



**18/HR**

**WP250rev.01**

**Smjernice o obavješćivanju o povredi osobnih podataka na temelju Uredbe 2016/679**

**Donesene 3. listopada 2017.**

**Kako su zadnje revidirane i donesene 6. veljače 2018.**

Radna skupina osnovana je na temelju članka 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnost. Njezine su zadaće opisane u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo osigurava Uprava C (Temeljna prava i građanstvo Unije) Europske komisije, Glavna uprava za pravosuđe, B-1049 Bruxelles, Belgija, ured br. MO-59 02/013.

Internetske stranice: [https://ec.europa.eu/info/law/law-topic/data-protection\\_hr](https://ec.europa.eu/info/law/law-topic/data-protection_hr)

## **RADNA SKUPINA ZA ZAŠTITU POJEDINACA U VEZI S OBRADOM OSOBNIH PODATAKA**

osnovana Direktivom 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995.,

uzimajući u obzir članke 29. i 30. te direktive,

uzimajući u obzir svoj poslovnik,

**DONIJELA JE OVE SMJERNICE:**

# SADRŽAJ

<b>UVOD.....</b>	<b>5</b>
<b>I. OBAVJEŠĆIVANJE O POVREDI OSOBNIH PODATAKA NA TEMELJU OPĆE UREDBE O ZAŠTITI PODATAKA ..</b>	<b>6</b>
A. OSNOVNA RAZMATRANJA O SIGURNOSTI.....	6
B. ŠTO JE TO POVREDA OSOBNIH PODATAKA? .....	7
1. Definicija.....	7
2. Vrste povreda osobnih podataka .....	7
3. Moguće posljedice povrede osobnih podataka.....	9
<b>II. ČLANAK 33. – OBAVJEŠĆIVANJE NADZORNOG TIJELA.....</b>	<b>10</b>
A. KADA JE OBAVJEŠĆIVANJE POTREBNO .....	10
1. Zahtjevi iz članka 33. ....	10
2. Kada se smatra da je voditelj obrade „saznao“ za povredu?.....	11
3. Zajednički voditelji obrade .....	13
4. Obveze izvršitelja obrade.....	14
B. PRUŽANJE INFORMACIJA NADZORNOM TIJELU .....	14
1. Informacije koje treba dostaviti .....	14
2. Postupno obavješćivanje.....	15
3. Odgođeno obavješćivanje .....	17
C. PREKOGRANIČNE POVREDE I POVREDE U SLUČAJEVIMA POSLOVNOG NASTANA IZVAN EU-A.....	17
1. Prekogranične povrede .....	17
2. Povrede u slučajevima poslovnog nastana izvan EU-a.....	18
D. UVJETI POD KOJIMA SE NE ZAHTIJEVA OBAVJEŠĆIVANJE .....	19
<b>III. ČLANAK 34. – OBAVJEŠĆIVANJE ISPITANIKA.....</b>	<b>20</b>
A. INFORMIRANJE POJEDINACA .....	20
B. INFORMACIJE KOJE TREBA DOSTAVITI.....	21
C. KONTAKTIRANJE S POJEDINCIMA.....	21
D. UVJETI POD KOJIMA SE NE ZAHTIJEVA OBAVJEŠĆIVANJE .....	22
<b>IV. PROCJENA RIZIKA I VISOKOG RIZIKA.....</b>	<b>23</b>
A. RIZIK KAO POKRETAČ OBAVJEŠĆIVANJA.....	23
B. ČIMBENICI KOJE TREBA UZETI U OBZIR PRI PROCJENI RIZIKA .....	24
<b>V. ODGOVORNOST I VOĐENJE EVIDENCIJE .....</b>	<b>27</b>
A. DOKUMENTIRANJE POVREDA .....	27

B.	ULOGA SLUŽBENIKA ZA ZAŠTITU PODATAKA .....	28
<b>VI.</b>	<b>OBVEZE OBAVJEŠĆIVANJA NA TEMELJU DRUGIH PRAVNIH INSTRUMENATA .....</b>	<b>29</b>
<b>VII.</b>	<b>PRILOG .....</b>	<b>31</b>
A.	DIJAGRAM TOKA NA KOJEM SU PRIKAZANI ZAHTJEVI ZA OBAVJEŠĆIVANJE .....	31
B.	PRIMJERI POVREDA OSOBNIH PODATAKA I KOGA TREBA OBAVIJESTITI .....	32

## UVOD

Općom uredbom o zaštiti podataka uvodi se zahtjev za obavješćivanje nadležnog nacionalnog nadzornog tijela<sup>1</sup> (ili vodećeg tijela, u slučaju prekogranične povrede) o povredi osobnih podataka (dalje u tekstu: „povreda”) te se u određenim slučajevima uvodi zahtjev za obavješćivanje pojedinaca na čije je osobne podatke povreda utjecala.

Obveze obavješćivanja u slučaju povreda trenutačno postoje za određene organizacije kao što su pružatelji javno dostupnih elektroničkih komunikacijskih usluga (kako je utvrđeno u Direktivi 2009/136/EZ i Uredbi (EU) br. 611/2013)<sup>2</sup>. Pojedine države članice EU-a već imaju i vlastite nacionalne obveze obavješćivanja u slučaju povrede. To može uključivati obvezu obavješćivanja o povredama koje se, osim na pružatelje javno dostupnih elektroničkih komunikacijskih usluga, odnose i na određene kategorije voditelja obrade (primjerice, u Njemačkoj i Italiji) ili obvezu prijavljivanja svih povreda koje se odnose na osobne podatke (kao što je slučaj u Nizozemskoj). Druge države članice mogu imati odgovarajuće kodekse pravilnog postupanja (primjerice, Irska<sup>3</sup>). Iako trenutačno mnoga tijela za zaštitu podataka iz EU-a potiču voditelje obrade na prijavljivanje povreda, Direktiva 95/46/EZ o zaštiti podataka<sup>4</sup>, koju je zamijenila Opća uredba o zaštiti podataka, ne sadržava posebnu obvezu obavješćivanja o povredama pa će stoga mnogim organizacijama taj zahtjev biti nov. Sada je, na temelju Opće uredbe o zaštiti podataka, obavješćivanje obvezno za sve voditelje obrade osim ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca<sup>5</sup>. Izvršitelji obrade u tome isto imaju važnu ulogu i moraju svoje voditelje obrade obavijestiti o svakoj povredi<sup>6</sup>.

Radna skupina iz članka 29. smatra da novi zahtjev za obavješćivanje donosi niz koristi. Pri obavješćivanju nadzornog tijela, voditelji obrade mogu dobiti savjet o tome treba li obavijestiti pojedince pogođene povredom. Zapravo, nadzorno tijelo može narediti voditelju obrade da te pojedince obavijesti o povredi<sup>7</sup>. Obavješćivanjem pojedinaca o povredi voditelju obrade omogućuje se da ih obavijesti o rizicima koji su proizašli iz povrede i o mjerama koje ti pojedinci mogu poduzeti kako bi se zaštitili od mogućih posljedica povrede. Svi planovi postupanja u slučaju povrede trebali bi biti usmjereni na zaštitu pojedinaca i njihovih osobnih podataka. Stoga bi obavješćivanje o povredi trebalo smatrati alatom za povećanje usklađenosti s obzirom na zaštitu osobnih podataka. Istodobno bi trebalo imati na umu da neprijavlivanje povrede pojedincu ili nadzornom tijelu može dovesti do mogućih sankcija za voditelja obrade na temelju članka 83.

---

<sup>1</sup> Vidjeti članak 4. točku 21. Opće uredbe o zaštiti podataka.

<sup>2</sup> Vidjeti <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32009L0136> i <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32013R0611>

<sup>3</sup> Vidjeti [https://www.dataprotection.ie/docs/Data\\_Security\\_Breach\\_Code\\_of\\_Practice/1082.htm](https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm)

<sup>4</sup> Vidjeti <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:31995L0046>

<sup>5</sup> Prava ugrađena u Povelju EU-a o temeljnim pravima, koja je dostupna na adresi: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>

<sup>6</sup> Vidjeti članak 33. stavak 2. To je slično konceptu iz članka 5. Uredbe (EU) br. 611/2013 u kojemu se navodi da pružatelj usluga (koji nije u izravnom ugovornom odnosu s pretplatnicima) s kojim je pružatelj usluga naručitelj sklopio ugovor o pružanju dijela elektroničkih komunikacijskih usluga obavezan obavijestiti pružatelja usluga naručitelja u slučaju povrede osobnih podataka.

<sup>7</sup> Vidjeti članak 34. stavak 4. i članak 58. stavak 2. točku (e).

Stoga se voditelje i izvršitelje obrade potiče da unaprijed planiraju i utvrde postupke kako bi mogli otkriti povredu, što prije je ograničiti i procijeniti rizik za pojedince<sup>8</sup> te potom utvrditi je li potrebno obavijestiti nadležno nadzorno tijelo i, prema potrebi, pojedince na koje se povreda odnosi. Obavješćivanje nadzornog tijela trebalo bi biti dijelom tog plana postupanja u slučaju incidenta.

Opća uredba o zaštiti podataka sadržava odredbe o tome kada i koga treba obavijestiti o povredi te o informacijama koje bi trebalo navesti u toj obavijesti. Informacije koje se zahtijevaju u okviru obveze obavješćivanja mogu se dostaviti postupno, ali voditelji obrade u svakom bi slučaju trebali pravodobno djelovati u slučaju bilo kakve povrede.

Radna skupina iz članka 29. u svojem je Mišljenju 03/2014 o obavješćivanju o povredi osobnih podataka<sup>9</sup> dala smjernice voditeljima obrade kako bi im pomogla pri odlučivanju treba li obavijestiti ispitanike u slučaju povrede. U tom se mišljenju razmatra obveza pružatelja elektroničkih komunikacija s obzirom na Direktivu 2002/58/EZ, te se, u kontekstu Opće uredbe o zaštiti podataka, koja je u trenutku izdavanja mišljenja bila u fazi nacрта, navode primjeri iz više sektora i prikazuju se primjeri dobre prakse za sve voditelje obrade.

U ovim se Smjericama objašnjavaju obvezni zahtjevi iz Opće uredbe o zaštiti podataka o obavješćivanju nadzornih tijela i pojedinaca o povredama i neke od mjera koje voditelji obrade i izvršitelji obrade mogu poduzeti kako bi ispunili te nove obveze. Navode se i primjeri raznih vrsta povreda te koga bi trebalo obavijestiti u različitim scenarijima.

## **I. Obavješćivanje o povredi osobnih podataka na temelju Opće uredbe o zaštiti podataka**

### **A. Osnovna razmatranja o sigurnosti**

Jedan od zahtjeva iz Opće uredbe o zaštiti podataka odnosi se na to da se, primjenom odgovarajućih tehničkih i organizacijskih mjera, osobni podaci moraju obrađivati na način kojim se osigurava odgovarajuća sigurnost tih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja<sup>10</sup>.

U skladu s tim, Općom uredbom o zaštiti podataka zahtijeva se da voditelji i izvršitelji obrade uspostave odgovarajuće tehničke i organizacijske mjere kako bi zajamčili razinu sigurnosti koja je primjerena riziku koji postoji s obzirom na osobne podatke koji se obrađuju. Voditelji i izvršitelji obrade trebali bi u obzir uzeti najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, te rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca<sup>11</sup>. Osim toga, Općom uredbom o zaštiti podataka zahtijeva se da se provedu sve odgovarajuće mjere

---

<sup>8</sup> To se može osigurati u okviru zahtjeva za praćenje i preispitivanje iz procjene učinka na zaštitu podataka, koja se zahtijeva za postupke obrade za koje je vjerojatno da će prouzročiti visok rizik za prava i slobode pojedinaca (članak 35. stavci 1. i 11.).

<sup>9</sup> Vidjeti Mišljenje 03/2014 o obavješćivanju o povredi osobnih podataka na adresi: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf)

<sup>10</sup> Vidjeti članak 5. stavak 1. točku (f) i članak 32.

<sup>11</sup> Članak 32., vidjeti i uvodnu izjavu 83.

tehnološke zaštite i organizacijske mjere kako bi se odmah utvrdilo je li došlo do povrede i na temelju toga utvrdilo je li nastupila obveza obavješćivanja<sup>12</sup>.

Stoga je ključan element svake politike sigurnosti podataka sposobnost da se, ako je moguće, povreda spriječi i da se, ako se ona ipak dogodi, na nju pravodobno reagira.

## B. Što je to povreda osobnih podataka?

### 1. Definicija

Kako bi voditelj obrade mogao odgovoriti na povredu, prvo je mora prepoznati. U Općoj uredbi o zaštiti podataka, u članku 4. točki 12., „povreda osobnih podataka” definira se kao:

„kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.”

Trebalo bi biti sasvim jasno što se podrazumijeva pod „uništenjem” osobnih podataka: radi se o tome da određeni podaci više ne postoje ili ne postoje u obliku koji je od ikakve koristi voditelju obrade. Pojam „šteta” isto bi trebao biti relativno jasan: radi se o situaciji u kojoj su osobni podaci izmijenjeni, oštećeni ili više nisu cjeloviti. Pojam „gubitka” osobnih podataka trebalo bi tumačiti tako da ti podaci možda i dalje postoje, no voditelj obrade izgubio je kontrolu nad njima ili pristup njima ili oni više nisu u njegovu posjedu. Naposljetku, neovlaštena ili nezakonita obrada može uključivati otkrivanje osobnih podataka primateljima (ili njihov pristup tim podacima) koji nisu ovlašteni primati te podatke (ili im pristupati) ili bilo koji drugi oblik obrade kojim se krši Opća uredba o zaštiti podataka.

#### **Primjer**

Primjer gubitka osobnih podataka može biti situacija u kojoj je uređaj koji sadržava kopiju baze podataka o klijentima voditelja obrade izgubljen ili ukraden. Još jedan primjer gubitka podataka može biti situacija u kojoj je jedina kopija baze osobnih podataka šifrirana s pomoću ucjenjivačkog softvera (*ransomware*) ili ju je voditelj obrade šifrirao s pomoću ključa koji više ne posjeduje.

