Smernice

Smernice 9/2022 o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Splošne uredbe o varstvu podatkov

Različica 2.0

Sprejete 28. marca 2023

Zgodovina različic

Različica 1.0	10. oktober 2022	Sprejetje smernic (posodobljena različica prejšnjih smernic WP250 (rev.01), ki jih je sprejela Delovna skupina iz člena 29 in jih je EOVP potrdil 25. maja 2018) za ciljno usmerjeno javno posvetovanje.
Različica 2.0	28. marec 2023	Sprejetje smernic po ciljno usmerjenem javnem posvetovanju na temo obveščanje o kršitvi varnosti osebnih podatkov za upravljavce, ki nimajo ustanovitve v EGP.

KAZALO

Evropski odbor za varstvo podatkov je –

ob upoštevanju točk e in l prvega odstavka 70. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju 12. in 22. člena svojega poslovnika,

ob upoštevanju Smernic Delovne skupine iz člena 29 o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679, WP250 rev.01 –

SPREJEL NASLEDNJE SMERNICE:

0 PREDGOVOR

1. Delovna skupina iz člena 29 je 3. oktobra 2017 sprejela Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679 (WP250 rev.01)[2], ki jih je Evropski odbor za varstvo podatkov (v nadaljevanju: EOVP) potrdil na svojem prvem plenarnem zasedanju[3]. Ta dokument je nekoliko posodobljena različica teh smernic. Vsako sklicevanje na Smernice Delovne skupine iz člena 29 o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679 (WP250 rev.01) je treba odslej razumeti kot sklicevanje na te smernice EOVP 9/2022.
2. EOVP je ugotovil, da je treba pojasniti zahteve po obveščanju glede kršitev varnosti osebnih podatkov v ustanovitvah zunaj EU. Odstavek, ki se nanaša to zadevo, je bil revidiran in posodobljen, preostali del dokumenta pa je ostal nespremenjen, razen pri redakcijskih spremembah. Natančneje, revizija se nanaša na odstavek 73 v oddelku II.C.2 tega dokumenta.

UVOD

3. S Splošno uredbo o varstvu podatkov se je uvedla zahteva, da je treba o kršitvi varnosti osebnih podatkov (v nadaljevanju: kršitev) obvestiti pristojni nacionalni nadzorni organ [4] (ali v primeru čezmejne kršitve vodilni nadzorni organ) in da je treba v nekaterih primerih o kršitvi obvestiti posameznike, na katere osebne podatke je kršitev vplivala.
4. Obveznosti obveščanja v primerih kršitev so že veljale za nekatere organizacije, kot so ponudniki javno dostopnih elektronskih komunikacijskih storitev (kot so določeni v Direktivi 2009/136/ES in Uredbi (EU)

[1] Sklicevanja na »države članice« v tem dokumentu je treba razumeti kot sklicevanja na »države članice Evropskega gospodarskega prostora (EGP)«.
[2] Smernice Delovne skupine iz člena 29 o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679 (WP250 rev.01) (nazadnje revidirane in posodobljene 6. februarja 2018) so na voljo na spletnem naslovu: https://ec.europa.eu/newsroom/article29/items/612052.
[3] Glej https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_sl.
[4] Glej enaindvajseti odstavek 4. člena Splošne uredbe o varstvu podatkov.

št. 611/2013)[5]. Tudi nekatere države članice so pred tem že uvedle nacionalno obveznost obveščanja o kršitvah. Ta je lahko vključevala obveznost obveščanja o kršitvah, ki je poleg ponudnikov javno dostopnih elektronskih komunikacijskih storitev vključevala 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 morda uvedle ustrezne kodekse ravnanja (na primer na Irskem[6]). Čeprav so številni nadzorni organi za varstvo osebnih podatkov v EU upravljavce spodbujali k poročanju o kršitvah, pa Direktiva 95/46/ES o varstvu podatkov[7], ki jo je Splošna uredba o varstvu podatkov nadomestila, ni vsebovala posebne obveznosti glede obveščanja o kršitvah. Zato je bila taka zahteva za številne organizacije nova. S Splošno uredbo o varstvu podatkov je obveščanje postalo obvezno za vse upravljavce, razen če ni verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov[8]. Pomembno vlogo imajo tudi obdelovalci, ki morajo o vsaki kršitvi obvestiti upravljavca[9].

5. Po mnenju EOVP ima 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 te posameznike obvestiti o kršitvi[10]. Upravljavec lahko z obveščanjem posameznikov o kršitvi 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 83. člena Splošne uredbe o varstvu podatkov naloži sankcija.

6. Upravljavci in obdelovalci so zato spodbujeni k vnaprejšnjemu načrtovanju in vzpostavitvi mehanizmov, s katerimi lahko kršitev odkrijejo in jo hitro omejijo, ocenijo tveganje za posameznike[11] ter presodijo, ali je treba obvestiti pristojni nadzorni organ, in o kršitvi po potrebi obvestiti zadevne posameznike. Obveščanje nadzornega organa mora biti del navedenega načrta odzivanja na incidente.

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

8. Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah varnosti osebnih podatkov[12] zagotovila smernice za upravljavce osebnih podatkov, ki bi jim morale v primeru kršitve pomagati pri odločitvi o obveščanju posameznikov, na katere se osebni podatki nanašajo. V njem je

---

[5] 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.

[6] Glej https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[7] Glej http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:31995L0046.

[8] Pravice, določene v Listini EU o temeljnih pravicah, na voljo na spletnem naslovu: http://eurlex.europa.eu/legal-content/SL/TXT/?uri=CELEX:12012P/TXT.

[9] Glej drugi odstavek 33. člena Splošne uredbe o varstvu podatkov. Ta je po zasnovi podoben 5. členu 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.

[10] Glej četrti odstavek 34. člena in točko e drugega odstavka 58. člena Splošne uredbe o varstvu podatkov.

[11] 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 (prvi in enajsti odstavek 35. člena).

[12] Glej Delovna skupina iz člena 29, Mnenje št. 03/2014 o obveščanju o kršitvah varnosti osebnih podatkov http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_sl.pdf.

obravnavana obveznost ponudnikov elektronskih komunikacij na podlagi Direktive 2002/58/ES, navedeni pa so primeri iz različnih sektorjev glede na tedanji osnutek Splošne uredbe o varstvu podatkov in predstavljena dobra praksa za vse upravljavce.

9. V teh smernicah so pojasnjene obvezne zahteve glede obveščanja o kršitvah in njihovega sporočanja iz Splošne uredbe o varstvu podatkov ter nekateri ukrepi, ki jih lahko upravljavci in obdelovalci sprejmejo za izpolnitev teh obveznosti. Navedeni so tudi primeri različnih vrst kršitev in pojasnjeno je, koga je treba obvestiti v različnih scenarijih.

I. OBVEŠČANJE O KRŠITVI VARNOSTI OSEBNIH PODATKOV NA PODLAGI SPLOŠNE UREDBE O VARSTVU PODATKOV

A. Osnovni varnostni preudarki

10. Ena od zahtev Splošne uredbe o varstvu podatkov je, da se z uporabo ustreznih tehničnih in organizacijskih ukrepov osebni podatki obdelujejo tako, da je zagotovljena ustrezna varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo[13].

11. Tako se s Splošno uredbo o varstvu podatkov 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[14]. S Splošno uredbo o varstvu podatkov 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[15].

12. Ključni element vsake politike varstva osebnih podatkov je torej zmožnost, da se kršitev po možnosti prepreči in, če do nje kljub vsemu pride, da se nanjo pravočasno odzove.

B. Kaj je kršitev varnosti osebnih podatkov?

1. Opredelitev

13. Pri vsakem poskusu obravnave kršitve bi moral biti upravljavec najprej zmožen kršitev prepoznati. V Splošni uredbi o varstvu podatkov je »kršitev varnosti osebnih podatkov« v dvanajstem odstavku 4. člena 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*«.

14. Kaj je mišljeno z »uničenjem« osebnih podatkov, bi moralo biti 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 niso 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 njihov prejem (ali dostop), ali katero koli drugo obliko obdelave, ki je v nasprotju s Splošno uredbo o varstvu podatkov.

---

[13] Glej točko f prvega odstavka 5. člena in 32. člen Splošne uredbe o varstvu podatkov.

[14] Člen 32; glej tudi uvodno izjavo 83 Splošne uredbe o varstvu podatkov.

