**Pojasnilo**

*Ta vzorec je pripravljen z namenom, da si lahko organizacije pri pripravi internih aktov (pravilnikov oz. politik) glede opredelitve postopkov v primeru zaznanih varnostnih incidentov, ki se lahko zgodijo na področju fizične varnosti, informacijske varnosti ali varnosti osebnih podatkov oz. posegajo na vsa ta področja, lahko pomagajo s primeri določb takšnih aktov. Vzorec je informativne narave in zavezanci se morajo zavedati, da mora biti prilagojen njihovim dejanskim okoliščinam, ki se lahko bistveno razlikujejo glede na njihovo področje delovanja in notranjo organizacijo, zato je bistveno, da se določbe internih aktov prilagodijo dejanskemu stanju zavezanca, kar vključuje tudi nekatere ključne definicije, kot so odgovorna oseba, vodstvo, pooblaščena oseba in osebe, ki so odgovorne za delovanje informacijskega sistema. Sprejem tovrstnih vzorčnih pravilnikov brez ustreznih prilagoditev dejanskemu stanju ni priporočljiv, saj morajo postopki in ukrepi za zagotavljanje varnosti osebnih podatkov ustrezati dejanskemu stanju.*

*Vzorec pokriva področje upravljanja varnostnih incidentov (fizična in informacijska varnost) in kršitev varnosti osebnih podatkov, torej na enem mestu širše področje obravnave varnostnih incidentov ter kršitev varnosti osebnih podatkov, ki so jih v določenih primerih zavezanci na podlagi 33. člena Splošne uredbe o varstvu podatkov (GDPR) dolžni sporočati nadzornemu organu (Informacijski pooblaščenec) oziroma o tem obvestiti posameznike (34. člen). Zavezanci se lahko odločijo uporabiti tudi samo tiste dele vzorca, ki se nanašajo na obravnavo kršitev varnosti osebnih podatkov – sprejem tovrstnih politik izrecno priporoča Evropski odbor za varstvo podatkov[[1]](#footnote-1).*

*Uporabniki dokumenta morajo opraviti predhodno oceno, ali so zavezanci tudi po 1. odstavku 23. člena ZVOP-2, ki določa, da se za določene informacijske sisteme smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov iz Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21; ZInfV), ki se nanašajo na izvajalce bistvenih storitev, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po ZInfV. Navedeno velja za organizacije, ki imajo informacijske sisteme, v katerih:*

* *se izvajajo obdelave osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali*
* *se obdelujejo osebni podatki več kot 100.000 posameznikov na podlagi zakona, razen obdelav osebnih podatkov iz 3. poglavja 2. dela ZVOP-2, ali*
* *upravljavec ali obdelovalec kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov, ali*
* *se obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov.*

*ZInfV zahteve glede informacijske varnosti izvajalcev bistvenih storitev ureja na naslednji način:*

* *11. člen določa varnostne zahteve,*
* *12. člen ureja zahteve glede varnostne dokumentacija in varnostnih ukrepov,*
* *13. člen ureja priglasitev incidentov nacionalnemu CSIRT (t.j. skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov).*

*V primeru, da je zavezanec organizacija, ki je zavezanec 1. odstavku 23. člena ZVOP-2, je treba pričujoči vzorec ustrezno dopolniti.*

Naziv organizacije:

Naslov:

Oznaka dokumenta:

Datum veljavnosti:

V skladu z 32., 33. in 34. členom Splošne 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) družba       (v nadaljevanju\_\_\_\_\_\_\_\_\_) sprejema naslednjo

**POLITIKO UPRAVLJANJA VARNOSTNIH INCIDENTOV IN KRŠITEV VARNOSTI OSEBNIH PODATKOV**

[**1.** **UVOD** 4](#_Toc162004190)

[**2.** **SHEMA UPRAVLJANJA VARNOSTNIH INCIDENTOV** 4](#_Toc162004191)

[**3.** **RAZVRSTITEV VARNOSTNIH DOGODKOV IN KRITERIJI** 6](#_Toc162004192)

[**4.** **POSTOPEK UPRAVLJANJA INCIDENTOV** 6](#_Toc162004193)

[4.1. ZAZNAVA, POROČANJE, ZBIRANJE INFORMACIJ, PRVA OCENA 6](#_Toc162004198)

[4.2. POSTOPKI TAKOJŠNJEGA ODZIVA ZAPOSLENIH 11](#_Toc162004199)

[**5.** **POSTOPANJE V PRIMERU KRŠITEV VARNOSTI OSEBNIH PODATKOV** 14](#_Toc162004200)

[5.1. O KRŠITVAH VARNOSTI OSEBNIH PODATKOV 14](#_Toc162004202)

[5.2. POSTOPEK OBRAVNAVE ZAZNANIH KRŠITEV VARNOSTI OSEBNIH PODATKOV 15](#_Toc162004203)

[5.3. OBVEŠČANJE INFORMACIJSKEGA POOBLAŠČENCA (33. ČLEN) 15](#_Toc162004204)

[5.4. OBVEŠČANJE POSAMEZNIKOV POOBLAŠČENCA (34. ČLEN)pooblašč16](#_Toc162004205)

