**18/SL**

**WP250rev.01**

**Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679**

**Sprejete 3. oktobra 2017**

**Kot so bile nazadnje revidirane in sprejete 6. februarja 2018**

**DELOVNA SKUPINA ZA VARSTVO POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV,**

ustanovljena z Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995, je –

ob upoštevanju členov 29 in 30 Direktive,

ob upoštevanju svojega poslovnika –

**SPREJELA NASLEDNJE SMERNICE:**

Vsebina

[UVOD 5](#_Toc521571116)

[I. Obveščanje o kršitvi varnosti osebnih podatkov na podlagi SUVP 6](#_Toc521571117)

[A. Osnovni varnostni preudarki 6](#_Toc521571118)

[B. Kaj je kršitev varnosti osebnih podatkov? 7](#_Toc521571119)

[1. Opredelitev 7](#_Toc521571120)

[2. Vrste kršitev varnosti osebnih podatkov 7](#_Toc521571121)

[3. Morebitne posledice kršitve varnosti osebnih podatkov 9](#_Toc521571122)

[II. Člen 33 – Obvestilo nadzornemu organu 10](#_Toc521571123)

[A. Kdaj je potrebno obvestilo? 10](#_Toc521571124)

[1. Zahteve iz člena 33 10](#_Toc521571125)

[2. Kdaj je upravljavec „seznanjen“? 10](#_Toc521571126)

[3. Skupni upravljavci 13](#_Toc521571127)

[4. Obveznosti obdelovalca 13](#_Toc521571128)

[B. Zagotavljanje informacij nadzornemu organu 14](#_Toc521571129)

[1. Informacije, ki jih je treba zagotoviti 14](#_Toc521571130)

[2. Postopno obveščanje 15](#_Toc521571131)

[3. Zamude pri obveščanju 16](#_Toc521571132)

[C. Čezmejne kršitve in kršitve v ustanovitvah zunaj EU 16](#_Toc521571133)

[1. Čezmejne kršitve 16](#_Toc521571134)

[2. Kršitve v ustanovitvah zunaj EU 17](#_Toc521571135)

[D. Okoliščine, v katerih se ne zahteva obveščanje 18](#_Toc521571136)

[III. Člen 34 – Sporočilo posamezniku, na katerega se nanašajo osebni podatki 19](#_Toc521571137)

[A. Obveščanje posameznikov 19](#_Toc521571138)

[B. Informacije, ki jih je treba zagotoviti 20](#_Toc521571139)

[C. Vzpostavljanje stika s posamezniki 20](#_Toc521571140)

[D. Okoliščine, v katerih se ne zahteva sporočanje 21](#_Toc521571141)

[IV. Ocenjevanje tveganja in velikega tveganja 22](#_Toc521571142)

[A. Tveganje kot dejavnik, ki zaradi katerega nastane potreba po obveščanju 22](#_Toc521571143)

[B. Dejavniki, ki jih je treba upoštevati pri ocenjevanju tveganja 23](#_Toc521571144)

[V. Odgovornost in vodenje evidenc 26](#_Toc521571145)

[A. Dokumentiranje kršitev 26](#_Toc521571146)

[B. Vloga pooblaščene osebe za varstvo podatkov 27](#_Toc521571147)

[VI. Obveznosti obveščanja na podlagi drugih pravnih instrumentov 28](#_Toc521571148)

[VII. Priloga 30](#_Toc521571149)

[A. Shematski prikaz zahtev po obveščanju 30](#_Toc521571150)

[B. Primeri kršitev varnosti osebnih podatkov in koga je treba obvestiti 31](#_Toc521571151)

# UVOD

S splošno uredbo o varstvu podatkov (v nadaljnjem besedilu: SUVP) se uvaja zahteva, da je treba o kršitvi varnosti osebnih podatkov (v nadaljnjem besedilu: kršitev) obvestiti pristojni nacionalni nadzorni organ[[1]](#footnote-2) (ali v primeru čezmejne kršitve vodilni organ) in da je treba v nekaterih primerih kršitev sporočiti posameznikom, na katerih osebne podatke je kršitev vplivala.

Obveznosti obveščanja v primerih kršitev trenutno veljajo za nekatere organizacije, kot so ponudniki javno dostopnih elektronskih komunikacijskih storitev (kot so določeni v Direktivi 2009/136/ES in Uredbi (EU) št. 611/2013)[[2]](#footnote-3). Tudi nekatere države članice EU so že uvedle nacionalno obveznost obveščanja o kršitvah. Ta lahko vključuje obveznost obveščanja o kršitvah, ki poleg ponudnikov javno dostopnih elektronskih komunikacijskih storitev vključujejo tudi kategorije upravljavcev (na primer v Nemčiji in Italiji), ali obveznost poročanja o vseh kršitvah, ki vključujejo osebne podatke (na primer na Nizozemskem). Druge države članice so lahko uvedle ustrezne kodekse ravnanja (na primer na Irskem[[3]](#footnote-4)). Čeprav številni organi EU za varstvo podatkov upravljavce zdaj spodbujajo k poročanju o kršitvah, pa Direktiva 95/46/ES o varstvu podatkov[[4]](#footnote-5), ki jo SUVP nadomešča, ne vsebuje posebne obveznosti glede obveščanja o kršitvah, zato bo taka zahteva nova za številne organizacije. S SUVP obveščanje zdaj postaja obvezno za vse upravljavce, razen če ni verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov[[5]](#footnote-6). Pomembno vlogo imajo tudi obdelovalci, ki morajo o vsaki kršitvi obvestiti upravljavca[[6]](#footnote-7).

Po mnenju Delovne skupine iz člena 29 ima nova zahteva po obveščanju številne koristi. Upravljavci lahko ob obvestitvi nadzornega organa dobijo nasvet o tem, ali je treba obvestiti prizadete posameznike. Dejansko lahko nadzorni organ upravljavcu odredi, da mora navedene posameznike obvestiti o kršitvi[[7]](#footnote-8). Upravljavec lahko s sporočanjem kršitve posameznikom zagotovi informacije o tveganjih, ki jih povzroča kršitev, in ukrepih, ki jih lahko ti posamezniki sprejmejo, da se zavarujejo pred njenimi morebitnimi posledicami. Vsak načrt odzivanja na kršitev bi moral biti osredotočen na varstvo posameznikov in njihovih osebnih podatkov. Obveščanje o kršitvah bi bilo zato treba razumeti kot orodje za izboljšanje skladnosti v zvezi z varstvom osebnih podatkov. Hkrati je treba opozoriti, da se lahko upravljavcu, ki o kršitvi ne poroča posamezniku ali nadzornemu organu, na podlagi člena 83 naloži sankcija.

Upravljavci in obdelovalci so zato spodbujeni k vnaprejšnjemu načrtovanju in vzpostavitvi postopkov, s katerimi lahko kršitev odkrijejo in jo hitro omejijo, ocenijo tveganje za posameznike[[8]](#footnote-9) ter presodijo, ali je treba obvestiti pristojni nadzorni organ, in kršitev po potrebi sporočijo zadevnim posameznikom. Obveščanje nadzornega organa bi moralo biti del navedenega načrta odzivanja na incidente.

SUVP vsebuje določbe o tem, kdaj je potrebno obveščanje o kršitvi in koga je treba obvestiti ter katere informacije je treba zagotoviti v okviru obveščanja. Informacije, potrebne za obveščanje, se lahko zagotovijo postopoma, vsekakor pa se morajo upravljavci pravočasno odzvati na vsako kršitev.

Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah varnosti osebnih podatkov[[9]](#footnote-10) zagotovila smernice za upravljavce podatkov, ki bi jim morale v primeru kršitve pomagati pri odločitvi o obveščanju posameznikov, na katere se nanašajo osebni podatki. V navedenem mnenju je obravnavana obveznost ponudnikov elektronskih komunikacij na podlagi Direktive 2002/58/ES, navedeni so primeri iz različnih sektorjev glede na tedanji osnutek SUVP in predstavljena je dobra praksa za vse upravljavce.

V teh smernicah so pojasnjeni obvezne zahteve glede obveščanja o kršitvah in njihovega sporočanja iz SUVP ter nekateri ukrepi, ki jih lahko upravljavci in obdelovalci sprejmejo za izpolnitev teh novih obveznosti. Navedeni so tudi primeri različnih vrst kršitev in pojasnjeno je, koga bi bilo treba obvestiti v različnih scenarijih.

# Obveščanje o kršitvi varnosti osebnih podatkov na podlagi SUVP

## Osnovni varnostni preudarki

Ena od zahtev SUVP je, da se z uporabo ustreznih tehničnih in organizacijskih ukrepov osebni podatki obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo[[10]](#footnote-11).

Tako se s SUVP od upravljavcev in obdelovalcev zahteva, da imajo vzpostavljene ustrezne tehnične in organizacijske ukrepe za zagotovitev ravni varnosti, ki je ustrezna glede na tveganje za osebne podatke, ki se obdelujejo. Upoštevati morajo najnovejši razvoj, stroške izvajanja ter naravo, obseg, okoliščine in namene obdelave, pa tudi tveganje za pravice in svoboščine posameznikov, ki se razlikuje po verjetnosti in resnosti[[11]](#footnote-12). S SUVP se tudi zahteva, da so vzpostavljeni vsi ustrezni tehnološki zaščitni in organizacijski ukrepi, da se takoj ugotovi, ali je prišlo do kršitve, od česar je nato odvisno, ali nastane obveznost obveščanja[[12]](#footnote-13).

Zato je ključni element vsake politike varstva podatkov zmožnost, da se kršitev po možnosti prepeči in, če do nje kljub vsemu pride, da se nanjo pravočasno odzove.

## Kaj je kršitev varnosti osebnih podatkov?

### Opredelitev

Pri vsakem poskusu obravnave kršitve bi moral biti upravljavec najprej zmožen prepoznati kršitev. V SUVP je „kršitev varstva osebnih podatkov“ v členu 4(12) opredeljena kot:

„kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani“.

Kaj je mišljeno z „uničenjem“ osebnih podatkov, bi moralo biti dokaj jasno: to je, ko podatki ne obstajajo več ali ne obstajajo več v obliki, ki bi upravljavcu kakor koli koristila. Tudi „poškodovanje“ bi moralo biti razmeroma jasno: to je, ko so osebni podatki spremenjeni, okvarjeni ali niso več popolni. „Izgubo“ osebnih podatkov bi bilo treba razumeti, kot da podatki morda še vedno obstajajo, vendar upravljavec nima več nadzora nad njimi ali dostopa do njih oziroma jih nima več na voljo. Nazadnje, nepooblaščena ali nezakonita obdelava lahko vključuje razkritje osebnih podatkov prejemnikom (ali dostop do teh podatkov s strani prejemnikov), ki niso pooblaščeni za prejem (ali dostop do) podatkov, ali katero koli drugo obliko obdelave, ki je v nasprotju s SUVP.

**Primer**

Osebni podatki so lahko izgubljeni, če se izgubi ali ukrade naprava, ki vsebuje kopijo zbirke podatkov upravljavca o strankah. Drug tak primer je lahko, če je edina kopija sklopa osebnih podatkov šifrirana z izsiljevalskim programjem ali če jo je upravljavec šifriral z uporabo ključa, ki ga nima več pri sebi.

Jasno bi moralo biti, da gre pri kršitvi za vrsto varnostnega incidenta. Kot pa je navedeno v členu 4(12), se SUVP uporablja samo v primeru kršitve varnosti *osebnih podatkov*. Posledica take kršitve je, da upravljavec ne more zagotoviti skladnosti z načeli, povezanimi z obdelavo osebnih podatkov, kot so določena v členu 5 SUVP. To pojasnjuje razliko med varnostnim incidentom in kršitvijo varnosti osebnih podatkov – bistveno je, da medtem ko so vse kršitve varnosti osebnih podatkov varnostni incidenti, pa niso vsi varnostni incidenti nujno kršitve varnosti osebnih podatkov[[13]](#footnote-14).

Morebitni škodljivi učinki kršitve na posameznike so obravnavani v nadaljevanju.

### Vrste kršitev varnosti osebnih podatkov

Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah pojasnila, da je mogoče kršitve razvrstiti na podlagi naslednjih treh dobro znanih načel varnosti informacij[[14]](#footnote-15):

* „kršitev zaupnosti“ – kadar gre za nepooblaščeno ali nenamerno razkritje osebnih podatkov ali nepooblaščen ali nenameren dostop do njih;
* „kršitev celovitosti“ – kadar gre za nepooblaščeno ali nenamerno spremembo osebnih podatkov;
* „kršitev razpoložljivosti“ – kadar gre za nenamerno ali nepooblaščeno izgubo dostopa[[15]](#footnote-16) do osebnih podatkov ali njihovo uničenje.

Opozoriti je treba še, da se lahko kršitev – odvisno od okoliščin – hkrati nanaša na zaupnost, celovitost in razpoložljivost osebnih podatkov ter na kakršno koli kombinacijo teh treh.

Medtem ko je ugotavljanje obstoja kršitve zaupnosti ali celovitosti razmeroma jasno, pa je lahko obstoj kršitev razpoložljivosti manj očiten. Kršitev se vedno šteje za kršitev razpoložljivosti, če se osebni podatki trajno izgubijo ali uničijo.

