

OBSAH

ČLÁNOK I	VŠEOBECNÉ USTANOVENIA.....	3
ČLÁNOK II	VÝKLAD POJMOV	3
ČLÁNOK III	ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV	12
ČLÁNOK IV	ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV	13
ČLÁNOK V	SPRACÚVANIE OSOBNÝCH ÚDAJOV NA ZÁKLADE SÚHLASU DOTKNUTEJ OSOBY	16
ČLÁNOK VI	OSOBITNÉ KATEGÓRIE OSOBNÝCH ÚDAJOV	17
ČLÁNOK VII	ZÍSKAVANIE OSOBNÝCH ÚDAJOV	17
ČLÁNOK VIII	ZÍSKAVANIE OSOBNÝCH ÚDAJOV KOPÍROVANÍM, SKENOVANÍM ALEBO INÝM ZAZNAMENÁVANÍM	18
ČLÁNOK IX	ZVEREJŇOVANIE, SPRÍSTUPŇOVANIE A POSKYTOVANIE OSOBNÝCH ÚDAJOV PREVÁDZKOVATEĽOM	19
ČLÁNOK X	POSKYTOVANIE INFORMÁCIÍ DOTKNUTEJ OSOBY O SPRACÚVANÍ JEJ OSOBNÝCH ÚDAJOV	19
ČLÁNOK XI	CEZHRANIČNÝ PRENOS OSOBNÝCH ÚDAJOV	20
ČLÁNOK XII	LIKVIDÁCIA OSOBNÝCH ÚDAJOV	20
ČLÁNOK XIII	MLČANLIVOSŤ	21
ČLÁNOK XIV	POVINNOSTI OPRÁVNENEJ OSOBY	21
ČLÁNOK XV	POVINNOSTI VEDÚCEHO ZAMESTNANCA PRI OCHRANE OSOBNÝCH ÚDAJOV	22
ČLÁNOK XVI	POSTUPY PRI HAVÁRIÁCH, PORUCHÁCH A INÝCH MIMORIADNYCH SITUÁCIÁCH VRÁTANE PREVENTÍVNYCH OPATRENÍ NA ZNÍŽENIE VZNIKU MIMORIADNYCH SITUÁCIÍ A MOŽNOSTÍ EFEKTÍVNEJ OBNOVY STAVU PRED HAVÁRIOU	24
ČLÁNOK XVII	MINIMÁLNE POŽADOVANÉ BEZPEČNOSTNÉ OPATRENIA	30
ČLÁNOK XVIII	ZÁVEREČNÉ USTANOVENIA	30
ČLÁNOK XIX	SÚVISIACA DOKUMENTÁCIA	31
ZMENOVÝ DENNÍK		32
ROZDELOVNÍK		32

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Článok I

VŠEOBECNÉ USTANOVENIA

- (1) Táto smernica je vydaná v zmysle GDPR – General Data Protection Regulation (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) a zákona na ochranu osobných údajov č.18/2018 Z. z.
- (2) Táto smernica upravuje činnosť zamestnancov, ktorí v rámci výkonu svojich pracovných povinností spracúvajú osobné údaje alebo pri plnení pracovných povinností sú im osobné údaje sprístupňované, alebo sú im určené povinnosti na základe tejto smernice.
- (3) Táto smernica sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie osobných údajov inými než automatizovanými prostriedkami, ak ide o osobné údaje, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.
- (4) Táto smernica sa nevzťahuje na osobné údaje, ktoré boli získané náhodne bez predchádzajúceho určenia účelu a prostriedkov spracúvania, bez zámeru ich ďalšieho spracúvania v usporiadanom systéme podľa osobitných kritérií a nie sú ďalej systematicky spracúvané.

Článok II


VÝKLAD POJMOV

1. Osobné údaje

– *Osobnými údajmi* sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

– *Identifikácia* sa realizuje prostredníctvom konkrétnych charakteristických znakov, t. j. „identifikátorov“, ktoré možno priradiť ku konkrétnej fyzickej osobe (napr.: meno, priezvisko, tetovanie, zdravotné postihnutie, dátum narodenia, adresa a iné). Miera, do akej sú určité identifikátory dostačujúce pre dosiahnutie identifikácie konkrétnej fyzickej osoby, závisí od konkrétnej situácie a komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti. V závislosti od kvality, kvantity a druhu údajov sa v určitom momente konvertuje určiteľnosť do určenia konkrétnej fyzickej osoby.

Fyzickú osobu považujeme za určenú, keď na základe dostupných údajov je jednoznačne identifikovaná a odlišená od ostatných osôb v informačnom systéme, v ktorom sa osobné údaje spracúvajú. Na určenie toho, či je fyzická osoba identifikovateľná, sa majú vziať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Osobnými údajmi tak môžu byť v konkrétnej situácii napríklad: titul, meno, priezvisko, adresa trvalého pobytu, dátum narodenia, rodné číslo, údaj o zdravotnom stave, tetovanie, lokalizačný údaj, on-line identifikátor a pod.

- 2. Informačný systém osobných údajov** – je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

Informačným systémom sa rozumie akýkoľvek usporiadaný súbor, sústava alebo databáza určená na zhromažďovanie osobných údajov alebo obsahujúca osobné údaje fyzických osôb, ktoré sú systematicky spracúvané pre potreby dosiahnutia vopred vymedzeného, alebo ustanoveného účelu podľa osobitných kritérií a podmienok s použitím automatizovaných, čiastočne automatizovaných alebo iných ako automatizovaných prostriedkov spracúvania bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom, alebo geografickom základe. Jedným informačným systémom osobných údajov sa rozumie aj situácia, kedy prevádzkovateľ spracúva osobné údaje viacerými prostriedkami spracúvania na jeden účel (papierová evidencia dochádzky a čipová karta zamestnanca sú súčasťou dochádzky zamestnancov, teda napriek využitiu viacerých prostriedkov spracúvania ide o jeden informačný systém osobných údajov, nakoľko účelom je sledovanie a zaznamenávanie dochádzky zamestnancov).

- 3. Súhlas dotknutej osoby** – súhlasom dotknutej osoby je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.

Súhlas dotknutej osoby je jedným z právnych základov spracúvania osobných údajov. Súhlas by sa mal poskytnúť výslovným a jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením vôle dotknutej osoby so spracúvaním osobných údajov – forma písomného vyhlásenia vrátane vyhlásenia prostredníctvom elektronických prostriedkov alebo ústnym vyhlásením, je za splnenia ostatných náležitostí súhlasu akceptovateľná. Nariadenie GDPR, resp. Zákon určujú podmienky pre udelenie súhlasu, ako aj pre spracúvanie osobných údajov na tomto právnom základe. Nariadenie GDPR, resp. Zákon vyžadujú aktívnu účasť dotknutej osoby pri udeľovaní súhlasu, je teda potrebné formulovať súhlas tak, aby dotknutá osoba musela konať. Nečinnosť dotknutej osoby, respektíve nevyjadrenie nesúhlasu dotknutej osoby nemožno považovať za vyjadrenie súhlasu. Dotknutá osoba má teda k súhlasu vždy pristupovať aktívne, teda z jej strany je očakávaná aktivita.

V prípade, ak je predmetom spracúvania spracúvanie osobitnej kategórie osobných údajov, je potrebné, aby bol súhlas dotknutej osoby výslovný, teda taký, ktorý je oddelený od inej časti dokumentu, do ktorej môže byť včlenený a hlavne v ktorom je výslovne uvedené, aké konkrétne osobitné kategórie osobných údajov majú na jeho základe byť predmetom spracúvania zo strany prevádzkovateľa a aký je účel ich spracúvania.

- 4. Genetické údaje** – genetickými údajmi sú osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických

znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.


Genetický údaj možno vymedziť ako osobný údaj týkajúci sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré sú najmä výsledkom analýzy biologických vzoriek danej fyzickej osoby, najmä analýzy chromozómov, deoxyribonukleovej kyseliny (DNA) alebo ribonukleovej kyseliny (RNA), alebo analýzy inej látky, ktorá umožňuje získanie rovnocenných informácií o konkrétnej dotknutej osobe. Genetické osobné údaje patria medzi osobitnú kategóriu osobných údajov, ktorá tiež býva označovaná ako „citlivé osobné údaje“.

- 5. Biometrické údaje** – biometrickými údajmi sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.

Biometrický údaj možno definovať ako biologickú alebo fyziologickú vlastnosť, alebo charakteristiku špecifickú pre konkrétneho jednotlivca a zároveň merateľnú veličinu s určitým stupňom zohľadnenej pravdepodobnosti. Príkladom biometrických údajov sú odtlačky prstov, biometrický snímok sietnice oka, tvaru tváre a vzdialenosti jednotlivých častí tváre, hlas, geometria ruky, geometria štruktúry žíl ruky alebo dlane určitého človeka, alebo určitá hlboko zakorenená schopnosť či vlastnosť týkajúca sa správania konkrétneho jedinca (napr. vlastnoručný podpis, spôsob jeho písania, vyvíjanie tlaku na podložku, udieranie na klávesnicu, osobitný spôsob chôdze alebo artikulácie atď.; v tomto prípade ide o tzv. behaviorálnu biometriu).

