Na podlagi 35. člena Uredbe (EU) 2016/679 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) izvajalec zdravstvene dejavnosti \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (v nadaljevanju izvajalec) sprejme

**OCENO UČINKA V ZVEZI Z VARSTVOM PODATKOV**

**1. člen**

Ocena učinka pomeni oceno izvora, narave, posebnosti in resnosti tveganja pri obdelavi osebnih podatkov ter ukrepe za omejitev tveganja pri obdelavi osebnih podatkov.

Izvajalec izdela in sprejme Oceno učinka v zvezi z varstvom podatkov z namenom pravočasne identifikacije tveganj in z namenom sprejema ustreznih ukrepov za obvladovanje tveganj, da se v največji možni meri prepreči, da bi prišlo do kršitve zakonodaje iz področja varstva podatkov.

Ocena učinka v zvezi z varstvom podatkov je preventivni ukrep varstva osebnih podatkov za zagotavljanje načela zakonitosti in odgovornosti pri obdelavi osebnih podatkov, ki poudarja in obenem zahteva preventivno in proaktivno ravnanje upravljavcev in obdelovalcev podatkov.

**2. člen**

**1. OPIS PROJEKTA – opis predvidenih dejanj obdelave in namenov obdelave**

|  |  |  |
| --- | --- | --- |
| **Opis dejanja obdelave** | **Obrazložitev in smernice** | **V praksi izvajalca** |
| **1. nabor osebnih podatkov** | Nabor osebnih podatkov, ki se bodo obdelovali moramo čim bolj natančno določiti. Pri tem pazimo na to, da: * obdelava pomeni kakršnokoli ravnanje z osebnimi podatki,
* je osebni podatek katera koli informacija v zvezi z določenim ali določljivim posameznikom; osebni podatek se nanaša na posameznika in sicer ne glede na obliko, v kateri je izražen;
* na določljivost ne smemo gledati samo skozi naše sposobnosti, podatke in znanje – temveč tudi, ali bi kdo drug brez nesorazmerno veliko naporov, časa, ali sredstev lahko ugotovil, na koga se podatek nanaša,
* za obdelavo osebnih podatkov potrebujemo pravno podlago (zakon ali pogodba oz. izrecna in jasna privolitev posameznika).
 | Vrste osebnih podatkov, ki jih obdelujemo:* osebni podatki: ime, priimek, naslov, izobrazba, poklic, zaposlitev, drugi podatki, ki jih posreduje posameznik;
* posebna vrsta osebnih podatkov: podatki o zdravstvenem stanju posameznikov, podatek o članstvu v sindikatu, podatki v zvezi s posameznikovim spolnim življenjem in spolno usmerjenostjo, biometrični podatki za namene avtentikacije ali identifikacije posameznika
 |
| **2. namen obdelave** | * samo za namen, določen z zakonom ali izrecno privolitvijo posameznika in le za namen, za katerega so zbrani
 | * razločevati obdelavo, ki ima podlago v zakonu in podlago v osebni privolitvi posameznika
 |
| **3.zakonitost:****način in sredstva za pridobivanje in obdelavo podatkov (mediji, internet, človeški vir) in podatkovni tokovi** | Podatke pridobivamo na podlagi zakona, pogodbe ali izrecne in jasne privolitve posameznika.Za zagotavljanje zakonitosti v procesu obdelave upoštevamo: * kako se bodo osebni podatki pridobivali (iz uradnih evidenc/od posameznika/ elektronsko/na papirju/...),
* kje se bodo hranili (v informacijskem sistemu/v fasciklih/...),
* kako se bodo obdelovali (v informacijskem sistemu/ človeški vir/,…),
* komu se bodo posredovali (drugim organom/ uporabnikom/...),
* kdo bo delal z osebnimi podatki (katere osebe),
* kako bodo podatki zavarovani pred naključnimi ali namernimi zlorabami, izgubo ali uničenjem (tehnično/organizacijsko),
* kako dolgo jih bomo hranili,
* kako jih bomo po preteku obdelave uničili (komisijsko/sami/prek pogodbenega partnerja).
 | Pravna podlaga za zbiranje, hrambo ali drugo vrsto obdelave osebnih podatkov:* posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
* obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
* obdelava je potrebna za izpolnitev zakonske obveznosti upravljavca;
* obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
* obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
* obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti v primeru otrok
 |
| **3. udeleženi subjekti pri obdelavi** | * vnaprej določene osebe na podlagi zakona ali pogodbe ali notranjega akta izvajalca
 | * izvajalec ali po izvajalcu pooblaščena oseba; drugim osebam se obdelava osebnih podatkov onemogoči.
 |