**Primer**

Primer izgube razpoložljivosti je, kadar se podatki izbrišejo nenamerno ali jih izbriše nepooblaščena oseba ali kadar se v primeru varno šifriranih podatkov izgubi ključ za dešifriranje. Če upravljavec ne more povrniti dostopa do podatkov, na primer iz varnostne kopije, se to potem obravnava kot trajna izguba razpoložljivosti.

Do izgube razpoložljivosti lahko pride tudi, kadar je znatno moteno normalno delovanje organizacije, na primer ob izpadu električnega toka ali napadu za zavrnitev storitve, kar pomeni, da osebni podatki niso več na voljo.

Vprašati se je mogoče, ali bi bilo treba začasno izgubo razpoložljivosti osebnih podatkov obravnavati kot kršitev in, če je tako, koga je treba obvestiti. V členu 32 SUVP, ki se nanaša na „varnost obdelave“, je pojasnjeno, da je treba pri izvajanju tehničnih in organizacijskih ukrepov za zagotovitev ustrezne ravni varnosti glede na tveganje med drugim upoštevati „zmožnost zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo“ ter „zmožnost pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta“.

Zato je tudi varnostni incident, zaradi katerega osebni podatki začasno niso več na voljo, vrsta kršitve, saj lahko pomanjkanje dostopa do podatkov pomembno vpliva na pravice in svoboščine fizičnih oseb. Jasno je, da kadar osebni podatki niso na voljo zaradi izvajanja načrtovanega vzdrževanja sistema, to ni „kršitev varnosti“, kot je opredeljena v členu 4(12).

Tako kot pri trajni izgubi ali uničenju osebnih podatkov (ali dejansko kateri koli drugi vrsti kršitve) je treba tudi kršitev, ki vključuje začasno izgubo razpoložljivosti, dokumentirati v skladu s členom 33(5). Tako upravljavec lažje dokaže odgovornost nadzornemu organu, ki lahko zahteva vpogled v navedene evidence[[16]](#footnote-17). Vendar glede na okoliščine kršitve to lahko pomeni, da je treba obvestiti nadzorni organ, prizadetim posameznikom pa sporočiti kršitev. Upravljavec mora oceniti verjetnost in resnost vpliva na pravice in svoboščine fizičnih oseb zaradi pomanjkanja razpoložljivosti osebnih podatkov. V skladu s členom 33 mora upravljavec obvestiti o kršitvi, razen če ni verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. Seveda je treba o tem presojati za vsak primer posebej.

**Primeri**

Če v primeru bolnišnice ključni zdravstveni podatki o bolnikih niso na voljo, četudi samo začasno, bi bile lahko ogrožene pravice in svoboščine posameznikov; zaradi morebitne odpovedi operacij so na primer lahko ogrožena življenja.

Nasprotno pa v primeru medijske družbe, katere sistemi več ur niso razpoložljivi (npr. zaradi izpada elektrike), to, da ta družba ne more pošiljati spletnih glasil svojim naročnikom, verjetno ne ogroža pravic in svoboščin posameznikov.

Opozoriti je treba, da čeprav je lahko izguba razpoložljivosti sistemov upravljavca zgolj začasna in ne vpliva na posameznike, je za upravljavca pomembno, da obravnava vse morebitne posledice kršitve, saj je lahko obveščanje vseeno potrebno iz drugih razlogov.

**Primer**

Okužba z izsiljevalskim programjem (zlonamerno programsko opremo, ki šifrira podatke upravljavca, dokler ta ne plača odkupnine) bi lahko vodila do začasne izgube razpoložljivosti, če se lahko podatki obnovijo iz varnostne kopije. Vendar je vseeno prišlo do vdora v omrežje, zato bi bilo lahko potrebno obveščanje, če se incident šteje za kršitev zaupnosti (tj. napadalec dostopa do osebnih podatkov) ter so tako ogrožene pravice in svoboščine posameznikov.

### Morebitne posledice kršitve varnosti osebnih podatkov

Kršitev ima lahko različne pomembne škodljive učinke na posameznike, kar lahko povzroči fizično, premoženjsko ali nepremoženjsko škodo. V SUVP je pojasnjeno, da to lahko vključuje izgubo nadzora nad njihovimi osebnimi podatki, omejitev njihovih pravic, diskriminacijo, krajo ali zlorabo identitete, finančno izgubo, neodobreno reverzijo psevdonimizacije, okrnitev ugleda in izgubo zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo. Vključuje lahko tudi katero koli drugo znatno gospodarsko ali socialno škodo za navedene posameznike[[17]](#footnote-18).

Tako se s SUVP od upravljavca zahteva, da o kršitvi obvesti pristojni nadzorni organ, razen če ni verjetno, da povzroča tveganje za nastanek takih škodljivih učinkov. Kadar je velika verjetnost za take negativne učinke, se s SUVP zahteva, da upravljavec kršitev sporoči prizadetim posameznikom, kakor hitro je to razumno mogoče[[18]](#footnote-19).

Pomembnost tega, da se lahko ugotovi kršitev, oceni tveganje za posameznike in nato po potrebi obvesti o kršitvi, je poudarjena v uvodni izjavi 87 SUVP:

„Preveriti bi bilo treba, ali so bili izvedeni vsi ustrezni tehnološki zaščitni in organizacijski ukrepi, da bi takoj ugotovili, ali je prišlo do kršitve varstva osebnih podatkov, ter o tem nemudoma obvestili nadzorni organ in posameznika, na katerega se nanašajo osebni podatki. Dejstvo, ali je bilo obvestilo poslano nemudoma, bi bilo treba ugotoviti ob upoštevanju zlasti narave in teže kršitve varstva osebnih podatkov ter njenih posledic in škodljivih učinkov za posameznika, na katerega se nanašajo osebni podatki. Na podlagi takšnega obvestila lahko nadzorni organ ukrepa v skladu s svojimi nalogami in pristojnostmi, določenimi v tej uredbi.“

Nadaljnje smernice za oceno tveganja škodljivih učinkov na posameznike so obravnavane v oddelku IV.

Če upravljavci nadzornega organa, posameznikov, na katere se nanašajo osebni podatki, ali obojih o kršitvi varnosti podatkov ne obvestijo, čeprav so izpolnjene zahteve iz členov 33 in/ali 34, lahko nadzorni organ izbira med vsemi popravnimi ukrepi, ki jih ima na voljo, kar bi zajemalo proučitev naložitve ustrezne upravne globe[[19]](#footnote-20), bodisi poleg popravnega ukrepa iz člena 58(2) bodisi samostojno. Če se izbere upravna globa, lahko ta znaša do 10 000 000 EUR ali do 2 % skupnega svetovnega letnega prometa podjetja v skladu s členom 83(4)(a) SUVP. Pomembno je tudi upoštevati, da bi lahko opustitev obveščanja o kršitvi v nekaterih primerih razkrila neobstoj varnostnih ukrepov ali neustreznost obstoječih varnostnih ukrepov. V smernicah Delovne skupine iz člena 29 o upravnih globah je navedeno: „Pri več različnih kršitvah, storjenih skupaj v katerem koli posameznem primeru, lahko nadzorni organ uporabi upravno globo v višini, ki je učinkovita, sorazmerna in odvračilna v okviru najhujše kršitve.“ V navedenem primeru ima nadzorni organ tudi možnost izreči sankcije zaradi opustitve obveščanja ali sporočanja kršitve (člena 33 in 34) na eni strani in neobstoja (ustreznih) varnostnih ukrepov (člen 32) na drugi strani, saj gre za ločeni kršitvi.

# Člen 33 – Obvestilo nadzornemu organu

## Kdaj je potrebno obvestilo?

### Zahteve iz člena 33

Člen 33(1) določa:

„V primeru kršitve varnosti osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej obvesti pristojni nadzorni organ v skladu s členom 55, razen če ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedba razlogov za zamudo.“

V uvodni izjavi 87 je navedeno[[20]](#footnote-21):

„Preveriti bi bilo treba, ali so bili izvedeni vsi ustrezni tehnološki zaščitni in organizacijski ukrepi, da bi takoj ugotovili, ali je prišlo do kršitve varstva osebnih podatkov, ter o tem nemudoma obvestili nadzorni organ in posameznika, na katerega se nanašajo osebni podatki. Dejstvo, ali je bilo obvestilo poslano nemudoma, bi bilo treba ugotoviti ob upoštevanju zlasti narave in teže kršitve varstva osebnih podatkov ter njenih posledic in škodljivih učinkov za posameznika, na katerega se nanašajo osebni podatki. Na podlagi takšnega obvestila lahko nadzorni organ ukrepa v skladu s svojimi nalogami in pristojnostmi, določenimi v tej uredbi.“

### Kdaj je upravljavec „seznanjen“?

Kot je pojasnjeno zgoraj, se s SUVP zahteva, da upravljavec v primeru kršitve o njej obvesti brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo. Tako se lahko postavi vprašanje, kdaj je mogoče šteti, da je upravljavec „seznanjen“ s kršitvijo. Delovna skupina iz člena 29 meni, da bi se moralo za upravljavca šteti, da je „seznanjen“, ko je z razumno gotovostjo prepričan, da je prišlo do varnostnega incidenta, zaradi katerega so ogroženi osebni podatki.

Kot pa je bilo že navedeno, se s SUVP zahteva, da upravljavec izvede vse ustrezne tehnološke zaščitne in organizacijske ukrepe, da takoj ugotovi, ali je prišlo do kršitve, ter nemudoma obvesti nadzorni organ in posameznike, na katere se nanašajo osebni podatki. Prav tako je navedeno, da bi bilo treba dejstvo, ali je bilo obvestilo poslano nemudoma, ugotoviti ob upoštevanju zlasti narave in teže kršitve ter njenih posledic in škodljivih učinkov za posameznika, na katerega se nanašajo osebni podatki[[21]](#footnote-22). S tem je upravljavcu naložena obveznost, da zagotovi njihovo pravočasno „seznanitev“ s kršitvami, da lahko sprejmejo ustrezne ukrepe.

Kdaj natančno se za upravljavca lahko šteje, da je „seznanjen“ s konkretno kršitvijo, je odvisno od okoliščin posamezne kršitve. V nekaterih primerih je že takoj bolj ali manj jasno, da je prišlo do kršitve, v drugih pa lahko traja nekaj časa, da se ugotovi, ali so bili ogroženi osebni podatki. Vendar bi moral biti poudarek na hitrem ukrepanju, da se razišče incident in ugotovi, ali je bila dejansko kršena varnost osebnih podatkov, ter, če je bila, da se sprejme popravni ukrep in po potrebi zagotovi obvestilo.

**Primeri**

1. Če se izgubi pomnilniški ključek USB z nešifriranimi osebnimi podatki, pogosto ni mogoče ugotoviti, ali so imele nepooblaščene osebe dostop do navedenih podatkov. Vendar tudi če upravljavec ne more ugotoviti, ali je prišlo do kršitve zaupnosti, je v takem primeru potrebno obveščanje, ker obstaja razumna gotovost, da je prišlo do kršitve razpoložljivosti; upravljavec bi se „seznanil“, ko je ugotovil, da se je izgubil pomnilniški ključek USB.

2. Tretja oseba obvesti upravljavca, da je po pomoti prejela osebne podatke ene od njegovih strank, in zagotovi dokaze o nepooblaščenem razkritju. Ker so bili upravljavcu predloženi jasni dokazi o kršitvi zaupnosti, ne more biti nobenega dvoma, da je bil „seznanjen“.

3. Upravljavec odkrije, da je morda prišlo do vdora v njegovo omrežje. Preveri svoje sisteme, da ugotovi, ali so osebni podatki, shranjeni v zadevnem sistemu, ogroženi, in potrdi, da je tako. Ker ima tudi tokrat upravljavec jasne dokaze o kršitvi, ne more biti nobenega dvoma, da je bil „seznanjen“.

4. Kibernetski kriminalec vzpostavi stik z upravljavcem, potem ko je vdrl v njegov sistem, in zahteva odkupnino. V takem primeru ima upravljavec, potem ko preveri svoj sistem in potrdi, da je bil napaden, jasne dokaze, da je prišlo do kršitve, in ni dvoma, da je bil seznanjen.

Potem ko je upravljavca o morebitni kršitvi obvestil posameznik, medijska organizacija ali drug vir ali ko sam odkrije varnostni incident, lahko opravi kratko preiskavo, da ugotovi, ali je do kršitve dejansko prišlo ali ne. V tem času za upravljavca ni mogoče šteti, da je „seznanjen“. Vendar bi se morala začetna preiskava začeti izvajati čim prej, da bi se z razumno gotovostjo ugotovilo, ali je prišlo do kršitve; nato lahko sledi podrobnejša preiskava.

Ko je upravljavec seznanjen, mora o kršitvi, za katero velja obveznost obveščanja, obvestiti brez nepotrebnega odlašanja, če je to izvedljivo, pa najpozneje v 72 urah. V tem času bi moral upravljavec oceniti verjetno tveganje za posameznike, da se ugotovi, ali je potrebno obveščanje in kateri ukrepi so potrebni za obravnavo kršitve. Vendar ima lahko upravljavec že na voljo začetno oceno morebitnega tveganja, ki bi ga lahko povzročila kršitev, in sicer v okviru ocene učinka v zvezi z varstvom podatkov[[22]](#footnote-23), izvedene pred zadevnim postopkom obdelave. Vendar je lahko navedena ocena učinka v zvezi z varstvom podatkov splošnejša v primerjavi s posameznimi okoliščinami dejanske kršitve, zato je vsekakor treba izvesti dodatno oceno, pri kateri se upoštevajo navedene okoliščine. Za več podrobnosti o ocenjevanju tveganja glej oddelek IV.

