**Smernica ochrana osobných údajov**

**Ústav výskumu sociálnej komunikácie SAV**

**Interná smernica 2/2019**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vypracoval:** | **Overil:** | **Schválil:** | **Dátum registrácie/účinnosť** |
| **Meno / funkcia:**  **Ing. Tomáš Hettych, Ratio Services s.r.o.** | **Meno / funkcia:**  **Mgr. Zuzana Dobrucká, sekretárka** | **Meno / funkcia:**  **Mgr. Barbara Lášticová, PhD., riaditeľka** | **3. 7. 2019** |
| **Podpis**: | **Podpis**: | **Podpis**: |  |

|  |  |
| --- | --- |
| **Evidencia zmien** | |
| **Číslo revízie** | **Obsah zmeny** |
| 1 | Návrh smernice upravený pre potreby ÚVSK SAV – doplnený názov a upravená zodpovedná osoba |

OBSAH

[1. DEFINÍCIE A KĽÚČOVÉ POJMY 1-2](#_Toc521699789)

[1.1. Termíny 1-2](#_Toc521699790)

[1.2. Vysvetlenie pojmov a skratiek 1-2](#_Toc521699791)

[2. OCHRANA SÚKROMIA A SPRACÚVANIE OSOBNÝCH ÚDAJOV 2-5](#_Toc521699792)

[3. PRÁVNE ZÁKLADY SPRACÚVANIA OSOBNÝCH ÚDAJOV 3-6](#_Toc521699793)

[4. SÚHLAS SO SPRACÚVANÍM 4-7](#_Toc521699794)

[5. PRÁVA DOTKNUTEJ OSOBY 5-8](#_Toc521699795)

[5.1. Právo byť informovaný 5-8](#_Toc521699796)

[5.2. Právo dotknutej osoby na prístup k údajom 5-10](#_Toc521699797)

[5.3. Právo na opravu 5-10](#_Toc521699798)

[5.4. Právo na vymazanie (právo na „zabudnutie“) 5-10](#_Toc521699799)

[5.5. Právo na obmedzenie spracúvania 5-11](#_Toc521699800)

[5.6. Právo na prenosnosť údajov 5-11](#_Toc521699801)

[5.7. Právo namietať 5-11](#_Toc521699802)

[5.8. Právo nebyť subjektom automatizovaného rozhodovania 5-12](#_Toc521699803)

[6. PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV 6-12](#_Toc521699804)

[7. KOMPETENCIE 7-12](#_Toc521699805)

[7.1. Všeobecné povinnosti zamestnancov 7-12](#_Toc521699806)

[7.2. Predstavenstvo Ústavu 7-13](#_Toc521699807)

[7.3. Vedúci oddelenia *iT* 7-13](#_Toc521699808)

[7.4. Zodpovedná osoba (DPO) 7-13](#_Toc521699809)

[7.5. Riadiaci zamestnanci Ústavu 7-14](#_Toc521699810)

[8. ZÁVEREČNÉ USTANOVENIA 8-14](#_Toc521699811)

[8.1. Zrušené predpisy 8-14](#_Toc521699812)

[8.2. Súvisiace predpisy 8-14](#_Toc521699813)

[9. ZÁZNAMY 9-15](#_Toc521699814)

# DEFINÍCIE A KĽÚČOVÉ POJMY

Táto kapitola definuje významnosť resp. dôležitosť požiadaviek. Pokiaľ je termín v ďalšom texte napísaný VEĽKÝMI PÍSMENAMI interpretuje sa nasledovne:

## Termíny

|  |  |
| --- | --- |
| Termín | Definícia |
| MUSÍ  JE POŽADOVANÝ  VYŽADUJE SA | Príslušné ustanovenie sa použije bez výnimky. |
| NESMIE  NEMÔŽE  ZAKAZUJE SA  JE ZAKÁZANÉ | Príslušné ustanovenie sa nepoužije nikdy. |
| MAL BY  ODPORÚČA SA  JE ODPORÚČANÉ | Príslušné ustanovenie sa použije vždy, s výnimkou prípadov, keď by jeho použitie vyvolalo nepriaznivé účinky. |
| NEMAL BY  NEODPORÚČA SA  NIE JE ODPORÚČANÉ | Príslušné ustanovenie sa nepoužije nikdy, s výnimkou prípadov ak je zrejmé, že jeho použitie nevyvolá nepriaznivé účinky. |
| MÔŽE  JE VOLITEĽNÝ | Uplatnenie ustanovenia je na rozhodnutí používateľa. |