[15] Glej uvodno izjavo 87 Splošne uredbe o varstvu podatkov.

Primer

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

15. Jasno je, da gre pri zadevni kršitvi za vrsto varnostnega incidenta. Kot je navedeno v dvanajstem odstavku 4. člena, se Splošna uredba o varstvu podatkov 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 5. členu Splošne uredbe o varstvu podatkov. To pojasnjuje razliko med varnostnim incidentom in kršitvijo varnosti osebnih podatkov. Bistveno je, da so vse kršitve varnosti osebnih podatkov varnostni incidenti, vsi varnostni incidenti pa niso nujno kršitve varnosti osebnih podatkov[16].

16. Morebitni škodljivi učinki kršitve na posameznike so obravnavani v nadaljevanju.

2. Vrste kršitev varnosti osebnih podatkov

17. 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[17]:

- »**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[18] do osebnih podatkov ali njihovo uničenje.

18. 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.

19. Ugotavljanje obstoja kršitve zaupnosti ali celovitosti je razmeroma jasno. Obstoj kršitev razpoložljivosti pa je lahko manj očiten. Kršitev se vedno šteje za kršitev razpoložljivosti, če se osebni podatki trajno izgubijo ali uničijo.

Primer

Primer izgube razpoložljivosti je, kadar se osebni podatki izbrišejo nenamerno ali jih izbriše nepooblaščena oseba ali kadar se v primeru varno šifriranih podatkov izgubi ključ za dešifriranje. Če

[16] 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, v zvezi katerimi se kršijo varnostna načela.
[17] Glej Mnenje št. 03/2014 Delovne skupine iz člena 29.
[18] 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«,. Ta jena voljo na spletnem naslovu: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Tudi v CNSSI-4009 je naveden »pravočasen in zanesljiv dostop do podatkov in informacijskih storitev za pooblaščene uporabnike«. Glej https://rmf.org/wpcontent/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:isoiec:27000:ed-4:v1:en.

upravljavec ne more povrniti dostopa do osebnih podatkov, na primer iz varnostne kopije, se to 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.

20. Vprašati se je mogoče, ali bi bilo treba začasno izgubo razpoložljivosti osebnih podatkov obravnavati kot kršitev in, če je tako, koga je treba v tem primeru obvestiti. V 32. členu Splošne uredbe o varstvu podatkov, 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*«.

21. Zato je treba tudi varnostni incident, zaradi katerega osebni podatki začasno niso več na voljo, obravnavati kot vrsto kršitve, saj lahko pomanjkanje dostopa do osebnih podatkov pomembno vpliva na pravice in svoboščine posameznikov. Jasno je, da kadar osebni podatki niso na voljo zaradi izvajanja načrtovanega vzdrževanja sistema, ne gre za »kršitev varnosti«, kot je opredeljena v dvanajstem odstavku 4. člena Splošne uredbe o varstvu podatkov.

22. 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 petim odstavkom 33. člena Splošne uredbe o varstvu podatkov. Na ta način lahko upravljavec lažje dokaže odgovornost nadzornemu organu, ki lahko zahteva vpogled v navedene evidence[19]. Glede na okoliščine kršitve pa bo morda treba tudi obvestiti nadzorni organ in prizadete posameznike. Upravljavec mora oceniti verjetnost in resnost vpliva na pravice in svoboščine posameznikov zaradi nerazpoložljivosti osebnih podatkov. V skladu s 33. členom Splošne uredbe o varstvu podatkov mora namreč upravljavec obvestiti o kršitvi, razen če ni verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. Seveda je treba o tem presojati vsak primer posebej.

Primer

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

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

23. 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 vendarle potrebno iz drugih razlogov.

Primer

Okužba z izsiljevalskim programjem (zlonamerno programsko opremo, ki šifrira podatke upravljavca, dokler ta ne plača odkupnine) lahko vodi do začasne izgube razpoložljivosti, če se lahko podatki obnovijo iz varnostne kopije. Vendar je kljub temu 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 pri tem ogrožene pravice in svoboščine posameznikov.

[19] Glej peti odstavek 33. člena Splošne uredbe o varstvu podatkov.

3. Morebitne posledice kršitve varnosti osebnih podatkov

24. Kršitev ima lahko različne pomembne škodljive učinke na posameznike, kar lahko povzroči fizično, premoženjsko ali nepremoženjsko škodo. V Splošni uredbi o varstvu podatkovje pojasnjeno, da to lahko vključuje izgubo nadzora nad njihovimi osebnimi podatki, omejitev njihovih pravic, diskriminacijo, krajo ali zlorabo identitete, finančno izgubo, nepooblaščeno razveljavitev psevdonimizacije, okrnitev ugleda in izgubo zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo. Vključuje lahko tudi katero koli drugo znatno gospodarsko ali socialno škodo za zadevne posameznike[20].

25. Tako se skladno s Splošno uredbo o varstvu podatkov 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 skladno s Splošno uredbo o varstvu podatkov zahteva, da upravljavec o kršitvi obvesti prizadete posameznike, kakor hitro je to razumno mogoče[21].

26. Pomembnost tega, da se lahko ugotovi kršitev, oceni tveganje za posameznike in nato po potrebi obvesti o kršitvi, je poudarjena v uvodni izjavi 87 Splošne uredbe o varstvu podatkov:

> »*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.*«

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

28. Če upravljavci o kršitvi varnosti osebnih podatkov ne obvestijo nadzornega organa, niti posameznikov, na katere se osebni podatki nanašajo, ali obojih , čeprav so izpolnjene zahteve iz 33. in/ali 34. člena Splošne uredbe o varstvu podatkov, lahko nadzorni organ izbira med vsemi popravljalnimi ukrepi, ki jih ima na voljo, kar bi zajemalo proučitev naložitve ustrezne upravne globe[22], bodisi poleg popravljalnega ukrepa iz drugega odstavka 58. člena Splošne uredbe o varstvu podatkov bodisi samostojno. Če se naloži upravna globa, lahko ta znaša do 10.000.000 EUR ali do 2 % skupnega svetovnega letnega prometa podjetja v skladu s točko a četrtega odstavka 83. člena Splošne uredbe o varstvu podatkov. Pomembno je tudi upoštevati, da bi lahko opustitev obveščanja o kršitvi v nekaterih primerih razkrila tudi neobstoj 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 tem primeru ima nadzorni organ tudi možnost izreči sankcije zaradi opustitve obveščanja ali sporočanja kršitve (33. in 34. člen Splošne uredbe o varstvu podatkov) na eni strani in neobstoja (ustreznih) varnostnih ukrepov (32. člen Splošne uredbe o varstvu podatkov) na drugi strani, saj gre v tem primeru za dve ločeni kršitvi.

---

[20] Glej tudi uvodni izjavi 85 in 75 Splošne uredbe o varstvu podatkov.

[21] Glej tudi uvodno izjavo 86 Splošne uredbe o varstvu podatkov.

[22] 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.

II. 33. ČLEN – OBVESTILO NADZORNEMU ORGANU

A. Kdaj je potrebno obvestilo?

1. Zahteve iz 33. člena

29. Prvi odstavek 33. člena Splošne uredbe o varstvu podatkov 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*.«

30. V uvodni izjavi 87 Splošne uredbe o varstvu podatkov je navedeno[23]:

> »*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*.«

2. Kdaj je upravljavec »seznanjen«?

31. Kot je pojasnjeno zgoraj, se s Splošno uredbo o varstvu podatkov zahteva, da upravljavec v primeru kršitve o njej obvesti brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo. To lahko vodi do vprašanja, kdaj lahko štejemo, da je upravljavec »seznanjen« s kršitvijo. EOVP meni, da je treba šteti, da je upravljavec »seznanjen«, ko je z razumno gotovostjo prepričan, da je prišlo do varnostnega incidenta, zaradi katerega so osebni podatki ogroženi.

32. Kot je bilo že navedeno, se s Splošno uredbo o varstvu podatkov 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[24]. Upravljavcu je s tem naložena obveznost, da zagotovi njihovo pravočasno »seznanitev« s kršitvami, z namenom, da ti lahko sprejmejo ustrezne ukrepe.

33. 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 primerih pa lahko traja nekaj časa, da se ugotovi, ali so bili osebni podatki ogroženi. Poudarek pa bi vendar mora biti na hitrem ukrepanju, z namenom, da se incident razišče in ugotovi, ali je bila dejansko kršena varnost osebnih podatkov, ter, če je tako, da se sprejme ustrezen sanacijski ukrep in po potrebi še obvesti posameznike.