V večini primerov bi morali biti ti začetni ukrepi dokončani kmalu po prvem opozorilu (tj. ko upravljavec ali obdelovalec sumita, da je prišlo do varnostnega incidenta, ki lahko vključuje osebne podatke) – dlje bi morali trajati samo v izjemnih primerih.

**Primer**

Posameznik obvesti upravljavca, da je prejel elektronsko sporočilo, v katerem se je nekdo izdajal za upravljavca in ki vsebuje osebne podatke v zvezi z njegovo (dejansko) uporabo storitve upravljavca, kar nakazuje, da je ogrožena varnost upravljavca. Upravljavec opravi kratko preiskavo ter odkrije vdor v svoj sistem in dokaze o nepooblaščenem dostopu do osebnih podatkov. Upravljavec, za katerega bi se zdaj štelo, da je „seznanjen“, mora obvestiti nadzorni organ, razen če ni verjetno, da so ogrožene pravice in svoboščine posameznikov. Upravljavec mora sprejeti ustrezne popravne ukrepe za obravnavo kršitve.

Upravljavec bi zato moral imeti vzpostavljene notranje postopke, da bi lahko odkril in obravnaval kršitev. Da se na primer odkrijejo nekatere nepravilnosti pri obdelavi podatkov, lahko upravljavec ali obdelovalec uporabi nekatere tehnične ukrepe, kot so analizatorji podatkovnega toka in dnevnika, na podlagi katerih je mogoče opredeliti dogodke in opozorila s korelacijo morebitnih podatkov iz dnevnika[[23]](#footnote-24). Ko se kršitev odkrije, je treba o njej poročati navzgor ustrezni ravni vodstva, da jo je mogoče obravnavati in po potrebi obvestiti o njej v skladu s členom 33 in po potrebi členom 34. Taki ukrepi in mehanizmi poročanja bi lahko bili podrobno določeni v načrtih upravljavca za odzivanje na incidente in/ali ureditvah upravljanja. Ti upravljavcu pomagajo pri učinkovitem načrtovanju in določanju, kdo v organizaciji nosi operativno odgovornost za upravljanje kršitve in kako oziroma ali je treba o incidentu poročati naprej, kakor je ustrezno.

Upravljavec bi moral imeti tudi vzpostavljene ureditve z obdelovalci, ki jih morda uporablja in ki imajo sami obveznost, da upravljavca obvestijo v primeru kršitve (glej spodaj).

Čeprav so za vzpostavitev primernih ukrepov, s katerimi je kršitev mogoče preprečiti, se nanjo odzvati in jo obravnavati, odgovorni upravljavci in obdelovalci, obstajajo nekateri praktični postopki, ki bi jih bilo treba izvesti v vseh primerih.

* Informacije v zvezi z vsemi dogodki, povezanimi z varnostjo, bi se morale usmeriti k odgovornim osebam, pristojnim za obravnavanje incidentov, ugotavljanje obstoja kršitve in ocenjevanje tveganja.
* Nato bi se moralo oceniti tveganje, ki ga kršitev povzroča za posameznike (tveganje ni verjetno, tveganje je verjetno, tveganje je zelo verjetno), ter o tem obvestiti ustrezne oddelke organizacije.
* Po potrebi bi bilo treba obvestiti nadzorni organ, prizadetim posameznikom pa po možnosti sporočiti kršitev.
* Hkrati bi moral upravljavec ukrepati za omejitev in obvladovanje kršitve.
* Kršitev bi bilo treba sproti dokumentirati.

Tako bi moralo biti jasno, da se mora upravljavec odzvati na vsako prvo opozorilo in ugotoviti, ali je do kršitve dejansko prišlo ali ne. V tem kratkem času je mogoča določena preiskava, upravljavec pa lahko zbere dokaze in druge pomembne podrobnosti. Ko pa upravljavec z razumno verjetnostjo ugotovi, da je prišlo do kršitve, mora nato, če so izpolnjeni pogoji iz člena 33(1), brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah, obvestiti nadzorni organ[[24]](#footnote-25). Če upravljavec ne ukrepa pravočasno in se izkaže, da je do kršitve dejansko prišlo, bi se to lahko v skladu s členom 33 štelo za opustitev obveščanja.

V členu 32 je jasno navedeno, da bi morala upravljavec in obdelovalec imeti vzpostavljene ustrezne tehnične in organizacijske ukrepe za zagotovitev ustrezne ravni varnosti osebnih podatkov: za bistven element teh ukrepov bi se morala šteti zmožnost pravočasnega odkrivanja, obravnavanja in prijave kršitev.

### Skupni upravljavci

Člen 26 se nanaša na skupne upravljavce in določa, da ti določijo dolžnosti vsakega od njih z namenom izpolnjevanja obveznosti v skladu s SUVP[[25]](#footnote-26). To vključuje določitev, kdo je odgovoren za izpolnjevanje obveznosti na podlagi členov 33 in 34. Delovna skupina iz člena 29 priporoča, naj pogodbeni dogovori med skupnimi upravljavci vključujejo določbe o tem, kateri upravljavec prevzame vodilno vlogo ali je odgovoren za izpolnjevanje obveznosti iz SUVP glede obveščanja o kršitvah.

### Obveznosti obdelovalca

Upravljavec ohrani splošno odgovornost za varstvo osebnih podatkov, obdelovalec pa ima pomembno vlogo pri zagotavljanju, da lahko upravljavec izpolni svoje obveznosti; to vključuje obveščanje o kršitvah. Dejansko člen 28(3) določa, da obdelavo s strani obdelovalca ureja pogodba ali drug pravni akt. V členu 28(3)(f) je navedeno, da pogodba ali drug pravni akt določa, da obdelovalec „upravljavcu pomaga pri izpolnjevanju obveznosti iz členov 32 do 36 ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu“.

Člen 33(2) jasno določa, da kadar upravljavec uporablja obdelovalca in je slednji seznanjen s kršitvijo varnosti osebnih podatkov, ki jih obdeluje v imenu prvega, mora tega obvestiti „brez nepotrebnega odlašanja“. Opozoriti je treba, da obdelovalcu pred obveščanjem upravljavca ni treba najprej oceniti verjetnosti tveganja, ki ga povzroča kršitev; to oceno mora po seznanitvi s kršitvijo izvesti upravljavec. Obdelovalec mora samo ugotoviti, ali je prišlo do kršitve, in nato obvestiti upravljavca. Upravljavec uporablja obdelovalca za dosego svojih ciljev; zato bi se načeloma moralo šteti, da je upravljavec „seznanjen“, ko ga obdelovalec obvesti o kršitvi. Obveznost obdelovalca, da obvesti svojega upravljavca, slednjemu omogoča, da obravnava kršitev in ugotovi, ali mora obvestiti nadzorni organ v skladu s členom 33(1) in prizadete posameznike v skladu s členom 34(1). Upravljavec morda tudi želi raziskati kršitev, saj obdelovalec morda ne more poznati vseh pomembnih dejstev v zvezi z zadevo, na primer, ali ima upravljavec še vedno kopijo ali varnostno kopijo osebnih podatkov, ki jih je obdelovalec uničil ali izgubil. To lahko vpliva na dolžnost obveščanja upravljavca.

SUVP ne določa izrecnega roka, v katerem mora obdelovalec opozoriti upravljavca, razen da mora to storiti „brez nepotrebnega odlašanja“. Delovna skupina iz člena 29 zato priporoča, naj obdelovalec upravljavca obvesti nemudoma, pri čemer se nadaljnje informacije o kršitvi zagotovijo postopoma, ko je na voljo več podrobnosti. To je pomembno, da upravljavec lažje izpolni zahtevo po obveščanju nadzornega organa v 72 urah.

Kot je bilo pojasnjeno zgoraj, bi moralo biti v pogodbi med upravljavcem in obdelovalcem določeno, kako bi bilo treba poleg drugih določb v SUVP izpolnjevati zahteve iz člena 33(2). To lahko vključuje zahteve po zgodnjem obveščanju s strani obdelovalca, s katerimi se podprejo obveznosti upravljavca, da poroča nadzornemu organu v 72 urah.

Če obdelovalec zagotavlja storitve več upravljavcem, pri čemer isti incident prizadene vse, mora obdelovalec sporočiti podrobnosti o incidentu vsakemu upravljavcu.

Obveščanje bi lahko v imenu upravljavca izvedel obdelovalec, če ga je prvi ustrezno pooblastil in je to del pogodbenih dogovorov med upravljavcem in obdelovalcem. Tako obveščanje mora potekati v skladu s členoma 33 in 34. Pomembno pa je opozoriti, da pravno odgovornost za obveščanje ohrani upravljavec.

## Zagotavljanje informacij nadzornemu organu

### Informacije, ki jih je treba zagotoviti

Ko upravljavec nadzorni organ obvesti o kršitvi, mora v skladu s členom 33(3) zagotoviti vsaj:

„(a) opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter kategorije in približno število zadevnih evidenc osebnih podatkov;

(b) sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;

(c) opis verjetnih posledic kršitve varstva osebnih podatkov;

(d) opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno“.

V SUVP niso opredeljene kategorije posameznikov, na katere se nanašajo osebni podatki, ali evidence osebnih podatkov. Vendar Delovna skupina iz člena 29 predlaga, naj kategorije posameznikov, na katere se nanašajo osebni podatki, vključujejo različne vrste posameznikov, na katerih osebne podatke je kršitev vplivala: odvisno od deskriptorjev, ki se uporabljajo, bi to lahko med drugim vključevalo otroke in druge ranljive skupine, invalide, zaposlene ali stranke. Podobno lahko kategorije evidenc osebnih podatkov vključujejo različne vrste evidenc, ki jih lahko obdeluje upravljavec, kot so zdravstveni podatki, šolska dokumentacija, informacije o socialni oskrbi, finančni podatki, številke bančnih računov, številke potnih listov itd.

V uvodni izjavi 85 je jasno navedeno, da je eden od namenov obveščanja omejiti škodo za posameznike. Če torej vrste posameznikov, na katere se nanašajo osebni podatki, ali vrste osebnih podatkov kažejo tveganje, da bi zaradi kršitve (npr. kraje identitete, goljufije, finančne izgube, ogrožanja poklicne skrivnosti) nastala določena škoda, je pomembno, da se te kategorije navedejo v obvestilu. Tako je obveščanje povezano z zahtevo, da se opišejo verjetne posledice kršitve.

Kadar niso na voljo natančne informacije (npr. točno število prizadetih posameznikov, na katere se nanašajo osebni podatki), to ne bi smelo ovirati pravočasnega obveščanja o kršitvi. S SUVP je dovoljeno, da se število prizadetih posameznikov in število zadevnih evidenc osebnih podatkov zaokrožita. Poudarek bi moral biti na obravnavi škodljivih učinkov kršitve in ne na zagotavljanju natančnih številk. Ko torej postane jasno, da je prišlo do kršitve, vendar njen obseg še ni znan, je varen način za izpolnitev obveznosti glede obveščanja postopno obveščanje (glej spodaj).

V členu 33(3) je navedeno, da upravljavec skupaj z obvestilom zagotovi „vsaj“ te informacije, tako da lahko po potrebi zagotovi tudi nadaljnje podrobnosti. Za različne vrste kršitev (zaupnosti, celovitosti ali razpoložljivosti) se lahko zahteva zagotovitev nadaljnjih informacij, da se v celoti razjasnijo okoliščine posamezne zadeve.

**Primer**

V okviru obveščanja nadzornega organa je lahko za upravljavca koristno, da navede svojega obdelovalca, če je ta glavni krivec za kršitev, zlasti če je zaradi tega nastal incident, ki je vplival na evidence osebnih podatkov številnih drugih upravljavcev, ki uporabljajo istega obdelovalca.

Vsekakor lahko nadzorni organ zahteva nadaljnje podrobnosti v okviru svoje preiskave kršitve.

### Postopno obveščanje

Glede na vrsto kršitve je lahko potrebno, da upravljavec izvede nadaljnjo preiskavo, da se ugotovijo vsa pomembna dejstva v zvezi z incidentom. Člen 33(4) zato določa:

„Kadar in kolikor informacij ni mogoče zagotoviti sočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.“

To pomeni, da se s SUVP priznava, da upravljavci ne dobijo vedno vseh potrebnih informacij v zvezi s kršitvijo v 72 urah po seznanitvi z njo, saj v tem začetnem obdobju morda niso vedno na voljo popolne in izčrpne podrobnosti o incidentu. Tako je dovoljeno postopno obveščanje. To je verjetnejše v primeru bolj zapletenih kršitev, kot so nekatere vrste incidentov na področju kibernetske varnosti, pri katerih je lahko na primer potrebna temeljita forenzična preiskava, da se v celoti ugotovita narava kršitve in stopnja ogroženosti osebnih podatkov. Posledično mora upravljavec v številnih primerih izvesti podrobnejšo preiskavo in pozneje preveriti dodatne informacije. To je v skladu s členom 33(1) dovoljeno, če upravljavec navede razloge za zamudo. Delovna skupina iz člena 29 priporoča, naj upravljavec ob prvem obveščanju nadzornega organa tega tudi opozori, če še nima vseh potrebnih informacij in bo več podrobnosti zagotovil pozneje. Nadzorni organ bi se moral strinjati, kako in kdaj naj bi bile zagotovljene dodatne informacije. To pa ne pomeni, da upravljavec ne more zagotoviti nadaljnjih informacij kadar koli pozneje, če se seznani z dodatnimi pomembnimi podrobnostmi o kršitvi, ki jih je treba posredovati nadzornemu organu.