# **UVOD**

Varnostni incidenti so kljub izvedenim analizam tveganja in vpeljanim ukrepom za zagotavljanje varnosti vedno možni in imajo lahko neposredne in posredne učinke na delovanje organizacije. Poleg tega se redno pojavljajo nove grožnje in odkrivajo ranljivosti informacijskih virov, česar v analizi tveganj ni mogoče vnaprej upoštevati, zato je ustrezna pripravljenost na predvidene možne incidente kakor tudi na nepredvidene dogodke z možnostjo vplivov na varnost informacij, informacijskih virov in poslovanje bistvenega pomena pri zmanjševanju škode, ki jih taki dogodki lahko povzročijo. Ustrezno upravljanje varnostnih incidentov, ki vključuje zaznavanje, obravnavanje, dokumentiranje in analiziranje varnostnih incidentov je pomemben ukrep za zagotavljanje informacijske varnosti in zagotavljanje skladnosti z zakonodajo o varstvu osebnih podatkov. Varnostni incidenti se lahko pojavijo ločeno ali skupaj na področjih fizične varnosti, informacijske varnosti ter varnosti osebnih podatkov.

**Namen dokumenta** je opredelitev pristopa in postopkov upravljanja varnostnih dogodkov in incidentov in sicer določa:

* postopek predvidevanja, ugotavljanja, poročanja in ocenjevanja varnostnih dogodkov in incidentov;
* postopek odzivanja na incidente vključno s sprejemom ukrepov za njihovo preprečevanje, zmanjšanje škode in okrevanje;
* postopek učenja na podlagi incidentov vključujoč pobude za vpeljavo preventivnih zaščit in izboljšav k sistemu varovanja in specifično vpeljavo izboljšav za upravljanje incidentov,
* postopek obravnave varnostnih incidentov, ki sodijo na področje kršitev varnosti osebni podatkov in s tem povezane dolžnosti obveščanja nadzornega organa.

**Cilji**, ki jih poskušamo doseči z upravljanjem varnostnih dogodkov in incidentov, so:

* učinkovito ugotavljanje in odločanje, ali je posamezen dogodek incident ali ne ter ukrepanje ob varnostnih dogodkih;
* ocenjevanje dogodkov in odgovarjanje na ugotovljene incidente na primeren in učinkovit način;
* čim uspešnejše zmanjševanje vplivov incidentov s pomočjo odgovora na incidente;
* ohranitev in po potrebi zavarovanje revizijskih sledi dogodkov ter dokaznega gradiva;
* zagotavljanje možnosti vpeljave ukrepov zoper kršilce v primeru resnejših incidentov,
* evidentiranje dogodkov in nastale škode;
* hitro učenje na podlagi incidentov in njihovega upravljanja;
* čim boljše preprečevanje nadaljnjih incidentov in izboljševanje upravljanja informacijske varnosti;
* zagotovitev skladnosti z zahtevami zakonodaje o varstvu osebnih podatkov glede obveznega poročanja kršitev varnosti osebnih podatkov nadzornemu organu.

# **SHEMA UPRAVLJANJA VARNOSTNIH INCIDENTOV**

Shema upravljanja varnostnih incidentov vsebuje podrobne opise postopkov upravljanja in vključuje:

* odkrivanje in poročanje o dogodkih;
* ocenjevanje dogodka in odločanje o njegovi naravi;
* odgovarjanje na incident;
* pregledovanja delovanja sheme;
* izboljševanje sheme.

Shema v **vertikalni smeri prikazuje časovno zaporedje po pojavu dogodka**, v **horizontalni pa z vertikalnimi ločnicami podaja prikaz oseb, ki pri izvajanju sheme sodelujejo**. Pravokotniki v shemi predstavljajo **postopke** v okviru upravljanja incidentov, rombi pa **odločitve**, ki potrebujejo kriterije v obliki notranjih standardov.

DOGODEK

NE

**IZBOLJŠAVE**

**INCIDENT OBVLADAN**

DA

DA

**ČAS**

**POROČANJE**

**ZAZNAVA**

*ODKRIVANJE,  
POROČANJE*

VODSTVO

EKIPA ZA ODZIV

EKIPA ZA ODZIV

UPORABNIK, VIR

NE

DA

NE

**RELEVANTNOST**

**DRUGA OCENA**

**RELEVANTNOST**

**ZBIRANJE   
INFORMACIJ**

**PRVA OCENA**

*OCENA,  
ODLOČANJE*

**KRIZNO VODENJE**

*ODGOVOR*

**KOMUNIKACIJE**

**ANALIZA**

**TAKOJŠNJI ODZIV**

**KASNEJŠI ODZIV**

**PREGLED**

**LAŽNI ALARM**

# **RAZVRSTITEV VARNOSTNIH DOGODKOV IN KRITERIJI**

Vsi zaposleni morajo biti sposobni prve ocene, ali gre za varnostni dogodek ali ne. **Med varnostne dogodke**, glede na specifike pooblastil, lokacije in uporabljenega fizičnega in tehničnega okolja organizacije **sodijo predvsem naslednji dogodki**:

* okvara električne napeljave,
* nenadzorovano puščanje vode v prostorih organizacije,
* razbita ali poškodovana okna ali vrata,
* proženje požarnega alarma,
* proženje alarma proti vlomu,
* pojav dima,
* poškodovanje, izguba ali tatvina opreme,
* vstop nepooblaščene osebe,
* fizične ali verbalne grožnje zaposlenim,
* neobičajne motnje pri delovanju organizacije,
* pomote pri posredovanju izhodne pošte, podatkov in druge komunikacije,
* izguba podatkov v fizični ali elektronski obliki,
* izguba nosilcev podatkov (USB ključ, prenosni disk, CD/DVD mediji ipd.),
* nepooblaščen dostop do informacijskih virov,
* prisotnost sumljivih ali neznanih predmetov,
* prisotnost škodljive ali nenamenske programske kode (virusi, črvi, trojanski konji ipd.).