Primeri

1. Če se izgubi pomnilniški ključek USB z nešifriranimi osebnimi podatki, pogosto ni mogoče ugotoviti, ali so imele nepooblaščene osebe dostop do teh podatkov. Tudi v primeru, če upravljavec

[23] Pomembna je tudi uvodna izjava 85 Splošne uredbe o varstvu podatkov.

[24] Glej uvodno izjavo 87 Splošne uredbe o varstvu podatkov.

ne more ugotoviti, ali je prišlo do kršitve zaupnosti, je potrebno obveščanje, ker obstaja razumna verjetnost, da je prišlo do kršitve razpoložljivosti; upravljavec bi se »seznanil«, ko je ugotovil, da se je pomnilniški ključek USB izgubil.

2. Tretja oseba obvesti upravljavca, da je po pomoti prejela osebne podatke ene od njegovih strank, in pri tem zagotovi dokaze o nepooblaščenem razkritju. Ker so bili upravljavcu predloženi jasni dokazi o kršitvi zaupnosti, ne more obstajati noben dvom, da je bil o tem »seznanjen«.

3. Upravljavec odkrije, da je prišlo do morebitnega vdora v njegovo omrežje. Preveri svoje sisteme, da ugotovi, ali so osebni podatki, shranjeni v zadevnem sistemu, ogroženi, kar se potrdi.. Ker ima tudi tokrat upravljavec jasne dokaze o kršitvi, ne more biti nobenega dvoma, da je bil o tem »seznanjen«.

4. Kibernetski kriminalec vzpostavi stik z upravljavcem, potem ko je vdrl v njegov sistem, in pri tem od upravljavca 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 o kršitvi seznanjen.

34. Potem ko je upravljavca o morebitni kršitvi obvestil posameznik, medij 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 že »seznanjen«. Začetna preiskava bi se vendarle morala začeti izvajati čim prej, z namenom, da se z razumno gotovostjo ugotovi, ali je prišlo do kršitve; šele kasneje lahko sledi podrobnejša preiskava.

35. 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 zadevne kršitve. Upravljavec ima vendarle že na voljo začetno oceno morebitnega tveganja, ki bi ga lahko povzročila kršitev, in sicer v okviru ocene učinka v zvezi z varstvom podatkov[25], izvedene pred zadevnim postopkom obdelave. Navedena ocena učinka v zvezi z varstvom podatkov pa je vendarle splošnejša v primerjavi s posameznimi okoliščinami dejanske kršitve, zato je vsekakor treba izvesti dodatno oceno, pri kateri se upoštevajo navedene okoliščine konkretnega primera. Za več podrobnosti o ocenjevanju tveganja glej oddelek IV.

36. 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 zgolj 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 hitro 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 sanacijske ukrepe za obravnavo kršitve.

37. Upravljavec zato mora imeti vzpostavljene notranje postopke, da lahko odkrije in obravnava kršitve. Da se na primer odkrijejo nekatere nepravilnosti pri obdelavi osebnih 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

[25] Glej smernice WP248 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.

dnevnika[26]. 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 33. členom in po potrebi 34. členom. 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.

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

39. 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, je treba usmeriti k odgovornim osebam, pristojnim za obravnavanje incidentov, ugotavljanje obstoja kršitve in ocenjevanje tveganja.
    - Nato je treba 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 je treba obvestiti nadzorni organ, prizadete posameznike pa o kršitvi obvestiti.
    - Hkrati bi moral upravljavec ukrepati za omejitev in obvladovanje kršitve. Kršitev je treba sproti dokumentirati.

40. S tem 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 možno izvesti preiskavo, upravljavec pa lahko zbere tudi dokaze in druge pomembne podrobnosti o kršitvi. Ko upravljavec z razumno verjetnostjo ugotovi, da je do kršitve prišlo, mora nato, če so izpolnjeni pogoji iz prvega odstavka 33. člena Splošne uredbe o varstvu podatkov, brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah, obvestiti nadzorni organ[27]. Če upravljavec ne ukrepa pravočasno in se izkaže, da je do kršitve dejansko prišlo, bi se to lahko v skladu s 33. členom Splošne uredbe o varstvu podatkov štelo kot opustitev obveščanja.

41. V 32. členu Splošne uredbe o varstvu podatkov 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 morali šteti zmožnost pravočasnega odkrivanja, obravnavanja in prijave kršitev.

3. Skupni upravljavci

42. Člen 26 Splošne uredbe o varstvu podatkov se nanaša na skupne upravljavce in določa, da ti določijo dolžnosti vsakega izmed njih z namenom izpolnjevanja obveznosti v skladu s Splošno uredbo o varstvu podatkov [28]. To vključuje določitev, kdo je odgovoren za izpolnjevanje obveznosti na podlagi 33. in 34. člena Splošne uredbe o varstvu podatkov. EOVP priporoča, naj pogodbeni dogovori med skupnimi upravljavci vključujejo tudi določbe o tem, kateri upravljavec prevzame vodilno vlogo ali je odgovoren za izpolnjevanje obveznosti iz Splošne uredbe o varstvu podatkov glede obveščanja o morebitnih kršitvah.

---

[26] Opozoriti je treba, da se lahko tudi podatki iz dnevnika, ki omogočajo preverljivost npr. hrambe, sprememb ali izbrisa podatkov, štejejo za osebne podatke, ki se nanašajo na posameznika, ki je sprožil zadevni postopek obdelave.

[27] 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.

[28] Glej tudi uvodno izjavo 79 Splošne uredbe o varstvu podatkov.

4. Obveznosti obdelovalca

43. Upravljavec ohrani splošno odgovornost za varstvo osebnih podatkov, obdelovalec pa ima pomembno vlogo pri zagotavljanju, da lahko upravljavec svoje obveznosti tudi izpolni; to vključuje tudi obveščanje o kršitvah. Dejansko tretji odstavek 28. člena Splošne uredbe o varstvu podatkov določa, da obdelavo s strani obdelovalca ureja pogodba ali drug pravni akt. V točki (f) tretjega odstavka 28. člena 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«.

44. Drugi odstavek 33. člena Splošne uredbe o varstvu podatkov 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 do kršitve prišlo, in o tem obvestiti upravljavca. Upravljavec uporablja obdelovalca za dosego svojih ciljev; zato je treba načeloma šteti, da je upravljavec »seznanjen«, ko ga obdelovalec o kršitvi obvesti. Obveznost obdelovalca, da obvesti svojega upravljavca, slednjemu omogoča, da kršitev obravnava in ugotovi, ali mora obvestiti nadzorni organ v skladu s prvim odstavkom 33. člena in prizadete posameznike v skladu s prvim odstavkom 34. člena. Upravljavec morda tudi želi kršitev raziskati, saj obdelovalec morda ne pozna 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 namreč lahko vpliva na dolžnost obveščanja upravljavca.

45. Splošna uredba o varstvu podatkov ne določa izrecnega roka, v katerem mora obdelovalec opozoriti upravljavca, razen da mora to storiti »brez nepotrebnega odlašanja«. EOVP zato priporoča, naj obdelovalec nemudoma obvesti upravljavca , 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.

46. Kot je bilo pojasnjeno zgoraj, bi moralo biti v dogovoru med upravljavcem in obdelovalcem določeno, kako bi bilo treba poleg drugih določb v Splošni uredbi o varstvu podatkov izpolnjevati zahteve iz drugega odstavka 33. člena. To lahko vključuje zahteve po zgodnjem obveščanju s strani obdelovalca, s katerimi se podprejo obveznosti upravljavca, da ta poroča nadzornemu organu v 72 urah.

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

48. Obveščanje bi lahko v imenu upravljavca izvedel tudi obdelovalec, če ga je prvi ustrezno pooblastil in je to del pogodbenih dogovorov med upravljavcem in obdelovalcem. Tako obveščanje mora potekati v skladu s 33. in 34. členom Splošne uredbe o varstvu podatkov. Pomembno je pri tem opozoriti, da pravno odgovornost za obveščanje ohrani in nosi upravljavec.

B. Zagotavljanje informacij nadzornemu organu

1. Informacije, ki jih je treba zagotoviti

49. Ko upravljavec nadzorni organ obvesti o kršitvi, mora v skladu s tretjim odstavkom 33. člena Splošne uredbe o varstvu podatkov 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*«.