Zahteva po obveščanju je osredotočena na spodbujanje upravljavcev, da se nemudoma odzovejo na kršitev, jo omejijo in po možnosti obnovijo ogrožene osebne podatke ter da poiščejo ustrezen nasvet pri nadzornem organu. Z obveščanjem nadzornega organa v prvih 72 urah lahko upravljavec poskrbi, da so odločitve o obveščanju ali neobveščanju posameznikov pravilne.

Vendar namen obveščanja nadzornega organa ni samo dobiti navodila o tem, ali je treba obvestiti prizadete posameznike. V nekaterih primerih je jasno, da mora upravljavec zaradi narave kršitve in resnosti tveganja nemudoma obvestiti prizadete posameznike. Če na primer obstaja neposredna nevarnost kraje identitete ali če se na spletu razkrijejo posebne kategorije osebnih podatkov[[26]](#footnote-27), bi moral upravljavec ukrepati brez nepotrebnega odlašanja, da omeji kršitev in o njej obvesti zadevne posameznike (glej oddelek III). Izjemoma lahko to stori še pred obveščanjem nadzornega organa. Splošneje, obveščanje nadzornega organa ne more biti opravičilo za to, da kršitev ni sporočena posamezniku, na katerega se nanašajo osebni podatki, kadar se to zahteva.

Prav tako bi bilo treba pojasniti, da lahko upravljavec po prvem obveščanju nadzornemu organu zagotovi nove informacije, če se z nadaljnjo preiskavo razkrijejo dokazi, da je bil varnostni incident omejen in dejansko ni prišlo do kršitve. S temi informacijami bi se nato lahko dopolnile informacije, ki so bile nadzornemu organu že zagotovljene, tako da se incident ne evidentira kot kršitev. Poročanje o incidentu, za katerega se na koncu izkaže, da ni kršitev, se ne kaznuje.

**Primer**

Upravljavec nadzorni organ v 72 urah po odkritju kršitve obvesti, da je izgubil pomnilniški ključek USB, ki vsebuje kopijo osebnih podatkov nekaterih njegovih strank. Pomnilniški ključek USB je pozneje najden kot narobe arhiviran v prostorih upravljavca in dobljen nazaj. Upravljavec posreduje nove informacije nadzornemu organu in zaprosi za spremembo obvestila.

Opozoriti je treba, da postopen pristop k obveščanju izhaja že iz obstoječih obveznosti na podlagi Direktive 2002/58/ES, Uredbe št. 611/2013 in drugih samoporočanih incidentov.

### Zamude pri obveščanju

Člen 33(1) jasno določa, da kadar obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedba razlogov za zamudo. S tem se skupaj s konceptom postopnega obveščanja priznava, da upravljavec ne more vedno obvestiti o kršitvi v navedenem roku in da je dovoljeno zapoznelo obvestilo.

To se lahko na primer zgodi, če se upravljavec v kratkem času sreča z več podobnimi kršitvami zaupnosti, ki enako vplivajo na veliko število posameznikov, na katere se nanašajo osebni podatki. Upravljavec bi lahko bil seznanjen s kršitvijo, med začetkom preiskave kršitve in pred obveščanjem o njej pa bi lahko odkril še druge podobne kršitve, ki imajo različne vzroke. Glede na okoliščine lahko traja nekaj časa, da upravljavec ugotovi obseg kršitev, in namesto, da bi o vsaki kršitvi obveščal posebej, poskrbi za smiselno obveščanje o več zelo podobnih kršitvah z možnimi različnimi vzroki. To bi lahko pomenilo, da bi bil nadzorni organ obveščen pozneje kot v 72 urah po prvi seznanitvi upravljavca s temi kršitvami.

Strogo gledano je vsaka posamezna kršitev incident, o katerem je treba poročati. Da pa to ne bi pomenilo prevelike obremenitve, lahko upravljavec predloži „združeno“ obvestilo, v katerem predstavi vse te kršitve, če zadevajo isto vrsto osebnih podatkov, ki so bili na enak način kršeni v razmeroma kratkem času. Če pride do vrste kršitev, ki se nanašajo na različne vrste osebnih podatkov, kršenih na različne načine, je potrebno običajno obveščanje, tako da se o vsaki kršitvi poroča v skladu s členom 33.

Čeprav so s SUVP v nekaterih primerih dovoljena zapoznela obvestila, se to ne sme šteti za redno prakso. Poudariti je treba, da je združena obvestila mogoče poslati tudi za več podobnih kršitev, o katerih se poroča v 72 urah.

## Čezmejne kršitve in kršitve v ustanovitvah zunaj EU

### Čezmejne kršitve

Kadar gre za čezmejno obdelavo[[27]](#footnote-28) osebnih podatkov, lahko kršitev vpliva na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici. Člen 33(1) jasno določa, da mora v primeru kršitve upravljavec o njej obvestiti nadzorni organ, pristojen v skladu s členom 55 SUVP[[28]](#footnote-29). Člen 55(1) določa:

„Vsak nadzorni organ je na ozemlju svoje države članice pristojen za opravljanje dodeljenih nalog in izvajanje prenesenih pooblastil v skladu s to uredbo.“

Vendar člen 56(1) določa:

„Nadzorni organ glavne ali edine ustanovitve upravljavca ali obdelovalca je brez poseganja v člen 55 pristojen, da deluje kot vodilni nadzorni organ za obdelavo, ki jo izvaja ta upravljavec ali obdelovalec na čezmejni ravni, v skladu s postopkom iz člena 60.“

Poleg tega člen 56(6) določa:

„Vodilni nadzorni organ je edini sogovornik upravljavca ali obdelovalca za njune obdelave na čezmejni ravni.“

To pomeni, da mora upravljavec, kadar do kršitve pride pri čezmejni obdelavi in se zahteva obveščanje, obvestiti vodilni nadzorni organ[[29]](#footnote-30). Zato mora upravljavec pri pripravi načrta odzivanja na kršitev oceniti, kateri nadzorni organ je vodilni nadzorni organ, ki ga mora obvestiti[[30]](#footnote-31). Tako se lahko nemudoma odzove na kršitev in izpolni svoje obveznosti v skladu s členom 33. Pojasniti bi bilo treba, da je treba v primeru kršitve, ki vključuje čezmejno obdelavo, obvestiti vodilni nadzorni organ, ki ni nujno v državi, kjer so zadevni posamezniki, na katere se nanašajo osebni podatki, ali v državi, kjer je prišlo do kršitve. Upravljavec bi moral ob obveščanju vodilnega organa po potrebi navesti, ali kršitev vključuje ustanovitve v drugih državah članicah in v katerih državah članicah je kršitev verjetno vplivala na posameznike, na katere se nanašajo osebni podatki. Če ima upravljavec kakršne koli pomisleke glede identitete vodilnega nadzornega organa, mora obvestiti vsaj lokalni nadzorni organ v državi, kjer je prišlo do kršitve.

### Kršitve v ustanovitvah zunaj EU

Člen 3 se nanaša na ozemeljsko veljavnost SUVP, tudi kadar osebne podatke obdeluje upravljavec ali obdelovalec, ki nima ustanovitve v EU. Natančneje, člen 3(2) določa[[31]](#footnote-32):

„Ta uredba se uporablja za obdelavo osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki so v Uniji, s strani upravljavca ali obdelovalca, ki nima ustanovitve v Uniji, kadar so dejavnosti obdelave povezane:

(a) z nudenjem blaga ali storitev takim posameznikom v Uniji, ne glede na to, ali je potrebno plačilo posameznika, na katerega se nanašajo osebni podatki, ali

(b) s spremljanjem njihovega vedenja, kolikor to vedenje poteka v Uniji.“

Pomemben je tudi člen 3(3), ki določa[[32]](#footnote-33):

„Ta uredba se uporablja za obdelavo osebnih podatkov s strani upravljavca, ki nima ustanovitve v Uniji, temveč v kraju, kjer se pravo države članice uporablja na podlagi mednarodnega javnega prava.“

Kadar se za upravljavca, ki nima ustanovitve v EU, uporablja člen 3(2) ali 3(3) in se ta upravljavec sreča s kršitvijo, ga tako še vedno zavezujejo obveznosti obveščanja na podlagi členov 33 in 34. V skladu s členom 27 mora upravljavec (in obdelovalec) določiti predstavnika v EU, kadar se uporablja člen 3(2). V takih primerih Delovna skupina iz člena 29 priporoča, da se obvesti nadzorni organ v državi članici, kjer ima ustanovitev predstavnik upravljavca v EU[[33]](#footnote-34).Kadar se za obdelovalca uporablja člen 3(2), ga podobno zavezujejo obveznosti za obdelovalce, pri čemer je v tem primeru še posebej pomembna dolžnost, da je o kršitvi obveščen upravljavec v skladu s členom 33(2).

## Okoliščine, v katerih se ne zahteva obveščanje

Člen 33(1) jasno določa, da obveščanje ni potrebno, „če ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov“. To je lahko v primeru, ko so osebni podatki že javno dostopni in razkritje takih podatkov ne pomeni verjetnega tveganja za posameznika. To je v nasprotju z obstoječimi zahtevami glede obveščanja o kršitvah za ponudnike javno dostopnih elektronskih komunikacijskih storitev v Direktivi 2009/136/ES, ki določajo, da je treba o vseh zadevnih kršitvah obvestiti pristojni organ.

Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah[[34]](#footnote-35) pojasnila, da je kršitev zaupnosti osebnih podatkov, ki so bili šifrirani z najsodobnejšim algoritmom, še vedno kršitev varnosti osebnih podatkov in je treba o njej obvestiti organ. Če pa je tajnost ključa nedotaknjena – tj. ključ ni bil ogrožen pri nobeni kršitvi varnosti in je bil ustvarjen tako, da ga s tehnološkimi sredstvi, ki so na voljo, ne more ugotoviti nobena oseba, k nima dovoljenja za dostop do njega –, so podatki načeloma nerazumljivi. Zato ni verjetno, da bi kršitev negativno vplivala na posameznike, ki jih torej ne bi bilo treba obvestiti[[35]](#footnote-36). Vendar ima lahko izguba ali sprememba negativne posledice za posameznike, na katere se nanašajo osebni podatki, tudi kadar so podatki šifrirani, če upravljavec podatkov nima ustreznih varnostnih kopij. V takem primeru bi se zahtevalo sporočanje posameznikom, na katere se nanašajo osebni podatki, tudi če so bili podatki ustrezno zaščiteni s šifriranjem.

Delovna skupina iz člena 29 je tudi pojasnila, da bi bilo podobno, če bi bili osebni podatki, kot so gesla, varno zgoščeni in soljeni, pri čemer je bila zgoščena vrednost izračunana z najsodobnejšo zgoščevalno funkcijo z uporabo šifrirnega ključa, ključ za zgoščevanje podatkov ni bil ogrožen pri nobeni kršitvi in ključ za zgoščevanje podatkov je bil ustvarjen tako, da ga s tehnološkimi sredstvi, ki so na voljo, ne more ugotoviti nobena oseba, ki nima dovoljenja za dostop do njega.

Posledično, če so osebni podatki postali v bistvu nerazumljivi za nepooblaščene osebe in če so podatki kopirani ali obstaja varnostna kopija, o kršitvi zaupnosti, ki vključuje ustrezno šifrirane osebne podatke, ni treba obvestiti nadzornega organa. Ni namreč verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. To seveda pomeni, da ne bi bilo treba obvestiti niti posameznika, saj ni verjetnosti za visoko tveganje. Vendar je treba upoštevati, da tudi če obveščanje prvotno ni potrebno, če ni verjetnega tveganja za pravice in svoboščine posameznikov, pa se to lahko sčasoma spremeni, tako da bi bilo treba tveganje ponovno oceniti. Če se na primer pozneje ugotovi, da je bil ogrožen ključ ali da je izpostavljena ranljivost programske opreme za šifriranje, je lahko še vedno potrebno obveščanje.

Poleg tega je treba opozoriti, da gre v primeru kršitve, pri kateri ni varnostnih kopij šifriranih osebnih podatkov, za kršitev razpoložljivosti, ki bi lahko ogrožala posameznike, tako da je lahko potrebno obveščanje. Podobno se lahko v primeru kršitve, ki vključuje izgubo šifriranih podatkov, tudi če obstaja varnostna kopija osebnih podatkov, to še vedno šteje za kršitev, o kateri je treba poročati, odvisno od tega, koliko časa traja, da se podatki povrnejo iz varnostne kopije, in kakšne so posledice, ki jih ima pomanjkanje razpoložljivosti za posameznike. Kot je navedeno v členu 32(1)(c), je pomemben dejavnik varnosti „zmožnos[t] pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta“.