# **POSTOPEK UPRAVLJANJA INCIDENTOV**

Ko se potrdi, da je dogodek incident, se je treba nanj ustrezno odzvati. Odziv poteka po shemi upravljanja incidentov.



# **ZAZNAVA, POROČANJE, ZBIRANJE INFORMACIJ, PRVA OCENA**

Varnostne dogodke zaznavajo zaposleni, ki opazijo razloge za zaskrbljenost tako na informacijskem področju kot tudi v zvezi s fizičnim varovanjem in kršitvami pravil organizacije. Zaznava lahko poteka tudi preko tehničnih naprav, kot so telefoni, detektorji požara ali alarmi, in avtomatično s pomočjo programske opreme, ki sporoča dogodke in napake. Zaposleni morajo biti dobro seznanjeni s postopki, tako da poročanje poteka nemoteno in učinkovito.

**Vsi zaposleni morajo zaznavo prepoznati in poročati o dogodku.** Poročanje poteka **ustno ali na elektronski naslov**, **poročilo o dogodku mora vsebovati**:

* datum in čas zaznave dogodka,
* identifikacijo osebe, ki je zaznala dogodek,
* kratek opis dogodka,
* čas in datum ter lokacijo dogodka,
* opis že sprejetih ukrepov za omejitev posledic dogodka,
* podatek o tem, kdo in kdaj je bil obveščen o dogodku,
* druge relevantne okoliščine dogodka.

Kadar je v dogodku vsebovana ranljivost (npr. obstoj virusa), zaposleni nikakor ne smejo poskusiti izkoristiti te ranljivosti (na primer z namenom, da jo dokažejo), temveč le prijavijo ranljivost oziroma sum nanjo.

Pri poročanju je pomembna tako **natančnost** kot tudi **pravočasnost**. Boljše je podati nepopolno poročilo in ga kasneje dopolniti, kot odlašati s poročilom.

Prejemniki obvestila o dogodku morajo **potrditi njihov sprejem**, jih zabeležiti na **skupno mesto v evidenco varnostnih incidentov** in jih **pregledati**.

Skupno mesto za evidentiranje poročil je \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Evidenca poročil vključuje najmanj:

* vrsto incidenta,
* datum, čas in kraj incidenta,
* vzrok incidenta,
* opis in vsebino prijave incidenta,
* izvedene ukrepe v zvezi z incidentom (kdo, kdaj in kako je ukrepal).

**Tudi če je dogodek označen kot lažni alarm, je potrebno pripraviti zapise o dogodku za evidenco.** Če je očitno, da je dogodek resen incident glede na sprejete kriterije, lahko osebje v skladu s postopki sproži ukrepe za blaženje posledic in stopnjuje dogodek z obveščanjem osebja za odziv v stiski.

Mogoča je tudi anonimna prijava varnostnih dogodkov, kar je še posebno pomembno pri prijavi kršitev notranjih pravil.

**PRVA OCENA**

**Odgovorne osebe za izvedbo prve ocene so[[2]](#footnote-2):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | DELOVNO MESTO | TELEFON | E-POŠTA |
| PODROČJE **FIZIČNE VARNOSTI** |  |  |  |
| PODROČJE **INFORMACIJSKE VARNOST**I |  |  |  |
| PODROČJE **VARSTVA OSEBNIH PODATKOV[[3]](#footnote-3)** |  |  |  |

1. **Zaposleni, ki zazna DOGODEK S PODROČJA FIZIČNE VARNOSTI** (vlomi, razbitja, tatvine, poškodovanja opreme ipd.), je dolžan o dogodku obvestiti **odgovorno osebo za področje fizične varnosti** in sicer ustno ali na elektronski naslov.

*PRIMER*: Zaposleni ugotovi, da je nekdo ponoči razbil steklo v njegovi pisarni. Zaposleni o tem obvesti \_\_\_\_\_\_\_\_\_\_\_\_, ki izvede prvo oceno in po potrebi drugo oceno.

1. Zaposleni, ki zazna **DOGODEK S PODROČJA INFORMACIJSKE TEHNOLOGIJE** (e-pošta, informacijski sistemi, aplikacije, delovne postaje, telefoni, podatki ipd.) mora to takoj sporočiti **informatiku** in sicer ustno ali na elektronski naslov**.** Informatik mora o prejemu obvestila o dogodku obvestiti **odgovorno** **osebo za področje informacijske varnosti.**

*PRIMER*: Zaposleni ugotovi, da je bilo e-sporočilo poslano na napačen e-naslov. Zaposleni o tem obvesti informatika, ki izvede prvo oceno in o tem obvesti osebo, ki je odgovorna za informacijsko varnost:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, ki po potrebi izvede drugo oceno.

1. Če je podana verjetnost, da je **DOGODEK OGROZIL VARNOST OSEBNIH PODATKOV**, se ukrepa skladno z določili **5. poglavja** te politike. Ob zaznani kršitvi oseba, ki zazna kršitev, obvesti **pooblaščeno oz. odgovorno osebo za področje varstvo osebnih podatkov,** ta pa oceni tveganja za nastanek posledic

*PRIMER*: Zaposleni prejme e-sporočilo, da je bila odtujena baza strank, ki vključuje tako pravne kot fizične osebe. Izsiljevalska organizacija predloži vzorec podatkov, s katero izkazuje resničnost navedb in zahteva odškodnino za vračilo podatkov. Zaposleni obvesti pooblaščeno osebo za varstvo osebnih podatkov, ki izvede prvo oceno.