## Vysvetlenie pojmov a skratiek

|  |  |  |
| --- | --- | --- |
| Pojem | Skratka | Výklad |
| aktívum |  | hmotné alebo nehmotné ekonomické prostriedky, ktoré pre Ústav priamo alebo nepriamo predstavuje súčasnú, alebo potenciálnu hodnotu. (Aktívami sú najmä: procesy, dáta, informácie, software, služby, objekty a priestory Ústavu). |
| bezpečnosť |  | ochrana fyzických a informačných aktív pred stratami, ktoré by mohli vzniknúť v dôsledku incidentov |
| bezpečnostné technológie |  | Integrovaný súbor informačných a komunikačných technológií používaných na zvýšenie bezpečnosti a ochrany informačných a fyzických aktív Ústavu |
| bezpečnostný incident |  | Udalosť, v rámci ktorej došlo ku strate integrity, alebo dôvernosti dát, zničeniu dát, prelomeniu integrity systému alebo obmedzeniu, či odmietnutiu dostupnosti služby, priestupok alebo riziko priestupku proti bezpečnostnej politike, prípadne proti akceptovateľnému použitiu bezpečnostných politík, alebo nesplnenie štandardných postupov. |
| Data Protection Officer / Zodpovedná osoba | DPO | hlavná kontaktná osoba pre všetky lokálne otázky a záležitosti týkajúce sa ochrany osobných údajov a hlavná kontaktná osoba pre porušenia ochrany osobných údajov. |
| dotknutá osoba |  | fyzická osoba, ktorej osobné údaje sa spracúvajú |
| hrozba |  | Akákoľvek okolnosť či udalosť, ktorá môže potenciálne využiť zraniteľné miesto informačných alebo fyzických aktív a spôsobiť Ústavu škodu. |
| informačné aktíva |  | Všetky objekty a informácie, ktoré pre Ústav priamo alebo nepriamo predstavujú súčasnú alebo potenciálnu hodnotu, alebo ktorých narušenie integrity, dôvernosti a dostupnosti môže mať na Ústav negatívny dopad. |
| monitoring |  | Vo všeobecnosti sledovanie, kontrola, získavanie informácie o stave, o pohybe, o zmene, o činnosti, o procese alebo o udalostiach a to nezávisle od vedomia sledovaného. Pravidlá pre vykonávanie elektronického monitorovania v Ústavu a zároveň zodpovednosti a právomoci zamestnancov v tejto oblasti sú stanovené samostatným predpisom. |
| neautorizovaná osoba |  | Vo vzťahu prístupu k informačným aktívam Ústavu sa rozumie fyzická osoba, ktorá nemá zo svojej pracovnej role prístup ku klasifikovaným informáciám, resp. fyzická osoba s iným ako zamestnaneckým vzťahom ku Ústavu, ktorej sa informácie netýkajú, nemá na takýto prístup povolenie od vlastníka informácií, resp. ktorá nie je oprávnená oboznamovať sa s informáciami a pristupovať k hodnotám nad rozsah, ktorý jej určený, alebo ak jej nevyplýva zo zákona. |
| obmedzenie spracúvania |  | označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti. |
| ochrana |  | Starostlivosť o odvrátenie nebezpečenstva; prostriedok na chránenie; prevencia - súhrn opatrení na odvrátenie alebo zmiernenie škodlivých vplyvov a následkov incidentov, mimoriadnych udalostí a krízových situácií. |
| organizačné opatrenia |  | Systém administratívnych pravidiel, ktoré vymedzujú pravidlá správania sa zamestnancov a tretích strán v súvislosti s ochranou fyzických a informačných aktív |
| partneri |  | Na účely tohto predpisu sú myslení zamestnanci tretích strán, pôsobiacich v Ústavu na základe zmluvného vzťahu. |
| porušenie ochrany osobných údajov |  | také porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim (typicky – bezpečnostný incident) |
| používateľ |  | Osoba, ktorá spracúva (vytvára, používa, mení, premiestňuje) informačné aktíva Ústavu v preddefinovaných procedúrach počas vykonávania pridelených úloh – špecificky zamestnanec Ústavu, alebo partner. |
| prevádzkovateľ |  | Je každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene. Ak nebude výslovne uvedené inak, bude v rámci tohto predpisu Ústav vystupovať ako prevádzkovateľ |
| 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, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov. |
| riešenie bezpečnostných incidentov |  | Aktivity vedúce k identifikácii, analýze, odozve na incident, odvráteniu hrozieb s úmyslom preventívne pôsobiť na možné opakovanie incidentu; návrh zrozumiteľného, predvídateľného a opakovateľného procesu odozvy na bezpečnostné incidenty. |
| riziko |  | Funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody pre Ústav. Bezpečnostné riziko je výraz na označenie potenciálnej možnosti narušenia bezpečnosti. |
| rizikový apetít |  | Definuje sa ako ochota Ústav prijať riziká tak, ako sú kvantifikované príslušnými ukazovateľmi |
| Ústav |  | Ústav výskumu sociálnej komunikácie SAV |
| spracúvanie OÚ |  | každá jednotlivá operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov |
| sprostredkovateľ |  | **každý, kto spracúva osobné údaje v mene Prevádzkovateľa** |
| Súhlas DO |  | Súhlas dotknutej osoby je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka |
| tretia strana |  | Orgán verejnej moci, právnická osoba alebo fyzická osoba, ktorá vo vzťahu k dôvernej informácii a hodnotám nie je považovaná za oprávnenú osobu, pokiaľ nie je týmto predpisom určené inak. |
| zamestnanci |  | Na účely tohto predpisu sú myslení zamestnanci Ústavu. |
| zraniteľnosť |  | Slabé miesto  fyzického alebo informačného aktíva, slabé miesto v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb (hrozba). |