**Primer**

Kršitev, o kateri ne bi bilo treba obvestiti nadzornega organa, bi bila izguba varno šifrirane mobilne naprave, ki jo uporabljata upravljavec in njegovo osebje. Če šifrirni ključ ostane na varnem pri upravljavcu in to ni edina kopija osebnih podatkov, potem napadalec ne bi imel dostopa do podatkov. To pomeni, da kršitev verjetno ne bi ogrožala pravic in svoboščin zadevnih posameznikov, na katere se nanašajo osebni podatki. Če se pozneje izkaže, da je bil šifrirni ključ ogrožen ali da sta programska oprema za šifriranje ali algoritem ranljiva, se ogrožanje pravic in svoboščin fizičnih oseb spremeni, tako da je lahko potrebno obveščanje.

Za neupoštevanje člena 33 pa gre, če upravljavec ne obvesti nadzornega organa v okoliščinah, ko podatki dejansko niso bili varno šifrirani. Zato bi morali upravljavci pri izbiri programske opreme za šifriranje skrbno pretehtati med kakovostjo in pravilnim izvajanjem šifriranja, ki je na voljo, ter razumeti, kakšno stopnjo zaščite dejansko zagotavlja in ali je ta ustrezna glede na prisotna tveganja. Upravljavci bi morali tudi poznati podrobno delovanje svojega izdelka za šifriranje. Naprava se na primer lahko šifrira ob izklopu, ne pa tudi v načinu pripravljenosti. Nekateri izdelki, ki uporabljajo šifriranje, imajo „privzete ključe“, ki jih mora vsak uporabnik spremeniti, da delujejo. Prav tako lahko strokovnjaki za varnost šifriranje trenutno štejejo za ustrezno, vendar lahko v nekaj letih postane zastarelo, tako da je vprašljivo, ali bi navedeni izdelek podatke zadostno šifriral in bi zagotavljal ustrezno stopnjo zaščite.

# Člen 34 – Sporočilo posamezniku, na katerega se nanašajo osebni podatki

## Obveščanje posameznikov

V nekaterih primerih mora upravljavec poleg obveščanja nadzornega organa kršitev sporočiti tudi prizadetim posameznikom.

Člen 34(1) določa:

„Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varnosti osebnih podatkov.“

Upravljavci bi morali obveščanje nadzornega organa šteti za obvezno, razen če zaradi kršitve verjetno niso ogrožene pravice in svoboščine posameznikov. Poleg tega je treba v primeru kršitve, ki verjetno zelo ogroža pravice in svoboščine posameznikov, obvestiti tudi posameznike. Prag za sporočanje kršitve posameznikom je torej višji kot za obveščanje nadzornih organov, zato vseh kršitev ni treba sporočiti posameznikom, da ti ne prejmejo preveč nepotrebnih obvestil.

V SUVP je navedeno, da je treba kršitev posameznikom sporočiti „brez nepotrebnega odlašanja“, kar pomeni čim prej. Glavni cilj obveščanja posameznikov je, da se jim zagotovijo konkretne informacije o tem, kaj morajo storiti, da se zaščitijo[[36]](#footnote-37). Kot je bilo navedeno zgoraj, se posamezniki glede na naravo kršitve in tveganja, ki ga pomeni, s pravočasnim sporočanjem lažje zaščitijo pred morebitnimi negativnimi posledicami kršitve.

Priloga B k tem smernicam vsebuje neizčrpen seznam primerov, v katerih je lahko verjetno, da kršitev povzroča visoko tveganje za posameznike, in posledično položajev, v katerih mora upravljavec kršitev sporočiti prizadetim osebam.

## Informacije, ki jih je treba zagotoviti

Pri obveščanju posameznikov člen 34(2) določa:

„V sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz odstavka 1 tega člena je v jasnem in preprostem jeziku opisana vrsta kršitve varnosti osebnih podatkov ter so vsebovane vsaj informacije in ukrepi iz točk (b), (c) in (d) člena 33(3).“

V skladu s to določbo bi moral upravljavec zagotoviti vsaj naslednje informacije:

* opis vrste kršitve;
* ime in kontaktne podatke pooblaščene osebe za varstvo podatkov ali druge kontaktne točke;
* opis verjetnih posledic kršitve in
* opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Kot primer ukrepov, sprejetih za obravnavo kršitve in ublažitev njenih morebitnih škodljivih učinkov, bi lahko upravljavec navedel, da je po obveščanju ustreznega nadzornega organa o kršitvi prejel nasvete za obvladanje kršitve in zmanjšanje njenega vpliva. Upravljavec bi moral po potrebi tudi zagotoviti konkretne nasvete posameznikom, da se zaščitijo pred morebitnimi škodljivimi posledicami kršitve, kot je ponastavitev gesel, če so bile ogrožene njihove poverilnice za dostop. Tudi v tem primeru lahko upravljavec poleg tistega, kar se zahteva tukaj, zagotovi še druge informacije.

## Vzpostavljanje stika s posamezniki

Načeloma je treba zadevno kršitev sporočiti neposredno zadevnim posameznikom, na katere se nanašajo osebni podatki, razen če bi bil zaradi tega potreben nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni (člen 34(3)(c)).

Posamezniki, na katere se nanašajo osebni podatki, bi morali biti o kršitvi obveščeni z namenskimi sporočili, ki ne bi smela biti poslana skupaj z drugimi informacijami, kot so redno sprotno obveščanje, glasila ali standardna sporočila. To prispeva k jasnemu in preglednemu sporočanju kršitve.

Primeri preglednih metod sporočanja vključujejo neposredno sporočanje (npr. elektronsko sporočilo, SMS, neposredno sporočilo), izpostavljene spletne pasice ali obvestila, poštno obveščanje in izpostavljene oglase v tiskanih medijih. Obvestilo, ki bi bilo omejeno samo na sporočilo za javnost ali spletni dnevnik podjetja, ne bi bil učinkovit način za sporočanje kršitve posamezniku. Delovna skupina iz člena 29 priporoča, naj upravljavci izberejo način, s katerim se povečujejo možnosti za pravilno sporočanje informacij vsem prizadetim posameznikom. Odvisno od okoliščin lahko to pomeni, da upravljavec uporabi različne metode sporočanja in ne samo enega kanala za stike.

Upravljavci morajo včasih zagotoviti tudi, da je sporočilo dostopno v primernih nadomestnih oblikah in ustreznih jezikih, da lahko posamezniki razumejo informacije, ki se jim zagotovijo. Na primer, pri sporočanju kršitve posamezniku je večinoma primerno uporabiti jezik, ki se je uporabljal pri predhodnem običajnem poslovanju s prejemnikom. Če pa kršitev zadeva posameznike, na katere se nanašajo osebni podatki, s katerimi upravljavec pred tem ni komuniciral, ali zlasti tiste, ki prebivajo v drugi državi članici ali drugi državi zunaj EU, ki ni država ustanovitve upravljavca, bi bilo lahko sprejemljivo sporočilo v lokalnem nacionalnem jeziku, pri čemer se upoštevajo potrebna sredstva. Ključno je, da se posameznikom, na katere se nanašajo osebni podatki, pomaga razumeti vrsta kršitve in ukrepi, s katerimi se lahko zaščitijo.

Upravljavci so najprimernejši, da določijo najustreznejši kanal za stik pri sporočanju kršitve posameznikom, zlasti če redno komunicirajo s svojimi strankami. Vendar bi moral biti upravljavec previden pri uporabi kanala za stik, ki je ogrožen zaradi kršitve, saj bi lahko tak kanal uporabljali tudi napadalci, ki se izdajajo za upravljavca.

Hkrati je v uvodni izjavi 86 pojasnjeno:

„Posamezniki, na katere se nanašajo osebni podatki, bi morali prejeti tako sporočilo, kakor hitro je to razumno mogoče in v tesnem sodelovanju z nadzornim organom ter ob upoštevanju smernic, ki jih je podal nadzorni organ ali drugi ustrezni organi, kot so organi za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Potreba po ublažitvi neposrednega tveganja nastanka škode bi na primer terjala takojšnjo sporočilo posameznikom, na katere se nanašajo osebni podatki, potreba po izvajanju ustreznih ukrepov zoper nadaljnje ali podobne kršitve varnosti osebnih podatkov pa bi lahko upravičila daljši rok za sporočilo.“

Upravljavci zato morda želijo vzpostaviti stik in se posvetovati z nadzornim organom, da bi dobili nasvet ne samo o obveščanju posameznikov, na katere se nanašajo osebni podatki, o kršitvi v skladu s členom 34, ampak tudi o ustreznih sporočilih, ki jih je treba poslati posameznikom, in najustreznejšem načinu za vzpostavitev stika z njimi.

S tem je povezan nasvet v uvodni izjavi 88, da je treba pri obveščanju o kršitvi „upoštevati zakoniti interes organov kazenskega pregona, kadar bi zgodnje razkritje lahko po nepotrebnem oviralo preiskavo okoliščin kršitve varstva osebnih podatkov“. To lahko pomeni, da lahko upravljavec v nekaterih okoliščinah, ko je to upravičeno, in po nasvetu organov kazenskega pregona s sporočanjem kršitve prizadetim posameznikom počaka tako dolgo, da to ne škoduje takim preiskavam. Vendar je treba posameznike, na katere se nanašajo osebni podatki, zatem še vedno nemudoma obvestiti.

Kadar upravljavec kršitve ne more sporočiti posamezniku, ker ni shranjenih dovolj podatkov za vzpostavitev stika z njim, bi moral v takem konkretnem primeru posameznika obvestiti takoj, ko je to razumno mogoče (npr. ko posameznik uveljavi svojo pravico iz člena 15 do dostopa do osebnih podatkov in upravljavcu zagotovi potrebne dodatne informacije za vzpostavitev stika z njim).

## Okoliščine, v katerih se ne zahteva sporočanje

V členu 34(3) so navedeni trije pogoji, ki, če so izpolnjeni, ne vsebujejo zahteve po obveščanju posameznikov v primeru kršitve. Ti so:

* Upravljavec je pred kršitvijo uporabil ustrezne tehnične in organizacijske ukrepe za varstvo osebnih podatkov, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih. To bi lahko vključevalo na primer zaščito osebnih podatkov z najsodobnejšim šifriranjem ali tokenizacijo.
* Upravljavec je takoj po kršitvi sprejel ukrepe za zagotovitev, da ni več verjetnosti, da bi se veliko tveganje za pravice in svoboščine posameznikov uresničilo. Na primer, upravljavec je glede na okoliščine zadeve morda takoj prepoznal posameznika, ki je dostopal do osebnih podatkov, in zoper njega ukrepal, preden je ta lahko z njimi kar koli počel. Še vedno je treba ustrezno upoštevati morebitne posledice kakršne koli kršitve zaupnosti, kar je tudi v tem primeru odvisno od narave zadevnih podatkov.
* Za vzpostavitev stika s posamezniki bi bil potreben nesorazmeren napor[[37]](#footnote-38), če so bili njihovi kontaktni podatki morda izgubljeni zaradi kršitve ali pa sploh niso znani. Na primer, skladišče statističnega urada je poplavilo, dokumenti, ki vsebujejo osebne podatke, pa so bili shranjeni samo v papirni obliki. Namesto tega mora upravljavec objaviti javno sporočilo ali izvesti podoben ukrep, s katerim so posamezniki enako učinkovito obveščeni. V primeru nesorazmernega napora bi se lahko predvidela tudi taka tehnična ureditev, da bi bile informacije o kršitvi na voljo na zahtevo, kar bi lahko bilo koristno za tiste posameznike, ki so lahko prizadeti zaradi kršitve, vendar upravljavec z njimi ne more drugače vzpostaviti stika.

V skladu z načelom odgovornosti bi morali biti upravljavci nadzornemu organu zmožni dokazati, da izpolnjujejo enega ali več teh pogojev[[38]](#footnote-39). Upoštevati je treba, da tudi če se obveščanje prvotno ne zahteva, kadar ni tveganja za pravice in svoboščine fizičnih oseb, pa se to lahko sčasoma spremeni, tako da je treba tveganje ponovno oceniti.

Če se upravljavec odloči, da kršitve ne bo sporočil posamezniku, je v členu 34(4) pojasnjeno, da lahko to od njega zahteva nadzorni organ, če meni, da bi kršitev verjetno povzročila veliko tveganje za posameznike. Lahko pa tudi ugotovi, da so izpolnjeni pogoji iz člena 34(3), tako da obveščanje posameznikov ni potrebno. Če nadzorni organ ugotovi, da odločitev o neobveščanju posameznikov, na katere se nanašajo osebni podatki, ni utemeljena, lahko razmisli o uporabi pristojnosti in sankcij, ki jih ima na voljo.

# Ocenjevanje tveganja in velikega tveganja

## Tveganje kot dejavnik, ki zaradi katerega nastane potreba po obveščanju

Čeprav je s SUVP uvedena obveznost obveščanja o kršitvi, se to ne zahteva v vseh okoliščinah:

* Obveščanje pristojnega nadzornega organa je obvezno, razen če ni verjetno, da bi bile zaradi kršitve ogrožene pravice in svoboščine posameznikov.
* Sporočilo posamezniku o kršitvi je nujno le, če bi ta verjetno povzročila veliko tveganje za njegove pravice in svoboščine.