- 6. Údaje týkajúce sa zdravia** – údajmi týkajúcimi sa zdravia sú osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

Osobné údaje týkajúce sa zdravia sú také osobné údaje, ktoré poskytujú informácie o minulom, súčasnom alebo možnom budúcom fyzickom, alebo duševnom zdravotnom stave dotknutej osoby. Patria sem aj údaje o zdraví fyzickej osoby získané pri jej registrácii na účely poskytovania služieb zdravotnej starostlivosti, služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo sociálnych služieb. Medzi osobné údaje týkajúce sa zdravia patrí tiež číslo, symbol alebo osobitný údaj, ktorý bol fyzickej osobe pridelený na jej individuálnu identifikáciu na zdravotné účely, informácie získané na základe vykonania testov alebo prehliadok častí jej organizmu, alebo skúmania jej telesných látok vrátane genetických údajov a biologických vzoriek a akékoľvek informácie o chorobe, zdravotnom postihnutí, riziku ochorenia, anamnéze, klinickej liečbe alebo o fyziologickom, alebo biomedicínskom stave dotknutej osoby, a to bez ohľadu na zdroj týchto informácií, ktorým môže byť lekár alebo iný zdravotnícky pracovník, nemocnica ako inštitúcia, zdravotnícka pomôcka pridelená konkrétnej osobe alebo informácie pochádzajúce z vykonania diagnostického testu in vitro. Medzi údaje o zdraví patria aj informácie o zdraví konkrétnej osoby získané z mobilných aplikácií slúžiacich k monitorovaniu životných funkcií alebo fyziologických parametrov osoby.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

- 7. Spracúvanie osobných údajov** – spracúvaním osobných údajov sa rozumie spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi, alebo so súbormi osobných údajov, 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.


Pod spracúvaním osobných údajov je potrebné chápať každú spracovateľskú operáciu alebo niekoľko na seba naväzujúcich operácií (naväznosť v čase nie je podstatná), ktoré prevádzkovateľ alebo sprostredkovateľ vykonáva na splnenie určitého vymedzeného účelu systematicky, a to bez ohľadu na spôsob a využité prostriedky (alebo ich kombináciu) spracúvania. Spracúvanie môže byť vykonávané rôznymi spôsobmi, napríklad formou ľudskej činnosti alebo automatizovane. Ide teda o charakteristiku toho, ako sú jednotlivé spracovateľské operácie u prevádzkovateľa alebo sprostredkovateľa vykonávané a technicky nastavené.

- 8. Obmedzenie spracúvania osobných údajov** – obmedzením spracúvania osobných údajov je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Pri obmedzení spracúvania osobných údajov sú spracúvané osobné údaje označené na účely obmedzenia ich spracúvania „pro futuro“ (do budúcnosti). Obmedzením nie je vždy potrebné chápať iba ich blokovanie, ale napríklad aj obmedzenie ich spracúvania na určitý účel. Osobné údaje, ktorých spracúvanie má byť obmedzené, by takto v informačnom systéme mali byť označené. Pod obmedzením spracúvania osobných údajov si možnosť predstaviť napríklad ich presun v rámci prevádzkovateľa do iného informačného systému alebo ich znepřístupnenie dovnútra, alebo navonok, teda voči verejnosti (napr.: „stiahnutie“ zverejnených osobných údajov z určitého dôvodu, no ich zachovanie u prevádzkovateľa). Obmedzenie spracúvania osobných údajov môže byť vykonané na účely ochrany dotknutej osoby a uplatnenia si jej práv v prípade, že namieta spracúvanie týchto svojich osobných údajov, má pochybnosti o správnosti alebo zákonnosti ich spracúvania, prípadne ak odpadla potreba spracúvania osobných údajov prevádzkovateľom, avšak dotknutá osoba potrebuje spracúvať tieto osobné údaje u daného prevádzkovateľa napríklad na účely domáhania sa svojich právnych nárokov v budúcnosti.

- 9. Profilovanie** – profilovaním je akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie 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.

Profilovaním sa rozumie spracúvanie osobných údajov, na základe ktorého možno získať, v závislosti od kvality a kvantity spracúvaných informácií, relatívne ucelený profil dotknutej osoby, ktorý možno s vysokým stupňom pravdepodobnosti využiť na predpovedanie správania konkrétnej dotknutej osoby do budúcnosti. Použitie profilovania je rozsiahle, jednou z možností jeho využitia, ktorá je na vzostupe, je využívanie na vytvorenie cielenej reklamy na mieru konkrétneho jedinca. Na účely profilovania by mali byť používané primerané matematické alebo štatistické postupy, mali by byť prijaté technické a organizačné opatrenia tak, aby sa zabezpečilo,

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

že faktory, ktoré vedú, alebo by mohli viesť k nesprávnosti osobných údajov, sa opravujú a riziko chýb sa minimalizuje.

Zabezpečí sa tak zohľadnenie súvisiacich potenciálnych rizík pre záujmy a práva dotknutej osoby. Zabráni sa tiež diskriminačným účinkom 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. Profilovanie založené na spracúvaní osobitných kategóriách osobných údajov je možné len za osobitných podmienok viažucich sa na spracúvanie osobitnej kategórie osobných údajov.

- 10. Pseudonymizácia** – pseudonymizáciou sa rozumie spracúvanie osobných údajov takým spôsobom, že ich bez použitia dodatočných informácií nie je možné priradiť ku konkrétnej dotknutej osobe, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na nich technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej alebo identifikovateľnej fyzickej osobe.


Pseudonymizácia je spracúvanie osobných údajov spočívajúce v takej forme, že dané údaje už následne nie je možné priradiť ku konkrétnej dotknutej osobe bez toho, aby sa na to museli použiť dodatočné informácie, ktoré by mali byť uchovávané oddelene a osobitne zabezpečené. Pseudonymizované údaje sú stále osobnými údajmi podliehajúcimi Nariadeniu GDPR, resp. Zákonom, ide však o jedno z bezpečnostných opatrení, ktoré môže prevádzkovateľ využiť, aby ním spracúvané osobné údaje chránil.

Rozdiel medzi anonymizovanými a pseudonymizovanými údajmi je v tom, že anonymizované údaje nemožno priradiť ku konkrétnej dotknutej osobe ani s použitím dodatočných informácií, naopak s pseudonymizovanými údajmi by to možné mohlo byť. Pokiaľ to možné nie je, ide o anonymizované osobné údaje.

Príkladom pseudonymizácie je, že osobné údaje „Eva Nová, narodená 12.12.1966, učiteľka“ sa zmenia na sadu písmen a čísiel „456mnb2b4gr47sDR, učiteľka“ no informácia, že skôr uvedený kód patrí pani Eve Novej bude u prevádzkovateľa uchovávaná osobitne. Práve na základe spojenia zvlášť uchovanej informácie, že daný kód patrí Eve Novej, bude stále možné zistiť, komu konkrétne kód patrí a daná dotknutá osoba bude stále v prostredí prevádzkovateľa identifikovateľná. Osobné údaje, ktoré boli pseudonymizované a ktoré by sa mohli použitím dodatočných informácií priradiť ku konkrétnej fyzickej osobe, by sa mali považovať za informácie o identifikovateľnej fyzickej osobe.

- 11. Log** – logom sa rozumie záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

Vedenie logov (logovanie) je bezpečnostné opatrenie slúžiace k zaznamenávaniu akýchkoľvek zmien, prehliadania, poskytovania, prenosu, kombinovania alebo vymazávania osobných údajov v rámci informačného systému osobných údajov alebo ich pokusov o zmenu, ktoré je založené na zachytení údajov o tom, kto, kedy a akú zmenu v automatizovanom informačnom systéme osobných údajov vykonal alebo sa pokúšal vykonať. Výsledkom logovania je zaznamenávanie logov, ktoré následne môžu slúžiť na vykonávanie analýzy a na zaznamenávanie činnosti používateľa v automatizovanom informačnom systéme. Logom je tiež akékoľvek používateľské

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

meno alebo heslo, alebo iný prihlasovací údaj, ktorý slúži na prihlásenie používateľa do automatizovaného informačného systému osobných údajov.

- 12. Šifrovanie** – šifrovaním sa rozumie transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč, alebo heslo.

Šifrovanie znamená zmenu obsahu informácie na skupinu bezvýznamných znakov, kedy na to, aby sa skupina týchto znakov opätovne transformovala do pôvodnej zmysluplnej informácie, je potrebné, aby prijímateľ správy disponoval správnym prístupovým kódom, heslom alebo iným, na to určeným parametrom.

- 13. On-line identifikátor** – online identifikátorom je identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do on-line služieb, rádiový frekvencný identifikátor, ktoré môžu zanechávať stopy a ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.

On-line identifikátor alebo jednoznačný identifikátor je využívaný pri vzájomnej komunikácii koncových zariadení užívateľov prostredníctvom komunikačných sietí. Takýmito identifikátormi sú napríklad IP adresa a cookies, či iné identifikátory využívajúce napríklad rádiovú frekvenciu (tzv. RFID identifikátory). On-line identifikátor je osobným údajom konkrétnej fyzickej osoby pokiaľ ho je možné k tejto osobe jednoznačne priradiť, teda pokiaľ sa možno s najvyššou pravdepodobnosťou domnievať alebo je potvrdené, že koncové zariadenie je vo vlastníctve konkrétnej osoby, teda z neho možno aj na základe informácií pochádzajúcich z identifikátorov vyčítať konkrétne aspekty správania a preferencií fyzickej osoby.