Trebalo bi biti jasno da je povreda vrsta sigurnosnog incidenta. Međutim, kako je navedeno u članku 4. točki 12., Opća uredba o zaštiti podataka primjenjuje se samo u slučaju povrede *osobnih podataka*. Posljedica je te povrede to da voditelj obrade neće moći osigurati poštovanje načela koja se odnose na obradu osobnih podataka kako su prikazana u članku 5. Opće uredbе o zaštiti podataka. Time se ističe razlika između sigurnosnog incidenta i povrede osobnih podataka – u osnovi, sve su povrede osobnih podataka sigurnosni incidenti, ali svi sigurnosni incidenti nisu nužno i povrede osobnih podataka<sup>13</sup>.

Potencijalni negativni učinci povrede na pojedince razmatraju se u nastavku.

### 2. Vrste povreda osobnih podataka

---

<sup>12</sup> Vidjeti uvodnu izjavu 87.

<sup>13</sup> Treba napomenuti da pojam sigurnosnog incidenta nije ograničen na modele prijetnji u kojima je organizacija napadnuta izvana, nego uključuje i incidente prouzročene unutarnjom obradom kojom se krše načela sigurnosti.

Radna skupina iz članka 29. u svojem je Mišljenju 03/2014 o obavješćivanju o povredi osobnih podataka objasnila da se povrede mogu razvrstati u kategorije na temelju sljedećih triju dobro poznatih načela informacijske sigurnosti<sup>14</sup>:

- „povreda povjerljivosti” – u slučaju neovlaštenog ili slučajnog otkrivanja osobnih podataka ili pristupa tim podacima
- „povreda cjelovitosti” – u slučaju neovlaštene ili slučajne izmjene osobnih podataka
- „povreda dostupnosti” – u slučaju slučajnog ili neovlaštenog gubitka pristupa osobnim podacima<sup>15</sup> ili uništenja tih podataka.

Treba napomenuti i da se, ovisno o okolnostima, povreda može istodobno odnositi na povjerljivost, cjelovitost i dostupnost osobnih podataka te na bilo koju kombinaciju tih elemenata.

Dok je utvrđivanje povrede povjerljivosti ili cjelovitosti relativno jasno, povreda dostupnosti može biti manje očita. Povreda će se uvijek smatrati povredom dostupnosti ako je došlo do trajnog gubitka ili uništenja osobnih podataka.

### **Primjer**

Primjeri gubitka dostupnosti uključuju situacije u kojima su podaci slučajno izbrisani ili ih je izbrisala neovlaštena osoba ili ako je, u primjeru sa šifriranim podacima, izgubljen ključ za dešifriranje. U slučaju da voditelj obrade ne može ponovno uspostaviti pristup podacima, primjerice, s pomoću sigurnosne kopije, tada se to smatra trajnim gubitkom dostupnosti.

Do gubitka dostupnosti može doći i u slučaju znatnog prekida u normalnom radu organizacije, primjerice, u slučaju nestanka električne energije ili napada uskraćivanjem usluga, pri čemu su osobni podaci postali nedostupni.

Može se postaviti pitanje o tome bi li se privremeni gubitak dostupnosti osobnih podataka trebao smatrati povredom i, ako je odgovor potvrđan, je li potrebno obavješćivanje o toj povredi. U članku 32. Opće uredbe o zaštiti podataka („sigurnost obrade”) objašnjava se da bi se pri provedbi tehničkih i organizacijskih mjera radi uspostave odgovarajuće razine sigurnosti s obzirom na rizik trebalo, među ostalim, uzeti u obzir „sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade” i „sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta”.

Stoga je i sigurnosni incident kojim je došlo do privremene nedostupnosti osobnih podataka vrsta povrede, s obzirom na to da nepostojanje pristupa podacima može znatno utjecati na prava i slobode pojedinaca. Jasno, ako su osobni podaci nedostupni zbog provođenja planiranog održavanja sustava, to nije „kršenje sigurnosti” kako je definirano u članku 4. točki 12.

Kao i u slučaju trajnog gubitka ili uništenja osobnih podataka (ili zapravo svake druge vrste povrede), povredu pri kojoj je došlo do privremenog gubitka dostupnosti trebalo bi dokumentirati u skladu s

<sup>14</sup> Vidjeti Mišljenje 03/2014.

<sup>15</sup> Poznato je da je „pristup” osnovni dio „dostupnosti”. Vidjeti, primjerice, publikaciju instituta NIST, NIST SP800-53rev4, u kojoj se „dostupnost” definira kao „osiguravanje pravodobnog i pouzdanog pristupa informacijama i korištenja njima”, dostupno na adresi: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. U publikaciji CNSSI-4009 upućuje se i na Pravovremen i pouzdan pristup podatkovnim i informacijskim uslugama za ovlaštene korisnike. Vidjeti <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>. U normi ISO/IEC 27000:2016 „dostupnost” se isto definira kao „svojstvo da ovlašteni subjekt na zahtjev može pristupiti podatku i koristiti se njime”: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en>



člankom 33. stavkom 5. Time se voditelju obrade pomaže u dokazivanju odgovornosti nadzornom tijelu, koje može zatražiti uvid u tu evidenciju<sup>16</sup>. Međutim, ovisno o okolnostima povrede, obavješćivanje nadzornog tijela i pogođenih pojedinaca može, ali i ne mora, biti potrebno. Voditelj obrade morat će procijeniti vjerojatnost i ozbiljnost učinka na prava i slobode pojedinaca koji je posljedica nedostupnosti osobnih podataka. U skladu s člankom 33., voditelj obrade morat će provesti obavješćivanje osim ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca. Naravno, potreba za time morat će se procijeniti u svakom pojedinom slučaju.

### **Primjeri**

U kontekstu bolnice, ako ključni zdravstveni podaci o pacijentima postanu nedostupni čak i privremeno, to bi moglo predstavljati rizik za prava i slobode pojedinaca. Primjerice, može doći do otkazivanja operacija i ugrožavanja života.

Za razliku od toga, u slučaju nedostupnosti sustava medijskog poduzeća tijekom razdoblja od nekoliko sati (npr. zbog nestanka električne energije), ako je to poduzeće potom spriječeno u slanju elektroničkih biltena svojim pretplatnicima, nije vjerojatno da bi to predstavljalo rizik za prava i slobode pojedinaca.

Treba napomenuti da, iako nedostupnost sustava voditelja obrade može biti samo privremena i ne mora utjecati na pojedince, važno je da voditelj obrade uzme u obzir sve moguće posljedice povrede jer bi obveza obavješćivanja i dalje mogla postojati zbog drugih razloga.

### **Primjer**

Zaraza ucjenjivačkim softverom (*ransomware* – zlonamjerni softver kojim se podaci voditelja obrade šifriraju dok se ne isplati otkupnina za njih) mogla bi dovesti do privremenog gubitka dostupnosti ako se ti podaci mogu oporaviti s pomoću sigurnosne kopije. Međutim, ipak se dogodio neovlašten upad u mrežu te bi se moglo zahtijevati obavješćivanje ako je utvrđeno da je incident povreda povjerljivosti (tj. napadač je pristupio osobnim podacima) i to predstavlja rizik za prava i slobode pojedinaca.

### 3. Moguće posljedice povrede osobnih podataka

Povreda potencijalno može imati niz značajnih negativnih učinaka na pojedince, koji im mogu prouzročiti fizičku, materijalnu ili nematerijalnu štetu. U Općoj uredbi o zaštiti podataka objašnjava se da to može uključivati gubitak nadzora nad osobnim podacima pojedinaca, ograničavanje njihovih prava, diskriminaciju, krađu identiteta ili prijevaru, financijske gubitke, neovlašteni obrnuti postupak pseudonimizacije, štetu za ugled i gubitak povjerljivosti osobnih podataka zaštićenih profesionalnom tajnom. To može uključivati i bilo koju drugu znatnu ekonomsku ili društvenu štetu za te pojedince<sup>17</sup>.

U skladu s tim, Općom uredbom o zaštiti podataka zahtijeva se da voditelj obrade obavijesti nadležno nadzorno tijelo o povredi, osim ako nije vjerojatno da će povreda prouzročiti rizik od nastanka tih negativnih učinaka. Ako je vrlo vjerojatno da će nastati ti negativni učinci, Općom uredbom o zaštiti podataka zahtijeva se da voditelj obrade što prije, u razumnim granicama, obavijesti pogođene pojedince o povredi<sup>18</sup>.

---

<sup>16</sup> Vidjeti članak 33. stavak 5.

<sup>17</sup> Vidjeti i uvodne izjave 85. i 75.

<sup>18</sup> Vidjeti i uvodnu izjavu 86.

Važnost sposobnosti da se utvrdi povreda, procijeni rizik za pojedince i da ih se potom, prema potrebi, obavijesti o tome naglašena je u uvodnoj izjavi 87. Opće uredbe o zaštiti podataka:

„Trebalo bi se utvrditi jesu li provedene sve odgovarajuće mjere tehnološke zaštite i organizacijske mjere da bi se odmah utvrdilo je li došlo do povrede osobnih podataka i odmah obavijestilo nadzorno tijelo i ispitanika. Trebalo bi utvrditi činjenicu je li obavijest pružena bez nepotrebnog odgađanja, posebno uzimajući u obzir prirodu i ozbiljnost povrede osobnih podataka i njezine posljedice i negativne učinke za ispitanika. Takva obavijest može dovesti do intervencije nadzornog tijela u skladu s njegovim zadaćama i ovlastima predviđenima ovom Uredbom.”

Daljnje smjernice o procjeni rizika negativnih učinaka na pojedince razmatraju se u odjeljku IV.

Ako voditelji obrade ne obavijeste nadzorno tijelo i/ili ispitanike o povredi podataka iako su ispunjeni zahtjevi iz članka 33. i/ili članka 34., nadzorno tijelo ima izbor koji se mora temeljiti na razmatranju svih raspoloživih korektivnih mjera, a to uključuje i razmatranje izricanja odgovarajuće upravne novčane kazne<sup>19</sup> ili uz to i neke korektivne mjere iz članka 58. stavka 2.. Upravna novčana kazna može iznositi do 10 000 000 EUR, ili, ako je riječ o poduzetniku, do 2 % ukupnog godišnjeg prometa na svjetskoj razini u skladu s člankom 83. stavkom 4. točkom (a) Opće uredbe o zaštiti podataka. Važno je imati na umu i da u nekim slučajevima neobavješćivanje o povredi može biti pokazatelj nepostojanja sigurnosnih mjera ili neprikladnosti postojećih sigurnosnih mjera. U Smjernicama Radne skupine iz članka 29. o upravnim novčanim kaznama navodi se sljedeće: „Ako se istodobno u okviru nekog pojedinačnog slučaja počini nekoliko različitih kršenja, to znači da nadzorno tijelo može izdati upravne novčane kazne u iznosu koji je učinkovit, proporcionalan i odvraćajući poštujući gornju granicu za najteže kršenje.” U tom će slučaju nadzorno tijelo imati i mogućnost izricanja sankcija za neobavješćivanje o povredi (članci 33. i 34.) s jedne strane i nepostojanje (prikladnih) sigurnosnih mjera (članak 32.) s druge strane, s obzirom na to da se radi o dva posebna kršenja.

## II. Članak 33. – Obavješćivanje nadzornog tijela

### A. Kada je obavješćivanje potrebno

#### 1. Zahtjevi iz članka 33.

Člankom 33. stavkom 1. predviđeno je sljedeće:

„U slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo nadležno u skladu s člankom 55. o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.”

U uvodnoj izjavi 87. navodi se sljedeće<sup>20</sup>:

<sup>19</sup> Za dodatne pojedinosti, vidjeti Smjernice Radne skupine iz članka 29. o primjeni i određivanju upravnih novčanih kazni, koje su dostupne na adresi: [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=47889](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889)

<sup>20</sup> Ovdje je važna i uvodna izjava 85.

„Trebalo bi se utvrditi jesu li provedene sve odgovarajuće mjere tehnološke zaštite i organizacijske mjere da bi se odmah utvrdilo je li došlo do povrede osobnih podataka i odmah obavijestilo nadzorno tijelo i ispitanika. Trebalo bi utvrditi činjenicu je li obavijest pružena bez nepotrebnog odgađanja posebno uzimajući u obzir prirodu i ozbiljnost povrede osobnih podataka i njezine posljedice i negativne učinke za ispitanika. Takva obavijest može dovesti do intervencije nadzornog tijela u skladu s njegovim zadaćama i ovlastima predviđenima ovom Uredbom.”

## 2. Kada se smatra da je voditelj obrade „saznao” za povredu?

Kao što je prethodno navedeno, Općom uredbom o zaštiti podataka zahtijeva se da, u slučaju povrede, voditelj obrade bez nepotrebne odgode obavijesti nadzorno tijelo i, ako je izvedivo, najkasnije u roku od 72 sata nakon što je saznao za povredu. Time se postavlja pitanje o tome kada se može smatrati da je voditelj obrade „saznao” za povredu. Prema mišljenju Radne skupine iz članka 29. voditelj obrade „saznao je” za povredu kada s razumnim stupnjem sigurnosti može smatrati da je došlo do sigurnosnog incidenta kojim su ugroženi osobni podaci.

Međutim, kako je prethodno navedeno, Općom uredbom o zaštiti podataka zahtijeva se da voditelj obrade provede sve odgovarajuće mjere tehnološke zaštite i organizacijske mjere kako bi se odmah utvrdilo je li došlo do povrede osobnih podataka i kako bi se hitno obavijestilo nadzorno tijelo i ispitanike. Navedeno je i da bi trebalo utvrditi je li obavijest pružena bez nepotrebne odgode posebno uzimajući u obzir prirodu i ozbiljnost povrede i njezine posljedice i negativne učinke za ispitanika<sup>21</sup>. Time se voditelja obrade obvezuje da osigura da pravodobno „sazna” za sve povrede kako bi mogao poduzeti odgovarajuće mjere.

Kada se točno može smatrati da je voditelj obrade „saznao” za određenu povredu ovisit će o okolnostima konkretne povrede. U nekim će slučajevima postojanje povrede biti relativno jasno od samog početka, dok će u ostalim slučajevima možda biti potrebno određeno vrijeme kako bi se utvrdilo jesu li ugroženi osobni podaci. Međutim, naglasak bi trebalo staviti na hitno djelovanje kako bi se incident istražio i kako bi se utvrdilo je li zaista došlo do povrede osobnih podataka te kako bi se u tom slučaju poduzele mjere za popravlanje štete i prema potrebi obavijestilo o povredi.