To pomeni, da je takoj po seznanitvi s kršitvijo ključnega pomena, da upravljavec ne samo omeji incident, ampak mora tudi oceniti tveganje, ki bi lahko iz njega izhajalo. Za to sta dva pomembna razloga: prvič, če upravljavec ve, kakšni sta verjetnost in morebitna resnost vpliva na posameznika, lažje sprejme učinkovite ukrepe za omejitev in obravnavo kršitve; drugič, lažje ugotovi, ali je treba obvestiti nadzorni organ in po potrebi zadevne posameznike.

Kot je pojasnjeno zgoraj, je obveščanje o kršitvi obvezno, razen če ni verjetno, da bi bile zaradi kršitve ogrožene pravice in svoboščine posameznikov, pri čemer je ključni dejavnik, zaradi katerega nastane potreba po sporočanju kršitve posameznikom, na katere se nanašajo osebni podatki, da bi verjetno povzročila *veliko* tveganje za njihove pravice in svoboščine. To tveganje obstaja, kadar bi lahko kršitev povzročila fizično, premoženjsko ali nepremoženjsko škodo za posameznike, katerih varnost podatkov je bila kršena. Primeri take škode so diskriminacija, kraja identitete ali goljufija, finančna izguba in okrnitev ugleda. Kadar kršitev vključuje osebne podatke, ki razkrivajo rasno ali etnično poreklo, politično mnenje, veroizpoved, ali filozofsko prepričanje ali članstvo v sindikatu ali vključuje genetske podatke ali podatke v zvezi z zdravjem ali podatke v zvezi s spolnim življenjem ali kazenskimi obsodbami in prekrški ali s tem povezanimi varnostnimi ukrepi, bi bilo treba nastanek take škode šteti za verjeten[[39]](#footnote-40).

## Dejavniki, ki jih je treba upoštevati pri ocenjevanju tveganja

V uvodnih izjavah 75 in 76 SUVP je predlagano, da bi bilo treba na splošno pri ocenjevanju tveganja upoštevati verjetnost in resnost tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Dalje je navedeno, da bi bilo treba tveganje oceniti na podlagi objektivne ocene.

Opozoriti je treba, da je poudarek pri ocenjevanju tveganja za pravice in svoboščine oseb zaradi kršitve drugačen kot pri tveganju, obravnavanem v oceni učinka v zvezi z varstvom podatkov[[40]](#footnote-41). V oceni učinka v zvezi z varstvom podatkov se obravnavajo tveganja pri obdelavi podatkov, ki se izvaja, kot je bilo načrtovano, in tveganja v primeru kršitve. Pri obravnavi morebitne kršitve se na splošno preučita verjetnost njenega nastanka in škoda, ki lahko iz tega izhaja za posameznika, na katerega se nanašajo osebni podatki; povedano drugače, gre za oceno hipotetičnega dogodka. Pri dejanski kršitvi se je dogodek dejansko že zgodil, tako da je poudarek v celoti na tveganju, ki izhaja iz vpliva kršitve na posameznike.

**Primer**

Ocena učinka v zvezi z varstvom podatkov pokaže, da je predlagana uporaba določene varnostne programske opreme za varstvo osebnih podatkov primeren ukrep za zagotovitev ustrezne ravni varnosti glede na tveganje, ki bi ga obdelava sicer povzročila za posameznike. Če pa je naknadno ugotovljena ranljivost, bi se s tem spremenila primernost programske opreme za omejitev tveganja za zaščitene osebne podatke, tako da bi jo bilo treba znova oceniti v okviru ocene učinka v zvezi z varstvom podatkov, ki poteka.

Pozneje se izkoristi ranljivost izdelka in pride do kršitve. Upravljavec bi moral oceniti konkretne okoliščine kršitve, prizadete podatke in morebitno raven vpliva na posameznike, pa tudi verjetnost, da se bo to tveganje uresničilo.

Tako bi moral upravljavec pri ocenjevanju tveganja za posameznike, ki izhaja iz kršitve, upoštevati konkretne okoliščine kršitve, vključno z resnostjo morebitnega vpliva in verjetnostjo za njegov nastanek. Delovna skupina iz člena 29 zato priporoča, da se pri oceni upoštevajo naslednja merila[[41]](#footnote-42):

* Vrsta kršitve

Vrsta kršitve, do katere je prišlo, lahko vpliva na stopnjo tveganja za posameznike. Na primer, kršitev zaupnosti, pri kateri so se zdravstvene informacije razkrile nepooblaščenim osebam, ima lahko drugačne posledice za posameznika kot kršitev, pri kateri so se zdravstveni podatki posameznika izgubili ali niso več na voljo.

* Narava, občutljivost in količina osebnih podatkov

Seveda sta pri ocenjevanju tveganja ključna dejavnika vrsta in občutljivost osebnih podatkov, katerih varnost je ogrožena zaradi kršitve. Običajno velja, da bolj kot so podatki občutljivi, večje je tveganje za škodo prizadetim osebam, vendar je treba upoštevati tudi druge osebne podatke, ki so lahko o posamezniku, na katerega se nanašajo, že na voljo. Na primer, v običajnih okoliščinah ni verjetno, da bi razkritje imena in naslova posameznika povzročilo večjo škodo. Če pa se biološkemu staršu razkrijeta ime in naslov posvojitelja, so lahko posledice zelo resne za posvojitelja in tudi za otroka.

Kršitve, ki vključujejo zdravstvene podatke, osebne dokumente ali finančne podatke, kot so podrobnosti o kreditni kartici, lahko vsaka posebej povzročijo škodo, skupaj pa se lahko uporabijo za krajo identitete. Kombinacija osebnih podatkov je navadno občutljivejša od posameznega osebnega podatka.

Nekatere vrste osebnih podatkov se lahko sprva zdijo razmeroma neškodljive, vendar je treba skrbno preučiti, kaj lahko taki podatki razkrijejo o prizadetem posamezniku. Seznam strank, ki prejemajo redne dostave, morda ni posebej občutljiv, vendar bi bili taki podatki o strankah, ki so prekinile dostavo med dopustom, koristne informacije za storilce kaznivih dejanj.

Podobno lahko majhna količina zelo občutljivih podatkov pomembno vpliva na posameznika, širok nabor podrobnosti pa lahko razkrije še večji nabor informacij o njem. Tudi kršitev, ki vpliva na velike količine osebnih podatkov o številnih posameznikih, lahko vpliva na ustrezno veliko število posameznikov.

* Enostavnost identifikacije posameznikov

Pomemben dejavnik, ki ga je treba upoštevati, je, kako enostavno lahko oseba, ki ima dostop do podatkov, katerih varnost je ogrožena, identificira konkretne posameznike ali podatke poveže z drugimi informacijami, da identificira posameznike. Glede na okoliščine bi bila identifikacija mogoča neposredno na podlagi osebnih podatkov, katerih varnost je kršena, ne da bi bilo treba posebej iskati, da bi ugotovili identiteto posameznika, lahko pa je osebne podatke tudi izjemno težko povezati s konkretnim posameznikom, kar bi bilo pod določenimi pogoji vseeno še vedno mogoče. Identifikacija je mogoča neposredno ali posredno na podlagi podatkov, katerih varnost je kršena, vendar je to lahko odvisno tudi od posebnih okoliščin kršitve in javne dostopnosti s tem povezanih podrobnosti o osebah. To je lahko pomembnejše pri kršitvah zaupnosti in razpoložljivosti.

Kot je navedeno zgoraj, osebni podatki, zaščiteni z ustrezno ravnjo šifriranja, nepooblaščenim osebam niso razumljivi brez ključa za dešifriranje. Poleg tega se lahko verjetnost za identifikacijo posameznikov v primeru kršitve zmanjša tudi s pravilno izvedeno psevdonimizacijo (ki je v členu 4(5) opredeljena kot „obdelav[a] osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku“). Vendar za same tehnike psevdonimizacije ni mogoče šteti, da z njimi podatki postanejo nerazumljivi.

* Resnost posledic za posameznike

Glede na naravo osebnih podatkov, zajetih s kršitvijo, na primer posebne kategorije podatkov, je lahko morebitna škoda za posameznike, ki bi jo to lahko povzročilo, še posebej resna, zlasti kadar bi lahko kršitev povzročila krajo identitete ali goljufijo, fizično škodo, psihično stisko, ponižanje ali okrnitev ugleda. Če se kršitev nanaša na osebne podatke o ranljivih posameznikih, bi lahko bilo tveganje škode v zvezi z njimi še večje.

To, ali je upravljavec seznanjen s tem, da so osebni podatki v rokah oseb, katerih nameni niso znani ali so potencialno zlonamerni, lahko vpliva na stopnjo morebitnega tveganja. Pride lahko do kršitve zaupnosti, s čimer se osebni podatki pomotoma razkrijejo tretji osebi, kot je opredeljena v členu 4(10), ali drugemu prejemniku. To se na primer lahko zgodi, kadar se osebni podatki nenamerno pošljejo napačnemu oddelku organizacije ali organizaciji ponudnika, ki se običajno uporablja. Upravljavec lahko od prejemnika zahteva, naj podatke, ki jih je prejel, bodisi vrne bodisi varno uniči. V obeh primerih se lahko prejemnik, glede na to, da je upravljavec v razmerju z njim in je lahko seznanjen z njegovimi postopki, zgodovino in drugimi pomembnimi podrobnostmi, šteje za „vrednega zaupanja“. Povedano drugače, upravljavec ima lahko določeno zagotovilo glede prejemnika, tako da lahko razumno pričakuje, da navedena oseba ne bo prebrala pomotoma poslanih podatkov ali do njih dostopala ter bo upoštevala navodila za njihovo vračilo. Tudi če se je dostopalo do podatkov, lahko upravljavec še vedno zaupa prejemniku, da ne bo sprejel nadaljnjih ukrepov v zvezi s podatki ter bo podatke nemudoma vrnil upravljavcu in sodeloval pri njihovi obnovitvi. V takih primerih se to lahko upošteva pri oceni tveganja, ki jo upravljavec izvede po kršitvi – dejstvo, da je prejemnik vreden zaupanja, lahko odpravi resnost posledic kršitve, vendar ne pomeni, da do kršitve ni prišlo. Se pa lahko s tem izključi verjetnost tveganja za posameznike, tako da se obveščanje nadzornega organa ali prizadetih posameznikov ne zahteva več. To je znova odvisno od posameznega primera. Vendar mora upravljavec še vedno hraniti informacije v zvezi s kršitvijo kot del splošne dolžnosti vodenja evidenc o kršitvah (glej oddelek V v nadaljevanju).

Upoštevati bi bilo treba tudi trajnost posledic za posameznike, pri čemer se lahko šteje, da je vpliv večji, če so učinki dolgoročni.

* Posebne značilnosti posameznika

Kršitev lahko vpliva na osebne podatke v zvezi z otroki ali drugimi ranljivimi posamezniki, ki so zato lahko v večji nevarnosti. V zvezi s posamezniki lahko obstajajo še drugi dejavniki, ki lahko vplivajo na raven vpliva kršitve nanje.

* Posebne značilnosti upravljavca podatkov

Narava in vloga upravljavca in njegovih dejavnosti lahko vplivata na raven tveganja, ki ga kršitev povzroča posameznikom. Na primer, zdravstvena organizacija obdeluje posebne kategorije osebnih podatkov, kar pomeni, da so v primeru kršitve varnosti svojih osebnih podatkov bolj ogroženi posamezniki kot pa poštni seznam glasila.

* Število prizadetih posameznikov

Kršitev lahko prizadene samo enega ali nekaj posameznikov ali pa več tisoč posameznikov, če ne še veliko več. Na splošno velja, da večje kot je število prizadetih posameznikov, večji vpliv ima lahko kršitev. Vendar lahko kršitev resno vpliva tudi na enega posameznika, odvisno od narave osebnih podatkov in okoliščin, v katerih je ogrožena njihova varnost. Tudi pri tem je ključno, da se upoštevata verjetnost in resnost vpliva na prizadete osebe.

* Splošni elementi

Zato bi moral upravljavec pri ocenjevanju tveganja, ki ga kršitev verjetno povzroča, upoštevati kombinacijo resnosti morebitnega vpliva na pravice in svoboščine posameznikov ter verjetnosti njegovega nastanka. Jasno je, da je v primeru resnejših posledic kršitve tudi tveganje večje, podobno pa se v primeru večje verjetnosti njihovega nastanka poveča tudi tveganje. Upravljavec bi moral biti v primeru dvoma previdnejši in obvestiti o kršitvi. V Prilogi B so navedeni nekateri koristni primeri različnih vrst kršitev, ki vključujejo tveganje ali veliko tveganje za posameznike.

Agencija Evropske unije za varnost omrežij in informacij (ENISA) je pripravila priporočila za metodologijo ocenjevanja resnosti kršitve, ki je lahko za upravljavce in obdelovalce koristna pri oblikovanju načrta odzivanja za obvladovanje kršitve[[42]](#footnote-43).