- 14. Porušenie ochrany** – porušením 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.

Za porušenie ochrany osobných údajov považujeme situácie, pri ktorých dochádza k nedovolenému resp. nezákonnému nakladaniu s osobnými údajmi či už úmyselne, alebo v dôsledku zanedbania povinností a opatrení prijatých na ich ochranu. Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu, alebo akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby. Porušenie ochrany môže byť vyvolané nielen zvonka prevádzkovateľa alebo sprostredkovateľa (napr. kybernetický útok), ale aj zvnútra prevádzkovateľa alebo sprostredkovateľa (napr. pochybenie zamestnanca). Pritom môže ísť o úmyselné, ako aj neúmyselné konanie, ktoré povedie k narušeniu integrity, dostupnosti a dôvernosti osobných údajov.

- 15. Analýza bezpečnosti informačného systému** – je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti.

- 16. Dotknutá osoba** – dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Dotknutou osobou je fyzická osoba, ktorej sa osobné údaje spracúvajú. Dotknutou osobou je fyzická osoba aj vtedy, ak sa jej osobné údaje, ktoré sa spracúvajú v informačnom systéme

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

osobných údajov, týkajú. Definícia dotknutej osoby korešponduje s článkom 8 Charty základných ľudských práv Európskej Únie a tiež s článkom 16 Zmluvy o fungovaní Európskej Únie.

- 17. Prevádzkovateľ** – prevádzkovateľom je každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.

Prevádzkovateľom je každý, kto sám alebo spoločne s inými pred začatím spracúvania osobných údajov vymedzí účel spracúvania osobných údajov a prostriedky ich spracúvania. Prevádzkovateľ spracúva osobné údaje vo vlastnom mene. Účel spracúvania môže byť ustanovený v osobitnom predpise (prevádzkovateľ ho musí rešpektovať a dodržiavať, napr. spracúvanie osobných údajov žiakov školou podľa školského zákona) alebo je prevádzkovateľovi daná možnosť, aby si ho vymedzil, napríklad na základe zamerania jeho podnikateľskej činnosti rešpektujúc právny poriadok a legálne možnosti, ktoré mu ponúka.


- 18. Sprostredkovateľ** – sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa. Právny vzťah na základe ktorého dochádza k spracúvaniu osobných údajov sprostredkovateľom v mene prevádzkovateľa, je založený na zmluve, plnej moci, poverení sprostredkovateľa prevádzkovateľom. Základné náležitosti zmluvy medzi prevádzkovateľom a sprostredkovateľom, plnej moci alebo poverenia ustanovuje čl. 28 Nariadenia GDPR, resp. ust. § 34 ods. 3 Zákona alebo iný osobitný zákon v rámci právneho poriadku Slovenskej republiky. Sprostredkovateľ spracúva osobné údaje na právnom základe, ktorý vymedzil prevádzkovateľ, t. j. sprostredkovateľ nevymedzuje osobitný právny základ od prevádzkovateľa odlišný, ale spracúvanie osobných údajov vykonáva na základe podmienok a prostriedkov, ktoré určil prevádzkovateľ, alebo ktoré prevádzkovateľovi ustanovuje napríklad osobitný zákon.

Nariadenie GDPR, resp. Zákon nevyučujú, aby subjekt mal postavenie sprostredkovateľa, kedy vykonáva spracovateľské operácie v mene prevádzkovateľa a na základe jeho pokynov, prípadne aj postavenie sprostredkovateľa pre viacerých prevádzkovateľov, ako aj postavenie prevádzkovateľa pre svoje vlastné spracovateľské operácie, ktoré vykonáva vo svojom mene a sám si pre takéto spracúvanie určil účel, podmienky a primeraný právny základ (napríklad vedenie informačného systému personalistika a mzdy, informačného systému účtovníctvo, informačného systému registratúra a pod.).

Tak prevádzkovateľ, ako aj sprostredkovateľ, ak je prevádzkovateľom poverený spracúvať v jeho mene osobné údaje, sú viazaní Nariadením GDPR, resp. Zákonom o ochrane osobných údajov, prípadne inými osobitnými zákonmi, ak tieto upravujú spracúvanie osobných údajov.

- 19. Subdodávateľ** – pokiaľ si sprostredkovateľ s prevádzkovateľom písomne v zmluve dohodne, že spracúvanie osobných údajov bude vykonávať prostredníctvom inej osoby (ďalej len

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

„subdodávateľ“). Subdodávateľ spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa. Na subdodávateľa úrad nahliada ako na sprostredkovateľa.

- 20. Prijemca** – príjemcom je každý, komu sa osobné údaje poskytnú, a to bez ohľadu na to či je treťou stranou, alebo nie; za príjemcu sa nepovažuje orgán verejnej moci, ktorý v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

Príjemcom sa rozumie teda každý, komu sú osobné údaje poskytnuté alebo sprístupnené, bez ohľadu na to či sa jedná o tretiu stranu, alebo nie. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade osobitným predpisom, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov orgánmi verejnej moci sa uskutočňuje v súlade s pravidlami ochrany osobných údajov v závislosti od účelov spracúvania im stanovených osobitnými právnymi predpismi. Vo vzťahu k zodpovednej osobe je používaný aj pojem kategória príjemcov. Možno si pod ňou predstaviť napríklad kategóriu prevádzkovateľov alebo sprostredkovateľov majúcich rovnaké alebo podobné podnikateľské zameranie – napríklad banky, poisťovne, živnostníkov s rovnakým predmetom podnikania a podobne.

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

Treťou stranou sa rozumie každý subjekt súkromného sektora alebo orgán verejnej moci, alebo fyzická osoba, ktorá nie je prevádzkovateľom, sprostredkovateľom alebo dotknutou osobou. Treťou stranou sú aj osoby, ktoré nie sú priamo poverené spracúvaním osobných údajov prevádzkovateľom alebo sprostredkovateľom. Tretia strana je užším pojmom ako príjemca. Príjemca je s výnimkou orgánov verejnej moci akýkoľvek subjekt, ktorému sa osobné údaje poskytujú. Pod kategóriou príjemcu sa rozumejú finančné inštitúcie, poisťovne, banky, zamestnávateľa a pod.

- 22. Zodpovedná osoba** – Zodpovednou osobou je oprávnená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa alebo sprostredkovateľa. Dohľad nad ochranou osobných údajov predstavuje súbor úloh a činností, ktoré je zodpovedná osoba povinná plniť v zmysle Nariadenia GDPR, resp. Zákona o ochrane osobných údajov.

Zodpovedná osoba je osoba určená prevádzkovateľom alebo sprostredkovateľom na základe jej odborných kvalít Nariadením GDPR, resp. Zákonom stanovených situáciách vždy, inak dobrovoľne. Zodpovednou osobou môže byť tak zamestnanec prevádzkovateľa alebo sprostredkovateľa, ako aj fyzická osoba vykonávajúca funkciu zodpovednej osoby na základe zmluvy. Základnou úlohou zodpovednej osoby je poskytovať informácie a poradenstvo prevádzkovateľovi a sprostredkovateľovi a ich zamestnancom pri spracúvaní osobných údajov a plnení úloh podľa Nariadenia GDPR, resp. Zákona. Úlohou zodpovednej osoby navyše je poskytovanie spolupráce úradu a vybavovanie žiadostí dotknutých osôb.

Zodpovedná osoba pre FNsP NZ za oblasť GDPR: Ing. Tomáš Dopirák
e-mail: zo@osobnyudaj.sk

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Tel.: 0907292832

osobnyudaj.sk, s.r.o. Garbiarska 5, 040 01 Košice na základe Zmluvy číslo: ZO2018Z7439;

- 23. Zástupca prevádzkovateľa/sprostredkovateľa** – zástupcom je fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril.

Zástupcom prevádzkovateľa za FNsP NZ (kontaktná osoba): **Mgr. Michal Bojnický, MPH.**

- 24. Podnik** – podnikom je fyzická osoba – podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane združení fyzických osôb, alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť.

Podnikom sa rozumie: Fakultná nemocnica s poliklinikou Nové Zámky, Slovenská 11 A, 940 34 Nové Zámky

zastúpená JUDr. Lenka Horváth Bodáková - právnik

kontakt: lenka.bodakova@nspnz.sk

+ 035/ 691 2446

- 25. Vnútropodnikové pravidlá** – vnútropodnikovými pravidlami sú postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine.

Záväznú vnútropodnikové pravidlá sú súčasťou internej politiky ochrany osobných údajov prevádzkovateľa alebo sprostredkovateľa, ktorý nimi definuje svoje postupy a pravidlá v rámci svojej obchodnej politiky s ohľadom na prenos mimo územia členských štátov Európskej únie. Možno ich považovať za istý druh bezpečnostného opatrenia, ktorým prevádzkovateľ a sprostredkovateľ zaisťujú primeranú úroveň ochrany spracúvaných osobných údajov v týchto tzv. tretích krajinách, ich častiach, prípadne medzinárodných organizáciách, ktoré takúto primeranú úroveň ochrany osobných údajov nezaručujú.

- 26. Kódex správania** – kódexom správania je súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať.