# OCHRANA SÚKROMIA A SPRACÚVANIE OSOBNÝCH ÚDAJOV

1. Ochrana súkromia a osobných údajov je jedným zo základných práv fyzickej osoby.
2. Osobné údaje sú akékoľvek informácie, týkajúce sa určitej, prípadne priamo, alebo nepriamo určiteľnej fyzickej osoby (tzv. dotknutej osoby). Osobné údaje je možné rozdeliť do rôznych kategórií, okrem iného s ohľadom na ich citlivosť.
3. Akékoľvek spracúvanie osobných údajov so sebou prináša riziká ich zneužiteľnosti, zásahu do súkromia fyzickej osoby alebo vzniku škody (majetkovej a nemajetkovej ujmy), rovnako aj poškodenie dobrej povesti. Neoprávnené nakladanie s osobnými údajmi môže mať aj trestnoprávne následky.
4. Spracúvanie osobných údajov je akákoľvek operácia alebo súbor operácií s osobnými údajmi v celom životnom cykle informácie, ktorá môže byť spracovateľskou činnosťou alebo môže byť časťou spracovateľskej činnosti nad osobnými údajmi, najmä:

* **Získavanie** - nadobúdanie, zber údajov
* **Šírenie** – okrem iného aj zasielanie na iné útvary alebo iným zamestnancom v rámciÚstavu, kde sa ďalej spracúvajú
* **Zaznamenávanie** – ukladanie už získaných údajov na akýkoľvek nosič informácií (t.j. do aplikácií, do systémov, na médiá, do dokumentov...)
* **Usporadúvanie** – triedenie údajov podľa určitých kategórií
* **Prepracúvanie alebo zmena** - vykonávanie rôznych zmien na údajoch v informačnom systéme
* **Vyhľadávanie** - prehľadávanie systému za účelom hľadania určitých údajov
* **Prehliadanie** - prezeranie údajov (bez ich modifikácie)
* **Kombinovanie** - spájanie rôznych údajov
* **Premiestňovanie** - prenos, preloženie, dopravenie dát z jedného miesta na druhé (od kopírovania až po fyzický prenos)
* **Využívanie** - používanie pre potreby a prospech Prevádzkovateľa
* **Uchovávanie (retencia)** – ponechanie, nevymazanie dát počas konkrétnej doby
* **Likvidácia** - zrušenie dát rozložením, vymazaním alebo fyzickým zničením **hmotných nosičov tak, aby sa z nich pôvodné údaje nedali reprodukovať**

1. Všeobecné zásady spracúvania osobných údajov:

* **Zákonnosť** – pre spracúvanie osobných údajov MUSÍ existovať účel a právny základ. Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby
* **Transparentnosť** - dotknutá osoba MUSÍ mať informácie a prehľad o tom, aké osobné údaje sú o nej spracúvané a akým spôsobom sa s jej osobnými údajmi nakladá,
* **Obmedzenie účelu spracúvania** - Osobné údaje sa smú získavať len na konkrétne určený́, výslovne uvedený́ a oprávnený́ účel a NESMÚ sa ďalej spracúvať spôsobom, ktorý́ nie je zlučiteľný́ s týmto účelom,
* **Minimalizácia údajov** - je možné spracúvať iba osobné údaje, ktoré sú nevyhnutné na príslušný účel a MUSIA byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý́ sa osobné údaje spracúvajú,
* **Správnosť a aktualizácia údajov** - spracúvané osobné údaje MUSIA byť správne a podľa potreby aktualizované; MUSIA sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.