Prva ocena se izvaja glede na pripravljen seznam možnih dogodkov, izvede jo prejemnik obvestila o dogodku. Pri neznanih dogodkih se prejemnik obvestila o dogodku sam odloči o nujnosti takojšnje druge ocene.

Pri ocenjevanju relevantnosti dogodkov se pri prvi oceni najprej poda **ocena relevantnosti**, ki ima lahko zaključka:

* dogodek zagotovo **nima vpliva na poslovanje** ali
* dogodek lahko **ima vpliv na poslovanje**, zato je potrebna še druga **podrobnejša** **ocena** (predvideva se, da je dogodek incident in spada v enega od razredov opisanih spodaj od E do A); nadalje se v tem primeru oceni, če je potrebno drugo oceno:
* napraviti takoj in ustno obvestiti ustreznega zaposlenega ali
* lahko ocena počaka nekaj časa, na primer do začetka rednega delovnega časa, in je obvestilo zgolj pisno po elektronski pošti.

**DRUGA OCENA**

Drugo oceno za:

* dogodke **fizične narave** opravlja \_\_\_\_\_\_\_,
* za **dogodke s področje informacijskih tehnologij** pa:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Druga ocena poda **natančnejšo razvrstitev dogodka** in **po potrebi nadalje stopnjuje odziv na dogodek**. Pri razvrstitvi uporablja zgornjo tabelo in seznam predvidenih incidentov (na primer požar, poplava, grožnja z bombo itd.) s smernicami za ukrepanje in takojšnjim odzivom v stiski, če je ta potreben.

V drugi ocena se lahko oceni dogodek za ne relevantnega ali pa označi dogodek za incident, ga razvrsti v enega od razredov in na tej podlagi sproži potreben odziv.

Incidente razvrščamo v 5 razredov:

|  |  |
| --- | --- |
| **Razred** | **Opis razreda** |
| **E** | Incident, ki ne predstavlja resne grožnje za nadaljevanje poslovanja, ne zahteva takojšnjega odziva in samostojne analize, vendar ga je smiselno zabeležiti zaradi sledljivosti in statistike. |
| **D** | Incident, ki ne predstavlja resne grožnje za nadaljevanje poslovanja, takojšnji odziv ni potreben, a je smiselno analizirati vzroke za njegov nastanek. |
| **C** | Incident, ki lahko zaustavi del poslovanja, povzroči gmotno škodo in večje dodatne interne stroške, ima potencialni vpliv zakonske in pogodbene obveznosti ali ugled organizacije, potreben je takojšnji odziv. |
| **B** | Incident, ki je zaustavil poslovanje ali njegov del, pričakuje se velika škoda, čas prekinitve lahko postane daljši od sprejemljivega. |
| **A** | Incident, ki očitno prekinja celotno poslovanje organizacije in huje ogroža zdravje in življenja ljudi. |

Vsak razred zahteva svoj odziv, ki je definiran v postopkih sheme upravljanja incidentov.

Izvajalec druge ocene **z drugo oceno seznani vodstvo.**

Po takojšnjem odzivu, kadar se izvede, in izvedenih predvidenih ukrepih, je potrebno ugotoviti, ali je situacija pod nadzorom oziroma obvladovana. Kriteriji za odločitev, da je dogodek obvladovan, so izpolnjeni, ko so v situaciji dani vsi naslednji pogoji:

* dogodek nima več vpliva na poslovanje, odziv v stiski, če je bil začet, je bil uspešen;
* poslovanje se bo normalno nadaljevalo in čas prekinitve ne bo daljši od ciljnega časa okrevanja poslovno kritične funkcije, kjer se je incident zgodil;
* potrebne sledi poteka dogodka so ustrezno zavarovane, forenzične aktivnosti so v toku ali zaključene, potrebno komuniciranje se zaključuje;
* ustrezno poročilo o dogodku je možno dokumentirati.

**Takojšnji odziv**

Glavne naloge ekipe za odziv so:

* ugotovitev potrebnih takojšnjih ukrepov, pri čemer se ekipa opre na pripravljene scenarije, ki se jih ustrezno prilagodi,
* zbiranje in dokumentiranje čim relevantnejših podatkov o incidentu,
* izvedba ukrepov s pomočjo predvidenega osebja.

Ukrepi so lahko začasni ali stalni.

**Kasnejši odziv**

Če je dogodek obvladovan in s tem ni potrebe po kriznem vodenju, potem so na vrsti kasnejši odzivi na incident. Ti vključujejo vračanje v normalno poslovanje, zaključevanje poročil o incidentu in obveščanje vpletenega osebja o zaključku aktivnosti v zvezi z incidentom.

Včasih je treba izvesti aktivnosti, ki bodo preprečevale ponovitev incidenta. To lahko, na primer, zahteva namestitev potrebnih programskih popravkov na informacijski opremi ali zamenjavo gesel ali pa izključitev nekaterih servisov opreme.

V določenih primerih se za potrebno izkaže dodatno spremljanje dogajanja na informacijski opremi, omrežju ali servisih, da bi se čim hitreje zasledilo podobno sumljivo dogajanje.