### **Primjeri**

1. U slučaju gubitka USB ključa s nešifriranim osobnim podacima često nije moguće utvrditi jesu li neovlaštene osobe dobile pristup tim podacima. Unatoč tome, iako voditelj obrade možda i ne može utvrditi je li došlo do povrede povjerljivosti, o takvom se slučaju mora provesti obavješćivanje jer postoji razuman stupanj sigurnosti da je došlo do povrede dostupnosti. U tom bi slučaju voditelj obrade „saznao” za povredu u trenutku u kojem je shvatio da je USB ključ izgubljen.

2. Treća strana obavijesti voditelja obrade da je slučajno primila osobne podatke jednog od njegovih klijenata i pruži dokaze o neovlaštenom otkrivanju. Budući da su voditelju obrade predstavljeni jasni dokazi o povredi povjerljivosti, nema dvojbe o tome da je voditelj obrade „saznao” za povredu.

3. Voditelj obrade otkrije da je došlo do neovlaštenog upada u njegovu mrežu. Voditelj obrade provjerava svoje sustave kako bi utvrdio jesu li ugroženi podaci koji se nalaze u tim sustavima i potvrđuje da se to dogodilo. Budući da voditelj obrade sada ima jasne dokaze o povredi, ponovno nema dvojbe o tome da je voditelj obrade „saznao” za povredu.

4. Počinitelj kiberkaznenog djela kontaktirao je s voditeljem obrade nakon što je neovlašteno ušao u njegov sustav kako bi zatražio otkupninu. U tom slučaju, nakon provjere svojeg sustava kako bi

<sup>21</sup> Vidjeti uvodnu izjavu 87.

potvrdio da je napadnut, voditelj obrade ima jasne dokaze o tome da je došlo do povrede pa nema dvojbe o tome da je „saznao” za povredu.

Nakon što ga prvi put o potencijalnoj povredi obavijesti pojedinac, medijska organizacija ili drugi izvor, ili nakon što je sam otkrio sigurnosni incident, voditelj obrade može tijekom kratkog razdoblja provoditi istragu kako bi utvrdio je li stvarno došlo do povrede. Tijekom tog razdoblja istrage ne može se smatrati da je voditelj obrade „saznao” za povredu. Međutim, očekuje se da bi početna istraga trebala početi što prije i njome bi se, s razumnim stupnjem sigurnosti, trebalo utvrditi je li došlo do povrede. Nakon toga može se provesti podrobija istraga.

Nakon što je saznao za nju, voditelj obrade mora bez nepotrebne odgode i, ako je izvedivo, najkasnije u roku od 72 sata obavijestiti o povredi koja podliježe obvezi obavješćivanja. Tijekom tog razdoblja voditelj obrade trebao bi procijeniti vjerojatni rizik za pojedince kako bi utvrdio je li zahtjev za obavješćivanje aktiviran te koje su mjere potrebne za rješavanje problema povrede. Međutim, moguće je da voditelj obrade već ima početnu procjenu potencijalnog rizika koji bi povreda mogla prouzročiti, a ta procjena postoji u okviru procjene učinka na zaštitu podataka<sup>22</sup> koja je provedena prije provođenja predmetnog postupka obrade. Međutim, procjena učinka na zaštitu podataka može biti općenitija u usporedbi s konkretnim okolnostima stvarne povrede pa će stoga u svakom slučaju biti potrebno provesti dodatnu procjenu uzimajući u obzir te okolnosti. Za dodatne pojedinosti o procjeni rizika vidjeti odjeljak IV.

U većini slučajeva preliminarna djelovanja trebalo bi dovršiti ubrzo nakon početnog upozorenja (tj. kada voditelj obrade ili izvršitelj obrade posumnja na postojanje sigurnosnog incidenta koji može uključivati osobne podatke), a samo u iznimnim slučajevima ta preliminarna djelovanja mogu trajati dulje.

### **Primjer**

Pojedinac obavijesti voditelja obrade da je e-poštom primio poruku od pošiljatelja koji se lažno predstavlja kao voditelj obrade. U poruci se nalaze osobni podaci koji se odnose na njegovu (stvarno) korištenje uslugom voditelja obrade, što upućuje na to da je sigurnost voditelja obrade dovedena u pitanje. Voditelj obrade provodi kratku istragu i utvrđuje neovlašteni upad u svoju mrežu i dokaze o neovlaštenom pristupu osobnim podacima. Od toga se trenutka smatra da je voditelj obrade „saznao” za povredu i obvezno je obavješćivanje nadzornog tijela, osim ako nije vjerojatno da će povredom nastati rizik za prava i slobode pojedinaca. Voditelj obrade morat će poduzeti odgovarajuće mjere za popravljavanje štete radi otklanjanja posljedica povrede.

Stoga bi voditelj obrade trebao imati uspostavljene unutarnje postupke kojima može otkriti povredu i otkloniti njezine posljedice. Primjerice, za pronalaženje određenih nepravilnosti u obradi podataka voditelj obrade ili izvršitelj obrade može primjenjivati određene tehničke mjere kao što su uređaji za analizu protoka podataka i zapisnika podataka s pomoću kojih je moguće utvrditi događaje i upozorenja otkrivanjem povezanosti među podacima iz zapisnika<sup>23</sup>. Važno je da se nakon otkrivanja povrede ona prijavi odgovarajućim višim upravljačkim razinama radi rješavanja tog problema i, ako se zahtijeva, obavješćivanja u skladu s člankom 33. i, ako je potrebno, obavješćivanja u skladu s člankom 34. Te mjere i mehanizmi za izvješćivanje mogu se podrobno opisati u planovima voditelja

<sup>22</sup> Vidjeti Smjernice Radne skupine iz članka 29. o procjeni učinka na zaštitu podataka koje su dostupne na adresi: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

<sup>23</sup> Trebalo bi imati na umu da podaci iz zapisnika kojima se olakšava provođenje revizije s obzirom na, primjerice, pohranu, izmjene ili brisanje podataka, mogu isto biti osobni podaci koji se odnose na osobu koja je pokrenula odgovarajući postupak obrade.

obrade za postupanje u slučaju incidenta i/ili u sustavima upravljanja. Time će se voditelju obrade pomoći u učinkovitim planiranju i određivanju tko je unutar organizacije operativno odgovoran za upravljanje povredom te kako i kada se provodi proširivanje postupanja u slučaju incidenta ako je to potrebno.

Voditelj obrade trebao bi uspostaviti i odgovarajuće mehanizme sa svim izvršiteljima obrade kojima se koristi, pri čemu su ti izvršitelji obrade i sami obvezni obavijestiti voditelja obrade u slučaju povrede (vidjeti u nastavku).

Iako su voditelji obrade i izvršitelji obrade odgovorni za uspostavljanje primjerenih mjera za sprečavanje povreda, reagiranje na njih i njihovo otklanjanje, postoje određene praktične mjere koje bi trebalo poduzeti u svim slučajevima.

- Informacije koje se odnose na sve događaje povezane sa sigurnošću trebale bi biti usmjerene prema odgovornoj osobi ili osobama čiji je zadatak odgovor na incidente, utvrđivanje postojanja povrede i procjenjivanje rizika.
- Potom bi trebalo procijeniti rizik za pojedince koji je prouzročen povredom (vjerojatnost da rizik ne postoji, postoji ili da postoji visoki rizik), pri čemu je potrebno obavijestiti relevantne odjele unutar organizacije.
- Ako se to zahtijeva, o povredi bi trebalo obavijestiti nadzorno tijelo, a možda i pogođene pojedince.
- Istodobno bi voditelj obrade trebao djelovati kako bi obuzdao povredu i otklonio njezine posljedice.
- Povredu bi trebalo kontinuirano dokumentirati tijekom njezina trajanja.

U skladu s tim, trebalo bi biti jasno da je voditelj obrade obavezan djelovati povodom svakog početnog upozorenja i utvrditi je li stvarno došlo do povrede. U tom kratkom razdoblju omogućuje se da voditelj obrade provede kratku istragu te prikupi dokaze i ostale relevantne pojedinosti. Međutim, nakon što voditelj obrade s razumnim stupnjem sigurnosti utvrdi da je došlo do povrede, i ako su ispunjeni uvjeti iz članka 33. stavka 1., on mora obavijestiti nadzorno tijelo bez nepotrebne odgode i, ako je izvedivo, najkasnije u roku od 72 sata<sup>24</sup>. Ako voditelj obrade ne reagira pravodobno i ako postane očito da je došlo do povrede, to bi se moglo smatrati neobavješćivanjem u skladu s člankom 33.

U članku 32. jasno se navodi da bi voditelj obrade i izvršitelj obrade trebali uspostaviti odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti osobnih podataka. Ključnim elementima tih mjera trebalo bi smatrati sposobnost pravodobnog otkrivanja povrede, rješavanja problema povezanih s njom i njezina prijavljivanja.

### 3. Zajednički voditelji obrade

Članak 26. odnosi se na zajedničke voditelje obrade i u njemu se utvrđuje da zajednički voditelji obrade moraju odrediti svoje odgovornosti za poštovanje Opće uredbe o zaštiti podataka<sup>25</sup>. To uključuje određivanje strane koja je odgovorna za poštovanje obveza iz članaka 33. i 34. Radna skupina iz članka 29. preporučuje da se u ugovorne dogovore među zajedničkim voditeljima obrade uključe odredbe kojima se određuje koji će voditelj obrade voditi ili biti odgovoran za poštovanje obveza obavješćivanja o povredama iz Opće uredbe o zaštiti podataka.

---

<sup>24</sup> Vidjeti Uredbu br. 1182/71 o utvrđivanju pravila koja se primjenjuju na razdoblja, datume i rokove, dostupnu na adresi: <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:31971R1182>

<sup>25</sup> Vidjeti i uvodnu izjavu 79.

#### 4. Obveze izvršitelja obrade

Voditelj zadržava opću odgovornost za zaštitu osobnih podataka, ali izvršitelj obrade ima važnu ulogu u omogućivanju voditelju obrade da ispuni svoje obveze, a to uključuje obavješćivanje o povredama. Zaista, u članku 28. stavku 3. utvrđuje se da se obrada koju provodi izvršitelj obrade uređuje ugovorom ili drugim pravnim aktom. U članku 28. stavku 3. točki (f) navodi se da se ugovorom ili drugim pravnim aktom propisuje da izvršitelj obrade „pomaže voditelju obrade u osiguravanju usklađenosti s obvezama u skladu s člancima od 32. do 36., uzimajući u obzir prirodu obrade i informacije koje su dostupne izvršitelju obrade”.

U članku 33. stavku 2. pojašnjava se da ako se voditelj obrade koristi izvršiteljem obrade, a izvršitelj obrade sazna za povredu osobnih podataka koje obrađuje u ime voditelja obrade, taj izvršitelj mora „bez nepotrebnog odgađanja” obavijestiti voditelja obrade. Trebalo bi imati na umu da izvršitelj obrade ne mora prije obavješćivanja voditelja obrade prvo procijeniti vjerojatnost da će povreda prouzročiti rizik jer je voditelj obrade taj koji mora napraviti tu procjenu nakon što sazna za povredu. Izvršitelj obrade mora samo utvrditi je li došlo do povrede i potom obavijestiti voditelja obrade. Voditelj obrade koristi se izvršiteljem obrade za postizanje svojih ciljeva. Stoga bi se u načelu trebalo smatrati da je voditelj obrade „saznao” za povredu nakon što ga je izvršitelj obrade o njoj obavijestio. Obveza izvršitelja obrade da obavijesti svojeg voditelja obrade omogućuje voditelju obrade da riješi problem povrede i utvrdi je li potrebno obavijestiti nadzorno tijelo u skladu s člankom 33. stavkom 1. i pogođene pojedince u skladu s člankom 34. stavkom 1. Voditelj obrade možda će htjeti i istražiti povredu, s obzirom na to da izvršitelj obrade možda nije u položaju da zna sve relevantne činjenice koje se odnose na to pitanje, primjerice, ima li voditelj obrade još uvijek kopiju ili sigurnosnu kopiju osobnih podataka koje je izvršitelj obrade uništio ili izgubio. To može utjecati na obvezu voditelja obrade o obavješćivanju.

Općom uredbom o zaštiti podataka nije predviđen nikakav izričit rok u kojem izvršitelj obrade mora upozoriti voditelja obrade, osim što se propisuje da to mora učiniti „bez nepotrebnog odgađanja”. Stoga Radna skupina iz članka 29. preporučuje da izvršitelj obrade odmah obavijesti voditelja obrade i da mu dodatne informacije o povredi dostavlja postupno u skladu s dostupnošću novih pojedinosti o povredi. To je važno kako bi se voditelju obrade pomoglo u ispunjavanju zahtjeva u pogledu obavješćivanja nadzornog tijela u roku od 72 sata.

Kako je prethodno objašnjeno, u ugovoru između voditelja obrade i izvršitelja obrade trebao bi se, osim ostalih odredbi iz Opće uredbe o zaštiti podataka, utvrditi i način ispunjavanja zahtjeva iz članka 33. stavka 2. To može uključivati zahtjeve u pogledu ranog obavješćivanja, koji su obveza izvršitelja obrade, kojima se pak podupiru obveze voditelja obrade u pogledu prijavljivanja povrede nadzornom tijelu u roku od 72 sata.

Ako izvršitelj obrade pruža usluge višestrukim voditeljima obrade koji su svi pogođeni istim incidentom, izvršitelj obrade morat će pojedinosti o incidentu prijaviti svakom pojedinom voditelju obrade.

Izvršitelj obrade može obavljati obavješćivanje u ime voditelja obrade ako je voditelj obrade izvršitelju obrade dao ispravno ovlaštenje koje je dio ugovornog dogovora između voditelja obrade i izvršitelja obrade. To obavješćivanje mora se obavljati u skladu s člancima 33. i 34. Međutim, važno je imati na umu da je pravna odgovornost za obavješćivanje i dalje na voditelju obrade.

##### B. Pružanje informacija nadzornom tijelu

###### 1. Informacije koje treba dostaviti

Ako voditelj obrade obavješćuje nadzorno tijelo o povredi, u članku 33. stavku 3. navodi se da on, u najmanjoj mjeri, mora:

„(a) opisati prirod[u] povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;

(b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;

(c) opisati vjerojatne posljedice povrede osobnih podataka;

(d) opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.”