* **Minimalizácia uchovávania** - spracúvané osobné údaje MUSIA byť primerané, relevantné a obmedzené na nevyhnutný́ rozsah daný́ účelom, na ktorý́ sa spracúvajú ak už údaje nie je potrebné spracúvať, tak je potrebné ich anonymizovať alebo zlikvidovať,
* **Integrita a dôvernosť** - 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,
* **Zodpovednosť** – Ústavu ako prevádzkovateľ je zodpovedná za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinná tento súlad na požiadanie preukázať,
* **Mlčanlivosť** - vo vzťahu k osobným údajom je nutné zachovávať mlčanlivosť.

# PRÁVNE ZÁKLADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

1. Na to, aby bolo možné spracúvať osobné údaje dotknutej osoby, je potrebný aspoň jeden tzv. **právny základ**. Právne základy na spracúvanie osobných údajov podľa § 13 ods. 1 ZOOÚ (resp. čl. 6 GDPR) sú nasledovné:

* dotknutá osoba vyjadrila **súhlas so spracúvaním** svojich osobných údajov aspoň na jeden konkrétny účel,
* spracúvanie osobných údajov je **nevyhnutné na plnenie zmluvy**, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
* spracúvanie osobných údajov je **nevyhnutné podľa osobitného predpisu** alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná:
  + osobitný zákon však musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov,
  + spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú,
* spracúvanie osobných údajov je **nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby** alebo inej fyzickej osoby,
* spracúvanie osobných údajov je **nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme** alebo pri výkone verejnej moci zverenej prevádzkovateľovi:
  + musí však byť osobitným zákonom stanovený účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov,
* spracúvanie osobných údajov je **nevyhnutné na účel oprávnených záujmov prevádzkovateľa** alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

1. Až v prípade, že neexistuje iný relevantný právny základ, je možné spracúvať osobné údaje dotknutej osoby len na základe jej súhlasu.
2. Ak prevádzkovateľ spracúva osobné údaje na základe iného právneho základu než súhlasu dotknutej osoby (napríklad na základe osobitného zákona alebo ak spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán), dochádza k spracúvaniu osobných údajov bez súhlasu dotknutej osoby, pokiaľ zákon neustanovuje inak. Ak by prevádzkovateľ aj napriek tomu („pre istotu“) získaval súhlas so spracúvaním osobných údajov, dotknutá osoba by mohla byť v omyle, že takýto súhlas MÔŽE kedykoľvek odvolať a že odvolaním súhlasu zanikne právny základ na spracúvanie jej osobných údajov. Preto v prípade existencie iného právneho základu BY NEMAL BYŤ získavaný súhlas.
3. Súhlas je viazaný na účel, na ktorý bol poskytnutý (napr. zasielanie odborných alebo marketingových správ, zaradenie do databázy, a pod.). Na iný účel je možné použiť osobné údaje len výnimočne, ak je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý bol súhlas udelený.