50. V Splošni uredbi o varstvu podatkov niso opredeljene kategorije posameznikov, na katere se osebni podatki nanašajo, ali evidence osebnih podatkov. EOVP kljub temu predlaga, da se kategorije posameznikov, na katere se nanašajo osebni podatki, uporabljajo za različne skupine posameznikov, na katere je kršitev vplivala: odvisno od opisov, 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.

51. V uvodni izjavi 85 Splošne uredbe o varstvu podatkov je jasno navedeno, da je eden od namenov obveščanja omejiti škodo za posameznike. Če torej skupine posameznikov, na katere se osebni podatki nanašajo, ali vrste osebnih podatkov kažejo tveganje, da bi zaradi kršitve (na primer kraje identitete, goljufije, finančne izgube, ogrožanja poklicne skrivnosti) nastala škoda, je pomembno te kategorije navesti že v obvestilu. Obveščanje je tako povezano z zahtevo, da se opišejo verjetne posledice kršitve.

52. Kadar niso na voljo natančne informacije (na primer točno število prizadetih posameznikov), to ne bi smelo ovirati pravočasnega obveščanja o kršitvi. S Splošno uredbo o varstvu podatkov je dovoljeno, da se število prizadetih posameznikov in število zadevnih evidenc osebnih podatkov zaokrožita. Poudarek bi moral biti na obravnavi škodljivih posledic kršitve in ne na zagotavljanju natančnih številk.

53. Ko torej postane jasno, da je do kršitve prišlo, vendar obseg kršitve še ni znan, postopno obveščanje (glej spodaj) predstavlja varen način za izpolnitev obveznosti obveščanja.

54. V tretjem odstavku 33. člena Splošne uredbe o varstvu podatkov je navedeno, da upravljavec skupaj z obvestilom zagotovi »vsaj« te informacije, tako da lahko po potrebi pozsneje zagotovi še ostale podrobnosti kršitve. Za različne vrste kršitev (zaupnosti, celovitosti ali razpoložljivosti) se lahko zahteva posredovanje nadaljnjih podrobnejših 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.

55. Vsekakor lahko nadzorni organ zahteva nadaljnje podrobnosti v okviru svojega nadzora nad kršitvijo.

2. Postopno obveščanje

56. Glede na vrsto kršitve je lahko potrebno, da upravljavec izvede nadaljnjo preiskavo za ugotovitev vseh pomembnih dejstev v zvezi z incidentom. Četrti odstavek 33. člena Splošne uredbe o varstvu podatkov zato določa:

»*Kadar in kolikor informacij ni mogoče zagotoviti sočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja*.«

57. To pomeni, da se s Splošno uredbo o varstvu podatkov priznava, da upravljavci ne dobijo vedno vseh potrebnih informacij v zvezi s kršitvijo v 72 urah po seznanitvi s kršitvijo, saj v tem začetnem obdobju morda niso vedno na voljo popolne in izčrpne podrobnosti o incidentu. Dovoljeno je zato 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. Zato mora upravljavec v številnih primerih izvesti podrobnejšo preiskavo in pozneje preveriti dodatne informacije. To je v skladu s prvim odstavkom 33. člena Splošne uredbe o varstvu podatkov dovoljeno, če upravljavec navede razloge za zamudo. EOVP priporoča, naj upravljavec ob prvem obveščanju nadzornega organa tega na to tudi opozori, zlasti 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.

58. 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.

59. Namen obveščanja nadzornega organa pa vendarle ni samo dobiti navodila o tem, ali je treba prizadete posameznike obvestiti ali ne. V nekaterih primerih je jasno, da mora upravljavec zaradi narave kršitve in resnosti tveganja prizadete posameznike obvestiti nemudoma. Če na primer obstaja neposredna nevarnost kraje identitete ali če se na spletu razkrijejo posebne kategorije osebnih podatkov[29], mora 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 osebni podatki nanašajo..

60. Prav tako je 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 lahko dopolnile informacije, ki so bile nadzornemu organu že zagotovljene, tako da se incident ne evidentira kot kršitev. Za poročanje o incidentu, za katerega se na koncu izkaže, da ne gre za kršitev, ni sankcij.

Primer

Upravljavec v 72 urah po odkritju kršitve obvesti nadzorni organ, 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 nadzornemu organu nove informacije in zaprosi za spremembo obvestila.

61. 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 samoprijavljenih incidentov.

3. Zamude pri obveščanju

62. Prvi odstavek 33. člena Splošne uredbe o varstvu podatkov jasno določa, da kadar nadzornemu organu ni podano obvestilo v 72 urah, se nadzornemu organu 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 zapoznelo obvestilo v določenih primerih dovoljeno.

63. 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. Upravljavec bi lahko bil s kršitvijo seznanjen, 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

[29] Glej 9. člen Splošne uredbe o varstvu podatkov.

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.

64. 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 kršitve, če te zadevajo isto vrsto osebnih podatkov, ki so bili na enak način kršeni v razmeroma kratkem času. Če pride do več kršitev, ki se nanašajo na različne vrste osebnih podatkov, kršenih na različne načine, je potrebno običajno ločeno obveščanje, tako da se o vsaki kršitvi poroča skladno s 33. členom.

65. Čeprav so s Splošno uredbo o varstvu podatkov v nekaterih primerih dovoljena zapoznela obvestila, to ne gre šteti kot redno prakso. Poudariti je treba, da je združena obvestila mogoče poslati tudi za več podobnih kršitev, o katerih se poroča v 72 urah.

C. Čezmejne kršitve in kršitve v ustanovitvah zunaj EU

1. Čezmejne kršitve

66. Kadar gre za čezmejno obdelavo[30] osebnih podatkov, lahko taka kršitev vpliva na posameznike tudi v več kot eni državi članici. Prvi odstavek 33. člena Splošne uredbe o varstvu podatkov jasno določa, da mora v primeru kršitve upravljavec o njej obvestiti nadzorni organ, pristojen v skladu s 55. členom Splošne uredbe o varstvu podatkov[31]. Prvi odstavek 55. člena Splošne uredbe o varstvu podatkov določa:

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

67. Vendar prvi odstavek 56. člena Splošne uredbe o varstvu podatkov 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*.«

68. Poleg tega šesti odstavek 56. člena Splošne uredbe o varstvu podatkov določa:

> »*Vodilni nadzorni organ je edini sogovornik upravljavca ali obdelovalca za njune obdelave na čezmejni ravni*.«

69. To pomeni, da mora upravljavec, kadar do kršitve pride pri čezmejni obdelavi in se zahteva obveščanje, obvestiti vodilni nadzorni organ[32]. Upravljavec mora zato pri pripravi načrta odzivanja na kršitev oceniti, kateri nadzorni organ je vodilni nadzorni organ, ki ga mora o kršitvi obvestiti[33]. Na ta način se lahko nemudoma na kršitev odzove in izpolni svoje obveznosti v skladu s 33. členom. V primeru kršitve, ki vključuje čezmejno obdelavo, je treba obvestiti vodilni nadzorni organ, ki ni nujno v državi, v kateri so zadevni posamezniki, na katere se osebni podatki nanašajo, ali v državi, v kateri 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 osebni podatki nanašajo. Če ima upravljavec kakršne koli pomisleke glede

---

[30] Glej triindvajseti odstavek 4. člena Splošne uredbe o varstvu podatkov.

[31] Glej tudi uvodno izjavo 122 Splošne uredbe o varstvu podatkov.

[32] 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.

[33] Seznam kontaktnih podatkov vseh evropskih nacionalnih organov za varstvo podatkov je na voljo na spletnem naslovu: https://edpb.europa.eu/about-edpb/about-edpb/members_sl

identitete vodilnega nadzornega organa, mora obvestiti vsaj lokalni nadzorni organ v državi, v kateri je prišlo do kršitve.