Kódex správania je súbor určitých ustanovení, ktorého účelom je upresniť, konkretizovať dodržiavanie jednotlivých povinností podľa Nariadenia GDPR, resp. Zákona týkajúceho sa spracúvania a ochrany osobných údajov s ohľadom na osobitné charakteristiky určitého odvetvia, pre ktoré konkrétny kódex správania bol schválený. Ku kódexom správania je možnosť pristúpiť a zaviazat' sa ich dodržiavať dobrovoľne, ak však prevádzkovateľ pristúpi k schválenému kódexu správania je povinný ho ako súčasť bezpečnostných opatrení dodržiavať a uplatňovať.

- 27. Sprístupňovanie osobných údajov** – je oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.

28. **Zverejňovanie osobných údajov** – predstavuje publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.
29. **Cezhraničný prenos** – je prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky.
30. **Likvidácia osobných údajov** – je zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
31. **Účel spracúvanie osobných údajov** – je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
32. **Aktíva informačného systému** – je to citlivá informácia, ktorú máme chrániť. Sú to jednotlivé časti informačného systému a osobné údaje v elektronickej a písomnej forme.
33. **Zraniteľné miesto** – je slabina systému využiteľná na spôsobenie škôd. Zahrňuje slabé miesta aktíva IS alebo skupiny aktív IS, ktoré môžu byť využité hrozbou.
34. **Hrozba** – je potenciálna možnosť využitia zraniteľného miesta.
35. **Riziko** – je pravdepodobnosť využitia zraniteľného miesta aktív IS a skupiny aktív IS, pravdepodobnosť uplatnenia hrozby.
36. **Zostatkovým rizikom** – sa rozumie bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.
37. **Incident** – je využitie zraniteľného miesta na spôsobenie škôd, strata na aktívach, prípadné ich poškodenie alebo zničenie.
38. **Audit bezpečnosti informačného systému** – je nezávislé odborné posúdenie spoľahlivosti a celkovej bezpečnosti informačného systému z hľadiska zabezpečenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov.


Použité skratky :

FNsP NZ	Fakultná nemocnica s poliklinikou Nové Zámky
GDPR	General DataProtectionRegulation
EÚ	Európska Únia
Zákon	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Článok III

ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV

- (1) Prevádzkovateľ spracúva osobné údaje na:
 - a) poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti,

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

- b) plnenie úloh zamestnávateľa pri výkone pracovnoprávných vzťahov a pri výbere nových zamestnancov, pričom rozsah spracúvaných osobných údajov, ich poskytovanie, sprístupňovanie a zverejňovanie ustanovujú osobitné predpisy,¹
- c) vykonávanie úloh súvisiacich so zabezpečením spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby,
- d) evidenciu osôb vstupujúcich do objektov prevádzkovateľa a osôb, ktorým je povolený vstup do objektov prevádzkovateľa na účel vykonávania zmluvne dohodnutých prác po 18 hodine
- e) vykonávanie ostatných úloh vyplývajúcich z povinností prevádzkovateľa,
- f) vykonávanie úloh vo verejnom záujme.

Článok IV

ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

Zásady spracúvania osobných údajov sú základnými mantinelmi, v rámci ktorých sa konkrétne spracúvanie osobných údajov fyzickej osoby posudzuje a vykonáva. Cieľom zásad spracúvania osobných údajov je vykonávanie spracúvania osobných údajov tak, aby boli rešpektované práva dotknutých osôb a aby spracúvaním osobných údajov nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do práva na ochranu súkromia.


1. **Zásada zákonnosti** – osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Každé spracúvanie osobných údajov má byť zákonné, teda založené na legálnom právnom základe podľa čl. 6 Nariadenia GDPR, resp. ust. § 13 zákona. Spracúvanie nesmie byť protiprávne, nesmie prebiehať na nelegálnom právnom základe a samotný účel spracúvania nesmie byť nelegitímny.

2. **Zásada obmedzenia účelu** – osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa čl. 89 ods. 1 Nariadenie GDPR, resp. § 78 ods. 8 Zákona, sa nepovažuje za nezlučiteľné s pôvodným účelom.

Spracúvané osobné údaje majú byť primerané, relevantné a obmedzené na zoznam alebo rozsah osobných údajov nevyhnutný vzhľadom na účel, na ktorý sa spracúvajú. Účel je základným obmedzujúcim faktorom najmä vo vzťahu k zoznamu alebo rozsahu spracúvaných osobných údajov a vo vzťahu k dobe spracúvania, ako aj uchovávanía spracúvaných osobných údajov. Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie

¹ Napríklad Zákonník práce, zákon č. 552/2003 Z. z. v znení neskorších predpisov, zákon č. 400/2009 Z. z. v znení neskorších predpisov ² Článok 6 nariadenia

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať.

Spracúvať osobné údaje na iný účel, než na ktorý boli získané je zakázané, okrem prípadu, že by tento iný účel úzko súvisel s pôvodným účelom spracúvania, alebo s ním bol aspoň zlučiteľný.


Spracúvanie osobných údajov získaných na stanovený účel nevylučuje, aby takto získané osobné údaje nemohli byť spracúvané na tzv. privilegované účely, a to na účely archivácie, na účely vedeckého alebo historického výskumu a na štatistické účely v súlade s Nariadením GDPR, resp. Zákonom a vo vzťahu k primeraným zárukám aj pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení, najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov, pseudonymizácie, pokiaľ sa týmito opatrením môžu dosiahnuť uvedené účely. Ďalšie spracúvanie na účely archivácie, na účely vedeckého či historického výskumu, alebo štatistické účely, sa považuje za zlučiteľné so zákonnými spracovateľskými operáciami.

3. Zásada minimalizácie osobných údajov – spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Spracúvanie osobných údajov má byť úzko naviazané na účel spracúvania osobných údajov, a to najmä pokiaľ ide o zoznam alebo rozsah spracúvaných osobných údajov, ktorý by mal byť nevyhnutný na to, aby sa spracúvaním daných osobných údajov účel mohol dosiahnuť. Nie je správne, aby sa zoznam alebo rozsah osobných údajov umelo alebo dodatočne rozširoval vzhľadom na účel. Ak je účel a zoznam alebo rozsah osobných údajov stanovený zákonom, je potrebné ho rešpektovať, ak si zoznam alebo rozsah spracúvaných osobných údajov určuje prevádzkovateľ, má dbať na to, aby ho zbytočne nad rámec účelu nerozširoval.

4. Zásada správnosti – 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.

Osobné údaje spracúvané na určitý účel musia byť správne, presné a podľa potreby aktualizované tak, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne bezodkladne vymažú alebo opravia. Ak nesprávny osobný údaj odhalí prevádzkovateľ, má povinnosť ho opraviť (ak je to možné), ak nie, má povinnosť ho zlikvidovať. V prípade ak nesprávny osobný údaj zistí dotknutá osoba, mala by sama iniciatívne kontaktovať prevádzkovateľa a požadovať opravu nesprávneho osobného údaj alebo jeho likvidáciu podľa Nariadenia GDPR, resp. Zákona, ak sa nesprávnosť údaju potvrdí, prevádzkovateľ má požiadavke dotknutej osoby na opravu vyhovieť. Zásada aktuálnosti znamená tiež to, že prevádzkovateľ má povinnosť spracúvané osobné údaje pravidelne kontrolovať a aktualizovať (pravidelnosť kontroly je potrebné nastaviť s ohľadom na ujmu, ktorá môže vzniknúť dotknutej osobe pri spracúvaní nesprávneho osobného údaj prevádzkovateľom), a to nielen po gramatickej, ale hlavne po obsahovej stránke, teda nemalo by sa stať, že osoba, ktorá uhradila svoj dlh, bude v systéme prevádzkovateľa stále vedená ako dlžník napriek tomu, že reálny aj právny stav tomu už nezodpovedá. Prevádzkovateľ nesie zodpovednosť za aktuálnosť osobného údaj v jeho informačnom systéme osobných údajov. V prípade, ak dotknutá osoba sama poskytne prevádzkovateľovi nesprávne osobné údaje, za ich

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

nesprávnosť v tomto prípade nenesie zodpovednosť prevádzkovateľ, okrem prípadu, že mal možnosť, prípadne zákonom stanovenú povinnosť, preveriť si ich správnosť.

5. 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 dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa čl. 89 ods. 1 Nariadenia GDPR, resp. § 78 ods. 8. Zákona.

Zásada minimalizácie uchovávania spracúvaných osobných údajov má za cieľ dosiahnuť, aby sa osobné údaje vo forme, kedy je ich možné priradiť ku konkrétnej fyzickej osobe, spracúvali iba dovtedy, kým je to potrebné na dosiahnutie sledovaného účelu spracúvania.

Ako náhle je tento cieľ spracúvania osobných údajov dosiahnutý, je možné, aby sa osobné údaje už spracúvali iba na účely archivácie, na účely vedeckého alebo historického výskumu či na štatistické účely podľa osobitného predpisu. To platí len za predpokladu, že prevádzkovateľ alebo sprostredkovateľ prijali primerané technické a organizačné opatrenia vyžadované Nariadením GDPR, resp. Zákomom na ochranu práv dotknutých osôb.