# Odgovornost in vodenje evidenc

## Dokumentiranje kršitev

Ne glede na to, ali je treba o kršitvi obvestiti nadzorni organ ali ne, mora upravljavec voditi dokumentacijo o vseh kršitvah, kot je pojasnjeno v členu 33(5):

„Upravljavec dokumentira vsako kršitev varnosti osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varnosti osebnih podatkov, njene učinke in sprejete popravne ukrepe. Ta dokumentacija nadzornemu organu omogoči, da preveri skladnost s tem členom.“

To je povezano z načelom odgovornosti iz SUVP, vsebovano v členu 5(2). Namen evidentiranja kršitev, za katere se ne zahteva obveščanje, in kršitev, za katere se zahteva obveščanje, je povezan tudi z obveznostmi upravljavca na podlagi člena 24, nadzorni organ pa lahko zahteva vpogled v te evidence. Upravljavci so zato spodbujeni k vzpostavitvi notranjega registra kršitev, ne glede na to, ali morajo o njih obveščati ali ne[[43]](#footnote-44).

Čeprav se upravljavec sam odloči, katero metodo in strukturo bo uporabil pri dokumentiranju kršitve, v smislu evidentiranih informacij obstajajo ključni elementi, ki bi jih bilo treba vključiti v vseh primerih. Kot se zahteva s členom 33(5), mora upravljavec evidentirati podrobnosti v zvezi s kršitvijo, ki bi morale vključevati vzroke zanjo, opis, kaj se je zgodilo, in osebne podatke, na katere je kršitev vplivala. Vključiti bi bilo treba tudi učinke in posledice kršitve, skupaj s popravnim ukrepom, ki ga je sprejel upravljavec.

V SUVP ni določeno obdobje hrambe take dokumentacije. Kadar take evidence vsebujejo osebne podatke, mora upravljavec določiti ustrezno obdobje hrambe v skladu z načeli v zvezi z obdelavo osebnih podatkov[[44]](#footnote-45) in imeti pravno podlago za obdelavo[[45]](#footnote-46). Dokumentacijo mora hraniti v skladu s členom 33(5), da lahko nadzornemu organu na zahtevo dokaže skladnost z navedenim členom ali na splošneje z načelom odgovornosti. Jasno je, da se načelo omejitve hrambe[[46]](#footnote-47) iz SUVP ne uporablja, če same evidence ne vsebujejo osebnih podatkov.

Delovna skupina iz člena 29 priporoča, naj upravljavec poleg teh podrobnosti dokumentira tudi svoje razloge za odločitve, sprejete v odziv na kršitev. Če ni obveščanja o kršitvi, bi bilo treba zlasti dokumentirati utemeljitev take odločitve. To bi moralo vključevati razloge, zaradi katerih upravljavec meni, da kršitev verjetno ne ogroža pravic in svoboščin[[47]](#footnote-48). Če pa upravljavec meni, da je izpolnjen kateri od pogojev iz člena 34(3), mora biti zmožen zagotoviti ustrezne dokaze o tem.

Kadar upravljavec o kršitvi obvesti nadzorni organ, vendar obvestilo zamuja, mora biti zmožen zagotoviti razloge za tako zamudo; dokumentacija v zvezi s tem bi lahko pomagala pri dokazovanju, da je zamuda pri poročanju upravičena in ni pretirana.

Kadar upravljavec kršitev sporoči prizadetim posameznikom, mora biti pri navedbi kršitve jasen ter jo sporočiti učinkovito in pravočasno. Tako bi upravljavec lažje dokazal odgovornost in skladnost s hrambo, če bi hranil dokaze o takem sporočanju.

Za lažje upoštevanje členov 33 in 34 bi bilo koristno, če bi imeli upravljavci in obdelovalci vzpostavljen dokumentiran postopek obveščanja, s katerim bi se določal postopek po odkritju kršitve, vključno s tem, kako omejiti, obvladovati in odpraviti incident, ter ocenjevalo tveganje in obveščalo o kršitvi. V zvezi s tem bi bilo lahko za dokazovanje skladnosti s SUVP tudi koristno dokazati, da so bili zaposleni obveščeni o obstoju takih postopkov in mehanizmov ter da vedo, kako se odzvati na kršitve.

Opozoriti je treba, da lahko nadzorni organ zaradi neustreznega dokumentiranja kršitve uporabi pristojnosti na podlagi člena 58 ali naloži upravno globo v skladu s členom 83.

## Vloga pooblaščene osebe za varstvo podatkov

Upravljavec ali obdelovalec ima lahko pooblaščeno osebo za varstvo podatkov[[48]](#footnote-49), bodisi kot se zahteva s členom 37 bodisi prostovoljno v skladu z dobro prakso. Člen 39 SUVP določa več obveznih nalog pooblaščene osebe za varstvo podatkov, vendar upravljavcu ne preprečuje, da ji po potrebi dodeli še druge naloge.

Med obvezne naloge pooblaščene osebe za varstvo podatkov, ki so posebnega pomena za obveščanje o kršitvah, med drugim spadajo zagotavljanje nasvetov o varstvu podatkov in informacij upravljavcu in obdelovalcu, spremljanje skladnosti s SUVP in zagotavljanje nasvetov glede ocen učinka v zvezi z varstvom podatkov. Pooblaščena oseba za varstvo podatkov mora tudi sodelovati z nadzornim organom in delovati kot kontaktna točka za nadzorni organ in posameznike, na katere se nanašajo osebni podatki. Opozoriti je treba še, da mora upravljavec pri obveščanju nadzornega organa o kršitvi v skladu s členom 33(3)(b) zagotoviti ime in kontaktne podatke svoje pooblaščene osebe za varstvo podatkov ali druge kontaktne točke.

V smislu dokumentiranja kršitev lahko upravljavec ali obdelovalec želi pridobiti mnenje svoje pooblaščene osebe za varstvo podatkov glede strukture, vzpostavitve in vodenja te dokumentacije. Dodatna naloga pooblaščene osebe za varstvo podatkov bi lahko bila tudi vodenje takih evidenc.

To pomeni, da bi morala pooblaščena oseba za varstvo podatkov zagotavljati ključno pomoč pri preprečevanju kršitev in pripravi nanje z zagotavljanjem nasvetov in spremljanjem skladnosti, pa tudi med kršitvijo (tj. ob obveščanju nadzornega organa) in med morebitno poznejšo preiskavo s strani nadzornega organa. Glede na to Delovna skupina iz člena 29 priporoča, da se pooblaščena oseba za varstvo podatkov nemudoma obvesti o obstoju kršitve ter da sodeluje v celotnem postopku obvladovanja kršitve in obveščanja o njej.

# Obveznosti obveščanja na podlagi drugih pravnih instrumentov

Poleg obveščanja o kršitvah in njihovega sporočanja na podlagi SUVP bi morali biti upravljavci ločeno seznanjeni tudi z morebitnimi zahtevami za obveščanje o varnostnih incidentih na podlagi druge s tem povezane zakonodaje, ki se lahko uporablja zanje, in s tem, ali lahko to tudi pomeni, da morajo nadzorni organ istočasno obvestiti o kršitvi varnosti osebnih podatkov. Take zahteve se lahko med državami članicami razlikujejo, vendar primeri zahtev po obveščanju v drugih pravnih instrumentih in načini, kako so ti medsebojno povezani s SUVP, vključujejo naslednje:

* Uredba (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (uredba o elektronski identifikaciji)[[49]](#footnote-50).

V skladu s členom 19(2) uredbe o elektronski identifikaciji morajo ponudniki storitev zaupanja o vsaki kršitvi varnosti ali izgubi celovitosti, ki znatno vpliva na zagotovljeno storitev zaupanja ali na osebne podatke, vsebovane v njej, obvestiti svoj nadzorni organ. Kadar je to ustrezno – tj. kadar taka kršitev ali izguba pomeni tudi kršitev varnosti osebnih podatkov na podlagi SUVP –, mora ponudnik storitve zaupanja obvestiti tudi nacionalni nadzorni organ.

* Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva o kibernetski varnosti)[[50]](#footnote-51).

V skladu s členoma 14 in 16 direktive o kibernetski varnosti morajo izvajalci bistvenih storitev in ponudniki digitalnih storitev o varnostnih incidentih obvestiti svoj pristojni organ.Kot je priznano v uvodni izjavi 63 direktive o kibernetski varnosti[[51]](#footnote-52), je zaradi incidentov pogosto ogrožena varnost osebnih podatkov.Medtem ko morajo v skladu z direktivo o kibernetski varnosti pristojni organi in nadzorni organi sodelovati ter si v okviru tega izmenjavati informacije, pa še vedno velja, da kadar taki incidenti pomenijo ali postanejo kršitve varnosti osebnih podatkov na podlagi SUVP, bi morali taki izvajalci in/ali ponudniki obvestiti nadzorni organ ločeno od zahtev po obveščanju o incidentih na podlagi direktive o kibernetski varnosti.

**Primer**

Ponudnik storitev v oblaku mora ob obveščanju o kršitvi na podlagi direktive o kibernetski varnosti morda obvestiti tudi upravljavca, če to vključuje kršitev varnosti osebnih podatkov. Podobno se lahko od ponudnika storitev zaupanja ob obveščanju na podlagi uredbe o elektronski identifikaciji zahteva tudi, da v primeru kršitve obvesti ustrezni organ za varstvo podatkov.

* Direktiva 2009/136/ES (direktiva o pravicah državljanov) in Uredba št. 611/2013 (uredba o obveščanju o kršitvah).

Ponudniki javno dostopnih elektronskih komunikacijskih storitev v okviru Direktive 2002/58/ES[[52]](#footnote-53) morajo o kršitvah obvestiti pristojne nacionalne organe.

Upravljavci bi morali biti seznanjeni tudi z morebitnimi dodatnimi pravnimi, zdravstvenimi ali poklicnimi dolžnostmi obveščanja na podlagi drugih veljavnih ureditev.

# Priloga

## Shematski prikaz zahtev po obveščanju

Ali je verjetno, da bo kršitev povzročila veliko tveganje za pravice in svoboščine posameznikov?

Ali je verjetno, da bo kršitev povzročila tveganje za pravice in svoboščine posameznikov?

Da.

Ne.

Obveščanje nadzornega organa ali posameznikov se ne zahteva.

Obvestite pristojni nadzorni organ.

Če kršitev vpliva na posameznike v več kot eni državi članici, obvestite vodilni nadzorni organ.

Da.

Ne.

Obveščanje posameznikov se ne zahteva.

Obvestite prizadete posameznike in jim po potrebi zagotovite informacije o tem, kako se lahko zaščitijo pred posledicami kršitve.

Vse kršitve je treba evidentirati v skladu s členom 33(5). Upravljavec bi moral kršitev dokumentirati in voditi evidenco.

Upravljavec je „seznanjen“ s kršitvijo varnosti osebnih podatkov in oceni tveganje za posameznike.