2. Kršitve v ustanovitvah zunaj EU

70. Člen 3 Splošne uredbe o varstvu podatkov se nanaša na ozemeljsko veljavnost Splošne uredbe o varstvu podatkov, tudi kadar osebne podatke obdeluje upravljavec ali obdelovalec, ki nima ustanovitve v EU. Natančneje, drugi odstavek 3. člena Splošne uredbe o varstvu podatkov določa[34]:

> »*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*.«

71. Pomemben je tudi tretji odstavek 3. člena Splošne uredbe o varstvu podatkov, ki določa[35]:

> »*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*.«

72. Kadar se za upravljavca, ki nima ustanovitve v EU, uporabljata drugi in tretji odstavek 3. člena Splošne uredbe o varstvu podatkov in pri tem upravljavcu pride do kršitve, ga tako še vedno zavezujejo obveznosti obveščanja na podlagi 33. in 34. člena Splošne uredbe o varstvu podatkov. V skladu s 27. členom Splošne uredbe o varstvu podatkov mora upravljavec (in obdelovalec) določiti predstavnika v EU, v primerih ko se uporablja drugi odstavek 3. člena Splošne uredbe o varstvu podatkov.

73. Zgolj prisotnost predstavnika v državi članici še ne sproži mehanizma »vse na enem mestu«.[36] O kršitvi je zato treba obvestiti vsak nadzorni organ, za katerega velja, da zadevni posamezniki, na katere se osebni podatki nanašajo, prebivajo v njegovi državi članici. Za to (ta) obvestilo(-a) je odgovoren upravljavec.[37]

74. Kadar se za obdelovalca uporablja drugi odstavek 3. člena Splošne uredbe o varstvu podatkov, ga podobno zavezujejo obveznosti za obdelovalce, pri čemer je v tem primeru še zlasti pomembna dolžnost, da je o kršitvi obveščen upravljavec v skladu z drugim odstavkom 33. člena Splošne uredbe o varstvu podatkov.

D. Okoliščine, v katerih se ne zahteva obveščanje

75. Prvi odstavek 33. člena Splošne uredbe o varstvu podatkov 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 takrat, 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

---

[34] Glej tudi uvodni izjavi 23 in 24 Splošne uredbe o varstvu podatkov.
[35] Glej tudi uvodno izjavo 25 Splošne uredbe o varstvu podatkov.
[36] 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.
[37] EOVP v skladu s smernicami št. 3/2018 o ozemeljski veljavnosti Splošne uredbe o varstvu podatkov (člen 3), ki so na voljo na spletnem naslovu https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_sl, meni, da funkcija predstavnika v Uniji ni združljiva z vlogo zunanje pooblaščene osebe za varstvo podatkov, zato je za obveščanje nadzornega organa v primeru kršitve varstva osebnih podatkov še naprej odgovoren upravljavec v skladu s petim odstavkom 27. člena Splošne uredbe o varstvu podatkov. Vendar je lahko predstavnik vključen v postopek obveščanja, če je to izrecno določeno v pisnem pooblastilu.

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.

76. Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah[38] pojasnila, da je kršitev zaupnosti osebnih podatkov, ki so bili šifrirani z najsodobnejšimi algoritmi, še vedno kršitev varnosti osebnih podatkov in je treba tudi glede teh zagotoviti obvestilo. V primerih, ko 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, ki nima dovoljenja za dostop do ključa –, so podatki načeloma neberljivi. V tem kontekstu ni verjetno, da bi kršitev negativno vplivala na posameznike in jih zato praviloma ne bi bilo treba obveščati[39]. Kljub temu pa ima lahko izguba ali sprememba osebnih podatkov, negativne posledice za posameznike, tudi kadar so ti podatki šifrirani, če upravljavec osebnih podatkov nima zagotovljenih ustreznih varnostnih kopij. V takem primeru bi se kljub zgoraj navedenim zahtevalo obveščanje posameznikov, če tudi so bili podatki ustrezno zaščiteni s šifriranjem.

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

78. Posledično, če so osebni podatki postali pravzaprav neberljivi oz. 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. V zvezi s tem namreč ni 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. Treba pa je vendarle 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 vnovič oceniti. Če se na primer pozneje ugotovi, da je bil ogrožen ključ ali da je izpostavljena ranljivost programske opreme za šifriranje, je obveščanje lahko še vedno potrebno.

79. 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 tudi kršitev, ki vključuje izgubo šifriranih podatkov, tudi če obstaja varnostna kopija osebnih podatkov, 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 točki c prvega odstavka 32. člena Splošne uredbe o varstvu podatkov, je pomemben dejavnik varnosti »*zmožnost[...] 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 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 obveščanje potrebno.

[38] Delovna skupina iz člena 29, Mnenje št. 03/2014 o obveščanju o kršitvah,http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_sl.pdf.

[39] Glej tudi prvi in drugi odstavek 4. člena Uredbe št. 611/2013.

80. Za neupoštevanje 33. člena Splošne uredbe o varstvu podatkov pa gre, če upravljavec ne obvesti nadzornega organa v okoliščinah, ko podatki dejansko niso bili varno šifrirani. Upravljavci bi zato morali pri izbiri programske opreme za šifriranje skrbno pretehtati med kakovostjo in pravilnim izvajanjem šifriranja, ki je na voljo, ter razumeti, kakšna stopnja zaščite se 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 ti 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.

III. 34. ČLEN – OBVEŠČANJE POSAMEZNIKA, NA KATEREGA SE NANAŠAJO OSEBNI PODATKI

A. Obveščanje posameznikov

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

Prvi odstavek 34. člena Splošne uredbe o varstvu podatkov 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*.«

82. 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 obveščanje posameznikov o kršitvi je torej višji kot za obveščanje nadzornih organov, zato vseh kršitev ni treba sporočiti posameznikom, da ti ne prejmejo preveč nepotrebnih obvestil.

83. V Splošni uredbi o varstvu podatkov 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[40]. Kot je bilo navedeno zgoraj, se posamezniki glede na naravo kršitve in tveganja, ki jih kršitev pomeni za posameznika, s pravočasnim obveščanjem lažje zaščitijo pred morebitnimi negativnimi posledicami kršitve.

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

B. Informacije, ki jih je treba zagotoviti

85. Pri obveščanju posameznikov drugi odstavek 34. člena Splošne uredbe o varstvu podatkov 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).*«

86. V skladu s to določbo mora upravljavec zagotoviti vsaj naslednje informacije:

- opis vrste kršitve;

[40] Glej tudi uvodno izjavo 86 Splošne uredbe o varstvu podatkov.

- 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.

87. 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.

C. Vzpostavljanje stika s posamezniki

88. Načeloma je treba zadevno kršitev sporočiti neposredno zadevnim posameznikom, na katere se osebni podatki nanašajo, razen če bi bil zaradi tega potreben nesorazmeren napor. V takem primeru se namesto tega lahko objavi javno obvestilo ali izvede podoben ukrep, s katerim so ti posamezniki enako učinkovito obveščeni (točka c tretjega odstavka 34. člena Splošne uredbe o varstvu podatkov).

89. Posamezniki bi morali biti o kršitvi obveščeni z namenskimi obvestili, ki ne bi smela biti poslana skupaj z drugimi informacijami, kot so redno sprotno obveščanje, glasila ali standardna obvestila. Tako postopanje pripomore k jasnemu in preglednemu obveščanju o kršitvi.

90. Primeri preglednih metod obveščanja vključujejo neposredno obveščanje (na primer 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 obveščanje kršitve posamezniku. EOVP priporoča, da upravljavci izberejo način, s katerim se povečujejo možnosti pravilnega sporočanja informacij vsem prizadetim posameznikom. Odvisno od okoliščin lahko to pomeni, da upravljavec uporabi različne metode obveščanja namesto zgolj enega komunikacijskega kanala.

91. Upravljavci morajo včasih zagotoviti tudi, da je obvestilo dostopno v primernih alternativnih oblikah in ustreznih jezikih, da lahko posamezniki razumejo informacije, ki se jim zagotovijo. Na primer, pri obveščanju posameznika o kršitvi je večinoma primerno uporabiti jezik, ki se je uporabljal pri predhodnem običajnem poslovanju s prejemnikom. Če pa kršitev zadeva posameznike, 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 ustrezno obvestilo v lokalnem nacionalnem jeziku, ob upoštevanju potrebnih virov. Ključno je, da se posameznikom pomaga razumeti vrsta kršitve in ukrepi, s katerimi se lahko zaščitijo.

92. Upravljavci so najprimernejši, da določijo najustreznejši komunikacijski kanal za obveščanje kršitve posameznikom, zlasti v primerih, ko redno komunicirajo s svojimi strankami. Upravljavec pa bi moral vendarle biti previden pri uporabi komunikacijskega kanala, ki bi bil morebiti ogrožen zaradi kršitve, saj bi lahko tak kanal uporabljali tudi napadalci, ki se izdajajo za upravljavca.