Općom uredbom o zaštiti podataka nisu definirane kategorije ispitanika ili evidencija osobnih podataka. Međutim, Radna skupina iz članka 29. upućuje na to da se kategorije ispitanika odnose na razne vrste pojedinaca na čije je osobne podatke povreda utjecala. Ovisno o korištenim opisnicima, to može uključivati, među ostalim, djecu i ostale osjetljive skupine, osobe s invaliditetom, zaposlenike ili klijente/kupce. Slično tomu, kategorije evidencija osobnih podataka mogu se odnositi na različite vrste evidencija koje bi voditelj obrade mogao obrađivati, kao što su zdravstveni podaci, evidencije o obrazovanju, informacije o socijalnoj skrbi, financijski podaci, brojevi bankovnih računa, brojevi putovnica itd.

U uvodnoj izjavi 85. pojašnjava se da je jedna od svrha obavješćivanja ograničavanje štete za pojedince. Prema tome, ako se pokaže da s obzirom na vrste ispitanika ili vrste osobnih podataka postoji rizik od posebne štete koji je prouzročen povredom (npr. krađa identiteta, prijevarena, financijski gubitak, prijetnja otkrivanja profesionalne tajne), tada je važno da se u predmetnoj obavijesti navеду te kategorije. Na taj je način to povezano sa zahtjevom da se opišu vjerojatne posljedice povrede.

Ako precizne informacije nisu dostupne (npr. točan broj pogođenih ispitanika), to ne bi trebalo spriječiti pravodobno obavješćivanje o povredi. Općom uredbom o zaštiti podataka dopušta se navođenje približnog broja predmetnih pogođenih pojedinaca i predmetnih evidencija osobnih podataka. Naglasak bi trebao biti na otklanjanju negativnih učinaka povrede, a ne na pružanju preciznih podataka. Stoga, ako je postalo jasno da je došlo do povrede, ali njezini razmjeri još nisu poznati, postupno obavješćivanje (vidjeti u nastavku) siguran je način ispunjavanja obveza obavješćivanja.

U članku 33. stavku 3. navodi se da voditelj obrade u okviru obavješćivanja „mora [pružati] barem” informacije koje su tamo navedene. Stoga voditelj obrade može, prema potrebi, odlučiti dostaviti dodatne pojedinosti. Za različite vrste povreda (povrede povjerljivosti, cjelovitosti ili dostupnosti) može se zahtijevati pružanje dodatnih informacija kako bi se u potpunosti objasnile okolnosti svakog pojedinog slučaja.

### **Primjer**

U okviru svojeg obavješćivanja nadzornog tijela, voditelj obrade može smatrati korisnim da navede svojeg izvršitelja obrade ako se glavni uzrok povrede nalazi na strani tog izvršitelja obrade, osobito ako je to dovelo do incidenta koji je utjecao na evidencije osobnih podataka mnogih drugih voditelja obrade koji koriste istog izvršitelja obrade.

U svakom slučaju, nadzorno tijelo može zatražiti dodatne pojedinosti u okviru svoje istrage o povredi.

## **2. Postupno obavješćivanje**

Ovisno o prirodi povrede, voditelj obrade možda će morati provesti dodatnu istragu kako bi utvrdio sve relevantne činjenice povezane s incidentom. U članku 33. stavku 4. stoga se navodi sljedeće:

„Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružiti bez nepotrebnog daljnjeg odgađanja.”

To znači da se u Općoj uredbi o zaštiti podataka priznaje da voditelji obrade neće uvijek imati sve potrebne informacije o povredi u roku od 72 sata nakon što su saznali za nju jer potpune i sveobuhvatne pojedinosti o incidentu možda neće uvijek biti dostupne tijekom tog početnog razdoblja. Stoga se Uredbom dopušta postupno obavješćivanje. Vjerojatnije je da će se to primjenjivati u slučaju složenijih povreda, kao što su neke vrste kibersigurnosnih incidenata u kojima će, primjerice, biti potrebna opsežna forenzička istraga kako bi se u potpunosti utvrdila priroda povrede i razmjer u kojem su osobni podaci ugroženi. Stoga će u mnogim slučajevima voditelj obrade morati provoditi više istraga i daljnjih praćenja nakon kojih će dostavljati dodatne informacije. To je dopušteno u skladu s člankom 33. stavkom 1., pod uvjetom da voditelj obrade navede razloge za kašnjenje. Radna skupina iz članka 29. preporučuje da bi voditelj obrade, ako još nema sve potrebne informacije pa će više pojedinosti dostaviti kasnije, trebao pri prvom obavješćivanju nadzornog tijela obavijestiti nadzorno tijelo i o tome. Nadzorno tijelo trebalo bi se složiti oko načina i vremena dostavljanja dodatnih informacija. Time se voditelja obrade ne sprječava da dodatne informacije dostavi u bilo kojem drugom trenutku ako sazna dodatne relevantne pojedinosti o povredi koje treba dostaviti nadzornom tijelu.

Naglasak u zahtjevu za obavješćivanje stavljen je na poticanje voditelja obrade da hitno djeluju povodom povrede, ograniče je i, po mogućnosti, oporave ugrožene osobne podatke te da zatraže odgovarajući savjet od nadzornog tijela. Obavješćivanjem nadzornog tijela u roku od prvih 72 sata može se omogućiti voditelju obrade da bude siguran u ispravnost odluke o tome treba li obavijestiti pojedince ili ne.

Međutim, svrha obavješćivanja nadzornog tijela nije samo dobivanje smjernica o tome je li potrebno obavijestiti pogođene pojedince. U nekim će slučajevima, zbog prirode povrede i ozbiljnosti rizika, biti očito da voditelj obrade mora bez odgode obavijestiti pogođene pojedince. Primjerice, ako postoji neposredna prijetnja od krađe identiteta ili ako su na internetu otkrivene posebne kategorije osobnih podataka<sup>26</sup>, voditelj obrade trebao bi djelovati bez nepotrebne odgode kako bi obuzdao povredu i o njoj obavijestio predmetne pojedince (vidjeti odjeljak III.). U iznimnim okolnostima to se može provesti čak i prije obavješćivanja nadzornog tijela. Općenitije rečeno, obavješćivanje nadzornog tijela ne može se smatrati opravdanjem za neobavješćivanje ispitanika o povredi ako je ono potrebno.

Trebalo bi biti jasno i to da voditelj obrade, nakon početnog obavješćivanja, može nadzornom tijelu dostaviti ažurirane informacije ako su daljnjom istragom otkriveni dokazi da je sigurnosni incident spriječen i da se zapravo nije dogodila nikakva povreda. Te se informacije potom mogu dodati informacijama koje su već dostavljene nadzornom tijelu te se u skladu s njima incident može evidentirati kao incident pri kojemu nije došlo do povrede. Nije predviđena nikakva kazna za prijavljivanje incidenta za koji se u konačnici pokaže da nije riječ o povredi.

### **Primjer**

Voditelj obrade u roku od 72 sata nakon otkrivanja povrede obavijesti nadzorno tijelo da je izgubio USB ključ s kopijom osobnih podataka nekih od svojih klijenata. Kasnije se utvrdi da je USB ključ bio pohranjen na krivom mjestu u poslovnim prostorijama voditelja obrade te je pronađen. Voditelj obrade dostavlja ažurirane informacije nadzornom tijelu i traži da se obavijest izmijeni.

Treba imati na umu da postupni pristup u obavješćivanju već postoji na temelju postojećih obveza iz Direktive 2002/58/EZ, Uredbe 611/2013 i ostalih samoprijavljenih incidenata.

<sup>26</sup> Vidjeti članak 9.



### 3. Odgođeno obavješćivanje

U članku 33. stavku 1. pojašnjava se da ako obavješćivanje nije učinjeno unutar 72 sata, ono mora biti popraćeno razlozima za kašnjenje. Time se, zajedno s konceptom postupnog obavješćivanja, priznaje da voditelj obrade možda neće uvijek moći obavijestiti nadzorno tijelo o povredi u tom roku te da se odgođeno obavješćivanje može dopustiti.

Takav scenarij može se pojaviti ako, primjerice, voditelj obrade u kratkom razdoblju doživi više sličnih povreda povjerljivosti koje na isti način utječu na velik broj ispitanika. Voditelj obrade mogao bi saznati za povredu i, tijekom započinjanja svoje istrage, a prije obavješćivanja, otkriti dodatne slične povrede s različitim uzrocima. Ovisno o okolnostima, voditelju obrade možda će biti potrebno određeno vrijeme da utvrdi razmjere tih povreda pa, umjesto da obavijesti nadzorno tijelo o svakoj povredi pojedinačno, voditelj obrade odluči izraditi smislenu obavijest u kojoj je prikazano nekoliko vrlo sličnih povreda za koje je moguće da imaju različite uzroke. To bi moglo dovesti do toga da obavijest nadzornom tijelu kasni više od 72 sata nakon što je voditelj obrade prvi put saznao za te povrede.

Strogo gledano, svaka pojedinačna povreda incident je o kojem je potrebno obavijestiti nadzorno tijelo. Međutim, kako bi izbjegao preveliko opterećenje, voditelj obrade mogao bi podnijeti „objedinjenu” obavijest u kojoj su prikazane sve te povrede, pod uvjetom da se one odnose na istu vrstu osobnih podataka koji su povrijeđeni na isti način tijekom relativno kratkog razdoblja. Ako se dogodi niz povreda koje se odnose na različite vrste osobnih podataka koji su povrijeđeni na različite načine, tada bi se postupak obavješćivanja trebao odvijati na uobičajen način tj. tako da se nadzorno tijelo pojedinačno obavijesti o svakoj povredi u skladu s člankom 33.

Iako su Općom uredbom o zaštiti podataka odgođene obavijesti dopuštene do određene mjere, ne bi ih trebalo smatrati redovnim postupanjem. Treba naglasiti da se objedinjene obavijesti mogu primjenjivati i za višestruke slične povrede koje su prijavljene u roku od 72 sata.

#### C. Prekogranične povrede i povrede u slučajevima poslovnog nastana izvan EU-a

##### 1. Prekogranične povrede

Ako se osobni podaci obrađuju prekogranično<sup>27</sup>, povreda može utjecati na ispitanike u više od jedne države članice. U članku 33. stavku 1. pojašnjava se da bi u slučaju povrede voditelj obrade trebao obavijestiti nadzorno tijelo nadležno u skladu s člankom 55. Opće uredbe o zaštiti podataka<sup>28</sup>. Članak 55. stavak 1. glasi:

„Svako nadzorno tijelo nadležno je za obavljanje zadaća koje su mu povjerene i izvršavanje ovlasti koje su mu dodijeljene u skladu s ovom Uredbom na državnom području vlastite države članice.”

Međutim, u članku 56. stavku 1. navedeno je sljedeće:

„Ne dovodeći u pitanje članak 55. nadzorno tijelo glavnog poslovnog nastana ili jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade nadležno je djelovati kao vodeće nadzorno tijelo za prekograničnu obradu koju provodi taj voditelj obrade ili izvršitelj obrade u skladu s postupkom utvrđenim u članku 60.”

Nadalje, u članku 56. stavku 6. navedeno je sljedeće:

<sup>27</sup> Vidjeti članak 4. točku 23.

<sup>28</sup> Vidjeti i uvodnu izjavu 122.

„Vodeće nadzorno tijelo jedini je sugovornik voditelja obrade ili izvršitelja obrade u prekograničnoj obradi koju provodi taj voditelj obrade ili izvršitelj obrade.”

To znači da kad god u kontekstu prekogranične obrade dođe do povrede o kojoj se mora obavijestiti, voditelj obrade morat će obavijestiti vodeće nadzorno tijelo<sup>29</sup>. Stoga, pri izradi svojeg plana postupanja u slučaju povrede, voditelj obrade mora procijeniti koje je nadzorno tijelo vodeće nadzorno tijelo koje će trebati obavijestiti o povredi<sup>30</sup>. To će voditelju obrade omogućiti da odmah reagira na povredu i da ispuni svoje obveze s obzirom na članak 33. Trebalo bi biti jasno da se u slučaju povrede u koju je uključena prekogranična obrada mora obavijestiti vodeće nadzorno tijelo, koje ne mora nužno biti nadzorno tijelo nadležno za lokaciju pogođenih ispitanika ili lokaciju na kojoj se dogodila povreda. Pri obavješćivanju vodećeg tijela, voditelj obrade trebao bi navesti, ako je prikladno, uključuje li povreda poslovne nastane u drugim državama članicama te u kojim se državama članicama nalaze ispitanici na koje je povreda vjerojatno utjecala. Ako voditelj obrade nije siguran koje je nadzorno tijelo vodeće tijelo, tada bi trebao obavijestiti barem lokalno nadzorno tijelo nadležno za lokaciju na kojoj se povreda dogodila.

## 2. Povrede u slučajevima poslovnog nastana izvan EU-a

Članak 3. odnosi se na teritorijalno područje primjene Opće uredbe o zaštiti podataka, uključujući kad se ona primjenjuje na obradu osobnih podataka koju obavlja voditelj obrade ili izvršitelj obrade koji nema poslovni nastan u EU-u. Konkretno, u članku 3. stavku 2. navedeno je sljedeće<sup>31</sup>:

„Ova se Uredba primjenjuje na obradu osobnih podataka ispitanikâ u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su aktivnosti obrade povezane s:

- (a) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili
- (b) praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije.”

Relevantan je i članak 3. stavak 3. u kojemu je navedeno sljedeće<sup>32</sup>:

„Ova se Uredba primjenjuje na obradu osobnih podataka koju obavlja voditelj obrade koji nema poslovni nastan u Uniji, već na mjestu gdje se pravo države članice primjenjuje na temelju međunarodnog javnog prava.”

Ako se povreda dogodi voditelju obrade koji nema poslovni nastan u EU-u i koji podliježe članku 3. stavku 2. ili članku 3. stavku 3., na njega se i dalje primjenjuju obveze obavješćivanja na temelju članaka 33. i 34. Člankom 27. zahtijeva se da voditelj obrade (i izvršitelj obrade) imenuje predstavnika u EU-u ako se primjenjuje članak 3. stavak 2. Radna skupina iz članka 29. u tim slučajevima preporučuje da bi predmetne obavijesti trebalo uputiti nadzornom tijelu u državi članici u

<sup>29</sup> Vidjeti Smjernice Radne skupine iz članka 29. za identifikaciju voditelja obrade ili vodećeg nadzornog tijela izvršitelja obrade, dostupne na adresi: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44102](http://ec.europa.eu/newsroom/document.cfm?doc_id=44102).