**2. TVEGANJA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **vrsta tveganja** | **Verjetnost** | **resnost** | **stopnja tveganja** | **ukrep** |
| obdelava podatkov brez podlage v zakonu | majhna, ker se večina podatkov pri izvajanju dejavnosti izvajalca obdeluje na podlagi zakona  | velika; v kolikor nastopi situacija, da bi izvajalec obdeloval podatke izven namena, določenega v zakonu, so predpisane visoke globe | nizka, saj se obdelujejo podlagi podatki, ki jih posreduje posameznik  | - omejimo obdelavo podatkov,- pridobimo ustrezno obliko privolitve posameznika,- pazimo, da pravilno vnesemo podatke posameznika v računalniški sistem vodenja podatkov,- pazimo, da v pridobljene podatke vpogledamo samo v primerih, ki jih določa zakon |
| privolitev posameznika ni veljavna | majhna, ker se večina podatkov obdeluje na podlagi zakona in ni potrebna privolitev posameznika | velika, ker so izjemno visoke kazni za primer nezakonite obdelave osebnih podatkov, izven okvirjev, ki jih določa zakon ali brez privolitve posameznika | nizka, saj se obdelujejo le podatki, ki jih posreduje posameznik in za namen izvedbe zdravstvene storitve | - podrobno preverimo pogoje za veljavnosti privolitve in jih upoštevamo pri snovanju obrazca za privolitev  |
| zbrani podatki niso točni | majhna, ker se večina podatkov pri obdelavi obdeluje in zbira neposredno od posameznika  | srednja, saj se uporabljajo podatki, ki se vnašajo v računalniški sistem največkrat neposredno po pridobitvi podatka od posameznika in lahko pride do napake pri vnosu podatkov v računalniški sistem | srednja  | - ažuriramo podatke in netočne nadomestimo s točnimi – po postopku, ki zagotavlja sledljivost spremembe podatkov |
| uničenje ali izguba podatkov (listine, računalniški mediji) | majhna, ker so podatki v obliki listin shranjeni v ustreznih omarah, v zaklenjenem prostoru; podatki na računalnikih so varovani z varnostnimi kopijami  | visoka, ker izguba osebnih podatkov lahko pomeni hudo škodo za posameznika  | visoka | - dokumente listine shranjujemo v zaklenjenih, protipožarnih omarah, predalih,- podatke na računalniških in elektronskih medijih kopiramo in delamo varnostne kopije;- podatke zaščitimo pred neželjenimi izbrisi podatkov  |
| obdelava podatkov izven namena obdelave | srednja, saj so vse osebe, ki sodelujejo v procesu obdelave podatkov ustrezno poučene o pomembnosti varstva osebnih podatkov; tveganje pa kljub temu obstaja, še posebej v primerih seznanitve s posebnimi podatki javnih oseb in/ali znancev, prijateljev  | visoka, saj nenamenska obdelava osebnih podatkov pomeni hudo škodo za posameznika | srednja | - uvede se sledljivost obdelave podatkov- uvede se izobraževanje oseb, ki sodelujejo v postopku obdelave podatkov- uvede se omejitev dostopa do osebnih podatkov |
| pošiljanje podatkov po elektronski poti | srednja, saj se lahko pri posredovanju posebnih vrst osebnih podatkov uporabljajo sistemi za ustrezno kodiranje in šifriranje; verjetnost tveganja pa obstaja v primeru, da podatek v pošiljanju prestrežejo računalniški in IT strokovnjaki | visoka, saj gre za obdelavo posebnih vrst osebnih podatkov in lahko zloraba podatkov pri pošiljanju povzroči posamezniku hudo škodo | srednja | - podatke lahko šifriramo in kriptiramo-šifrirno kodo pošljemo naslovniku po drugem mediju, ne istem, po katerem pošiljamo podatek |
| sodelovanje s pogodbenimi obdelovalci osebnih podatkov | visoka, v kolikor nimamo sklenjene ustrezne pogodbe o obdelavi osebnih podatkov, s točno določenim namenom obdelave in varnostnimi ukrepi pri obdelavi | visoka, saj se s podatki lahko seznani širok krog oseb, izven nadzora in kontrole upravljavca podatkov | visoka | - sklenjena ustrezna pogodba o obdelavi podatkov z zunanjimi poslovnimi subjekti – tretjimi osebami, z določenimi ukrepi varovanja tveganj pri obdelavi osebnih podatkov  |

**3. UKREPI ZA OMEJITEV TVEGANJA (ukrepi za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostni ukrepi ter mehanizmi za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti )**

|  |  |
| --- | --- |
| **VRSTE UKREPOV** | **OBRAZLOŽITEV** |
| **ukrepi, ki prispevajo k varstvu pravic posameznika**  | * informiranje posameznika o obdelavi podatkov;
* pravica do seznanitve in prenosljivosti podatkov;
* pravica do popravka in izbrisa podatkov;
* pravica do ugovora in omejitve obdelave;
* odnosi s (pogodbenimi) obdelovalci;
* varovalke glede prenosa podatkov v tretje države;
* predhodno posvetovanje.
 |
| **ocena potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen**  | Ukrepi, ki prispevajo k upoštevanju nujnosti in sorazmernosti:* določeni, izrecni in zakoniti nameni obdelave;
* zakonitost obdelave;
* obdelava je ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki;
* upoštevana je omejitev shranjevanja – roki hrambe.

