat', ak nesúhlasí so spracovaním údajov**, nakoľko nie je jednoznačné, či si používateľ prečítal informácie, ktoré mu boli poskytnuté, a teda či poskytol svoj súhlas slobodne, s uvedomením si skutočnosti, že jeho poskytnutie mohol odmietnuť.
- požiadavka samostatného súhlasu** - činnosť, ktorej sa používateľ venuje na internete a poskytnutie súhlasu nemôžu tvoriť jeden a ten istý úkon, najmä z pohľadu účastníka sa poskytnutie súhlasu nemôže javiť ako vedľajšie popri účasti na výhernej hre, ale musí ísť o **dva rovnocenné úkony**.
- požiadavka informovať subjekt v plnom rozsahu**, ktorá umožňuje používateľom posúdiť, či je určitá činnosť na internete podmienená poskytnutím súhlasu, ako aj či sú následne ochotní za účelom realizácie tejto činnosti takýto súhlas poskytnúť



Závěrečný test

■ Test: ...

KC KB UPJŠ - Laik, odborný zamestnanec, manažér - Modul č. 6 - Test

Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“ - Modul č. 6 - Úvod do práva IKT I.

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Meno a priezvisko *

Enter your answer

2. Názov organizácie *

Enter your answer

3. Dátum testu *

Please input date (M/d/yyyy)



4. Právna úprava ochrany osobných údajov je obsiahnutá v: (1 Point) *

zákone č. 18/2018 Z.z. o ochrane osobných údajov

Obchodnom zákonníku



Spättná väzba

- Spättná väzba: ...


Spättná väzba

KCKB: Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „laik“, „odborný zamestnanec“ a „manažér“

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Dátum školenia *

Please input date (M/d/yyyy) 

2. Číslo modulu *

Modul č. 1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB)

Modul č. 2 - Kritické myslenie a dezinformácie

Modul č. 3 - Sociálne inžinierstvo



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

 meno.priezvisko@upjs.sk

 <https://cyberawareness.sk>