<sup>30</sup> Popis s kontaktnim podacima svih europskih nacionalnih tijela za zaštitu podataka nalazi se na adresi: [http://ec.europa.eu/justice/data-protection/bodies/authorities/index\\_en.htm](http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm)

<sup>31</sup> Vidjeti i uvodne izjave 23. i 24.

<sup>32</sup> Vidjeti i uvodnu izjavu 25.

kojoj predstavnik voditelja obrade u EU-u ima poslovni nastan<sup>33</sup>. Slično tomu, ako izvršitelj obrade podliježe članku 3. stavku 2., na njega se primjenjuju obveze izvršitelja obrade, pri čemu je ovdje od posebne važnosti dužnost da o povredi obavijesti voditelja obrade na temelju članka 33. stavka 2.

#### D. Uvjeti pod kojima se ne zahtijeva obavješćivanje

U članku 33. stavku 1. pojašnjava se da se u slučaju povreda kod kojih „nije vjerojatno da će [...] prouzročiti rizik za prava i slobode pojedinaca” ne zahtijeva obavješćivanje nadzornog tijela. Primjer toga mogao bi biti slučaj u kojem su osobni podaci već javno dostupni i otkrivanje tih podataka ne predstavlja vjerojatan rizik za pojedinca. To je u suprotnosti s postojećim zahtjevima o obavješćivanju za pružatelje javno dostupnih elektroničkih komunikacijskih usluga iz Direktive 2009/136/EZ u kojoj se navodi da se o svim relevantnim povredama mora obavijestiti nadležno tijelo.

U svojem Mišljenju 03/2014 o obavješćivanju o povredi osobnih podataka<sup>34</sup>, Radna skupina iz članka 29. objasnila je da je povreda povjerljivosti osobnih podataka koji su bili šifrirani s pomoću najnaprednijeg algoritma i dalje povreda osobnih podataka i na nju se odnosi obveza obavješćivanja. Međutim, ako je povjerljivost ključa netaknuta – tj. ključ nije bio ugrožen nijednom povredom, a izrađen je tako da ga nijedna osoba koja nije ovlaštena za pristup ključu ne može utvrditi s pomoću dostupnih tehničkih sredstava – tada su ti podaci u načelu nerazumljivi. Stoga nije vjerojatno da će ta povreda negativno utjecati na pojedince pa stoga nije obvezno obavješćivanje tih pojedinaca<sup>35</sup>. Međutim, čak i ako su podaci šifrirani, gubitak ili izmjena podataka mogu imati negativne posljedice za ispitanike ako voditelj obrade ne posjeduje nikakvu primjerenu sigurnosnu kopiju tih podataka. U tom bi se slučaju zahtijevalo obavješćivanje ispitanika, čak i ako su ti podaci primjereno šifrirani.

Radna skupina iz članka 29. objasnila je da bi sličan slučaj postojao kada bi osobni podaci, kao što su lozinke, bili sigurno raspršeni (*hashed*) uz primjenu proizvoljnog niza znakova (*salted*), pri čemu je raspršena vrijednost (*hashed value*) izračunana s pomoću vrhunske funkcije raspršivanja primjenom kriptografskog ključa, ključ korišten za raspršivanje podataka nije bio ugrožen nijednom povredom te je ključ korišten za raspršivanje podataka izrađen na takav način da ga s pomoću dostupnih tehnoloških sredstava ne može utvrditi nijedna osoba koja nije ovlaštena pristupiti ključu.

Stoga, ako su osobni podaci u osnovi nečitljivi neovlaštenim stranama i ako su predmetni podaci kopija ili ako postoji sigurnosna kopija, tada o povredi povjerljivosti koja uključuje ispravno šifrirane osobne podatke možda neće trebati obavijestiti nadzorno tijelo. To je zbog toga što nije vjerojatno da će takva povreda predstavljati rizik za prava i slobode pojedinaca. To, naravno, znači da nije potrebno obavijestiti ni pojedinca jer nije vjerojatno da postoji visoki rizik. Međutim, treba imati na umu da iako se na početku možda ne zahtijeva obavješćivanje ako nije vjerojatno da postoji rizik za prava i slobode pojedinaca, to se s vremenom može promijeniti te bi rizik trebalo ponovno procijeniti. Primjerice, ako se naknadno utvrdi da je ključ ugrožen ili ako se otkrije slaba točka u softveru za šifriranje, tada bi se ipak moglo zahtijevati obavješćivanje.

Nadalje, treba napomenuti da će se u slučaju povrede u kojem ne postoje sigurnosne kopije šifriranih osobnih podataka raditi o povredi dostupnosti, koja bi mogla prouzročiti rizike za pojedince pa bi se u tom slučaju moglo zahtijevati obavješćivanje. Slično tomu, ako dođe do povrede koja uključuje gubitak šifriranih podataka, moglo bi se raditi o povredi za koju se zahtijeva obavješćivanje čak i ako

---

<sup>33</sup> Vidjeti uvodne izjave 80. i članak 27.

<sup>34</sup> Radna skupina iz članka 29., Mišljenje 03/2014 o obavješćivanju o povredi osobnih podataka, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf)

<sup>35</sup> Vidjeti i članak 4. stavke 1. i 2. Uredbe 611/2013.

postoji sigurnosna kopija osobnih podataka. To će ovisiti o duljini vremena koje je potrebno za ponovno vraćanje tih podataka iz te sigurnosne kopije i o učinku nedostupnosti podataka na pojedince. Kako je navedeno u članku 32. stavku 1. točki (c), važan je čimbenik sigurnosti „sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta”.

### **Primjer**

Povreda povodom koje se ne bi zahtijevalo obavješćivanje nadzornog tijela bila bi gubitak šifriranog mobilnog uređaja kojim se koristi voditelj obrade i članovi njegova osoblja. Pod uvjetom da ključ za šifriranje ostane u sigurnom posjedu voditelja obrade i da se ne radi o jedinoj kopiji tih osobnih podataka, osobni podaci bili bi nedostupni napadaču. To znači da nije vjerojatno da će povreda prouzročiti rizik za prava i slobode predmetnih ispitanika. Ako kasnije postane očito da je ključ za šifriranje ugrožen ili da računalni program ili algoritam za šifriranje ima slabih točaka, promijenit će se rizik za prava i slobode pojedinaca promijenit će se pa će se stoga možda zahtijevati obavješćivanje.

Međutim, neusklađenost s člankom 33. postojat će ako voditelj obrade ne obavijesti nadzorno tijelo u situaciji u kojoj podaci zapravo nisu bili sigurno šifrirani. Stoga bi pri odabiru softvera za šifriranje voditelji obrade trebali pažljivo odvagnuti kvalitetu i ispravnu provedbu ponuđenog šifriranja, razumjeti koju razinu zaštite ono stvarno pruža te je li to primjereno s obzirom na postojeće rizike. Voditelji obrade trebali bi biti upoznati i sa pojedinostima o načinu rada njihova proizvoda za šifriranje. Primjerice, uređaj može biti šifriran nakon što ga se isključi, no ne i dok je u stanju pripravnosti. Neki proizvodi koji koriste šifriranje imaju „zadane ključeve” koje svaki kupac mora promijeniti kako bi bili djelotvorni. Osim toga, stručnjaci za sigurnost mogu neko šifriranje trenutačno smatrati primjerenim, no ono može zastarjeti u roku od nekoliko godina što znači da bi postalo upitno bi li podaci bili dostatno šifrirani s pomoću tog proizvoda i bi li njime bila osigurana odgovarajuća razina zaštite.

### **III. Članak 34. – Obavješćivanje ispitanika**

#### **A. Informiranje pojedinaca**

U određenim slučajevima, osim obavješćivanja nadzornog tijela, od voditelja obrade zahtijeva se i obavješćivanje pogođenih pojedinaca o povredi.

U članku 34. stavku 1. navedeno je sljedeće:

„U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.”

Voditelji obrade trebali bi imati u vidu da je obavješćivanje nadzornog tijela obvezno, osim ako nije vjerojatno da će doći do rizika za prava i slobode pojedinaca. Osim toga, ako je vjerojatno da je povredom prouzročen visok rizik za prava i slobode pojedinaca, o povredi se moraju obavijestiti i pojedinci. Prag za obavješćivanje pojedinaca o povredi stoga je viši nego za obavješćivanje nadzornih tijela pa se stoga neće zahtijevati da se o svim povredama obavijeste pojedinci, čime ih se štiti od nepotrebnog umaranja prekomjernim obavijestima.

U Općoj uredbi o zaštiti podataka navodi se da bi pojedince o povredi trebalo obavijestiti „bez nepotrebnog odgađanja”, a to znači da ih treba obavijestiti što prije. Glavni je cilj obavješćivanja pojedinaca pružanje konkretnih informacija o mjerama koje bi trebali poduzeti kako bi se zaštitili<sup>36</sup>. Kao što je prethodno navedeno, ovisno o prirodi povrede i riziku koji ona predstavlja, pravodobnim obavješćivanjem pomoći će se pojedincima u poduzimanju mjera kako bi se zaštitili od svih negativnih posljedica povrede.

U Prilogu B ovim Smjernicama navodi se neiscrpan popis primjera u kojima je vjerojatno da će povreda prouzročiti visok rizik za pojedince te time i popis slučajeva u kojima će voditelj obrade morati o povredi obavijestiti one koji su njome pogođeni.

#### B. Informacije koje treba dostaviti

U slučaju obavješćivanja pojedinaca, člankom 34. stavkom 2. predviđeno je sljedeće:

„Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 33. stavka 3. točaka (b), (c) i (d).”

U skladu s tom odredbom, voditelj obrade dužan je dostaviti barem sljedeće informacije:

- opis prirode povrede
- ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke
- opis vjerojatnih posljedica povrede i
- opis mjera koje je voditelj obrade poduzeo ili predložio da se poduzmu za rješavanje problema povrede, uključujući, prema potrebi, mjere za umanjivanje njezinih mogućih štetnih posljedica.

Kao primjer mjera poduzetih za rješavanje problema povrede i umanjivanje njezinih mogućih štetnih posljedica, voditelj obrade mogao bi navesti da je, nakon obavješćivanja odgovarajućeg nadzornog tijela, dobio savjete o upravljanju povredom i umanjivanju njezina učinka. Osim toga, voditelj obrade trebao bi, prema potrebi, pojedincima dati konkretne savjete kako bi se zaštitili od mogućih štetnih posljedica povrede, primjerice, savjet o promjeni lozinke u slučaju da su ugroženi njihovi podaci za pristup. Još jednom, voditelj obrade može odlučiti pružiti i druge informacije uz ove koje se ovdje zahtijevaju.

#### C. Kontaktiranje s pojedincima

U načelu bi pogođene ispitanike trebalo izravno obavijestiti o odgovarajućoj povredi, osim ako bi to zahtijevalo nerazmjerni napor. U takvom se slučaju umjesto toga daje javna obavijest ili se poduzima slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način (članak 34. stavak 3. točka (c)).

Pri obavješćivanju ispitanika o povredi trebalo bi upotrebljavati namjenske poruke i u njima se ne bi smjele slati druge informacije kao što su redovite novosti, bilteni ili standardne poruke. Time se pridonosi jasnom i transparentnom obavješćivanju o povredi.

Primjeri metoda transparentnog obavješćivanja uključuju slanje izravnih poruka (npr. poruke e-pošte, SMS poruke, izravne poruke), istaknute oglase na internetskim stranicama, obavijesti koje se šalju poštom i istaknute oglase u tiskanim medijima. Obavijest koja je ograničena samo na objavu za medije ili korporativni blog ne bi bila učinkovito sredstvo obavješćivanja pojedinaca o povredi. Radna

---

<sup>36</sup> Vidjeti i uvodnu izjavu 86.

skupina iz članka 29. preporučuje da bi voditelji obrade trebali odabrati ono sredstvo kojim se u najvećoj mogućoj mjeri povećava vjerojatnost da će informacije biti ispravno priopćene svim pogođenim pojedincima. Ovisno o okolnostima, to može značiti da voditelj obrade koristi nekoliko metoda obavješćivanja, umjesto da se oslanja na samo jedan kanal za kontakt.

Voditelji obrade možda će morati osigurati i da je obavijest dostupna u odgovarajućim alternativnim formatima i na odgovarajućim jezicima kako bi se osiguralo da pojedinci mogu razumjeti informacije koje im se pružaju. Primjerice, pri obavješćivanju pojedinca o povredi, općenito se smatra primjerenim korištenje jezika koji se inače koristi u uobičajenom poslovanju s primateljem. Međutim, ako povreda utječe na ispitanike s kojima voditelj obrade nije imao prethodnih interakcija, ili osobito na one koji žive u državi članici ili trećoj zemlji koja je različita od one u kojoj voditelj obrade ima poslovni nastan, obavješćivanje na lokalnom nacionalnom jeziku moglo bi biti prihvatljivo, uzimajući u obzir potrebna sredstva. Najvažnije je pomoći ispitanicima da shvate prirodu povrede i mjere koje mogu poduzeti kako bi se zaštitili.

Voditelji obrade nalaze se u najboljem položaju da utvrde koji je kanal za kontakt najprimjereniji za obavješćivanje pojedinaca o povredi, osobito ako redovito komuniciraju sa svojim klijentima. Međutim, jasno je da bi voditelj obrade trebao biti oprezan oko upotrebe kanala za kontakt koji je ugrožen povredom jer bi se i napadači mogli koristiti tim kanalom lažno se predstavljajući kao voditelj obrade.

Istodobno, u uvodnoj izjavi 86. objašnjava se sljedeće:

„Takva bi se obavijest ispitanicima trebala pružiti što je prije, u razumnim granicama, izvedivo i u bliskoj suradnji s nadzornim tijelom, poštujući njegove upute ili upute drugih relevantnih tijela vlasti, kao što su tijela za izvršavanje zakonodavstva. Na primjer, o potrebi za umanjivanjem neposrednog rizika od štete bilo bi potrebno odmah obavijestiti ispitanike, dok potreba za provedbom odgovarajućih mjera protiv daljnje ili slične povrede osobnih podataka može opravdati duži rok za obavijest.”

Stoga će voditelji obrade možda htjeti kontaktirati nadzorno tijelo i savjetovati se s njim ne samo kako bi dobili savjet o obavješćivanju ispitanika o povredi u skladu s člankom 34., nego i u pogledu odgovarajućih poruka koje treba poslati pojedincima i najprimjerenijem načinu da se s njima stupi u kontakt.