Pri zakonskih podlagah obdelave podatkov načeloma sorazmernost upošteva že zakonodajalec z vsebino zakonske določbe. Pri projektih morajo odgovorni na projektu določiti minimalni zadostni nabor osebnih podatkov, s katerim lahko dosežemo namen obdelave: * če določeni osebni podatki niso potrebni, potem naj se jih ne zbira (pogosto zadostujejo anonimizirani ali statistični podatki),
* če so osebni podatki potrebni, potem uporabiti manj občutljive/posebne od bolj občutljivih, ne zbirati več enoličnih identifikatorjev, če to ni nujno potrebno.

Nabor osebnih podatkov poskusimo skrčiti na minimum.Na sorazmernost pazimo v vseh fazah – tudi npr. pri: * oblikovanju iskalnikov (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja);
* uporabniških pravicah (ali določen uporabnik res potrebuje dostop do določenih podatkov-nivojski dostop) – več podatkov pomeni večje zahteve za sledljivost.

DOSTOP DO OSEBNIH PODATKOV: * vnaprej določeni osebi, minimalen nabor podatkov, sledljivost.

Kjer je možno - ohraniti osebne podatke pod nadzorom posameznika (npr. biometrijski vzorci in druge vrste posebnih podatkov je varneje in skladneje z načelom sorazmernosti imeti na kartici ali drugem mediju, s katerim razpolaga posameznik, ki ima pooblastila za obdelavo osebnih podatkov). Preverimo, ali lahko zmanjšamo tveganje za zlorabe in se izognemo centralizirani hrambi podatkov. |
| **preveritev pravne podlage** | Pravno podlago za obdelavo osebnih podatkov lahko daje zakon ali osebna privolitev posameznika ali pogodba. Če je pravna podlaga privolitev posameznika, moramo biti pozorni, da: * preučimo in redno spremljamo način pridobivanja, dokazovanja in preklica privolitve,
* da se kot privolitev ne šteje molk posameznika,
* da se za privolitev šteje le prostovoljna, jasna in svobodna izjava volje posameznika, da se določeni njegovi osebni podatki obdelujejo za določene namene,
* da je informiranost posameznika le predpogoj za pravno podlago, ne nadomesti pa njegove privolitve,
* da je privolitev lahko pisna, ustna ali tudi na drug način podana privolitev (npr. klik na povezavo ali gumb na spletni strani),
* da je npr. na spletnih straneh ali drugih oblikah privolitvene izjave pravilno postaviti potrditvena okenca privzeto prazna, ne pa vnaprej zapolnjena.
 |
| **preveritev pogodbene obdelave** | Če bo določena opravila nad osebnimi podatki izvajal pogodbeni obdelovalec, moramo upoštevati zahteve iz Zakona o varstvu osebnih podatkov in evropske Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov – pisna pogodba in konkretizirani postopki za zavarovanje osebnih podatkov pri pogodbenem partnerju. VEDETI MORAMO: obdelava pomeni kakršnokoli ravnanje z osebnimi podatki – tudi samo shranjevanje, pošiljanje ali uničenje podatkov se šteje za obdelavo osebnih podatkov! Pri tem je nepomembno celo, ali pogodbeni obdelovalec (ne) ve, na koga se osebni podatki nanašajo! Na pogodbeno obdelavo moramo gledati skozi oči posameznika – ali bi lahko prišlo do zlorabe osebnih podatkov pri pogodbenem obdelovalcu. Pogodbena obdelava Pogodbenega obdelovalca imamo pravico in dolžnost nadzorovati, saj gre le za našo podaljšano roko! Tako kot bi sami morali varovati osebne podatke, jih mora tudi pogodbeni obdelovalec. VEDETI MORAMO: zaposleni pri pogodbenem obdelovalcu morajo biti natančno poučeni, kaj smejo in kaj ne smejo z osebnimi podatki!  |
| **preveritev točnosti in ažurnosti** | * osebni podatki morajo biti točni in ažurni;
* pred vnosom osebnih podatkov v zbirko se lahko preveri točnost podatkov z vpogledom v osebni dokument,
* predvidene imamo postopke za dopolnitev, brisanje ali popravek netočnih in neažurnih podatkov;
 |
| **uporaba istega povezovalnega znaka** | * isti povezovalni znaki so npr.: EMŠO, davčna številka, številka zdravstvenega zavarovanja,…
* pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, sodstva, državnega tožilstva ter kazenske evidence in prekrškovnih evidenc ni dovoljena uporaba istega povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil samo ta znak;