V določenih primerih je treba ponovno vzpostaviti delovanje informacijske opreme, ki mora nadaljevati svoje operacije na varen način, kar lahko vključuje inštalacijo popravkov, izključevanje delov sistema, ki jim ne moremo zagotoviti varnega poslovanja ali pa ponovno zgraditev sistema od začetka, če so sledi v zvezi z incidentom izbrisane in je situacija nejasna.

**Forenzična analiza**

Forenzična analiza se izvede, če se pokaže za tem potreba v toku prejšnjega ocenjevanja. Izvaja se pri vseh incidentih s pomočjo zunanjih strokovnih služb (policija, kriminalistična služba), z notranjimi viri pa se delno izvaja predvsem v okviru informacijske tehnologije. Opis v nadaljevanju je namenjen v glavnem izvajanju analize z notranjimi viri.

Uporabljajo se tehnike in orodja, ki so podprta z ustreznimi navodili za izvajanje, z namenom zavarovati dokaze in poglobiti poznavanje incidenta in njegovega ozadja. Preiskava in analiza mora potekati urejeno, pri tem pa je potrebno ugotoviti, kaj se lahko uporabi za dokaz:

* za interne disciplinske postopke,
* za potrebe sodnega pregona,
* za pogajanja o nadomestilu škode z dobavitelji opreme in izvajalci storitev.

Sredstva za izvajanje forenzične analize predstavljajo postopki, osebje, tehnična sredstva in oprema za varovanje prostorov. **Vse aktivnosti morajo biti v celoti dokumentirane**, **kar lahko vključuje fotografije, poročila o analizi revizijske sledi, zapise beleženja in podobno**. Vse zbrane zapise o incidentu, vključno z rezultati forenzične analize, je treba fizično varovati, tako da nepooblaščene osebe do njih ne morejo dostopati in jih na kakršenkoli način spremeniti. Tehnična sredstva in druga oprema morajo biti skladna z aktualnimi standardi in tehnološkim razvojem, tako da se jim na sodišču iz tega razloga ne da oporekati oziroma zmanjševati dokazno vrednost.

**Komunikacije z osebjem in tretjimi strankami**

V okviru obvladovanja incidenta prihaja na mnogih točkah do potrebe po komuniciranju bodisi interno bodisi z zunanjim svetom in tiskom. Te točke so lahko na primer: odločitev, da je dogodek incident, ali je ta obvladan, ali se sproži krizno vodenje, ali so sprejeti zaključki po analizi in učenju na podlagi incidenta in podobno. Način in obseg komunikacije z zaposlenimi in tretjimi osebami, glede na potrebe po komuniciranju, določi organizacija vsakič sproti.

**Sledljivost aktivnosti, zavarovanje dokazov**

Za potrebe poznejše analize je potrebno sproti beležiti vse aktivnosti v okviru obvladovanja incidenta. Vse prijave in analize se zbira in vodi na enem mestu, ki mora biti ustrezno rezervno kopirano. Skupno mesto za evidentiranje poročil je \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Ekipa za odziv na incidente**

Cilj delovanja ekipe za odziv na incidente je učinkovito in pravočasno odgovoriti na varnostne dogodke in incidente, tako da ti v čim manjši meri vplivajo na poslovanje organa. V pristojnosti ekipe so vsi incidenti torej predvideni in nepredvideni. Ekipo za odziv na incidente sestavlja glede na rezultate druge ocene sproti določi vodstvo.

**Pravni vidiki**

V primeru, da ima lahko varnostni dogodek pravne posledice za organizacijo ali zaposlene, mora ekipa za odziv obvestiti vodstvo. Če je podana verjetnost, da je dogodek ogrozil varnost osebnih podatkov, se ukrepa skladno z določili 5. poglavja te politike.

**Ozaveščanje in izobraževanje**

Ker so zaznave in prijave incidentov nujno povezane z vsemi zaposlenimi, morajo biti te primerno seznanjeni s politiko in postopki sheme upravljanja incidentov. Splošno seznanjanje je potrebno tudi za vse novo zaposlene takoj po pričetku opravljanja poslovnih dejavnosti, usmerjeno izobraževanje za člane ekipe za odziv na incidente pa glede na njihove vloge v ekipi. Seznanitve morajo med drugim vsebovati opise:

* delovanja sheme za upravljanje incidentov,
* poročanja o varnostnih dogodkih,
* zaščite identitete osebja, ki poroča, če je to potrebno,
* predvidenih odzivnih časov,
* načina obveščanja o rezultatih prijav,
* morebitnih omejitev zaradi veljavnih sporazumov o varovanju poslovnih skrivnosti z zunanjimi strankami,
* organizacije ekipe za odziv na incidente in njeno poročanje,
* upravljanja poročil in zapisov, ki nastanejo pri delovanju sheme.

Z določili o prijavi dogodkov in načinom prijave dogodkov morajo biti na primeren način seznanjene tudi zunanje stranke (zunanji izvajalci, poslovni partnerji, ...). Za to so odgovorne, ki pokrivajo odnose s posameznimi zunanjimi strankami, tako da je odgovoren vsak za svoje stranke.

# **POSTOPKI TAKOJŠNJEGA ODZIVA ZAPOSLENIH**

**1. Požar, eksplozija**

Zaposleni ukrepajo v skladu s Požarnim redom organizacije.