S time je povezan savjet iz uvodne izjave 88. o tome da bi pri obavješćivanju o povredi trebalo „uzeti u obzir legitime interese tijela za izvršavanje zakonodavstva kada rano otkrivanje može nepotrebno naškoditi istrazi okolnosti povrede osobnih podataka”. To može značiti da u određenim okolnostima, ako je to opravdano, i nakon savjetovanja s tijelima za izvršavanje zakonodavstva, voditelj može odgoditi obavješćivanje pogođenih pojedinaca o povredi do onog trenutka u kojem se time ne bi dovodile u pitanje takve istrage. Međutim, nakon toga bi i dalje trebalo odmah obavijestiti ispitanike.

Ako voditelj obrade nije u mogućnosti obavijestiti pojedinca o povredi zbog toga što nema dovoljno podataka za stupanje u kontakt s njim, u tim posebnim okolnostima voditelj obrade trebao bi tog pojedinca obavijestiti čim je to razumno izvedivo (npr. kada pojedinac ostvaruje svoje pravo iz članka 15. na pristup osobnim podacima i pritom dostavi voditelju obrade dodatne informacije koje su potrebne kako bi se s njime stupilo u kontakt).

#### D. Uvjeti pod kojima se ne zahtijeva obavješćivanje

U članku 34. stavku 3. navedena su tri uvjeta pod kojima se, ako su ispunjeni, ne zahtijeva obavješćivanje pojedinaca u slučaju povrede. Ti su uvjeti sljedeći:

- voditelj obrade prije povrede primijenio je odgovarajuće tehničke i organizacijske mjere kako bi zaštitio osobne podatke, osobito one mjere koje osobne podatke čine nečitljivima bilo kojoj

osobi koja im nije ovlaštena pristupiti. To, primjerice, može uključivati zaštitu osobnih podataka najnaprednijim šifriranjem ili tokenizacijom.

- odmah nakon povrede, voditelj obrade poduzeo je mjere kako bi osigurao da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika. Primjerice, ovisno o okolnostima slučaja, moguće je da je voditelj obrade odmah identificirao i poduzeo mjere protiv pojedinca koji je pristupio osobnim podacima prije nego što je taj pojedinac uspio išta napraviti s tim podacima. I dalje je potrebno uzeti u obzir moguće posljedice svake povrede povjerljivosti, ponovo, ovisno o prirodi predmetnih podataka
- bio bi potreban nerazmjern napor<sup>37</sup> kako bi se stupilo u kontakt s pojedincima, možda zbog toga što su njihovi kontaktni podaci izgubljeni kao posljedica povrede ili nisu uopće bili poznati. Primjerice, skladište statističkog ureda poplavljeno je, a dokumenti s osobnim podacima bili su pohranjeni samo u papirnatom obliku. Umjesto toga, voditelj obrade mora provesti javno obavješćivanje ili poduzeti sličnu mjeru kojom se pojedinci obavješćuju na jednako djelotvoran način. U slučaju nerazmjernog napora mogla bi se predvidjeti i tehnička rješenja kako bi se informacije o povredi učinile dostupnima na zahtjev. To bi se moglo pokazati korisnim za one pojedince na koje je povreda možda utjecala, ali s kojima voditelj obrade ne može na drugi način stupiti u kontakt.

U skladu s načelom odgovornosti, voditelji obrade trebali bi moći dokazati nadzornom tijelu da ispunjavaju jedan od tih uvjeta ili više njih<sup>38</sup>. Treba imati na umu da iako se na početku ne bi zahtijevalo obavješćivanje ako ne postoji rizik za prava i slobode pojedinaca, to se s vremenom može promijeniti te bi rizik trebalo ponovno procijeniti.

Ako voditelj obrade odluči da pojedinca neće obavijestiti o povredi, u članku 34. stavku 4. objašnjava se da nadzorno tijelo može od njega zahtijevati da to učini ako ono smatra da je vjerojatno da će povreda prouzročiti visok rizik za pojedince. Alternativno, nadzorno tijelo može smatrati da su ispunjeni uvjeti iz članka 34. stavka 3. pa se u tom slučaju ne zahtijeva obavješćivanje pojedinaca. Ako nadzorno tijelo utvrdi da odluka o tome da se ispitanike ne obavijesti o povredi nije utemeljena, ono može razmotriti primjenu svojih ovlasti i sankcija kojima raspolaže.

#### IV. Procjena rizika i visokog rizika

##### A. Rizik kao pokretač obavješćivanja

Iako se Općom uredbom o zaštiti podataka uvodi obveza obavješćivanja o povredi, to se ne zahtijeva u svim okolnostima:

- zahtijeva se obavješćivanje nadležnog nadzornog tijela, osim ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca
- obveza obavješćivanja pojedinaca o povredi nastaje samo ako je vjerojatno da će povreda prouzročiti visok rizik za njihova prava i slobode.

To znači da je od presudne važnosti da voditelj obrade neposredno nakon što sazna za povredu ne bi trebao samo nastojati obuzdati incident, nego bi trebao procijeniti i rizik koji bi taj incident mogao prouzročiti. Dva su važna razloga za to. Kao prvo, poznavanje vjerojatnosti i potencijalne ozbiljnosti učinka na pojedinca pomoći će voditelju obrade u poduzimanju djelotvornih mjera za obuzdavanje i

---

<sup>37</sup> Vidjeti Smjernice Radne skupine iz članka 29. o transparentnosti u kojima se razmatraju pitanja nerazmjernog napora, dostupne na adresi: [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48850](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850).

<sup>38</sup> Vidjeti članak 5. stavak 2.

rješavanje problema povrede. Kao drugo, ono će mu pomoći da utvrdi je li nužno obavijestiti nadzorno tijelo i, prema potrebi, predmetnih pojedinaca.

Kako je prethodno objašnjeno, zahtijeva se da se nadzorno tijelo obavijesti o povredi, osim ako nije vjerojatno da će ona prouzročiti rizik za prava i slobode pojedinaca, a ključni pokretač na temelju kojeg se zahtijeva obavješćivanje ispitanika o povredi slučaj je u kojem je vjerojatno da će povreda prouzročiti *visok* rizik za prava i slobode pojedinaca. Taj rizik postoji kad povreda može dovesti do fizičke, materijalne ili nematerijalne štete za pojedince čiji su podaci povrijeđeni. Primjeri su takve štete diskriminacija, krađa identiteta ili prijevarena, financijski gubitak i šteta za ugled. Ako povreda uključuje osobne podatke o rasnom ili etničkom podrijetlu, političkim mišljenjima, religijskim ili filozofskim uvjerenjima ili članstvu u sindikatima ili ako uključuje genetske podatke, podatke koji se odnose na zdravlje ili spolni život ili kaznene osude i kažnjiva djela ili povezane sigurnosne mjere, trebalo bi se smatrati da će vjerojatno doći do takve štete<sup>39</sup>.

#### B. Čimbenici koje treba uzeti u obzir pri procjeni rizika

U uvodnim izjavama 75. i 76. Opće uredbe o zaštiti podataka navodi se da bi se općenito pri procjeni rizika u obzir trebala uzeti i vjerojatnost i ozbiljnost rizika za prava i slobode ispitanika. U njima se nadalje navodi da bi rizik trebalo procjenjivati na temelju objektivne procjene.

Treba napomenuti da je procjena rizika za prava i slobode pojedinaca drugačije usmjerena od procjene rizika koji se razmatra u okviru procjene učinka na zaštitu podataka<sup>40</sup>. U procjeni učinka na zaštitu podataka razmatraju se i rizici obrade podataka koja se provodi kako je planirano i rizici u slučaju povrede. Kod razmatranja potencijalne povrede općenito se razmatra vjerojatnost da se ona dogodi i šteta za ispitanika koja bi mogla nastati. Drugim riječima, radi se o procjeni hipotetskog događaja. Kod stvarne povrede događaj se već dogodio pa je naglasak u potpunosti na riziku koji je proizašao iz učinka povrede na pojedince.

#### **Primjer**

Procjena učinka na zaštitu podataka pokazuje da je predložena upotreba konkretnog sigurnosnog softvera za zaštitu osobnih podataka prikladna mjera kojom se može zajamčiti odgovarajuća razina sigurnosti s obzirom na rizik za pojedince koji bi inače proizlazio iz predmetne obrade. Međutim, ako bi se naknadno saznalo za slabu točku u softveru, to bi promijenilo prikladnost računalnog programa za ograničavanje rizika za osobne podatke koji se štite pa bi ga trebalo ponovno procijeniti u okviru kontinuirane procjene učinka na zaštitu podataka.

Slaba točka u tom sigurnosnom proizvodu kasnije se iskorištava i dolazi do povrede. Voditelj obrade trebao bi procijeniti konkretne okolnosti povrede, podatke na koje je ona utjecala i potencijalnu razinu učinka na pojedince te stupanj vjerojatnosti da će do rizika doći.

Prema tome, kada procjenjuje rizik za pojedince koji je prouzročen povredom, voditelj obrade trebao bi uzeti u obzir konkretne okolnosti povrede, uključujući ozbiljnost potencijalnog učinka i vjerojatnost

<sup>39</sup> Vidjeti uvodne izjave 75. i 85.

<sup>40</sup> Vidjeti Smjernice Radne skupine o procjeni učinka na zaštitu podataka koje su dostupne na adresi: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137).



da do njega dođe. Radna skupina iz članka 29. stoga preporučuje da bi se pri procjeni u obzir trebali uzeti sljedeći kriteriji<sup>41</sup>:

- Vrsta povrede

Vrsta povrede koja se dogodila može utjecati na razinu rizika koji postoji za pojedince. Primjerice, povreda povjerljivosti kojom su medicinski podaci otkriveni neovlaštenim stranama može imati različite posljedice za pojedinca od povrede u kojoj su medicinski podaci pojedinca izgubljeni ili više nisu dostupni.

- Priroda, osjetljivost i količina osobnih podataka

Naravno, pri procjeni rizika ključan je čimbenik vrsta i osjetljivost osobnih podataka koji su ugroženi povredom. Obično, što su podaci osjetljiviji to će biti veći rizik od štete za pogođene pojedince, ali trebalo bi uzeti u obzir i ostale osobne podatke o ispitaniku koji su možda već dostupni. Primjerice, nije vjerojatno da bi se otkrivanjem imena i adrese pojedinca u normalnim okolnostima prouzročila znatna šteta. Međutim, ako se ime i adresa posvojitelja otkrije biološkom roditelju, posljedice bi mogle biti vrlo ozbiljne i za posvojitelja i za dijete.

Povrede koje uključuju podatke o zdravlju, osobne identifikacijske dokumente ili financijske podatke, kao što su pojedinci o kreditnim karticama, mogu prouzročiti štetu same po sebi, no ako se ti podaci koriste zajedno mogu se iskoristiti za krađu identiteta. Kombinacija osobnih podataka obično je osjetljivija nego samo jedan osobni podatak.

Neke vrste osobnih podataka mogu se na prvi pogled činiti bezopasnima, međutim, trebalo bi pažljivo razmotriti ono što ti podaci mogu otkriti o pogođenom pojedincu. Popis klijenata koji primaju redovite dostave ne mora biti naročito osjetljiv, no popis klijenata koji su zatražili da im se dostave obustave dok su na godišnjem odmoru korisna je informacija za kriminalce.

Slično tomu, mala količina vrlo osjetljivih osobnih podataka može imati velik učinak na pojedinca, a velik broj pojedinci može otkriti veću količinu informacija o tom pojedincu. Isto tako, povreda koja utječe na velike količine osobnih podataka o brojnim ispitanicima može imati učinak na odgovarajući velik broj pojedinaca.

- Lakoća identificiranja pojedinaca

Važan čimbenik koji treba uzeti u obzir odnosi se na lakoću s kojom će strana koja ima pristup ugroženim osobnim podacima moći identificirati konkretne pojedince ili povezati te podatke s ostalim informacijama kako bi ih identificirala. Ovisno o okolnostima, identifikacija bi se mogla provesti izravno s pomoću osobnih podataka dobivenih povredom bez potrebe za posebnim istraživanjem. Isto tako, može biti izrazito teško povezati osobne podatke s konkretnim pojedincem, no i dalje je to moguće pod određenim uvjetima. Identifikacija može biti izravno ili neizravno moguća na temelju podataka dobivenih povredom, no ona može ovisiti i o konkretnom kontekstu povrede i javnoj dostupnosti povezanih osobnih podataka. To može biti relevantnije u slučaju povreda povjerljivosti i dostupnosti.

Kako je prethodno navedeno, osobni podaci koji su zaštićeni odgovarajućom razinom šifriranja bit će nečitljivi neovlaštenim osobama koje nemaju ključ za dešifriranje. Osim toga, primjereno provedenom pseudonimizacijom (koja je definirana u članku 4. točki 5. kao „obrada osobnih podataka

---

<sup>41</sup> U članku 3. stavku 2. Uredbe 611/2013 daju se smjernice o čimbenicima koji bi se trebali razmotriti s obzirom na obavješćivanje o povredama u sektoru elektroničkih komunikacijskih usluga i te bi smjernice mogle biti korisne u kontekstu obavješćivanja na temelju Opće uredbe o zaštiti podataka. Vidjeti <https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32013R0611&from=HR>

na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi") isto se može smanjiti vjerojatnost identifikacije pojedinaca u slučaju povrede. Međutim, ne može se smatrati da se podaci čine nečitljivima samo s pomoću tehnika pseudonimizacije.

- Ozbiljnost posljedica za pojedince

Ovisno o prirodi osobnih podataka koji su obuhvaćeni povredom, primjerice, posebne kategorije podataka, potencijalna šteta za pojedince koja bi se mogla prouzročiti može biti vrlo ozbiljna, osobito ako bi povreda mogla dovesti do krađe identiteta ili prijave, tjelesnih ozljeda, psihičke uznemirenosti, poniženja ili štete za ugled. Ako se povreda odnosi na osobne podatke o pojedincima iz ugroženih skupina, oni bi mogli biti izloženi većem riziku od štete.