* iskalnike in uporabo šifrantov moramo ustrezno prilagoditi.
 |
| **posredovanje** | * osebne podatke se lahko posreduje uporabnikom osebnih podatkov, ki razpolagajo z ustrezno pravno podlago., na podlagi obrazložene zahteve.
 |
| **informacijska varnost - interni akti** | Osebni podatki morajo biti med obdelavo ustrezno zavarovani s postopki in ukrepi, s katerimi preprečujemo, da bi podatki bili dostopni nepooblaščenim osebam, bili uničeni, spremenjeni ali na drug način zlorabljeni. Upoštevamo naslednje ukrepe za obvladovanje splošnih tveganj v povezavi z varnostjo podatkov:* sprejete imamo interne akte o varnosti osebnih podatkov,
* ob uvedbi novega projekta je treba posodobiti interni akt;
* s pogodbenimi obdelovalci osebnih podatkov imamo sklenjene ustrezne pogodbe,
* uporabljamo ukrepe za fizično in komunikacijsko varnost podatkov,
* podatki so šifrirani med prenosom in med hrambo,
* opredeljene in vzdrževane so pravice uporabnikov za dostop do podatkov,
* beležimo dostope do osebnih podatkov,
* udeležene osebe smo ozavestili glede zakonodaje o varstvu osebnih podatkov,
* drugo (*navedite*):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **določitev odgovornih oseb** | * določen, dokumentiran ter ažuriran mora biti nabor odgovornih oseb za posamezno zbirko osebnih podatkov ter oseb, ki imajo pooblastila za dostop do osebnih podatkov (dostopne pravice/varnostna shema).
 |
| **notranja sledljivost obdelave** | * sistem mora omogočati poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil;
* zavarovanje je potrebno in dopustno prilagoditi naravi in tveganju, ki ga prinaša obdelava določenih vrst osebnih podatkov;
* pri posebnih vrstah osebnih podatkih, pri velikih zbirkah osebnih podatkov in v primerih, kjer je tveganje za zlorabe ali »vrednost« osebnih podatkov velika, je treba slediti vsak vpogled v osebne podatke;
* posebno pozornost nameniti nadzoru sistemskih administratorjev in verodostojnosti revizijskih sledi/dnevnikov aktivnosti!
* pri zbirkah, ki se vodijo na papirju (npr. kadrovska evidenca), izvesti analizo tveganja in prilagoditi ukrepe za zavarovanje (zaklenjene omare, z omejenim dostopom za le vnaprej določene osebe).
 |
| **zunanja sledljivost obdelave (posredovanje)** | * za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni pravni podlagi
 |
| **sistem za uveljavljanje varovanja informacij** | * pri kompleksnejših projektih velja razmisliti o uvedbi celovitega in sistematičnega pristopa k varovanju informacij – uvedbi sistema za upravljanje varovanja informacij (SUVI). Priporočila podaja npr. standard ISO 27001.
 |
| **interni nadzor** | * redno izvajanje internega nadzora s preverjanjem:
* ali znamo odkriti zlorabe osebnih podatkov?
* ali znamo ločiti, če naši zaposleni uporabljajo osebne podatke za legitimne in zakonite namene, ali gre za radovednost in usluge prijateljem?
* varnost osebnih podatkov temelji tudi na ustrezni izobraženosti in ozaveščenosti zaposlenih – človeški faktor je pogost vzrok zlorab.
 |
| **evidence obdelav osebnih podatkov** | * za vsako zbirko osebnih podatkov moramo pravočasno oblikovati evidence obdelav osebnih podatkov
 |
| **videonadzor** | * tudi pri videonadzoru je pomembna sorazmernost - snemanje morda ni potrebno ves čas, področje snemanja naj se omeji samo na tista področja, kjer je to potrebno za varovanje premoženja ali ljudi;
* izognimo se snemanju na delovnem mestu, če res ni nujno potrebno – le zaradi varovanja varnosti ljudi in premoženja ali zaradi varovanja javne koristi;
* obveza po vodenju dnevnika obdelav podatkov, pridobljenih z videnodzorom;
* zbrane osebne podatke lahko obdeluje le pooblaščena oseba;
* obvestilo o videonadzoru mora biti nameščeno na način, da se posameznik seznani z videonadzorom preden stopi v območje videonadzora
 |

V \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dne 1.3.2023

IZVAJALEC