**2. Potres**

|  |
| --- |
| **Vsi zaposleni** |
| * Zaklonite se pod mizo ali stojte oziroma sedite ob notranjem nosilnem zidu ali pod podbojem; izogibajte se bližini oken, ne uporabljate dvigal in ne tecite na prosto. * Trdno se držite mize, dokler potresni sunek ne preneha. * Odmaknite se od oken ali predmetov, ki bi lahko padli na vas. * Ne tecite ven med potresnim sunkom. * Izogibajte se uporabi telefona (telefonske slušalke, ki jih je tresenje vrglo z vilic, vrnite nanje). * Ne uporabljajte odprtega ognja. * Po sunku rešujte človeška življenja, če so ogrožena. * Če je ukazana evakuacija, nadaljujte po scenariju za evakuacijo. |

**3. Izliv vode, poplava**

|  |
| --- |
| **Vsi zaposleni** |
| * Takoj izključite opremo v območju vode z vira napajanja z energijo; če je vir vode nad napravo in če je le mogoče, jo pokrijte z vodo-odpornim materialom. * Nadzorujte stanje in ubežne poti, da se lahko umaknete. * Če je varno, primerno in možno, umaknite naprave iz dosega vode. * Izklopite električno napajanje in naprave v vašem dosegu, če je poplava neizbežna. * Obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. |

**4. Vlom**

|  |  |
| --- | --- |
| **Vsi zaposleni** | |
| * Če na kraju vloma ni varnostne službe ali policije, takoj pokličite varnostno službo in ukrepajte po njihovih navodilih. * Ko je varno in če varnostna služba ali policija še ni na mestu vloma, zavarujte mesto incidenta in ogroženo opremo: * zaprite neposredno okolico in ne spreminjajte ničesar na kraju vloma, * zavarujte sledi (npr. prstne odtise, odtise obuval,…), * zavarujte vredne stvari. |

**5. Grozilno pismo**

|  |
| --- |
| **Vsi zaposleni** |
| * Če prejmete grozilno pismo in ga kot takega spoznate, se ga zaradi zavarovanja sledi ne dotikajte več, kot je nujno potrebno, temveč ga takoj vložite v prozoren ovoj (mapo). * O prejemu takoj obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. |

**6. Grozilni telefonski klic, grožnja s podtaknjeno bombo, sumljiv predmet**

|  |
| --- |
| **Vsi zaposleni** |
| *Grozilni telefonski klic* |
| * V primeru grožnje po telefonu si zabeležite natančen čas in če je možno, izvorno številko klica; ugotovite, če klic izvira od znotraj ali od zunaj * Zabeležite si natančne besede kličočega; dovolite kličočemu, da pove čim več, brez prekinitve: * klicatelja poskusite zaplesti v pogovor, * vedno znova postavljajte vprašanja, pri čemer recite, da niste razumeli, * če ima vaš telefon napravo za dodatno poslušanje (npr. slušalke ali zvočnik), z rokami signalizirajte sodelavcu, naj posluša pogovor in dela zabeležke, * klicatelju morate dati občutek, da se zavedate resnosti položaja, in obljubite, da boste razmislili o njegovih zahtevah, * ponovite vsako navodilo, ki vam ga da, tako da bo vedel, da ste razumeli; čim bolj natančno si zapišite: * vsebino pogovora, * višino, barvo in morebitne posebnosti glasu (tuj naglas, narečje; moški, ženski, otroški glas; globok, visok, hropeč, piskajoč, mehak, vznemirjen, jezen, jecljav, pogrkujoč, prestrašen glas) * kakršen koli hrup v ozadju (zvoki predmetov, ropot strojev, glasba, zvok letala ali vlaka, govorica v lokalu in podobno), * vse ostalo, kar vzbudi vašo pozornost. * Obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. * **V primeru grožnje s tempirano bombo vprašajte kličočega (odgovore zabeležite):** * ali bo eksplodirala, * kje je locirana, * kako izgleda, * zakaj je bila nastavljena, * kdo kliče. * Čimprej pripravite snemalno napravo ali magnetofon za morebitne nadaljnje klice. * Obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. * Preprečujte paniko – delujte umirjeno, a brez nepotrebnega zavlačevanja. * Zavarujte zbrano in prepoznano dokazno gradivo. * Pripravite se za možno evakuacijo in v primeru grožnje z bombo upoštevajte: * če je le možno, vrata premikajte samo, če je mogoče videti, da na kljuko ali druge dele niso povezane žice ali vrvice. * Če je ukazana evakuacija, nadaljujte po scenariju za evakuacijo. * V primeru prihoda preiskovalcev jim lahko pomagate z informacijami o prostorih in zgradbi. |
| * **Sumljiv predmet, pisemska bomba** * Kakršnekoli neznane posode, aktovke, škatle ali zavoje pustite, kjer so; njihovo odstranitev prepustite strokovnjakom.   Obvestite:odgovorno osebo za upravljanje varnostnih incidentov,   * svojega nadrejenega delavca. * Preprečujte paniko – delujte umirjeno, a brez nepotrebnega zavlačevanja. * Preprečujte dostop do sumljivega predmeta do prihoda policije, če je možno, izza zaklona. |