Je li voditelj obrade svjestan ili nije da se osobni podaci nalaze u rukama osoba čije namjere nisu poznate ili potencijalno zlonamjernih osoba, može utjecati na razinu potencijalnog rizika. Može doći do povrede povjerljivosti kojom se osobni podaci greškom otkrivaju trećoj strani, kako je definirana u članku 4. točki 10., ili drugom primatelju. To se može dogoditi, primjerice, ako se osobni podaci slučajno pošalju pogrešnom odjelu organizacije ili uobičajenom dobavljaču. Voditelj obrade može zatražiti da primatelj vrati ili na siguran način uništi podatke koje je primio. Primatelje se u oba slučaja može smatrati „pouzdanima” s obzirom na to da voditelj obrade s njima ima stalni odnos te možda poznaje njihove postupke, povijest i ostale relevantne pojedinosti. Drugim riječima, voditelj može imati razinu povjerenja u primatelja na temelju koje može razumno očekivati da ta strana neće čitati ili pristupiti podacima koji su joj greškom poslani i da će poštovati upute voditelja obrade da te podatke vrati. Čak i ako je primatelj pristupio tim podacima, voditelj obrade mogao bi mu i dalje vjerovati da neće ništa više raditi s njima i da će ih odmah vratiti voditelju obrade i surađivati u postupku vraćanja podataka. U tim se slučajevima to može uzeti u obzir u procjeni rizika koju voditelj obrade provodi nakon povrede – na temelju činjenice da se radi o primatelju od povjerenja može se otkloniti ozbiljnost posljedica povrede, ali to ne znači da nije došlo do povrede. Međutim, time se može otkloniti vjerojatnost rizika za pojedince zbog čega više nije potrebno obavijestiti nadzorno tijelo ili pogođene pojedince. Ponovo, to će ovisiti o okolnostima svakog pojedinog slučaja. Unatoč tomu, voditelj obrade i dalje mora čuvati informacije o povredi u okviru opće dužnosti vođenja evidencije o povredama (vidjeti odjeljak V. u nastavku).

U obzir bi trebalo uzeti i trajnost posljedica za pojedince, pri čemu se učinak može smatrati većim ako su posljedice dugotrajne.

- Posebna obilježja pojedinca

Povreda može utjecati na osobne podatke koji se odnose na djecu ili druge pojedince iz ugroženih skupina, koji bi mogli biti izloženi većem riziku od opasnosti kao posljedice toga. Mogli bi postojati drugi čimbenici povezani s pojedincima koji bi mogli utjecati na razinu učinka koji je povreda imala na njih.

- Posebna obilježja voditelja obrade podataka

Priroda i uloga voditelja obrade i njegovih aktivnosti mogu utjecati na razinu rizika koji postoji za pojedince kao posljedica povrede. Primjerice, zdravstvena organizacija obrađuje posebne kategorije osobnih podataka što znači da postoji veća prijetnja za pojedince ako dođe do povrede njihovih osobnih podataka, u usporedbi s popisom adresa čitatelja novina.

- Broj pogođenih pojedinaca

Povreda može utjecati na samo jednog pojedinca, nekoliko njih ili na tisuće njih, ako ne i mnogo više. Općenito gledano, što je veći broj pogođenih pojedinaca to je i veći učinak koji povreda može imati. Međutim, povreda može imati ozbiljan učinak čak i na samo jednog pojedinca, ovisno o prirodi osobnih podataka i kontekstu u kojemu su oni ugroženi. Ponovo, najvažnije je uzeti u obzir vjerojatnost i ozbiljnost učinka na one koji su pogođeni povredom.

- Opće napomene

Stoga, kada procjenjuje rizik koji će povreda vjerojatno prouzročiti voditelj obrade trebao bi uzeti u obzir kombinaciju ozbiljnosti potencijalnog učinka na prava i slobode pojedinaca i vjerojatnosti da će do njega doći. Jasno, ako su posljedice povrede ozbiljnije, veći je i rizik te, slično tomu, ako je vjerojatnost da se to dogodi veća, veći je i rizik. U slučaju dvojbe, voditelj obrade trebao bi biti oprezan i provesti obavješćivanje. U Prilogu B nalaze se neki korisni primjeri različitih vrsta povreda koje uključuju rizik ili visok rizik za pojedince.

Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) izradila je preporuke za metodologiju procjenjivanja ozbiljnosti povrede koja bi mogla biti korisna voditeljima obrade i izvršiteljima obrade pri osmišljavanju njihova plana postupanja za upravljanje povredama<sup>42</sup>.

## V. Odgovornost i vođenje evidencije

### A. Dokumentiranje povreda

Neovisno o tome treba li o povredi obavijestiti nadzorno tijelo, voditelj obrade mora čuvati dokumentaciju o svim povredama, kako je objašnjeno u članku 33. stavku 5.:

„Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljavanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštovanja ovog članka.”

To je povezano s načelom odgovornosti iz Opće uredbe o zaštiti podataka, koje se nalazi u članku 5. stavku 2. Svrha evidentiranja povreda za koje se ne zahtijeva obavješćivanje, kao i povreda za koje se ono zahtijeva, povezana je i s obvezama voditelja obrade na temelju članka 24. te nadzorno tijelo može zatražiti uvid u tu evidenciju. Voditelje obrade stoga se potiče da uspostave interni registar povreda, neovisno o tome zahtijeva li se u pogledu njih obavješćivanje ili ne<sup>43</sup>.

Iako je na voditelju obrade da odredi kojom će se metodom i strukturom koristiti za dokumentiranje povrede, s obzirom na informacije o kojima se mora voditi evidencija postoje određeni ključni elementi koje bi trebalo uključiti u svim slučajevima. Kako se zahtijeva u članku 33. stavku 5., voditelj obrade mora evidentirati pojedinosti koje se odnose na povredu, a to bi trebalo obuhvaćati uzroke povrede, pojedinosti o tome što se dogodilo i osobne podatke na koje je povreda utjecala. Trebalo bi navesti i učinke i posljedice povrede, zajedno s mjerama koje je voditelj obrade poduzeo radi popravljavanja štete.

---

<sup>42</sup> ENISA, Preporuke za metodologiju procjene ozbiljnosti povreda osobnih podataka, <https://www.enisa.europa.eu/publications/dbn-severity>.

<sup>43</sup> Voditelj obrade može odlučiti dokumentirati povrede u okviru svoje evidencije aktivnosti obrade koju vodi u skladu s člankom 30. Ne zahtijeva se zasebni registar, pod uvjetom da se informacije koje su relevantne za povredu mogu jasno utvrditi kao takve i da se na zahtjev mogu izdvojiti.

U Općoj uredbi o zaštiti podataka nije utvrđeno razdoblje tijekom kojeg se ta dokumentacija mora čuvati. Ako te evidencije sadržavaju osobne podatke, voditelj obrade bit će obvezan odrediti odgovarajuće razdoblje čuvanja u skladu s načelima povezanim s obradom osobnih podataka<sup>44</sup> i bit će obvezan ispunjavati kriterije o zakonitoj osnovi za obradu<sup>45</sup>. Morat će čuvati dokumentaciju u skladu s člankom 33. stavkom 5. u onoj mjeri u kojoj bi se od njega moglo tražiti da nadzornom tijelu dostavi dokaze o usklađenosti s tim člankom, ili, općenitije, s načelom odgovornosti. Jasno, ako se u samoj evidenciji ne nalaze osobni podaci tada se ne primjenjuje načelo ograničenja pohrane<sup>46</sup> iz Opće uredbe o zaštiti podataka.

Osim tih pojedinosti, Radna skupina iz članka 29. preporučuje da voditelj obrade dokumentira i svoja obrazloženja odluka koje su donesene kao odgovor na povredu. Posebno, ako o povredi nije provedeno obavješćivanje, obrazloženje te odluke trebalo bi dokumentirati. To bi trebalo uključivati razloge zbog kojih voditelj obrade smatra da nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca<sup>47</sup>. Alternativno, ako voditelj obrade smatra da je ispunjen bilo koji uvjet iz članka 34. stavka 3., tada bi to trebao moći na odgovarajući način dokazati.

Ako je voditelj obrade o povredi obavijestio nadzorno tijelo, ali je to obavješćivanje odgođeno, voditelj obrade mora moći obrazložiti tu odgodu. Dokumentacija povezana s time mogla bi pomoći u dokazivanju da je odgoda prijavljivanja opravdana i da nije prekomjerna.

Ako voditelj obrade o povredi obavijesti pogođene pojedince, to obavješćivanje trebalo bi biti transparentno, djelotvorno i pravodobno. Prema tome, čuvanje dokaza o tom obavješćivanju pomoglo bi voditelju obrade pri dokazivanju odgovornosti i usklađenosti.

Kao pomoć u usklađivanju s člancima 33. i 34., za voditelje obrade i izvršitelje obrade bilo bi korisno da uspostave dokumentirani postupak obavješćivanja u kojemu su utvrđeni postupci koje treba slijediti nakon što se otkrije povreda, među ostalim o tome kako ograničiti incident, upravljati njime i ponovno uspostaviti stanje prije incidenta te postupci za procjenu rizika i obavješćivanje o povredi. U tom bi pogledu, kako bi se pokazala usklađenost s Općom uredbom o zaštiti podataka, moglo biti korisno i dokazati da su zaposlenici informirani o postojanju tih postupaka i mehanizama te da znaju kako trebaju reagirati na povrede.

Treba napomenuti da, ako se povreda ne dokumentira ispravno, nadzorno tijelo može izvršiti svoje ovlasti na temelju članka 58. i/ili izreći upravnu novčanu kaznu u skladu s člankom 83.

## B. Uloga službenika za zaštitu podataka

Voditelj obrade ili izvršitelj obrade mogu imati službenika za zaštitu podataka<sup>48</sup>, u skladu sa zahtjevima iz članka 37. ili na dobrovoljnoj osnovi kao pitanje dobre prakse. U članku 39. Opće uredbe o zaštiti podataka utvrđen je niz obveznih zadaća službenika za zaštitu podataka, no time se ne sprječava voditelju obrade da, prema potrebi, službeniku za zaštitu podataka dodijeli dodatne zadaće.

---

<sup>44</sup> Vidjeti članak 5.

<sup>45</sup> Vidjeti članak 6. i članak 9.

<sup>46</sup> Vidjeti članak 5. stavak 1. točku (e).

<sup>47</sup> Vidjeti uvodnu izjavu 85.

<sup>48</sup> Vidjeti Smjernice Radne skupine o službenicima za zaštitu podataka koje su dostupne na adresi: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083).

Za obavješćivanje u slučaju povrede osobito su važne obvezne zadaće službenika za zaštitu podataka koje uključuju, među ostalim dužnostima, savjetovanje i informiranje voditelja obrade ili izvršitelja obrade o zaštiti podataka, praćenje usklađenosti s Općom uredbom o zaštiti podataka i pružanje savjeta u pogledu procjenâ učinka na zaštitu podataka. Osim toga, službenik za zaštitu podataka mora surađivati s nadzornim tijelom i djelovati kao kontaktna točka za nadzorno tijelo i ispitanike. Trebalo bi napomenuti i da se, pri obavješćivanju nadzornog tijela o povredi, u skladu s člankom 33. stavkom 3. točkom (b), od voditelja obrade zahtijeva da navede ime i kontaktne podatke svojeg službenika za zaštitu podataka ili druge kontaktne točke.

S obzirom na dokumentiranje povreda, voditelj obrade ili izvršitelj obrade možda će htjeti dobiti mišljenje svojeg službenika za zaštitu podataka u pogledu strukture i uspostavljanja te dokumentacije te upravljanja njome. Službeniku za zaštitu podataka mogla bi se dodatno dodijeliti i zadaća vođenja te evidencije.

Ti čimbenici znače da bi službenik za zaštitu podataka trebao imati ključnu ulogu u pomaganju u sprečavanju povreda ili pripremanju na njih pružanjem savjeta i praćenjem usklađenosti, a trebao bi imati i ključnu ulogu tijekom povrede (tj. pri obavješćivanju nadzornog tijela) i tijekom svih kasnijih istraga koje provodi nadzorno tijelo. S obzirom na to, Radna skupina iz članka 29. preporučuje da se službenika za zaštitu podataka odmah obavijesti o postojanju povrede i da ga se uključi u cjelokupni postupak upravljanja povredom i obavješćivanja.

## VI. Obveze obavješćivanja na temelju drugih pravnih instrumenata

Osim, i zasebno od, obavješćivanja u slučaju povrede na temelju Opće uredbe o zaštiti podataka, voditelji obrade trebali bi imati na umu sve zahtjeve za obavješćivanje u slučaju sigurnosnih incidenata na temelju ostalog srodnog zakonodavstva koje bi se moglo primjenjivati na njih te imati na umu da bi se time moglo zahtijevati istodobno obavješćivanje nadzornog tijela o povredi osobnih podataka. Ti zahtjevi mogu se razlikovati među državama članicama, no primjeri zahtjeva za obavješćivanje iz drugih pravnih instrumenata, i o tome kako su oni međusobno povezani s Općom uredbom o zaštiti podataka, uključuju sljedeće:

- Uredbu (EU) br. 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (Uredba eIDAS)<sup>49</sup>

U članku 19. stavku 2. Uredbe eIDAS zahtijeva se da pružatelji usluga povjerenja obavješćuju svoje nadzorno tijelo o povredi sigurnosti ili gubitku cjelovitosti koji znatno utječu na pruženu uslugu povjerenja ili u njoj sadržane osobne podatke. Prema potrebi, tj. ako je ta povreda ili gubitak istodobno i povreda na temelju Opće uredbe o zaštiti podataka – pružatelj usluga povjerenja trebao bi obavijestiti i nadzorno tijelo za zaštitu podataka.

- Direktivu (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (Direktiva NIS)<sup>50</sup>

U člancima 14. i 16. Direktive NIS zahtijeva se da operatori ključnih usluga i pružatelji digitalnih usluga obavješćuju svoje nadležno tijelo o sigurnosnim incidentima. Kako se priznaje u uvodnoj

---

<sup>49</sup> Vidjeti [https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv%3AOJ.L\\_.2014.257.01.0073.01.HRV](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.HRV).

<sup>50</sup> Vidjeti [https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.HRV](https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HRV).

izjavi 63. Direktive NIS<sup>51</sup>, sigurnosni incidenti često mogu uključivati ugrožavanje osobnih podataka. Iako se Direktivom NIS zahtijeva da nadležna tijela i nadzorna tijela za zaštitu podataka surađuju i razmjenjuju informacije u tom kontekstu, ako ti incidenti jesu, ili postanu, povrede osobnih podataka na temelju Opće uredbe o zaštiti podataka, od tih operatora i/ili pružatelja i dalje bi se zahtijevalo da obavijeste nadzorno tijelo neovisno o zahtjevu za obavješćivanje iz Direktive NIS.