Zásada minimalizácie uchovávania má za cieľ, aby sa osobné údaje uchovávali vo forme, ktorá umožňuje identifikáciu dotknutých osôb len v nevyhnutnom rozsahu a len dovtedy, dokiaľ je to s ohľadom na účel spracúvania potrebné a nevyhnutné.

6. Zásada integrity a dôveryhodnosti – 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.

Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila ich primeraná bezpečnosť a dôveryhodnosť vrátane predchádzania neoprávnenému prístupu k osobným údajom a prostriedkom spracúvania osobných údajov. Prijaté bezpečnostné opatrenia musia byť adekvátne spracúvaným osobným údajom, a to tak po technickej, personálnej, ako aj po organizačnej stránke.

7. 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.

Zásada zodpovednosti za spracúvané osobné údaje pre prevádzkovateľa znamená zodpovednosť za dodržiavanie všetkých povinností stanovených Nariadením GDPR, resp. Zákomom a zároveň povinnosť navonok deklarovat', že všetky požadované povinnosti si skutočne aj plní. Prevádzkovateľ pri prijímaní bezpečnostných opatrení a plnení si aj iných svojich povinností podľa Nariadenia GDPR, resp. Zákona musí vystupovať aktívne a snažiť sa splniť si všetky povinnosti tak, ako mu ich Nariadenie GDPR, resp. Zákon ukladá. Nariadenie GDPR, resp. Zákon mu k preukazovaniu splnenia niektorých jeho povinností dávajú nástroje ako napríklad možnosť pristúpiť ku kódexom správania a využiť ich ako deklaratórne nástroje smerom von

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	


ohľadom ním prijatých bezpečnostných opatrení. Prevádzkovateľ je povinný prijať primerané a účinné opatrenia a vedieť preukázať súlad spracovateľských činností s Nariadením GDPR, resp. Zákonom vrátane primeraných a účinných bezpečnostných opatrení. V uvedených opatreniach by sa mala zohľadniť povaha, rozsah, kontext a účel spracúvania a riziko pre práva fyzických osôb. Na účely prijatia zodpovednosti by mal prevádzkovateľ najmä prijímať adekvátne politiky ochrany osobných údajov, ktorými bude deklarovať svoju zodpovednosť za spracúvanie a ochranu osobných údajov. Prevádzkovateľ zodpovedá aj za spracúvanie osobných údajov ním povereného sprostredkovateľa, či so sprostredkovateľom dohodnutého ďalšieho sprostredkovateľa, ktorí spracúvajú osobné údaje v jeho mene a na základe jeho pokynov. So zásadou zodpovednosti je spojené aj vedenie patričnej dokumentácie tak, aby v prípade potreby prevádzkovateľ vedel a mohol deklarovať, že vykonal posúdenie vplyvu, alebo opätovne hodnotil a snažil sa znížiť vysoké riziko, ktoré mu v rámci posúdenia vplyvu na osobné údaje, vyšlo ako zvyškové riziko.

Článok V

SPRACÚVANIE OSOBNÝCH ÚDAJOV NA ZÁKLADE SÚHLASU DOTKNUTEJ OSOBY

- (1) 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. Súhlas musí byť odlišný od iných skutočností a musí byť vyjadrený jasne, v zrozumiteľnej a ľahko dostupnej forme. Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Písomný súhlas sa preukazuje dokladom, ktorý potvrdzuje poskytnutie súhlasu a musí obsahovať tieto náležitosti:
 - a) kto súhlas dáva – identifikačné údaje dotknutej osoby (titul, meno, priezvisko, dátum narodenia, adresa trvalého pobytu),
 - b) komu sa tento súhlas dáva – identifikačné údaje prevádzkovateľa,
 - c) účel, na aký sa tento súhlas dáva,
 - d) čas platnosti súhlasu,
 - e) dátum a vlastnoručný podpis dotknutej osoby,
 - f) poučenie dotknutej osoby.

Súhlas môže byť poskytnutý aj inou formou ako písomnou, napr. videozáznamom alebo zvukovým záznamom, avšak musí byť hodnoverne preukázateľný.
- (2) Ak má dotknutá osoba menej ako 16 rokov, spracúvanie jej osobných údajov je zákonné iba za podmienky a v rozsahu súhlasu, ktorý poskytol alebo schválil jej zákonný zástupca.
- (3) Súhlas dotknutej osoby sa nesmie vyžadovať pre účely spracúvania osobných údajov na základe ostatných právnych základov.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Článok VI


OSOBITNÉ KATEGÓRIE OSOBNÝCH ÚDAJOV

- (1) Spracúvať osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické či biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života, alebo sexuálnej orientácie fyzickej osoby, sa zakazuje, pokiaľ dotknutá osoba k tomu nedala výslovný súhlas alebo pokiaľ ide o spracúvanie osobných údajov podľa článku 9 ods. 2 Nariadenia, najmä ak je spracúvanie nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom, a podlieha podmienkam a zárukám uvedeným v článku 9 ods. 3 Nariadenia.
- (2) Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom (rodné číslo) len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania alebo to vyžaduje osobitný zákon. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje.

Článok VII

ZÍSKAVANIE OSOBNÝCH ÚDAJOV

- (1) Prevádzkovateľ je povinný poskytnúť dotknutej osobe, pri získavaní jej osobných údajov, tieto informácie:
 - a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
 - b) kontaktné údaje zodpovednej osoby, ak je určená,
 - c) účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
 - d) oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú na tomto základe,
 - e) identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
 - f) informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácie, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie o primeranosti, alebo odkaz na primerané záruky či vhodné záruky a prostriedky na získanie ich kópie, alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos do tretích krajín,
 - g) informácie o dobe uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia,
 - h) informáciu o práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby, o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietat' spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,
 - i) informáciu o práve kedykoľvek svoj súhlas odvolať, v prípade, ak je právnym základom spracúvania osobných údajov súhlas dotknutej osoby,


Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FN sP NZ	

- j) informáciu o práve podať návrh na začatie konania na Úrade v zmysle vzoru uverejneného na webovom sídle Úradu,
 - k) informáciu o tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov,
 - l) informáciu o existencii automatizovaného individuálneho rozhodovania vrátane profilovania; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.
- (2) Ak osobné údaje nie sú získavané od dotknutej osoby, prevádzkovateľ je povinný poskytnúť dotknutej osobe pri získavaní jej osobných údajov okrem informácií uvedených v odseku 1 aj informáciu o zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov.
- (3) Prevádzkovateľ je povinný poskytnúť informácie:
- a) najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú,
 - b) najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou alebo
 - c) najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.
- (4) Prevádzkovateľ neposkytuje dotknutej osobe vyššie menované informácie, pokiaľ ich už dotknutá osoba má alebo sa poskytnutie takýchto informácií ukáže ako nemožné, alebo by si vyžadovalo neprimerané úsilie, alebo ak to prevádzkovateľovi umožňuje osobitný predpis, alebo ak osobné údaje musia ostať dôverné.
- (5) Osobné údaje o dotknutej osobe možno získať od inej fyzickej osoby a spracúvať v informačnom systéme len s predchádzajúcim písomným súhlasom dotknutej osoby; to neplatí, ak poskytnutím osobných údajov o dotknutej osobe do informačného systému iná fyzická osoba chráni svoje práva alebo právom chránené záujmy, oznamuje skutočnosti, ktoré odôvodňujú uplatnenie právnej zodpovednosti dotknutej osoby, alebo sa osobné údaje spracúvajú na základe osobitného zákona podľa článku 6 bodu 1 písmena c) a e) Nariadenia.
- (6) Ak dotknutá osoba nežije, súhlas vyžadovaný podľa Zákona môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.

Článok VIII

ZÍSKAVANIE OSOBNÝCH ÚDAJOV KOPÍROVANÍM, SKENOVANÍM ALEBO INÝM ZAZNAMENÁVANÍM

Získavať osobné údaje, nevyhnutné na dosiahnutie účelu spracúvania, kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií, možno len vtedy, ak s tým dotknutá osoba písomne súhlasí, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby. To neplatí, ak ide o získavanie osobných údajov na účely uzatvorenia pracovnoprávneho alebo obdobného vzťahu. Po uzatvorení pracovnoprávneho vzťahu je potrebné dokumenty s osobnými údajmi zlikvidovať.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Článok IX

ZVEREJŇOVANIE, SPRÍSTUPŇOVANIE A POSKYTOVANIE OSOBNÝCH ÚDAJOV PREVÁDZKOVATEĽOM

- (1) Prevádzkovateľ zverejňuje osobné údaje v rozsahu určenom v súhlase dotknutej osoby alebo v rozsahu určenom zákonom, alebo osobitnými predpismi, alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná.²
- (2) Prevádzkovateľ poskytuje alebo sprístupňuje osobné údaje, ktoré eviduje vo svojich informačných systémoch a ktoré nie sú zverejňované podľa odseku 1 len na základe súhlasu dotknutej osoby. Bez súhlasu dotknutej osoby poskytne alebo sprístupní osobné údaje, len ak to ustanovuje Zákon.
- (3) Prevádzkovateľ je oprávnený poskytovať alebo zverejniť osobné údaje zamestnancov v rozsahu: titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca, alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresu elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností, alebo funkčných povinností zamestnanca. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.


Zakazuje sa poskytovanie a sprístupňovanie osobných údajov cez elektronickú poštu, telefón a fax, ak osobitný predpis neustanovuje inak.