93. Hkrati je v uvodni izjavi 86 Splošne uredbe o varstvu podatkov 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*.«

94. Upravljavci zato morda želijo vzpostaviti stik in se posvetovati z nadzornim organom, da bi poleg nasveta o obveščanju posameznikov glede kršitve v skladu s 34. členom, prejeli tudi ustrezna sporočila, ki jih je treba poslati posameznikom, in nasvet o najustreznejšem načinu za vzpostavitev stika s posamezniki.

95. S tem je povezan nasvet v uvodni izjavi 88 Splošne uredbe o varstvu podatkov, 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 tako obvestilo ne škoduje zadevnim preiskavam. Posameznike pa je kljub temu takoj ko je mogoče, še vedno treba nemudoma obvestiti.

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

D. Okoliščine, v katerih se ne zahteva obvestila

97. V tretjem odstavku 34. člena Splošne uredbe o varstvu podatkov 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 udejanjilo. 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 osebnimi podatki 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 osebnih podatkov.
- Za vzpostavitev stika s posamezniki bi bil potreben nesorazmeren napor[41], 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 obvestilo 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 na drug način vzpostaviti kakršnegakoli stika.

98. Skladno z načelom odgovornosti bi morali upravljavci biti zmožni nadzornemu organu dokazati, da izpolnjujejo enega ali več teh pogojev [42]. 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 vnovič oceniti.

---

[41] 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.

[42] Glej drugi odstavek 5. člena Splošne uredbe o varstvu podatkov.

99. Če se upravljavec odloči, da kršitve ne bo sporočil posamezniku, je v četrtem odstavku 34. člena Splošne uredbe o varstvu podatkov pojasnjeno, da lahko to od njega zahteva nadzorni organ, če meni, da bi kršitev verjetno povzročila veliko tveganje za posameznike. Nadzorni organ pa lahko tudi ugotovi, da so izpolnjeni pogoji iz tretjega odstavka 34. člena Splošne uredbe o varstvu podatkov, tako da obveščanje posameznikov ni potrebno. Če nadzorni organ ugotovi, da odločitev o neobveščanju posameznikov, na katere se osebni podatki nanašajo, ni utemeljena, lahko premisli o uporabi ukrepov in sankcij, ki jih ima na voljo.

IV. OCENJEVANJE TVEGANJA IN VELIKEGA TVEGANJA

A. Tveganje kot dejavnik, zaradi katerega nastane potreba po obveščanju

100. Čeprav je s Splošno uredbo o varstvu podatkov 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.

101. To pomeni, da je takoj po seznanitvi s kršitvijo bistveno, da upravljavec ne samo omeji incident, ampak tudi oceni 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 prizadete posameznike.

102. 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 obveščanju o kršitvi posameznikom, 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 s kršitvijo ogrožena. 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[43].

B. Dejavniki, ki jih je treba upoštevati pri ocenjevanju tveganja

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

104. Opozoriti je treba, da je poudarek pri ocenjevanju tveganja za pravice in svoboščine posameznikov zaradi kršitve drugačen kot pri tveganju, obravnavanem v oceni učinka v zvezi z varstvom podatkov[44]. V oceni učinka v zvezi z varstvom podatkov se obravnavajo tveganja pri načrtovani obdelavi osebnih podatkov, in tveganja v primeru nastanka kršitve. Pri obravnavi morebitne kršitve se na splošno preučita verjetnost njenega nastanka in škoda, ki lahko iz tega izhaja za posameznika; povedano drugače, gre za oceno hipotetičnega dogodka. Pri dejanski kršitvi se je

[43] Glej uvodni izjavi 75 in 85 Splošne uredbe o varstvu podatkov.

[44] 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.

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 tekoče ocene učinka v zvezi z varstvom podatkov. Pozneje se izrabi 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.

105. Upravljavec bi v tem primeru pri ocenjevanju tveganja za posameznike, ki izhaja iz kršitve, upoštevati konkretne okoliščine kršitve, vključno z resnostjo morebitnega vpliva in verjetnostjo za njegov nastanek. EOVP zato priporoča, da se pri oceni upoštevajo naslednja merila[45]:

- **Vrsta kršitve**

106. Vrsta kršitve, do katere je prišlo, lahko vpliva na stopnjo tveganja za posameznike. Na primer, kršitev zaupnosti, pri kateri so se zdravstveni podatki razkrili 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**

107. 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 pa je v tem primeru še vedno treba upoštevati tudi druge osebne podatke, ki so lahko o posamezniku že dostopne. 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 kot tudi za otroka.

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

109. 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.

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

- **Enostavnost identifikacije posameznikov**

[45] Drugi odstavek 3. člena Uredbe št. 611/2013 določa usmeritve glede dejavnikov, ki bi jih bilo treba upoštevati v zvezi z obveščanjem o kršitvah v sektorju elektronskih komunikacijskih storitev, kar je lahko koristno tudi v kontekstu obveščanja na podlagi Splošne uredbe o varstvu podatkov. Glej http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sl:PDF.

111. Pomemben dejavnik, ki ga je treba upoštevati, je, kako preprosto lahko oseba, ki ima dostop do podatkov, katerih varnost je ogrožena, identificira konkretne posameznike ali podatke poveže z drugimi informacijami, da posameznike identificira ali določi. Glede na okoliščine bi bila identifikacija mogoča neposredno na podlagi osebnih podatkov, katerih varnost je kršena, brez potrebe po ugotavljanju identitete posameznika. Osebne podatke pa bi bilo lahko tudi izjemno težko povezati s konkretnim posameznikom, a bi kljub temu identifikacija bila vendarle pod določenimi pogoji še vedno možna. Identifikacija je lahko neposredno ali posredno mogoča na podlagi podatkov o kršitvi, odvisna pa je lahko tudi od posebnih okoliščin kršitve in javne dostopnosti povezanih osebnih podatkov.. To je lahko še toliko bolj pomembno pri kršitvah zaupnosti in razpoložljivosti.

112. Kot je navedeno zgoraj, osebni podatki, zaščiteni z ustrezno ravnjo šifriranja, nepooblaščenim posameznikom niso razumljivi brez ključa za dešifriranje. Verjetnost za identifikacijo posameznikov se poleg tega v primeru kršitve zmanjša tudi s pravilno izvedeno psevdonimizacijo (ki je v petem odstavku 4. člena Splošne uredbe o varstvu podatkov 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*«). Kljub temu pa samo na podlagi tehnik psevdonimizacije ni mogoče trditi, da zaradi njih osebni podatki postanejo nerazumljivi.

- **Resnost posledic za posameznike**

113. Glede na naravo osebnih podatkov, zajetih s kršitvijo, na primer posebne kategorije osebnih podatkov, je lahko morebitna škoda za posameznike, ki bi jo kršitev povzročila, 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, je lahko tveganje škode v zvezi z njimi toliko večje.

114. To, ali je upravljavec seznanjen s tem, da so osebni podatki v rokah posameznikov, katerih nameni niso znani ali so potencialno zlonamerni, lahko vpliva na stopnjo morebitnega tveganja. Pride lahko namreč do kršitve zaupnosti, s čimer se osebni podatki pomotoma razkrijejo tretji osebi, kot je opredeljena v desetem odstavku 4. člena, ali drugemu prejemniku. To se na primer lahko zgodi, kadar se osebni podatki nenamerno pošljejo napačnemu oddelku organizacije ali pogosto uporabljeni organizaciji ponudnika.. 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 naveden posameznik ne bo prebral pomotoma poslanih podatkov ali do njih dostopal ter bo upošteval navodila za njihovo vračilo oz. uničenje. 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, jih izbrisal ali po potrebi 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. Vsekakor pa se s tem izključi verjetnost tveganja za posameznike, tako da se obveščanje nadzornega organa ali prizadetih posameznikov ne zahteva. Ponovno pa je to odvisno od vsakega posameznega primera. Upravljavec mora kljub temu še vedno hraniti informacije v zvezi s kršitvijo kot del splošne dolžnosti vodenja evidenc o kršitvah (glej oddelek V v nadaljevanju).

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

- **Posebne značilnosti posameznika**

116. 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.

- **Posebne značilnosti upravljavca podatkov**

117. Narava in vloga upravljavca ter 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 osebnih podatkov posamezniki bolj ogroženi kot v primeru nepooblaščenega razkritja poštnega seznama prejemnikov glasila.