# 

## Primeri kršitev varnosti osebnih podatkov in koga je treba obvestiti

Naslednji neizčrpni primeri upravljavcem pomagajo pri ugotavljanju, ali se v različnih scenarijih kršitve varnosti osebnih podatkov zahteva obveščanje. Ti primeri lahko tudi pomagajo razlikovati med tveganjem in velikim tveganjem za pravice in svoboščine posameznikov.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primer** | **Ali je treba obvestiti nadzorni organ?** | **Ali je treba obvestiti posameznika, na katerega se nanašajo osebni podatki?** | **Opombe/priporočila** |
| i. Upravljavec je shranil varnostno kopijo arhiva šifriranih osebnih podatkov na pomnilniški ključek USB. Med vlomom je ključek ukraden. | Ne. | Ne. | Če so podatki šifrirani z najsodobnejšim algoritmom, če obstaja varnostna kopija podatkov, če ni ogrožen enkratni ključ in če je mogoče podatke obnoviti pravočasno, o tej kršitvi morda ni treba poročati. Če pa je pozneje ogrožena varnost podatkov, se zahteva obveščanje. |
| ii. Upravljavec upravlja spletno storitev. Zaradi kibernetskega napada na to storitev odtekajo osebni podatki posameznikov.  Upravljavec ima stranke v eni sami državi članici. | Da, v primeru verjetnih posledic za posameznike poročajte nadzornemu organu. | Da, glede na naravo zadevnih osebnih podatkov in v primeru zelo resnih verjetnih posledic za posameznike poročajte posameznikom. |  |
| iii. Zaradi kratkega, nekajminutnega izpada elektrike v klicnem centru upravljavca stranke ne morejo priklicati upravljavca in dostopati do svojih evidenc. | Ne. | Ne. | To ni kršitev, pri kateri bi bilo potrebno obveščanje, še vedno pa gre za incident, ki ga je treba evidentirati v skladu s členom 33(5).  Ustrezno evidenco bi moral voditi upravljavec. |
| iv. Upravljavec je žrtev izsiljevalskega napada, ki povzroči, da se vsi podatki šifrirajo. Varnostne kopije niso na voljo in podatkov ni mogoče obnoviti. Med preiskavo postane jasno, da je bila edina funkcija izsiljevalskega programja šifriranje podatkov in da v sistemu ni bilo druge zlonamerne programske opreme. | Da, poročajte nadzornemu organu, če so posledice za posameznike verjetne, saj gre za izgubo razpoložljivosti. | Da, glede na naravo zadevnih osebnih podatkov, morebitni učinek pomanjkanja razpoložljivosti podatkov ter druge verjetne posledice poročajte posameznikom. | Če bi bila na voljo varnostna kopija in bi bilo mogoče podatke pravočasno obnoviti, ne bi bilo treba poročati nadzornemu organu ali posameznikom, saj ne bi bilo trajne izgube razpoložljivosti ali zaupnosti. Če pa je bil nadzorni organ seznanjen z incidentom kako drugače, lahko razmisli o izvedbi preiskave, da se oceni skladnost s širšimi varnostnimi zahtevami iz člena 32. |
| v. Posameznik pokliče v klicni center banke in prijavi kršitev varnosti podatkov. Prejel je mesečni izpisek nekoga drugega.  Upravljavec izvede kratko preiskavo (tj. dokončano v 24 urah) in z razumno gotovostjo ugotovi, ali je prišlo do kršitve varnosti osebnih podatkov in ali ima sistemsko pomanjkljivost, zaradi katere so ali bi lahko bili prizadeti še drugi posamezniki. | Da. | Če je tveganje veliko in je jasno, da drugi niso bili prizadeti, se obvestijo samo prizadeti posamezniki. | Če se po nadaljnji preiskavi ugotovi, da je prizadetih več posameznikov, je treba nadzornemu organu zagotoviti najnovejše informacije, upravljavec pa sprejme dodaten ukrep obveščanja drugih posameznikov, če je tveganje v zvezi z njimi veliko. |
| vi. Upravljavec upravlja spletno tržnico in ima stranke iz več držav članic. Tržnica je žrtev kibernetskega napada, pri čemer napadalec na spletu objavi uporabniška imena, gesla in zgodovino nakupov. | Da, če gre za čezmejno obdelavo, poročajte vodilnemu nadzornemu organu. | Da, saj bi lahko kršitev povzročila veliko tveganje. | Upravljavec bi moral ukrepati, npr. s prisilno ponastavitvijo gesel prizadetih računov ter drugimi ukrepi za zmanjšanje tveganja.  Upravljavec bi moral upoštevati še morebitne druge obveznosti obveščanja, npr. na podlagi direktive o kibernetski varnosti kot ponudnik digitalnih storitev. |
| vii. Družba za spletno gostovanje, ki deluje kot obdelovalec podatkov, odkrije napako v kodi, ki nadzoruje uporabniška dovoljenja. Napaka povzroči, da lahko kateri koli uporabnik dostopa do podatkov o računu katerega koli drugega uporabnika. | Družba za spletno gostovanje mora kot obdelovalec brez nepotrebnega odlašanja obvestiti svoje prizadete stranke (upravljavce).  Ob predpostavki, da je družba za spletno gostovanje izvedla svojo preiskavo, bi morali dobiti prizadeti upravljavci razumno zagotovilo, da je bil vsak od njih žrtev kršitve in da se bo zato verjetno štelo, da je bil „seznanjen“, ko ga je obvestila družba za gostovanje (obdelovalec). Upravljavec mora nato obvestiti nadzorni organ. | Če verjetno ni visokega tveganja za posameznike, teh ni treba obvestiti. | Družba za spletno gostovanje (obdelovalec) mora upoštevati vse druge obveznosti obveščanja (npr. na podlagi direktive o kibernetski varnosti kot ponudnik digitalnih storitev).  Če ni dokazov, da se je ta ranljivost izkoristila pri katerem koli od njegovih upravljavcev, morda ni šlo za kršitev, v zvezi s katero se zahteva obveščanje, vendar jo je verjetno treba evidentirati ali pa gre za vprašanje neskladnosti na podlagi člena 32. |
| viii. Zdravstvene kartoteke v bolnišnici zaradi kibernetskega napada niso na voljo 30 ur. | Da, bolnišnica mora obvezno obvestiti nadzorni organ, saj sta lahko zelo ogrožena dobro počutje in zasebnost pacientov. | Da, poročajte prizadetim posameznikom. |  |
| ix. Osebni podatki velikega števila študentov se pomotoma pošljejo napačnemu poštnemu seznamu z več kot 1 000 prejemniki. | Da, poročajte nadzornemu organu. | Da, glede na obseg in vrsto osebnih podatkov, ki jih to zadeva, in resnost morebitnih posledic poročajte posameznikom. |  |
| x. Elektronsko sporočilo za neposredno trženje se pošlje prejemnikom v poljih „za:“ (to:) ali „kp:“ (cc:), tako da lahko vsak prejemnik vidi elektronske naslove drugih prejemnikov. | Da, obveščanje nadzornega organa je lahko obvezno, če je prizadetih veliko posameznikov, če so razkriti občutljivi podatki (npr. poštni seznam psihoterapevta) ali če drugi dejavniki pomenijo veliko tveganje (npr. sporočilo vsebuje začetna gesla). | Da, glede na obseg in vrsto osebnih podatkov, ki jih to zadeva, ter resnost morebitnih posledic poročajte posameznikom. | Obveščanje morda ni potrebno, če niso razkriti občutljivi podatki in če je razkrito le manjše število elektronskih naslovov. |

1. Glej člen 4(21) SUVP. [↑](#footnote-ref-2)
2. Glej <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:32009L0136> in [http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32013R0611](http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32013R0611). [↑](#footnote-ref-3)
3. Glej <https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm>. [↑](#footnote-ref-4)
4. Glej <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:31995L0046>. [↑](#footnote-ref-5)
5. Pravice, določene v Listini EU o temeljnih pravicah, na voljo na spletnem naslovu: <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:12012P/TXT>. [↑](#footnote-ref-6)
6. Glej člen 33(2). To je po zasnovi podobno členu 5 Uredbe (EU) št. 611/2013, ki določa, da mora ponudnik, ki se ga najame za opravljanje dela elektronskih komunikacijskih storitev (in ni v neposrednem pogodbenem razmerju z naročniki), v primeru kršitve varnosti osebnih podatkov o tem nemudoma obvestiti ponudnika, ki ga je najel. [↑](#footnote-ref-7)
7. Glej člena 34(4) in 58(2)(e). [↑](#footnote-ref-8)
8. To je mogoče zagotoviti v okviru zahteve po spremljanju in pregledu iz ocene učinka v zvezi z varstvom podatkov, ki se zahteva za postopke obdelave, ki bi povzročili veliko tveganje za pravice in svoboščine posameznikov (člen 35(1) in (11)). [↑](#footnote-ref-9)
9. Glej Mnenje št. 03/2014 o obveščanju o kršitvah varnosti osebnih podatkov <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_sl.pdf>. [↑](#footnote-ref-10)
10. Glej člen 5(1)(f) in člen 32. [↑](#footnote-ref-11)
11. Člen 32; glej tudi uvodno izjavo 83. [↑](#footnote-ref-12)
12. Glej uvodno izjavo 87. [↑](#footnote-ref-13)
13. Opozoriti je treba, da varnostni incident ni omejen na modele groženj, ko je organizacija napadena iz zunanjega vira, temveč vključuje tudi incidente pri notranji obdelavi, s katerimi se kršijo varnostna načela. [↑](#footnote-ref-14)
14. Glej Mnenje št. 03/2014. [↑](#footnote-ref-15)
15. Splošno je znano, da je „dostop“ v osnovi del „razpoložljivosti“. Glej na primer NIST SP800-53rev4, v katerem je „razpoložljivost“ opredeljena kot „zagotavljanje pravočasnega in zanesljivega dostopa do informacij in njihove uporabe“, na voljo na spletnem naslovu: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. Tudi v CNSSI-4009 je navedeno, da je „pravočasen in zanesljiv dostop do podatkov in informacijskih storitev za pooblaščene uporabnike“, glej <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>. Tudi v ISO/IEC 27000:2016 je „razpoložljivost“ opredeljena kot to, da so „podatki dostopni ter na voljo za uporabo na zahtevo pooblaščenega subjekta“: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en>. [↑](#footnote-ref-16)
16. Glej člen 33(5). [↑](#footnote-ref-17)
17. Glej tudi uvodni izjavi 85 in 75. [↑](#footnote-ref-18)
18. Glej tudi uvodno izjavo 86. [↑](#footnote-ref-19)
19. Za več podrobnosti glej Smernice Delovne skupine iz člena 29 o uporabi in določanju upravnih glob, ki so na voljo na spletnem naslovu: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889>. [↑](#footnote-ref-20)
20. Pomembna je tudi uvodna izjava 85. [↑](#footnote-ref-21)
21. Glej uvodno izjavo 87. [↑](#footnote-ref-22)
22. Glej smernice Delovne skupine iz člena 29 o ocenah učinka v zvezi z varstvom podatkov na spletnem naslovu: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137>. [↑](#footnote-ref-23)
23. Opozoriti je treba, da se lahko tudi dnevniški podatki, zaradi katerih je možnost revizije na primer hrambe, sprememb ali brisanja podatkov lažja, štejejo za osebne podatke v zvezi z osebo, ki je začela zadevni postopek obdelave. [↑](#footnote-ref-24)
24. Glej Uredbo št. 1182/71 o določitvi pravil glede rokov, datumov in iztekov rokov, ki je na voljo na spletnem naslovu: <http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:31971R1182&from=SL>. [↑](#footnote-ref-25)
25. Glej tudi uvodno izjavo 79. [↑](#footnote-ref-26)
26. Glej člen 9. [↑](#footnote-ref-27)
27. Glej člen 4(23). [↑](#footnote-ref-28)
28. Glej tudi uvodno izjavo 122. [↑](#footnote-ref-29)
29. Glej Smernice Delovne skupine iz člena 29 za opredelitev vodilnega nadzornega organa upravljavca ali obdelovalca, na voljo na spletnem naslovu: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44102>. [↑](#footnote-ref-30)
30. Seznam kontaktnih podatkov vseh evropskih nacionalnih organov za varstvo podatkov je na voljo na spletnem naslovu: <http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm>. [↑](#footnote-ref-31)
31. Glej tudi uvodni izjavi 23 in 24. [↑](#footnote-ref-32)
32. Glej tudi uvodno izjavo 25. [↑](#footnote-ref-33)
33. Glej uvodno izjavo 80 in člen 27. [↑](#footnote-ref-34)
34. Delovna skupina iz člena 29, Mnenje št. 03/2014 o obveščanju o kršitvah<http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_sl.pdf>. [↑](#footnote-ref-35)
35. Glej tudi člen 4(1) in (2) Uredbe št. 611/2013. [↑](#footnote-ref-36)
36. Glej tudi uvodno izjavo 86. [↑](#footnote-ref-37)
37. Glej smernice Delovne skupine iz člena 29 o preglednosti, v katerih je obravnavano vprašanje nesorazmernega napora in ki so na voljo na spletnem naslovu: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>. [↑](#footnote-ref-38)
38. Glej člen 5(2). [↑](#footnote-ref-39)
39. Glej uvodni izjavi 75 in 85. [↑](#footnote-ref-40)
40. Glej smernice Delovne skupine iz člena 29 o ocenah učinka v zvezi z varstvom podatkov na spletnem naslovu: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137>. [↑](#footnote-ref-41)
41. Člen 3(2) Uredbe št. 611/2013 določa smernice glede dejavnikov, ki bi jih bilo treba upoštevati v zvezi z obveščanjem o kršitvah v sektorju elektronskih komunikacijskih storitev, kar je lahko koristno v okviru obveščanja na podlagi SUVP. Glej <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sl:PDF>. [↑](#footnote-ref-42)
42. ENISA, Priporočila za metodologijo ocenjevanja resnosti kršitev varnosti osebnih podatkov, <https://www.enisa.europa.eu/publications/dbn-severity>. [↑](#footnote-ref-43)
43. Upravljavec se lahko odloči za dokumentiranje kršitev v okviru svoje evidence dejavnosti obdelave, ki jo vodi v skladu s členom 30. Če so informacije v zvezi s kršitvijo jasno prepoznavne kot take in jih je mogoče pridobiti na zahtevo, ločena evidenca ni potrebna. [↑](#footnote-ref-44)
44. Glej člen 5. [↑](#footnote-ref-45)
45. Glej člen 6 in tudi člen 9. [↑](#footnote-ref-46)
46. Glej člen 5(1)(e). [↑](#footnote-ref-47)
47. Glej uvodno izjavo 85. [↑](#footnote-ref-48)
48. Glej smernice Delovne skupine iz člena 29 o pooblaščenih osebah za varstvo podatkov na spletnem naslovu: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>. [↑](#footnote-ref-49)
49. Glej <https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32014R0910&from=SL>. [↑](#footnote-ref-50)
50. Glej <https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016L1148&from=sl>. [↑](#footnote-ref-51)
51. Uvodna izjava 63: *„V številnih primerih je zaradi incidentov ogrožena varnost osebnih podatkov. Zato bi morali pristojni organi in organi za varstvo podatkov pri odpravljanju kršitev varnosti osebnih podatkov, nastalih zaradi incidentov, med seboj sodelovati in si izmenjevati pomembne informacije.“* [↑](#footnote-ref-52)
52. Evropska komisija je 10. januarja 2017 predlagala uredbo o zasebnosti in elektronskih komunikacijah, ki bo nadomestila Direktivo 2009/136/ES in odpravila zahteve po obveščanju. Dokler pa tega predloga ne odobri Evropski parlament, ostaja veljavna obstoječa zahteva po obveščanju, glej <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>. [↑](#footnote-ref-53)