Článok X

POSKYTOVANIE INFORMÁCIÍ DOTKNUTEJ OSOBY O SPRACÚVANÍ JEJ OSOBNÝCH ÚDAJOV

- (1) Pri poskytovaní informácií dotknutej osobe, je oprávnená osoba, ktorá je príslušná na vybavenie žiadosti, povinná podať dotknutej osobe informácie o:
 - a) účele spracúvania osobných údajov,
 - b) kategórii spracúvaných osobných údajov,
 - c) identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli, alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine, alebo o medzinárodnej organizácii, ak je to možné,
 - d) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
 - e) práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov,
 - f) práve podať návrh na začatie konania na Úrade v zmysle vzoru uverejneného na webovom sídle Úradu,
 - g) zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby, existenciou automatizovaného individuálneho rozhodovania vrátane profilovania; v týchto prípadoch

² Napríklad zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FNsP NZ	

poskytne prevádzkovateľ dotknutej osobe informácie najmä o použitom postupe, ak za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

- (2) Poskytnutie osobných údajov nesmie mať nepriaznivé dôsledky na práva iných fyzických osôb. Prevádzkovateľ môže odoprieť právo na poskytnutie osobných údajov, pokiaľ je toto právo požadované neoprávnene a opakovane bez oprávnených dôvodov alebo by tým ohrozil práva iných fyzických osôb.

Článok XI


CEZHRANIČNÝ PRENOS OSOBNÝCH ÚDAJOV

- (1) Voľný pohyb osobných údajov medzi Slovenskou republikou a členskými štátmi Európskej únie a štátmi, ktoré sú zmluvnou stranou Dohody o Európskom hospodárskom priestore sa zaručuje.
- (2) Prenos osobných údajov do tretej krajiny, ktorá zaručuje primeranú úroveň ochrany osobných údajov možno uskutočniť, ak prevádzkovateľ dotknutej osobe predtým poskytol informácie podľa článku 7 ods. 1 písm. f.)
- (3) Prenos osobných údajov do tretej krajiny, ktorá nezaručuje primeranú úroveň ochrany osobných údajov, možno uskutočniť, ak dotknutá osoba pred jeho uskutočnením poskytla písomný súhlas s vedomím, že tretia krajina nezaručuje primeranú úroveň ochrany osobných údajov. Súhlas musí obsahovať názov krajiny, do ktorej bude uskutočnený prenos osobných údajov, ako aj upozornenie, že táto krajina nezaručuje primeranú úroveň ochrany osobných údajov.

Článok XII

LIKVIDÁCIA OSOBNÝCH ÚDAJOV

- (1) Po skončení účelu spracovania osobných údajov je potrebné tieto osobné údaje zlikvidovať, pokiaľ osobitný zákon nenariaďuje inak.
- (2) Dokumenty prevádzkovateľa v listinnej podobe, obsahujúce osobné údaje, možno uchovávať po dobu určenú na ich uchovanie, v zmysle registratúrneho poriadku prevádzkovateľa. Po ukončení doby uchovania je potrebné tieto dokumenty zlikvidovať.
- (3) Osobné údaje, ktoré sú v informačných systémoch prevádzkovateľa spracúvané v elektronickej podobe automatizovane prostredníctvom počítačovej techniky (ďalej len „elektronická podoba“), vrátane osobných údajov na pamäťových médiách, ako napríklad pevné disky, USB kľúče, DVD, CD, veľkokapacitné externé pevné disky, sa uchovávajú v tejto podobe len na nevyhnutne potrebnú dobu, ktorá je určená účelom informačného systému. Po jej uplynutí sa bezpečným spôsobom likvidujú tak, aby osobné údaje nebolo možné obnoviť. Pamäťové médiá, vrátane diskov v serveroch a pracovných staniciach, ktoré boli použité na uloženie osobných údajov v elektronickej podobe, musia byť pred svojim trvalým vyradením upravené tak, aby z nich nebolo možné obnoviť osobné údaje, ktoré na nich boli zapísané. Oddelenie informatiky, archívu a registratúry v koordinácii s príslušným odborom to

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

zabezpečí prepísaním celého pamäťového média náhodnými údajmi alebo fyzickým zničením pamäťového média.

- (4) Osobné údaje je potrebné zlikvidovať aj vtedy, ak si dotknutá osoba uplatní právo na výmaz osobných údajov v zmysle článku 17 Nariadenia. Oprávnená osoba zabezpečí likvidáciu osobných údajov za podmienok a spôsobom uvedeným v Smernici pre vybavovanie práv dotknutých osôb smerom k ich osobným údajom.


Článok XIII MLČANLIVOSŤ

Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť zachovávať mlčanlivosť je aj po skončení pracovného pomeru alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné, na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.³

Článok XIV POVINNOSTI OPRÁVNENEJ OSOBY

- (1) Oprávnená osoba je povinná najmä:
- získavať na základe svojho pracovného zaradenia len nevyhnutné osobné údaje výlučne na vopred ustanovený účel podľa tejto smernice; je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
 - spracúvať jedine také osobné údaje, ktoré sú nevyhnutne potrebné na dosiahnutie cieľa spracovania alebo osobné údaje, ktoré boli prevádzkovateľovi poskytnuté iným prevádzkovateľom na základe osobitného predpisu,
 - spracúvať osobné údaje len v priestoroch na to určených; o preprave osobných údajov v písomnej forme alebo na pamäťových médiách mimo týchto priestorov môže rozhodnúť jedine príslušný vedúci zamestnanec; v takom prípade musí byť zabezpečená ochrana, dôvernosť, dostupnosť a integrita prepravovaných osobných údajov,
 - bezodkladne opraviť alebo doplniť nesprávne, alebo neúplné osobné údaje; osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, je povinná oprávnená osoba blokovat', kým sa rozhodne o ich likvidácii,
 - zachovávať mlčanlivosť o osobných údajoch; povinnosť mlčanlivosti trvá aj po zániku pracovnoprávneho vzťahu oprávnenej osoby,
 - oznámiť príslušnému vedúcemu zamestnancovi a zodpovednej osobe každý bezpečnostný incident (napríklad podozrenie na únik osobných údajov, neoprávnené zasahovanie do osobných údajov) a oznámiť každé zistenie o nedostatočnej účinnosti existujúcich bezpečnostných opatrení prijatých na ochranu osobných údajov,

³ Napríklad zákon č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. v znení neskorších predpisov

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

- g) chrániť osobné údaje v listinnej alebo elektronickej podobe pred stratou, poškodením, zneužitím, odcudzením, neoprávneným prístupnením, poskytnutím, alebo inými neprípustnými formami spracúvania,
- h) umožniť vstup do miestnosti, v ktorej oprávnená osoba spracúva osobné údaje neoprávneným osobám (napríklad upratujúci personál, servisní zamestnanci, návštevy...) až po zabezpečení ochrany osobných údajov najmä uzatvorením dokumentov v elektronickej podobe, zatvorením spisového materiálu v listinnej podobe.

(2) Oprávnená osoba je povinná pri spracúvaní osobných údajov v listinnej podobe:

- a) využiť všetky dostupné prostriedky na zabezpečenie osobných údajov pred prístupom neoprávnenej osoby (napríklad uchovávanie dokumentov v uzamknutých častiach nábytku, uzamykanie miestnosti počas dočasnej neprítomnosti...),
- b) vrátiť odosielateľovi poštovú zásielku doručnú prevádzkovateľovi, ktorá obsahuje osobné údaje, ak sa na ich spracúvanie vyžaduje súhlas dotknutej osoby a dotknutá osoba ho prevádzkovateľovi vopred neposkytla; odosielateľ poštovej zásielky musí byť v odpovedi upozornený, že na spracúvanie osobných údajov sa vyžaduje súhlas dotknutej osoby.

(3) Ak oprávnená osoba spracúva osobné údaje, určené na zverejnenie podľa osobitného predpisu alebo súhlasu dotknutej osoby, povinnosti a obmedzenia na ochranu osobných údajov uplatní oprávnená osoba primerane.

(4) Oprávnená osoba je povinná dodržať ďalšie postupy upravené poučením, touto smernicou, iným vnútorným predpisom prevádzkovateľa, zákonom alebo iným všeobecne záväzným právnym predpisom.


(5) Pokiaľ oprávnená osoba nebola poučená k spracúvaniu osobných údajov pred začatím jeho spracovania alebo z poučenia iných vnútorných predpisov prevádzkovateľa jej nie je zrejmé, ako má plniť vyššie pomenované úlohy, je povinná o tejto skutočnosti informovať svojho nadriadeného a spracovanie osobných údajov obmedziť len na úlohy, ktoré sú jej zrejmé.