# SÚHLAS SO SPRACÚVANÍM

1. Súhlasom dotknutej osoby je akýkoľvek vážny a slobodne daný́, konkrétny, informovaný́ a jednoznačný́ prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.
2. Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.
3. Ak Ústav žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený́ jasne a v zrozumiteľnej a ľahko dostupnej forme.
4. Súhlas musí byť dostatočne konkrétny a špecifický. Z toho dôvodu je potrebné, aby obsahoval určité náležitosti, z ktorých je možné určiť obsah a špecifiká súhlasu, a teda to, s akým spracúvaním osobných údajov dotknutá osoba súhlasí.
5. ODPORÚČA SA, aby samotný súhlas (okrem informácií poskytnutých dotknutej osobe v súlade so zákonnými požiadavkami) obsahoval aspoň nasledovné informácie:

* kto súhlas udeľuje (dotknutá osoba),
* komu sa súhlas udeľuje (prevádzkovateľ),
* na aký účel sa súhlas udeľuje,
* na akú dobu sa súhlas udeľuje,
* zoznam osobných údajov,
* poučenie o možnosti odvolať súhlas.

1. Spôsob udelenia súhlasu BY MAL BYŤ nastavený tak, aby jeho udelenie bolo vždy aktívnym úkonom dotknutej osoby (tzv. „opt-in“):

* v prípade písomného udelenia napr. vlastnoručným podpisom,
* ak je súhlas súčasťou zmluvy alebo iného dokumentu, napr. aktívnym začiarknutím alebo zakrúžkovaním príslušnej možnosti (áno/nie),
* v prípade elektronického udelenia je možné použiť napr. políčko, ktoré musí užívateľ elektronického systému aktívne označiť / kliknúť.

1. NESMIE SA používať pasívny súhlas (tzv. „opt-out“)., t.j. taký spôsob, podľa ktorého by musela dotknutá osoba vykonať úkon za účelom vyjadrenia nesúhlasu so spracúvaním (napr. označenie možnosti, že nesúhlasí so spracúvaním alebo napr. vopred začiarknuté políčko, na ktoré musí dotknutá osoba kliknúť, aby neudelila svoj súhlas) Pasívny súhlas nebude považovaný za jednoznačne udelený.
2. Súhlas BY MAL zároveň obsahovať jednoznačný prejav súhlasu dotknutej osoby, resp. vôle dotknutej osoby udeliť súhlas (napr. „Týmto udeľujem prevádzkovateľovi súhlas so spracúvaním mojich vyššie uvedených osobných údajov na účely a za podmienok uvedených vyššie.“).
3. Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.
4. Pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý́ nie je na plnenie tejto zmluvy nevyhnutný.

# PRÁVA DOTKNUTEJ OSOBY

1. Práva dotknutých osôb v súvislosti so spracúvaním osobných údajov podľa § 19-28 ZOOÚ (resp. čl. 12-22 GDPR) sú najmä:

* Právo byť informovaný
* Právo na prístup k údajom
* Právo na opravu
* Právo na vymazanie (na „zabudnutie“)
* Právo na obmedzenie spracúvania
* Právo na prenosnosť údajov
* Právo namietať
* Právo súvisiace s automatizovaným individuálnym rozhodovaním a profilovaním

## Právo byť informovaný

1. Právo nariaďuje prevádzkovateľovi poskytnúť dotknutým osobám pravdivé informácie o spracúvaní, obvykle pomocou oznámenia o spracúvaní osobných údajov.
2. Informácie poskytnuté dotknutým osobám MUSIA byť:

* Stručné, jasné a zrozumiteľné
* Ľahko dostupné
* Poskytnuté zdarma a bez poplatkov

1. Obsah poskytovaných informácií:

|  |  |  |
| --- | --- | --- |
|  | Ak OÚ  sú získané priamo od DO | Ak OÚ  nie sú získané priamo od DO |
| Totožnosť a kontaktné údaje prevádzkovateľa a zodpovednej osoby | X | X |
| Účely spracúvania a právny základ spracúvania | X | X |
| Kategórie dotknutých osobných údajov |  | X |
| Ak existujú príjemcovia alebo kategórie príjemcov osobných údajov | X | X |
| Informácia o presunoch osobných údajov do tretích krajín a primeraných zárukách | X | X |
| Doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie | X | X |
| Existencia jednotlivých práv pre dotknuté osoby | X | X |
| Právo odvolať súhlas so spracúvaním osobných údajov kedykoľvek keď je to relevantné | X | X |
| Právo podať sťažnosť dozornému orgánu | X | X |
| Informácia o tom, z akého zdroja pochádzajú osobné údaje, či pochádzajú z verejných zdrojov |  | X |
| Informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou ako aj možné následky neposkytnutia údajov | X |  |
| Existencia automatizovaného rozhodovania vrátane profilovania, informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu | X | X |

1. Ak boli osobné údaje získané priamo od dotknutej osoby, informácie majú byť poskytnuté v čase získania osobných údajov
2. Ak osobné údaje neboli získané priamo od dotknutej osoby, informácie majú byť poskytnuté v primeranej lehote po získaní osobných údajov, najneskôr však do 1 mesiaca. Ak sa osobné údaje používajú na komunikáciu s dotknutou osobou, najneskôr v čase prvej komunikácie. Ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi, informácie majú byť poskytnuté najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú.
3. Prevádzkovateľ oznámi každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie.
4. Informačná povinnosť sa neviaže len na okamih získavania osobných údajov. Ústav je povinný oznámiť dotknutým osobám každú zmenu, a zabezpečiť túto povinnosť od získania až po výmaz osobných údajov.

## Právo dotknutej osoby na prístup k údajom

1. Dotknutá osoba má právo získať od Ústavu ako od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom.
2. Ústav JE POVINNÝ poskytnúť kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, Ústav MÔŽE účtovať primeraný poplatok zodpovedajúci administratívnym nákladom.
3. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.
4. Informácie MUSIA byť poskytnuté okamžite, najneskôr v lehote 1 mesiaca. Ústav má právo predĺžiť dobu spracovania žiadosti o ďalšie 2 mesiace pokiaľ je požiadavka zložitá alebo častá. Musí však dotknutej osobe do 1 mesiaca oznámiť dôvod predĺženia doby spracovania.

## Právo na opravu

1. Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú.
2. Dotknutá osoba má právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.
3. Ústav má lehotu na opravu údajov 1 mesiac, je možné ju predĺžiť o 2 mesiace v prípade, že je oprava náročná. Musí o tom informovať dotknutú osobu a odôvodniť prečo nastalo predĺženie lehoty. V prípade, že kroky na opravu prevádzkovateľ nepodnikne MUSÍ informovať dotknutú osobu prečo tak neučinil a o práve dotknutej osoby podať sťažnosť dozornému orgánu

## Právo na vymazanie (právo na „zabudnutie“)

1. Dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:

* osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali
* dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva a ak neexistuje iný právny základ pre spracúvanie
* dotknutá osoba namieta voči spracúvaniu a neprevažujú žiadne oprávnené dôvody na spracúvanie. (Oprávneným dôvodom môže byť napr. pracovno-právny vzťah medzi zamestnancom a zamestnávateľom)
* osobné údaje sa spracúvali nezákonne (nastalo porušenie práv)
* neexistuje rodičovský súhlas na spracovanie osobných údajov detí
* osobné údaje MUSIA byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha

1. Ústav MÔŽE odmietnuť žiadosť o vymazanie. K odmietnutiu vymazania môže dôjsť výhradne z nasledujúcich dôvodov:

* uplatnenie práva na slobodu prejavu a na informácie
* Ústav plní zákonnú povinnosť, plní úlohu realizovanú vo verejnom záujme alebo pri výkone verejnej moci zverenej Ústavu ako prevádzkovateľovi
* Ústav plní verejný záujem v oblasti verejného zdravia
* Ústav vykonáva úlohy na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely
* Ústav potrebuje spracúvať osobné údaje na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov

1. Pokiaľ došlo k sprístupneniu osobných údajov tretím stranám, je prevádzkovateľ povinný informovať ich o vymazaní týchto údajov.

## Právo na obmedzenie spracúvania

1. Pokiaľ je spracúvanie obmedzené má Ústav právo osobné údaje len ukladať a ďalej ich nespracúvať iným spôsobom.
2. Obmedzenie spracúvania môže nastať v týchto prípadoch:

* dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov
* spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia
* prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov
* dotknutá osoba namieta voči spracúvaniu a prevádzkovateľ overuje, či dôvody na strane prevádzkovateľa prevažujú nad dôvodmi na strane dotknutej osoby

1. Prevádzkovateľ je povinný overiť, či boli osobné údaje poskytnuté tretím osobám a informovať ich o obmedzení spracúvania.
2. Pri zrušení obmedzenia spracúvania MUSIA byť o tom informované dotknuté osoby.

## Právo na prenosnosť údajov

1. Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil. Právo na prenosnosť nesmie mať nepriaznivé dôsledky na práva a slobody iných.
2. Právo na prenosnosť platí ak:

* sa spracúvanie zakladá na súhlase alebo zmluve, a
* sa spracúvanie vykonáva automatizovanými prostriedkami

1. Ústav MUSÍ splniť lehotu na prenos údajov 1 mesiac, túto lehotu je možné predĺžiť o 2 mesiace v prípade, že je prenos technicky zložitý. O tomto predĺžení lehoty MUSÍ Ústav informovať dotknutú osobu.

## Právo namietať

1. Pokiaľ dotknutá osoba nedostane možnosť uplatniť niektoré zo svojich práv, má právo kedykoľvek namietať z dôvodov tykajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka.
2. Právo namietať MUSÍ viesť k obmedzeniu spracúvania tých dát, ktorých sa námietka týka, pokiaľ však Ústav nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.
3. Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré sa jej týka, na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom. Ak dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu, osobné údaje sa už na také účely NESMÚ spracúvať.
4. Organizácia MUSÍ na existenciu práva namietať výslovne dotknutú osobu upozorniť a to najneskôr pri prvej komunikácii s ňou, pričom sa toto právo prezentuje jasne a oddelene od akýchkoľvek iných informácií.

## Právo nebyť subjektom automatizovaného rozhodovania

1. Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.
2. Právo nebyť subjektom automatizovaného rozhodovania neplatí, ak je rozhodnutie:

* nevyhnutné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom
* povolené právom EÚ alebo právom členského štátu, ktorému prevádzkovateľ podlieha a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby
* založené na výslovnom súhlase dotknutej osoby

1. Ústav MUSÍ mať zavedený proces, ktorý umožní preskúmať automatizované rozhodovanie určeným zamestnancom, pokiaľ o to požiada dotknutá osoba.

# PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV

1. Porušenie ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.
2. Pri každom porušení ochrany osobných údajov sú zamestnanci aj partneri POVINNÍ riadiť sa pravidlami uvedenými v samostatnom internom predpise o riešení bezpečnostných incidentov.
3. Pri každom identifikovanom porušení ochrany osobných údajov, ako aj pri každom podozrení na porušenie ochrany osobných údajov sú zamestnanci aj partneri POVINNÍ bezodkladne informovať DPO.