- **Število prizadetih posameznikov**

118. 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. Kljub temu pa lahko kršitev resno vpliva tudi zgolj 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 posameznike.

- **Splošni elementi**

119. Upravljavec bi zato moral 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 večje tveganje, podobno pa se v primeru večje verjetnosti njihovega nastanka tveganje poveča . Upravljavec bi moral v primeru dvoma biti previdnejši in o kršitvi zagotoviti obvestilo. V Prilogi B so navedeni nekateri koristni primeri različnih vrst kršitev, ki vključujejo tveganje ali veliko tveganje za posameznike.

120. 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[46].

V. ODGOVORNOST IN VODENJE EVIDENC

A. Dokumentiranje kršitev

121. 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 petem odstavku 33. člena Splošne uredbe o varstvu podatkov:

»*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*.«

122. To je povezano z načelom odgovornosti iz drugega odstavka 5. člena Splošne uredbe o varstvu podatkov. Namen evidentiranja kršitev, za katere se ne zahteva obveščanje, in kršitev, za katere se zahteva obveščanje, je povezan tudi z obveznostmi upravljavca na podlagi 24. člena Splošne uredbe o varstvu podatkov, nadzorni organ pa lahko zahteva vpogled v te evidence. Upravljavce se zato spodbuja k vzpostavitvi notranjega registra kršitev, ne glede na to, ali morajo o njih obveščati ali ne[47].

[46] ENISA, Priporočila za metodologijo ocenjevanja resnosti kršitev varnosti osebnih podatkov, https://www.enisa.europa.eu/publications/dbn-severity.

[47] Upravljavec se lahko odloči za dokumentiranje kršitev v okviru svoje evidence dejavnosti obdelave, ki jo vodi v skladu s 30. členom Splošne uredbe o varstvu podatkov. Če so informacije v zvezi s kršitvijo jasno prepoznavne kot take in jih je mogoče pridobiti na zahtevo, ločena evidenca ni potrebna.

123. 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 petim odstavkom 33. člena Splošne uredbe o varstvu podatkov, 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 je treba tudi učinke in posledice kršitve, skupaj s sanacijskimi ukrepi, ki jih je sprejel upravljavec.

124. V Splošni uredbi o varstvu podatkov ni določeno obdobje hrambe tovrstne dokumentacije. Kadar take evidence vsebujejo osebne podatke, mora upravljavec določiti ustrezno obdobje hrambe v skladu z načeli obdelave osebnih podatkov[48] in imeti pravno podlago za obdelavo[49]. Dokumentacijo mora hraniti v skladu s petim odstavkom 33. člena Splošne uredbe o varstvu podatkov, da lahko nadzornemu organu na zahtevo dokaže skladnost z navedenim členom ali na splošneje z načelom odgovornosti. Jasno je, da se načelo omejitve hrambe[50] iz Splošne uredbe o varstvu podatkov ne uporablja, če evidence ne vsebujejo osebnih podatkov.

125. EOVP priporoča, naj upravljavec poleg teh podrobnosti dokumentira tudi svoje razloge za odločitve, sprejete kot odziv na kršitev. Če ni obveščanja o kršitvi, je treba dokumentirati zlasti utemeljitev take odločitve. To mora vključevati razloge, zaradi katerih upravljavec meni, da kršitev verjetno ne ogroža pravic in svoboščin posameznikov[51]. Če pa upravljavec meni, da je izpolnjen kateri od pogojev iz tretjega odstavka 34. člena Splošne uredbe o varstvu podatkov, mora o tem biti zmožen zagotoviti ustrezne dokaze.

126. 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.

127. Kadar upravljavec o kršitvi obvesti prizadete posameznike, mora biti pri opisu kršitve jasen ter o kršitvi obveščati učinkovito in pravočasno. Če bi upravljavec hranil dokaze o poslanem obvestilu bi tudi lažje dokazal svojo odgovornost in skladnost. . ,.

128. Za lažje upoštevanje 33. in 34. člena Splošne uredbe o varstvu podatkov 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 Splošno uredbo o varstvu podatkov tudi koristno dokazati, da so bili zaposleni obveščeni o obstoju takih postopkov in mehanizmov ter da vedo, kako se na kršitve odzvati.

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

B. Vloga pooblaščene osebe za varstvo podatkov

130. Upravljavec ali obdelovalec ima lahko pooblaščeno osebo za varstvo podatkov[52], bodisi kot se zahteva s 37. členom Splošne uredbe o varstvu podatkov bodisi prostovoljno v skladu z dobro prakso. Člen 39 Splošne uredbe o varstvu podatkov določa več obveznih nalog pooblaščene osebe za varstvo podatkov, vendar upravljavcu ne preprečuje, da ji po potrebi dodeli še druge naloge.

---

[48] Glej 5. člen Splošne uredbe o varstvu podatkov.

[49] Glej 6. in tudi 9. člen Splošne uredbe o varstvu podatkov.

[50] Glej točko e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov.

[51] Glej uvodno izjavo 85 Splošne uredbe o varstvu podatkov.

[52] 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.

131. 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 Splošno uredbo o varstvu podatkov 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 osebni podatki nanašajo. Opozoriti je treba še, da mora upravljavec pri obveščanju nadzornega organa o kršitvi v skladu s točko (b) tretjega odstavka 33. člena Splošne uredbe o varstvu podatkov zagotoviti ime in kontaktne podatke svoje pooblaščene osebe za varstvo podatkov ali druge kontaktne točke.

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

133. To pomeni, da mora 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 morebitnim poznejšim nadzorom s strani nadzornega organa. Glede na to EOVP priporoča, da se pooblaščeno osebo za varstvo podatkov nemudoma obvešča o obstoju kršitve ter da je vključena v celoten postopek obvladovanja kršitve in obveščanja o njej.

VI. OBVEZNOSTI OBVEŠČANJA NA PODLAGI DRUGIH PREDPISOV

134. Poleg obveščanja o kršitvah in njihovega sporočanja na podlagi Splošne uredbe o varstvu podatkov 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, da lahko to tudi pomeni, da morajo nadzorni organ sočasno obvestiti tudi o kršitvi varnosti osebnih podatkov. Take zahteve se lahko med državami članicami razlikujejo, vendar primeri zahtev po obveščanju po drugih predpisih in načini, kako so ti medsebojno povezani s Splošno uredbo o varstvu podatkov, vključujejo naslednje:

- *Uredba (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (uredba o elektronski identifikaciji)*[53].

135. V skladu z drugim odstavkom 19. člena 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 Splošne uredbe o varstvu podatkov –, 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)*[54].

136. V skladu s 14. in 16. členom Direktive o kibernetski varnosti morajo izvajalci bistvenih storitev in ponudniki digitalnih storitev o varnostnih incidentih obvestiti svoj pristojni organ. Kot je poudarjeno v uvodni izjavi 63 Direktive o kibernetski varnosti[55], je zaradi incidentov pogosto ogrožena varnost osebnih podatkov. V skladu z Direktivo o kibernetski varnosti morajo pristojni organi in nadzorni organi za varstvo osebnih podatkov sodelovati ter si v okviru tega izmenjavati informacije, še vedno pa velja,

[53] Glej http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32014R0910.

[54] Glej http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016L1148.

[55] 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.«*

da kadar taki incidenti pomenijo ali postanejo kršitve varnosti osebnih podatkov na podlagi Splošne uredbe o varstvu podatkov, morajo 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 osebnih podatkov.