**7. Nasilna oseba, streljanje, kraja**

|  |  |
| --- | --- |
| **Vsi zaposleni** | |
| *Nasilna oseba* |  |
| * Če odkrijete nasilno tujo osebo ali zaposlenega, takoj obvestite varnostno službo in jim čim bolje opišite dogajanje; če osebe ne poznate, poskušajte sporočiti njegov opis, kamor spada: * višina, * teža, * barva las, * tip in barva oblačil in obutve * posebnosti. * Obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. | |
| *Streljanje* |  |
| * Če zaslišite strele v zgradbi: * zaprite, zaklenite in zabarikadirajte vrata sobe, * ugasnite luči, * pomirite sodelavce in ostanite vsi čim tišji, * ostanite v prostoru, dokler vas ne obvesti policija, da je to varno, * ne sprožite požarnega alarma, * ne evakuirajte se, razen če ste prav v prostoru, kjer se strelja. | |
| *Kraja* |  |
| * Tatvino oziroma krajo takoj prijavite: * odgovorni osebi za upravljanje varnostnih incidentov, * svojemu nadrejenemu delavcu. | |

**8. Resne telesne poškodbe in bolezni**

|  |
| --- |
| **Vsi zaposleni** |
| * Pokličite reševalno službo na telefon 112 in javite: * vaše ime, organizacijo, * opis poškodbe ali bolezni, * ocenjeno število prizadetih, * vašo lokacijo, * ostalo pomembno za situacijo in ostanite na zvezi, dokler je operater na drugi strani ne prekine. * Obvestite: * odgovorno osebo za upravljanje varnostnih incidentov, * svojega nadrejenega delavca. * Ostanite pri žrtvi oziroma: * zagotovite, da se žrtev ne premika (razen v primeru zaščite pred dodatnimi tveganji), * pridobite potrebne informacije o stanju žrtve, povezanih preteklih dogodkih in njenih posebnih potrebah. | |
| * Vsi, ki niste povezani z nujnim primerom, ostanite zunaj področja. | |

# **POSTOPANJE V PRIMERU KRŠITEV VARNOSTI OSEBNIH PODATKOV**



# **O KRŠITVAH VARNOSTI OSEBNIH PODATKOV**

Splošna uredba o varstvu podatkov (GDPR) je uvedla **dolžnost obveščanja nadzornega organa** (Informacijskega pooblaščenca) o zaznanih kršitvah varnosti osebnih podatkov, če je verjetno, da bi bile s kršitvijo **ogrožene pravice in svoboščine posameznikov**. Obvestilo nadzornemu organu (angl. *data breach notification* – DBN) je treba podati takoj po zaznani kršitvi, najkasneje pa **v 72 urah**.

**Kršitev varnosti osebnih podatkov** v smislu 33. in 34. člena Splošne uredbe **pomeni kršitev, ki vodi do nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja oziroma dostopa ali nedostopnosti osebnih podatkov**, torej kršitev načel celovitosti, zaupnosti ali razpoložljivosti osebnih podatkov. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev pomeni (realiziran) varnostni incident, ki ogroža zaupnost, celovitost ali razpoložljivost osebnih podatkov.

**Primeri kršitev varnosti osebnih podatkov** so npr.:

* dostop do osebnih podatkov s strani nepooblaščene osebe;
* posredovanje osebnih podatkov nepravemu naslovniku;
* izguba ali kraja računalniške opreme, ki vsebuje osebne podatke;
* nepooblaščeno uničenje baz z osebnimi podatki;
* sprememba osebnih podatkov brez potrebnega dovoljenja;
* izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t.i.  kripto ali izsiljevalski virusi).

**Podrobnejši seznam primerov kršitev** je na voljo v **smernicah Evropskega odbora za varstvo osebnih podatkov** (EDPB: *Smernice 01/2021 o primerih v zvezi z uradnim obveščanjem o kršitvah varstva osebnih podatkov*) na naslovu:

<https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_sl.pdf>

Glede na določbe smernic EDPB sta za upravljavce in obdelovalce bistvena tudi **usposabljanje in ozaveščanje zaposlenih o vprašanjih varstva podatkov s poudarkom na obvladovanju kršitev varnosti osebnih podatkov** (prepoznavanje incidenta kršitve varnosti osebnih podatkov in nadaljnji ukrepi, ki jih je treba sprejeti, itd.), zato **pooblaščena oziroma odgovorna oseba za varstvo podatkov vsaj enkrat letno izvede ozaveščanje zaposlenih glede določb te politike**.

# **POSTOPEK OBRAVNAVE ZAZNANIH KRŠITEV VARNOSTI OSEBNIH PODATKOV**

V primeru zaznave kršitve je treba oceniti **verjetnost in resnost posledic** za pravice in svoboščine posameznikov. **Verjetnost je povezana z možnostjo nastanka posledic, resnost pa s škodo, ki jo kršitev lahko povzroči posameznikom.**

Kršitev varnosti osebnih podatkov, ko se ne obravnavajo ustrezno in pravočasno lahko posameznikom povzroči fizično, premoženjsko ali nepremoženjsko škodo, kot je izguba nadzora nad njihovimi osebnimi podatki ali omejitev njihovih pravic, diskriminacija, kraja ali zloraba identitete, finančna izguba, neodobrena reverzija psevdonimizacije, okrnitev ugleda, izguba zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo, ali katera koli druga znatna gospodarska ali socialna škoda. **Kršitev varnosti osebnih podatkov ima lahko resne posledice tudi za organizacijo v obliki izgube zaupanja in dobrega imena, popravljalnih ukrepov in denarnih kazni.**

**Ob zaznani kršitvi oseba, ki zazna kršitev, obvesti pooblaščeno osebo za varstvo podatkov, ta pa oceni tveganja za nastanek posledic.** Pooblaščena oz. odgovorna oseba za varstvo osebnih podatkov mora izvesti oceno, ali je potrebno obveščanje nadzornega organa in ali posameznikov.