Článok XV

POVINNOSTI VEDÚCEHO ZAMESTNANCA PRI OCHRANE OSOBNÝCH ÚDAJOV

(1) Vedúci zamestnanec, riadiaci organizačný útvar, zabezpečujúci agendy, v ktorých sa spracúvajú osobné údaje:

- a) zodpovedá za ochranu osobných údajov, v záujme čoho samostatne alebo v súčinnosti prijíma potrebné organizačné, personálne a technické opatrenia,
- b) poskytuje nevyhnutnú súčinnosť zodpovednej osobe pri výkone dohľadu nad ochranou osobných údajov a v spolupráci so zodpovednou osobou zabezpečuje, aby informačné systémy v jeho riadiacej pôsobnosti boli pod dohľadom,
- c) konzultuje s kontaktnou a zodpovednou osobou potrebu vykonania posúdenia vplyvu na ochranu osobných údajov ešte pred začatím samotného spracúvania osobných údajov, ktoré môže viesť k vysokému riziku pre práva fyzických osôb,
- d) konzultuje s kontaktnou a zodpovednou osobou potrebu vykonania záznamu o spracovateľských činnostiach ešte pred začatím samotného spracúvania osobných údajov,

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	


- e) konzultuje s kontaktnou a zodpovednou osobou zriadenie spolupráce so sprostredkovateľom či sprostredkovateľom sprostredkovateľa, posúdenie schopnosti sprostredkovateľa zabezpečiť primeranú ochranu osobných údajov a zmluvné náležitosti sprostredkovateľskej zmluvy,
- f) konzultuje s kontaktnou a zodpovednou osobou zamýšľaný prenos osobných údajov do tretích krajín,
- g) konzultuje s kontaktnou a zodpovednou osobou prijatie rozhodnutí založených výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania,
- h) bez odkladu informuje zodpovednú osobu a vedenie prevádzkovateľa o každom porušení ochrany osobných údajov s pravdepodobnosťou vzniku rizika pre práva dotknutých osôb so zreteľom na povinnosť prevádzkovateľa, ktorá mu plynie z článku 33 Nariadenia; oznamovacia povinnosť prevádzkovateľa, kde prevádzkovateľ je povinný nahlásiť Úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel,
- i) navrhuje okruh oprávnených osôb zo zamestnancov v jeho riadiacej pôsobnosti,
- j) dohliada na to, aby oprávnená osoba spracúvala len také osobné údaje, ktoré nevyhnutne potrebuje na plnenie uložených úloh,
- k) rozhoduje o poskytnutí alebo sprístupnení osobných údajov a o poskytnutí informácií dotknutej osobe podľa článku 9 a 10; ak je to potrebné, vyžiada si pred prijatím rozhodnutia stanovisko zodpovednej osoby,
- l) plní ďalšie úlohy v poučení, ustanovené v tejto smernici, inom vnútornom predpise prevádzkovateľa, zákone alebo inom všeobecne záväznom právnom predpise.

Vedúci zamestnanec je povinný pri riešení bezpečnostných incidentov, narušení ochrany osobných údajov upovedomiť

- a) **kontaktnú osobu za FNsP NZ** pre oblasť GDPR a ochranu osobných údajov: Bc. Marek Vasek, klapka č. 2166, e-mail: marek.vasek@nspnz.sk alebo
- b) **zodpovednú osobu za FNsP NZ** pre oblasť GDPR a ochranu osobných údajov: Ing. Tomáš Dopirák (osobnyudaj.sk, s.r.o.) e-mailom: zo@osobnyudaj.sk / 0907 292 832,
- c) **v prípade incidentov v oblasti IT**: Ing. Ladislav Sloboda, klapka č. 2272, e-mail: ladislav.sloboda@nspnz.sk.

V prípade zmien (napr. organizačná zmena, zmena hlavných činností organizačných útvarov, a pod.), v dôsledku ktorých dôjde u prevádzkovateľa k vzniku novej alebo rozšíreniu existujúcej agendy, je príslušný vedúci zamestnanec povinný bezodkladne preskúmať, či sa v rámci novej alebo rozšírenej agendy budú spracúvať osobné údaje. Ak sa budú spracúvať osobné údaje, je povinný bezodkladne a v spolupráci so zodpovednou osobou:

- a) určiť účel a právny základ spracúvania osobných údajov, zoznam alebo rozsah osobných údajov vyžadovaných na účel vedenia príslušnej agendy,
- b) aktualizovať existujúci informačný systém, ak je to potrebné,
- c) navrhnúť oprávnené osoby, ktoré budú spracúvať osobné údaje.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

Článok XVI

POSTUPY PRI HAVÁRIÁCH, PORUCHÁCH A INÝCH MIMORIADNYCH SITUÁCIÁCH VRÁTANE PREVENTÍVNYCH OPATRENÍ NA ZNÍŽENIE VZNIKU MIMORIADNYCH SITUÁCIÍ A MOŽNOSTÍ EFEKTÍVNEJ OBNOVY STAVU PRED HAVÁRIOU

Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa najmenej raz ročne.

Narušenie personálnej bezpečnosti:

1. *Strata, vyzradenie alebo krádež hesiel pre vstup do IS* – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov
 - a) zmena všetkých prihlasovacích hesiel do informačného systému (aj administrátorských),
 - b) vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS,
 - c) ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup neoprávnenej osobe oprávnenou osobou, vykonať disciplinárne opatrenie.

2. *Oprávnený vstup neoprávnenej osoby* – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov
 - a) zmena všetkých prihlasovacích hesiel do informačného systému (aj administrátorských),
 - b) vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS,
 - c) ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup neoprávnenej osobe oprávnenou osobou, vykonať disciplinárne opatrenie.


Narušenie fyzickej bezpečnosti:

3. *Krádež počítača* – môže dôjsť k zneužitiu osobných údajov
 - a) zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran,
 - b) zakúpenie nového počítača s vyššími bezpečnostnými prvkami, inštalácia systému a obnova dát zo záloh,
 - c) zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.

4. *Krádež, alebo strata kľúčov* – môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi
 - a) okamžitá výmena zámkov, prípadne doplnenie bezpečnostných ochrán IS – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran.

5. *Strata záložných médií* – môže dôjsť k zneužitiu osobných údajov
 - a) zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

6. *Krádež záložných médií* – môže dôjsť k zneužitiu osobných údajov
 - a) zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran,

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FN sP NZ	

b) zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

Narušenie technicko-sofтверovej bezpečnosti

7. *Havárie IS spôsobené technickou chybou niektorého komponentu centrálného počítača-serveru*

a) preventívne opatrenia:

- zabezpečiť záložné zdroje s automatickým shutdownom,
- monitorovať činnosť serverov, kontrolovať chybové hlásenia,
- v serveroch používať diskové polia s hotswap diskami,
- zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať server každé tri roky,
- zachovávať pravidlo - novší server sa stáva hlavným a starší záložným
- zálohovať,

b) postup na zabezpečenie stavu obnovy:

- pri výpadku servera presmerovať prevádzku na záložný server,
- obnoviť zálohy,
- presmerovať aplikácie a užívateľov na záložný server,
- odstrániť poruchu na hlavnom serveri,
- po odstránení poruchy presmerovať prevádzku na hlavný server.


8. *Vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi*

a) preventívne opatrenia:

- zabezpečiť antivírusovú ochranu,
- inštalovať len autorizované programy oprávnenými zamestnancami,
- preverovať cudzie nosiče (FD, CD ROM, USB...),
- nepripájať nepreverené PC bez vedomia admin do LAN,
- nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN,
- neotvárať nevyžiadané e-mailové prílohy,
- sledovať aktuálne dianie na LAN a v sieti internet,

b) postup na zabezpečenie stavu obnovy:

- odpojiť každého užívateľa,
- okamžite skontrolovať aktualizácie antivírusového programu, prípadne nainštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírusový program,
- aktualizovaným antivírusovým programom vykonať kontrolu všetkých počítačov zapojených do spoločnej LAN siete,
- detekovať spôsob narušenia,
- odstrániť príčiny,
- opraviť narušenú funkčnosť,
- opätovne skontrolovať systém antivírusovým programom,
- prekontrolovať všetky PC,

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovnne manažmentu FN sP NZ	

- nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie,
- znovu spustiť systém a pripojiť užívateľov,
- nainštalovať doplnkové programy uvedených v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača.

9. *Neautorizovaný vstup z internetu* – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi

a) preventívne opatrenia:

- nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou,
- nesťahovať neautorizované programy z prostredia internetu,

b) postup na zabezpečenie stavu obnovy:


- Kontrolovať a vyhodnotiť logy súborov firewallu, routerov, antivírového programu a pod.,
- zabezpečiť súborovú integritu OS a obnovu poškodených alebo infikovaných údajov zo záloh,
- zvýšiť bezpečnosť firewallov,
- nastaviť kryptované prenosy v LAN sieti,
- pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu vstupov meno a heslo, ale prívátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite, prípadne využiť zabezpečenú VPN
- nainštalovať doplnkové programy uvedených v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača.

10. *Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS*

- pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správania je nutná výmena),
- procesor – môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena)
- CD/DVD-RW – môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade že sa zistí že na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotenú informácie, je nutná výmena zálohovacieho zariadenia),
- harddisk – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotenú údaje, je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotenú, alebo použiť dáta zo záloh),
- wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).

11. *Porucha napájania, strata dodávky elektrickej energie*

a) preventívne opatrenia:

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovnne manažmentu FNsP NZ	

- dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,
- b) postup na zabezpečenie stavu obnovy:
- v čase výpadku sa musí záložný zdroj automaticky aktivovať,
 - pri dlhodobejšom výpadku sa server musí automaticky korektné vypnúť (shutdown),
 - po nábehu elektrickej energie je nutné server spustiť a skontrolovať.