# KOMPETENCIE

## Všeobecné povinnosti zamestnancov

1. Každý zamestnanec je povinný v rozsahu svojej pracovnej zodpovednosti a podľa svojich najlepších vedomostí zabezpečiť ochranu osobných údajov dotknutých osôb.
2. Každý zamestnanec je povinný ohlásiť zodpovedným riadiacim zamestnancom akékoľvek podozrenie z možného porušenia pravidiel ochrany osobných údajov, alebo podozrenie na potenciálny bezpečnostný incident.
3. Porušenie týchto povinností a ďalších povinností v súvislosti s ochranou informačných aktív, najmä osobných údajov, ktoré vyplývajú z interných predpisov MÔŽE byť považované za závažné porušenie pracovnej disciplíny a byť dôvodom pre okamžité skončenie pracovného pomeru zo strany zamestnávateľa v zmysle zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov a zároveň dôvodom pre uplatňovanie nároku na náhradu škody.

## Vedenie Ústavu

* prijíma strategické rozhodnutia v oblasti ochrany osobných údajov a informačnej bezpečnosti,
* zabezpečuje dostupnosť zdrojov pre procesy ochrany osobných údajov a pre systém riadenia informačnej bezpečnosti,
* dozerá na integráciu požiadaviek ochrany osobných údajov a systému riadenia informačnej bezpečnosti do procesov v organizácii,
* stanovuje rizikový apetít Ústavu,
* rozhoduje o akceptácii zvyškových rizík.

## Vedúci oddelenia iT

* je vlastníkom procesu bezpečnosť ako aj procesu riadenia rizík v informačnej bezpečnosti,
* zabezpečuje koordináciu bezpečnostných cieľov s ostatnými záujmami Ústavu,
* spracováva a aktualizuje bezpečnostnú politiku, navrhuje zmeny bezpečnostnej stratégie,
* prostredníctvom externého, nezávislého audítora predkladá predstavenstvu správu auditu informačnej bezpečnosti,
* zabezpečuje implementáciu protiopatrení na identifikované IT riziká,
* koncepčne a metodicky vedie ostatné útvary Ústavu v oblasti informačnej bezpečnosti,
* sleduje a vyhodnocuje účinnosť systému riadenia informačnej bezpečnosti a jednotlivých bezpečnostných opatrení,
* monitoruje a vyhodnocuje bezpečnostne významné udalosti v informačných technológiách a bezpečnostných systémoch Ústavu.

## Zodpovedná osoba (DPO)

Ústav výskumu sociálnej komunikácie vzhľadom na rozsah a predmet svojej činnosti nemá zákonnú povinnosť stanoviť zodpovednú osobu. Pre uplatnenie nižšie uvedených práv môžete kontaktovať našu organizáciu prostredníctvom emailu: ksbkksbk@savba.sk,  alebo poštou na adrese: Dúbravská cesta 9, 841 04 Bratislava

## Riadiaci zamestnanci Ústavu

* pravidelne preverujú súlad spracúvania informácií v rámci nimi riadených procesov so znením príslušných bezpečnostných politík, predpismi o ochrane osobných údajov a iných bezpečnostných požiadaviek.

# ZÁVEREČNÉ USTANOVENIA

## Zrušené predpisy

1. Táto verzia predpisu nenadväzuje na predchádzajúce verzie
2. Tento predpis neruší žiaden iný predpis

## Súvisiace predpisy

1. Tento predpis súvisí najmä s:

* Politikou Riadenie informačnej bezpečnosti v platnom znení,
* politikou Riadenie rizík v informačnej bezpečnosti v platnom znení,
* štandardom Bezpečnostný monitoring a riešenie bezpečnostných incidentov v platnom znení
* štandardom Klasifikácia informačných aktív v platnom znení,
* politikou Riadenie kontinuity činnosti v platnom znení.

# ZÁZNAMY

|  |  |  |
| --- | --- | --- |
| Kód dokumentu | Názov dokumentu | Zodpovedný za dokument |
| Smernica revízia 1 | Smernica ochrana osobných údajov  Ústav výskumu sociálnej komunikácie SAV, 3.7. 2019 | Barbara Lášticová |
|  |  |  |
|  |  |  |
|  |  |  |