Od te ocene je odvisno, ali bo treba o kršitvi obvestiti:

* nadzorni organ za varstvo osebnih podatkov (Informacijskega pooblaščenca) in/ali
* je treba obvestiti tudi prizadete posameznike.

# **OBVEŠČANJE INFORMACIJSKEGA POOBLAŠČENCA (33. ČLEN SPLOŠNE UREDBE)**

Obveščanje Informacijskega pooblaščenca **brez odlašanja, najkasneje pa v 72 urah** po zaznani kršitvi izvede **pooblaščena oseba za varstvo podatkov** ali **za to posebej določena oseba** in sicer s pomočjo **obrazca *»Obrazec - Uradno obvestilo o kršitvi varnosti osebnih podatkov (člen 33 Splošne uredbe)«****,* ki je dostopen na[[4]](#footnote-4):

<https://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/>

V primeru, da ima kršitev varnosti osebnih podatkov **čezmejne komponente** (npr. da se nanaša na osebe izven RS), **se izpolni in posreduje tudi priloga**, ki je dostopna na:

<https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/Priloga%202%20-%20Cezmejna%20krsitev%20varnosti%20OP.docx>.

Obveščanje nadzornega organa se izvede **po elektronski pošti na naslov:** [**gp.ip@ip-rs.si**](mailto:gp.ip@ip-rs.si)**.**

Tudi ko ni verjetno, da bodo pravice in svoboščine ogrožene, se vse zaznane kršitve dokumentirajo, kakor tudi morebitni razlogi za zamudo pri podaji popolnega obvestila o kršitvi.

Skupno mesto za evidentiranje poročil je: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

# **OBVEŠČANJE POSAMEZNIKOV POOBLAŠČENCA (34. ČLEN SPLOŠNE UREDBE)**

Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči **veliko tveganje za pravice in svoboščine posameznikov**, Splošna uredba o varstvu podatkov zahteva, da upravljavec o kršitvi neposredno obvesti **zadevne posameznike** in da to stori brez odlašanja (člen 34).

Za obveščanje posameznikov Splošna uredba postavlja standard 'veliko tveganje', ki je višja stopnja ogroženosti pravic in svoboščin posameznikov, kot velja za uradno obvestilo nadzornemu organu. Kot je že bilo poudarjeno, je treba stopnjo tveganja ocenjevati v vsakem primeru posebej, upoštevaje verjetnost nastanka posledic in resnost teh posledic. Treba je zlasti upoštevati, da je potreba po obveščanju večja, če obstaja velika verjetnost neugodnih posledic, pri tem pa lahko ukrep obveščanja zmanjša tveganje za nastanek teh posledic. Cilj in smoter zahteve po obveščanju posameznikov o kršitvi je prav v možnosti zmanjševanja tveganj za nastanek neugodnih posledic. Na ta način se torej pomaga posameznikom preprečiti neugodne posledice, ki bi sicer lahko pomenile tudi premoženjsko ali nepremoženjsko škodo (upravljavec je lahko odškodninsko odgovoren poleg sankcij, ki jih lahko izreče nadzorni organ). **Oceno, ali je potrebno izvesti obveščanje posameznikov, poda pooblaščena oseba za varstvo podatkov.**

Predlog o obveščanju posameznikov, ki vsebuje besedilo ter način obveščanja, sprejme **pooblaščena oseba za varstvo osebnih podatkov** ali **za to določena oseba**. **Predlog mora potrditi vodstvo**. Neupravičeno, nepotrebno ali napačno obveščanje posameznikov ima lahko velik negativen vpliv na zaupanje in dobro ime organizacije ter negativen vpliv na posameznike, zato mora biti odločitev o tovrstnem obveščanju sprejeta na podlagi vseh potrebnih informacije in s podrobnim premislekom.

Obvestilo posameznikom mora biti v **jasnem in preprostem jeziku**. V obvestilu se opiše kršitev in sporoči vsaj:

* kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov (ali druge kontaktne osebe), pri kateri lahko posameznik prejme več informacij oziroma pojasnil o kršitvi,
* informacijo o posledicah,
* informacijo o sprejetih ali predlaganih ukrepih in kjer je to mogoče, dodatna pojasnila posameznikom, kako lahko sami zmanjšajo tveganje za nastanek posledic.

Posameznike se obvesti neposredno ( z uporabo razpoložljivih kontaktov), le izjemoma, ko bi to zahtevalo nesorazmeren napor, se obveščanje izvede z javnim sporočilo na predlog pooblaščene osebe za varstvo podatkov in **po odobritvi vodstva**.

1. Glej točko 13 na str.7: <https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_sl.pdf> [↑](#footnote-ref-1)
2. V zelo majhnih organizacijah, kjer ni druge možnosti, gre lahko tudi za isto osebo. [↑](#footnote-ref-2)
3. Tudi če organizacija nima uradno imenovane pooblaščene osebe za varstvo osebnih podatkov (t. i. DPO) glede na določbe Splošne uredbe in ZVOP-2 je priporočljivo, da vseeno vnaprej opredeli vsaj osebo, ki je odgovorna za osebne podatke v smislu enotne točke. [↑](#footnote-ref-3)
4. Obrazec formalno ni obvezen, je pa priporočljiv. [↑](#footnote-ref-4)