12. Porucha prostriedkov demilitarizovanej zóny

- a) preventívne opatrenia:
- monitorovať činnosť zariadení,
 - monitorovať funkčnosť všetkých zariadení,
 - zabezpečiť prístup len pre pracovníkov s oprávnením,
 - periodicky meniť administrátorské a užívateľské prístupy s heslami,
 - zabezpečiť antivírusovú ochranu všetkých PC, ako aj e-mailového prístupu,
 - zabezpečiť programovú aktuálnosť,
 - zabezpečiť technickú aktuálnosť,
 - kontrolovať súbory zaznamenávajúce činnosť systému,
 - kontrolovať súbory,
- b) v prípade narušenia:
- odpojiť LAN od prostriedkov demilitarizovanej zóny,
 - vyhľadať príčinu nefunkčnosti,
 - odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku,
 - preveriť prostriedky firewallu, prekladu adres (DNS) a proxy,
 - po otestovaní funkčnosti pripojiť LAN.

13. Porucha aktívnych prvkov siete

- a) preventívne opatrenia:
- monitorovať činnosť,
 - zabezpečiť dostatočnú kapacitu,
 - pripájať ich prostredníctvom záložného zdroja,
 - zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.
- b) postup na zabezpečenie stavu obnovy:
- vymeniť nefunkčnú časť.

14. Porucha pasívnej časti siete

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FN sP NZ	

- a) preventívne opatrenia:
- premerať kabeláž, zásuvky a konektory,
- b) postup na zabezpečenie stavu obnovy:
- opraviť, prípadne vymeniť chybnú časť.

15. Havária databáz


- a) preventívne opatrenia:
- sledovať konfiguračné súbory,
 - monitorovať hlásenia programov a včas na nich reagovať,
 - denne kontrolovať chybové hlásenia aplikácie a databázy,
- b) postup na zabezpečenie stavu obnovy:
- po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.

16. Havária aplikácie

- a) preventívne opatrenia:
- sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
 - sledovať konfiguračné súbory,
 - monitorovať hlásenia a včas na nich reagovať,
 - denne kontrolovať chybové hlásenia aplikácie.
- b) postup na zabezpečenie stavu obnovy:
- preinštalovať aplikáciu,
 - nainštalovať novšiu verziu aplikácie,
 - konzultovať chyby s dodávateľom.

17. Porucha pracovných staníc

- a) preventívne opatrenia:
- používať len autorizované programy,
 - inštalovať antivírové programy,
 - inštalovať nové programy smie len poverený zamestnanec,
 - užívatelia nesmú zasahovať do konfiguračných súborov,
 - chybové hlásenia sú povinný hlásiť správcovi systému,
 - zálohovať dáta na určené média,
 - za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec.
- b) postup pre zabezpečenie stavu obnovy:

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FNsP NZ	

- technická chyba – zabezpečiť opravu nefunkčnej časti,
- softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírusovú ochranu.

18. Narušenie dverí, okien


- preventívne opatrenia:
 - pravidelne sledovať funkčnosť aktív,
- postup pre zabezpečenie stavu obnovy:
 - neodkladne zabezpečiť opravu,
 - hľadať príčinu a odstrániť.

19. Narušenie monitorovaného objektu

- preventívne opatrenia:
 - pravidelne sledovať funkčnosť,
- postup pre zabezpečenie stavu obnovy:
 - hľadať a eliminovať príčinu narušenia.

20. Mimoriadne udalosti spôsobené vplyvom zvyškových rizík

- preventívne opatrenia:
 - zabezpečiť niekoľkonásobné záložné kópie,
 - vyhotoviť havarijné plány na zabezpečenie kontinuity činnosti,
 - kontrolovať, či sú splnené protipožiarne opatrenia,
 - kontrolovať osoby pri vstupe do budovy,
 - vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere,
 - zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov.
- v prípade vyradenia aktív IS z činnosti:
 - zvolať krízový štáb,
 - koordinovať činnosť podľa bezpečnostných záverov,
 - aktivovať záložne pracovisko,
 - skontrolovať úplnosť systému na záložnom pracovisku,
 - spustiť záložnú prevádzku,
 - odstrániť škody na pôvodnom pracovisku,
 - po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko,
- v prípade napadnutia len časti aktív IS:

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovně manažmentu FNsP NZ	

- presunúť aktíva do vyhovujúcich priestorov,
- inštalovať záložné databázy a pripojenia ak sú nutné,
- spustiť prevádzku,
- po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

Článok XVII


MINIMÁLNE POŽADOVANÉ BEZPEČNOSTNÉ OPATRENIA

- (1) Je potrebné viesť knihu návštev, v nej evidovať nasledujúce údaje: titul, meno, priezvisko, čas príchodu a odchodu, účel návštevy; údaje získať nahliadnutím (nie uschovaním do odchodu návštevy) do osobných dokladov.
- (2) Pri získaní osobných údajov zamestnancov použiť dotazník, ktorého súčasťou je dohoda, že zamestnanec je povinný oznámiť zmenu osobných údajov.
- (3) Pri automatizovanom spracúvaní osobných údajov používať programové vybavenie, ktoré vyžaduje meno a heslo používateľa.
- (4) Údaje, ktoré sa spracúvajú automatizovaným spôsobom je potrebné pravidelne zálohovať.
- (5) Osobné údaje je v závislosti od ich citlivosti potrebné pseudonymizovať a šifrovať.
- (6) Na všetkých vstupoch do automatizovaného informačného systému je nevyhnutné používať antivírusovú ochranu.
- (7) Priestory určené pre spracúvanie osobných údajov musia byť zamknuté mimo pracovnej doby, aj pri dočasnej pracovnej neprítomnosti oprávnenej osoby.
- (8) Všetci zamestnanci musia byť poučení o povinnostiach súvisiacich s ochranou osobných údajov.
- (9) Písomné dokumenty je potrebné archivovať v uzamykateľných skrinách (kovových).
- (10) Mať zaužívaný transparentný systém zaznamenávania bezpečnostných incidentov, ako aj iných otázok zo strany dotknutých osôb.
- (11) Zamestnanci, ktorí sú oprávnenými osobami, musia byť minimálne 1-krát ročne poučení.
- (12) Zamestnanci musia nepotrebné písomné dokumenty likvidovať skartovaním.

Článok XVIII

ZÁVEREČNÉ USTANOVENIA


- (1) Každý zamestnanec FNsP Nové Zámky je povinný upozorniť spracovateľa na nedostatky vo vydanom dokumente a je oprávnený vznášať spracovateľovi návrhy na zmeny.
- (2) Vydaný dokument je záväzný pre všetkých zamestnancov a všetci zamestnanci sú povinní sa preukázateľne oboznámiť s týmto dokumentom. Zodpovední vedúci zamestnanci sú povinní oboznámiť s týmto dokumentom svojich podriadených.
- (3) Za kontrolu dodržiavania tohto dokumentu sú zodpovední vedúci zamestnanci.

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

- (4) Nedodržanie ustanovení tohto dokumentu sa klasifikuje ako závažné porušenie pracovnej disciplíny s následkami podľa zákonníka práce.
- (5) Tento dokument je dostupný na intranete nemocnice.
- (6) Výnimky z tohto dokumentu podliehajú predchádzajúcemu písomnému schváleniu radou riaditeľov FNsP.
- (7) Externé strany FNsP môžu dostať výtlačok dokumentu riadenej dokumentácie po odsúhlasení štatutárnym zástupcom. V prípade rozdelenia riadenej dokumentácie v elektronickej podobe túto zabezpečuje manažér kvality.

Článok XIX SÚVISIACA DOKUMENTÁCIA

1. Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 z 27. apríla 2016
2. Zákon č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
3. Organizačný poriadok
4. Smernica o hlásení bezpečnostných incidentov a vybavovaní práv dotknutých osôb
5. Registratúrny poriadok
6. IT smernica

Číslo IRA: 2019- 13/SM_REMK	Fakultná nemocnica s poliklinikou Nové Zámky	
	Dokument 1. úrovne manažmentu FNsP NZ	

ZMENOVÝ DENNÍK

Majiteľom procesu aktualizácie tohto dokumentu je kontaktná osoba pre ochranu osobných údajov a GDPR. Zmenu definitívne schvaľuje rada riaditeľov FNsP.

Systemovú zodpovednosť za zmeny týkajúce sa tohto dokumentu/normy nesie manažér kontroly.

Spracovateľ je zároveň správca dokumentu a je zodpovedný za jeho pravidelnú trojročnú revíziu.

Revízia 1:	Revízia 2:	Revízia 3:	Revízia 4:	Revízia 5:
Dátum:	Dátum:	Dátum:	Dátum:	Dátum:
Podpis:	Podpis:	Podpis:	Podpis:	Podpis:

Por. č. vydania	Dátum platnosti nového vydania	Poznámka (základný popis, dôvod zmeny, nového vydania)

ROZDELOVNÍK

ČÍSLO VÝTLAČKU	PRIDELENÉ		DÁTUM	PODPIS
	MENO A PRIEZVISKO	FUNKCIA		
1	JUDr. Lenka HORVÁTH BODÁKOVÁ	Právnik		
2	Mgr. Michal BOJNICKÝ, MPH	Referát kontroly		
3	Ing. Ladislav ČERI, PhD.	Manažér kvality		