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

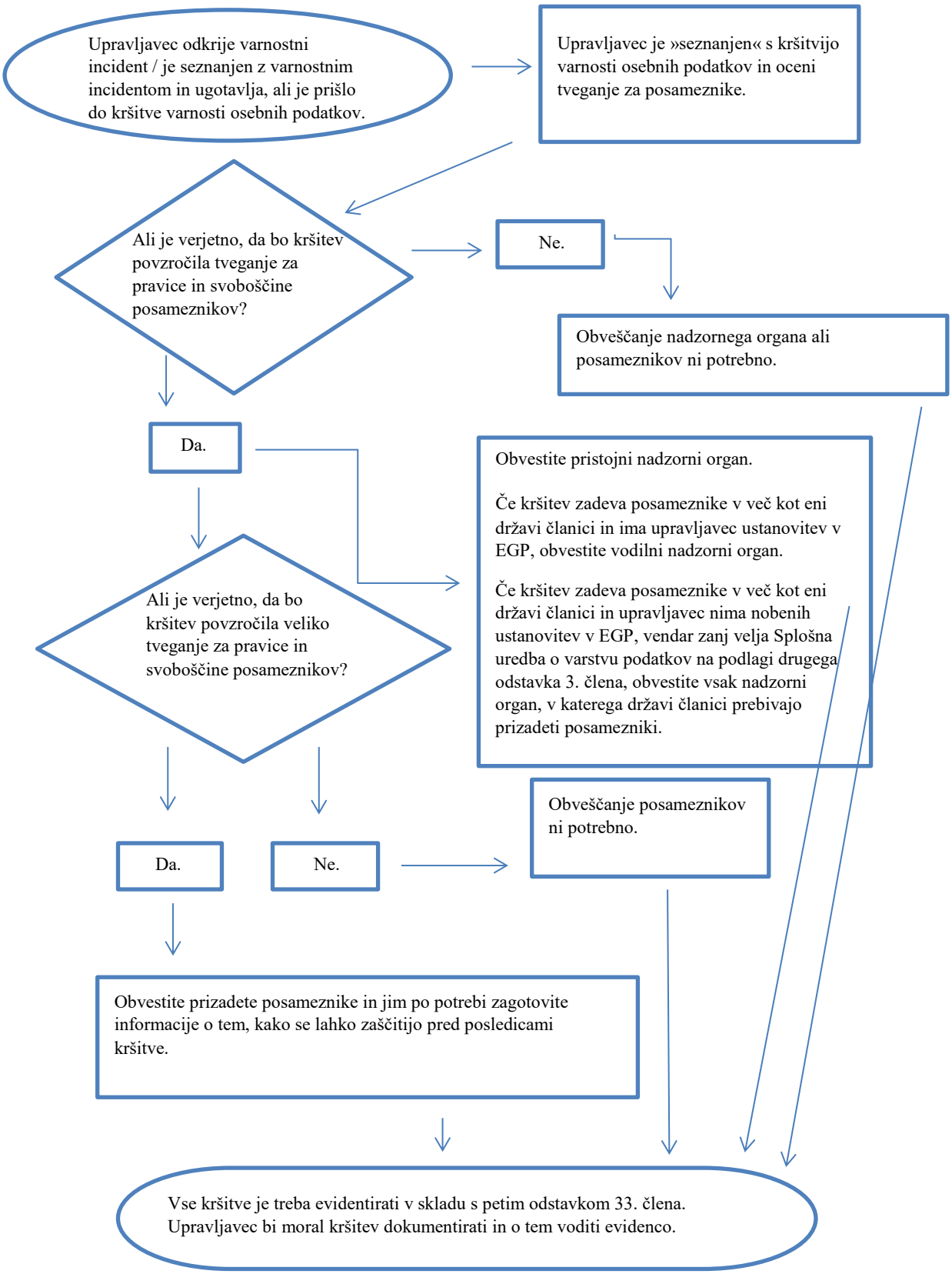
137. Ponudniki javno dostopnih elektronskih komunikacijskih storitev v okviru Direktive 2002/58/ES[56] morajo o kršitvah obvestiti pristojne nacionalne organe.

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

[56] Evropska komisija je 10. januarja 2017 predlagala Uredbo o zasebnosti in elektronskih komunikacijah, ki naj bi nadomestila Direktivo 2009/136/ES in odpravila zahteve po obveščanju. Dokler 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-electroniccommunications.

VII. PRILOGA

A. Shematski prikaz zahtev po obveščanju



B. 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 prizadetih posameznikov. Ti primeri lahko med drugim 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 osebni podatki nanašajo?	Opombe/priporočila
i	Upravljavec je shranil varnostno kopijo arhiva šifriranih osebnih podatkov na pomnilniški ključek USB. Med vlomom je bil ključek ukraden.	Ne.	Ne.	Če so osebni podatki šifrirani z najsodobnejšim algoritmom, če obstaja varnostna kopija podatkov, če ni ogrožen enkratni ključ in če je mogoče podatke pravočasno obnoviti, o tej kršitvi morda ni treba obveščati. Če je kljub temu pozneje ogrožena varnost osebnih podatkov, se obveščanje zahteva.
ii	Upravljavec zagotavlja 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 obvestite nadzorni organ.	Da, glede na naravo zadevnih osebnih podatkov in v primeru zelo resnih verjetnih posledic za posameznike obvestite prizadete posameznike.	
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 petim odstavkom 33. člena. Upravljavec mora o tem voditi ustrezno evidenco.
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 napada postane jasno, da je bila	Da, obvestite nadzorni organ, če so posledice za posameznike verjetne, saj gre za izgubo razpoložljivosti osebnih podatkov.	Da, obvestite posameznika glede na naravo zadevnih osebnih podatkov in morebitni učinek izgube nad razpoložljivostjo osebnih podatkov ter druge verjetne posledice.	V primeru, ko je voljo varnostna kopija in je podatke možno pravočasno obnoviti, obvestilo nadzornemu organu ali posameznikom ni potrebno, saj ne pride do trajne izgube razpoložljivosti ali zaupnosti. Če je bil nadzorni organ seznanjen z incidentom

	edina funkcija izsiljevalskega programja šifriranje podatkov in da v sistemu ni bilo druge zlonamerne programske opreme.			kako drugače, lahko ta razmisli o uvedbi nadzora, s katerim bi ocenil skladnost s širšimi varnostnimi zahtevami iz 32. člena.

v	Posameznik pokliče v klicni center banke in prijavi kršitev varnosti osebnih 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 posamezniki niso bili prizadeti, se obvesti zgolj prizadete posameznike.	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 zagotavlja 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 strank.	Da, če gre za čezmejno obdelavo, poročajte vodilnemu nadzornemu organu.	Da, saj bi lahko kršitev povzročila veliko tveganje.	Upravljavec mora ukrepati, na primer s prisilno ponastavitvijo gesel prizadetih računov strank ter drugimi ukrepi za zmanjšanje tveganja. Upravljavec mora upoštevati še morebitne druge obveznosti obveščanja, na primer na podlagi Direktive o kibernetski varnosti kot ponudnik digitalnih storitev.
vii	Družba za spletno gostovanje, ki deluje kot obdelovalec osebnih podatkov, odkrije napako v kodi, ki nadzoruje avtorizacijo uporabnikov.	Družba za spletno gostovanje mora kot obdelovalec brez nepotrebnega odlašanja obvestiti svoje prizadete stranke (upravljavce).	Če verjetno ni visokega tveganja za posameznike, teh ni treba obveščati.	Družba za spletno gostovanje (obdelovalec) mora upoštevati vse druge obveznosti obveščanja (na primer na podlagi Direktive o kibernetski varnosti kot ponudnik digitalnih storitev).

	Napaka povzroči, da lahko kateri koli uporabnik dostopa do podatkov o računu katerega koli drugega uporabnika.	Ob predpostavki, da je družba za spletno gostovanje izvedla lastno preiskavo, bi morali prizadeti upravljavci prejeti 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 ni dokazov, da se je ta ranljivost izrabila 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 bi šlo lahko za neskladnost z zahtevami iz 32. člena.
viii	Zdravstvene kartoteke v bolnišnici zaradi kibernetskega napada niso na voljo 30 ur.	Da, bolnišnica mora obvezno obvestiti nadzorni organ, saj lahko pride do tveganja za pacientovo dobro počutje in zasebnost.	Da, obvestite prizadete posameznike.	
ix	Osebni podatki velikega števila študentov se pomotoma pošljejo napačnemu poštnemu seznamu z več kot 1.000 prejemniki.	Da, obvestite nadzorni organ.	Da, obvestite posameznike glede na obseg in vrsto osebnih podatkov, ki jih kršitev zadeva, ter resnost morebitnih posledic.	
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 potrebno, če je prizadetih veliko število posameznikov, če so razkriti občutljivi osebni podatki (na primer poštni seznam psihoterapevta) ali če obstajajo drugi dejavniki, ki pomenijo veliko tveganje (na primer sporočilo vsebuje začetna gesla).	Da, obvestite posameznike glede na obseg in vrsto osebnih podatkov, ki jih to zadeva, ter resnost morebitnih posledic.	Obveščanje morda ni potrebno, če niso razkriti občutljivi osebni podatki in če je razkrito le manjše število elektronskih naslovov.