### **Primjer**

Pružatelj usluga u oblaku koji obavješćuje o povredi na temelju Direktive NIS možda će trebati obavijestiti i voditelja obrade ako ta povreda uključuje i povredu osobnih podataka. Slično tomu, od pružatelja usluga povjerenja na temelju Uredbe eIDAS možda će se zahtijevati i da obavijesti odgovarajuća tijela za zaštitu podataka u slučaju povrede.

- Direktivu 2009/136/EZ (Direktiva o pravima građana) i Uredbu 611/2013 (Uredba o obavješćivanju o povredama)

Pružatelji javno dostupnih elektroničkih komunikacijskih usluga u kontekstu Direktive 2002/58/EZ<sup>52</sup> moraju o povredama obavješćivati nadležna nacionalna tijela.

Voditelji obrade trebali bi imati na umu i sve dodatne pravne, medicinske ili profesionalne dužnosti obavješćivanja na temelju drugih primjenjivih režima.

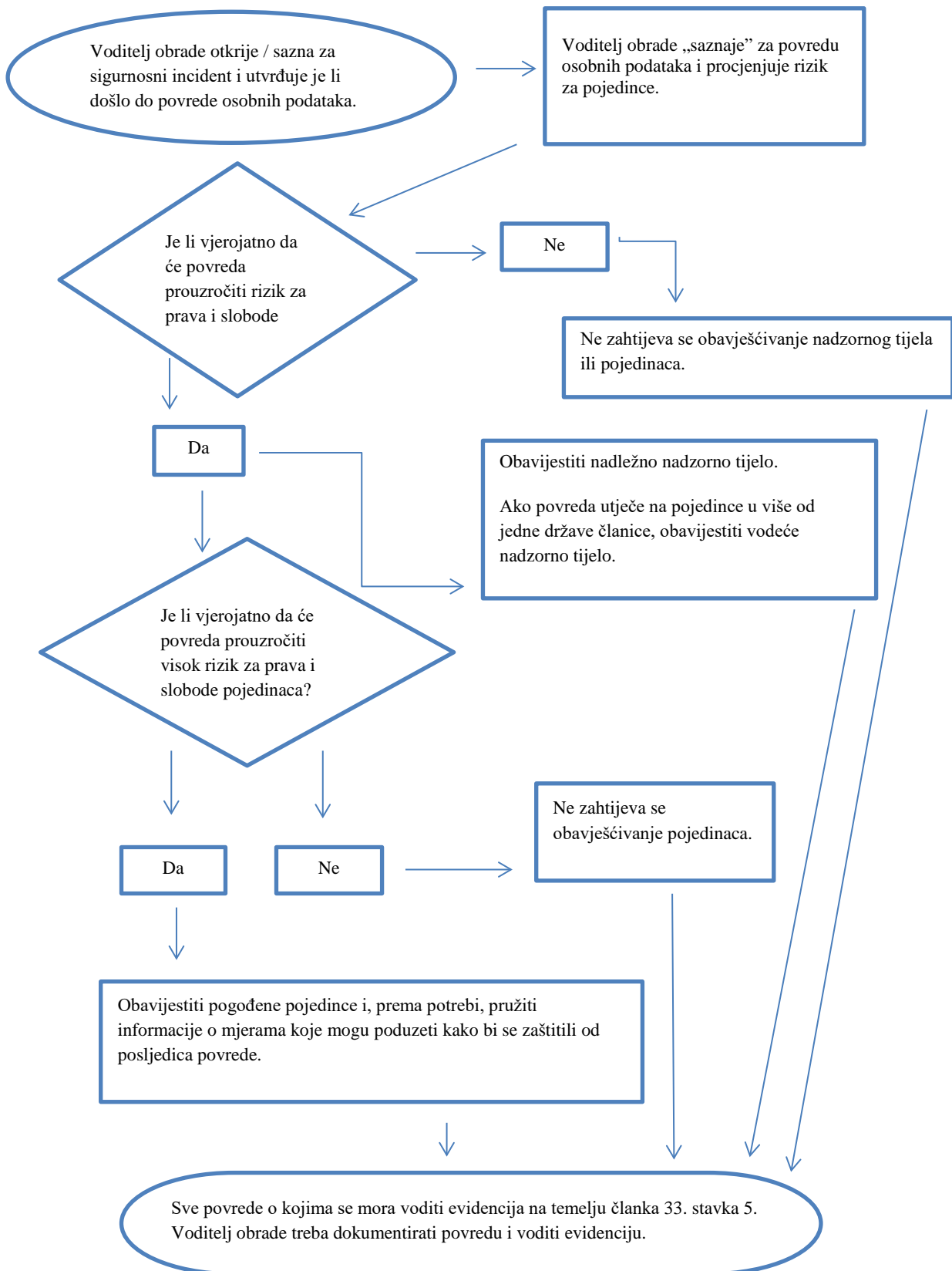
---

51 Uvodna izjava 63.: „U mnogim slučajevima osobni podaci ugroženi su zbog incidenata. U tom kontekstu nadležna tijela i tijela za zaštitu podataka trebala bi surađivati i razmjenjivati informacije o svim relevantnim temama za rješavanje kršenja tajnosti osobnih podataka uzrokovanih incidentima.”

52 Europska komisija predložila je 10. siječnja 2017. Uredbu o privatnosti i elektroničkim komunikacijama koja će zamijeniti Direktivu 2009/136/EZ i ukloniti zahtjeve za obavješćivanje. Međutim, dok Europski parlament ne odobri taj prijedlog i dalje je na snazi postojeći zahtjev za obavješćivanje, vidjeti <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>.

## VII. Prilog

### A. Dijagram toka na kojem su prikazani zahtjevi za obavješćivanje



## B. Primjeri povreda osobnih podataka i koga treba obavijestiti

Sljedeći otvoreni popis primjera pomoći će voditeljima obrade pri utvrđivanju potrebe za obavješćivanjem u različitim scenarijima povreda osobnih podataka. Ti primjeri mogu pomoći i u razlikovanju između rizika i visokog rizika za prava i slobode pojedinaca.

Primjer	Obavijestiti nadzorno tijelo?	Obavijestiti ispitanika?	Napomene/preporuke
i. Voditelj obrade pohranio je sigurnosnu kopiju s arhivom osobnih podataka koji su šifrirani na USB ključu. Ključ je ukraden tijekom provale.	Ne.	Ne.	Sve dok su podaci šifrirani s pomoću najnaprednijeg algoritma, dok postoje sigurnosne kopije podataka i jedinstveni ključ nije ugrožen, a podaci se mogu pravodobno oporaviti, to ne mora biti povreda koju treba prijaviti. Međutim, ako podaci kasnije postanu ugroženi, zahtijeva se obavješćivanje.
ii. Voditelj obrade održava internetsku uslugu. Kao posljedica kibernetičkog napada na tu uslugu, izvučeni su osobni podaci pojedinaca.  Klijenti voditelja obrade nalaze se u jednoj državi članici.	Da, prijaviti nadzornom tijelu ako je vjerojatno da su nastale posljedice za pojedince.	Da, prijaviti pojedincima ovisno o prirodi osobnih podataka na koje je povreda utjecala i ako je ozbiljnost vjerojatnih posljedica za pojedince visoka.	
iii. Kratki nestanak električne energije u pozivnom centru voditelja obrade koji je trajao nekoliko minuta, što znači da klijenti nisu mogli nazvati voditelja obrade i pristupiti svojim podacima.	Ne.	Ne.	Ovo nije povreda za koju se zahtijeva obavješćivanje, ali je i dalje incident o kojemu se mora voditi evidencija na temelju članka 33. stavka 5.  Voditelj obrade trebao bi voditi odgovarajuću evidenciju.
iv. Voditelj obrade pretrpio je napad ucjenjivačkim softverom kojim su svi podaci šifrirani. Nema dostupnih sigurnosnih	Da, prijaviti nadzornom tijelu ako je vjerojatno da su nastale posljedice za pojedince jer se tu radi	Da, prijaviti pojedincima, ovisno o prirodi osobnih podataka na koje je povreda utjecala i mogućem učinku	Ako je sigurnosna kopija bila dostupna i podaci bi se pravodobno mogli ponovno vratiti, to ne bi trebalo prijaviti nadzornom tijelu ili



<p>kopija, a podaci se ne mogu oporaviti. Nakon istrage postalo je jasno da je jedina funkcija ucjenjivačkog softvera bila šifriranje podataka te je utvrđeno da u sustavu nije prisutan nikakav drugi zlonamjerni softver.</p>	<p>o gubitku dostupnosti.</p>	<p>nedostupnosti podataka te o ostalim vjerojatnim posljedicama.</p>	<p>pojedincima jer ne bi postojao trajan gubitak dostupnosti ili povjerljivosti. Međutim, ako nadzorno tijelo sazna za incident na drugi način, ono može razmotriti pokretanje istrage kako bi procijenilo usklađenost sa širim sigurnosnim zahtjevima iz članka 32.</p>
<p>v. Pojedinac nazove pozivni centar banke kako bi prijavio povredu podataka. Taj pojedinac primio je mjesečni izvadak neke druge osobe.</p> <p>Voditelj obrade provodi kratku istragu (koja završava u roku od 24 sata) i utvrđuje, s razumnim stupnjem pouzdanosti, da se dogodila povreda osobnih podataka i postoji li pogreška u sustavu koja može značiti da je povreda utjecala ili može utjecati na druge pojedince.</p>	<p>Da.</p>	<p>Obavješćuju se samo pojedinci na koje je povreda utjecala ako postoji visok rizik, a jasno je da povreda nije utjecala na druge.</p>	<p>Ako se nakon daljnje istrage utvrdi da je povreda utjecala na više pojedinaca, izrađuje se ažurirana obavijest za nadzorno tijelo, a voditelj obrade poduzima dodatnu mjeru obavješćivanja drugih pojedinaca ako za njih postoji visok rizik.</p>
<p>vi. Voditelj obrade vodi internetsko tržište i ima klijente u više država članica. Tržište pretrpi kibernetički napad nakon kojeg napadač na internetu objavi korisnička imena, lozinke i povijest kupnje.</p>	<p>Da, prijaviti vodećem nadzornom tijelu ako je uključena prekogranična obrada.</p>	<p>Da, jer bi moglo dovesti do visokog rizika.</p>	<p>Voditelj obrade trebao bi poduzeti mjere, npr. prisiliti korisnike računa na koje je povreda utjecala da promijene lozinke, te druge mjere za smanjenje rizika.</p> <p>Voditelj obrade trebao bi uzeti u obzir i sve ostale obveze obavješćivanja, npr. na temelju Direktive NIS kao pružatelj digitalnih usluga.</p>
<p>vii. Poduzeće koje pruža usluge smještaja</p>	<p>Kao izvršitelj obrade, poduzeće za smještaj i</p>	<p>Ako je vjerojatno da ne postoji visok rizik</p>	<p>Poduzeće za smještaj i održavanje internetskih</p>

<p>i održavanja internetskih stranica utvrđuje, kao izvršitelj obrade, grešku u kodu koji kontrolira ovlaštenja korisnika. Ta greška znači da svaki korisnik može pristupiti pojedinostima o računu svakog drugog korisnika.</p>	<p>održavanje internetskih stranica mora bez nepotrebne odgode obavijestiti svoje klijente (voditelje obrade) na koje povreda utječe.</p> <p>Pod pretpostavkom da je poduzeće za smještaj i održavanje internetskih stranica provelo vlastitu istragu, pogođeni voditelji obrade trebali bi s razumnom pouzdanošću znati jesu li pretrpjeli povredu pa je stoga vjerojatno da se može smatrati da su „saznali” za povredu nakon što ih je o njoj obavijestilo poduzeće za smještaj i održavanje internetskih stranica (izvršitelj obrade). Nakon toga voditelj obrade mora obavijestiti nadzorno tijelo.</p>	<p>za pojedince, nije ih potrebno obavijestiti.</p>	<p>stranica (izvršitelj obrade) mora uzeti u obzir sve ostale obveze obavješćivanja (npr. na temelju Direktive NIS kao pružatelj digitalnih usluga).</p> <p>Ako ne postoje dokazi o tome da je ta slaba točka iskorištavana s obzirom na bilo kojeg od njegovih voditelja obrade, moguće je da nije došlo do povrede za koju bi se zahtijevalo obavješćivanje, ali je vjerojatno da se radi o povredi koju treba evidentirati ili o pitanju neusklađenosti na temelju članka 32.</p>
<p>viii. Medicinska dokumentacija u bolnici nedostupna je tijekom razdoblja od 30 sati zbog kibernetičkog napada.</p>	<p>Da, bolnica je obvezna obavijestiti nadzorno tijelo jer bi moglo doći do visokog rizika za dobrobit i privatnost pacijenata.</p>	<p>Da, prijaviti pojedincima na koje povreda utječe.</p>	
<p>ix. Osobni podaci velikog broja studenata greškom su poslani na krivi popis adresa s više od 1000 primatelja.</p>	<p>Da, prijaviti nadzornom tijelu.</p>	<p>Da, prijaviti pojedincima ovisno o opsegu i vrsti osobnih podataka uključenih u povredu i ozbiljnosti mogućih posljedica.</p>	
<p>x. Poruka e-pošte (izravni marketing) poslana je primateljima u poljima „prima:” ili „kopija:” čime je svakom</p>	<p>Da, obavješćivanje nadzornog tijela može biti obvezno ako povreda utječe na velik broj pojedinaca, ako su otkriveni osjetljivi</p>	<p>Da, prijaviti pojedincima ovisno o opsegu i vrsti osobnih podataka uključenih u povredu i ozbiljnosti mogućih posljedica.</p>	<p>Obavješćivanje možda neće biti potrebno ako nisu otkriveni osjetljivi podaci i ako je otkriven samo manji broj adresa e-pošte.</p>

primatelju omogućeno da vidi adrese e-pošte ostalih primatelja.	podaci (npr. popis adresa koji pripada psihoterapeutu) ili ako su visoki rizici nastali zbog drugih čimbenika (npr. e-pošta sadržava početne lozinke).		
---	--	--	--