UREDBE

UREDBA KOMISIJE (EU) št. 611/2013

z dne 24. junija 2013

o ukrepih, ki veljajo za obveščanje o kršitvi varnosti osebnih podatkov v skladu z Direktivo 2002/58/ES Evropskega parlamenta in Sveta o zasebnosti in elektronskih komunikacijah

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) ([1]) ter zlasti člena 4(5) Direktive,

po posvetovanju z Evropsko agencijo za varnost omrežij in informacij (ENISA),

po posvetovanju z Delovno skupino za varstvo posameznikov pri obdelavi osebnih podatkov iz člena 29 Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([2]) (v nadaljnjem besedilu: delovna skupina iz člena 29),

po posvetovanju z Evropskim nadzornikom za varstvo podatkov (ENVP),

ob upoštevanju naslednjega:

(1) Direktiva 2002/58/ES določa uskladitev nacionalnih določb držav članic, ki je potrebna za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v Uniji.

(2) Ponudniki javno razpoložljivih elektronskih komunikacijskih storitev morajo v skladu s členom 4 Direktive 2002/58/ES obvestiti pristojne nacionalne organe ter v nekaterih primerih tudi zadevne naročnike in posameznike o kršitvah varnosti osebnih podatkov. Kršitve varnosti osebnih podatkov so v členu 2(i) Direktive 2002/58/ES opredeljene kot kršitve varnosti, ki povzročijo nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v Uniji.

(3) Komisija je na podlagi člena 4(5) Direktive 2002/58/ES pooblaščena za sprejetje tehničnih izvedbenih ukrepov v zvezi z okoliščinami, predpisano obliko in postopki, ki se uporabljajo za zahteve glede informacij in obvestil iz navedenega člena, da se zagotovi doslednost pri izvajanju ukrepov iz člena 4(2), (3) in (4) navedene direktive.

(4) Različne zahteve držav članic na tem področju lahko povzročijo pravno negotovost, bolj zapletene in dolgotrajne postopke ter visoke upravne stroške ponudnikov, ki poslujejo v več državah članicah. Zato Komisija meni, da je treba sprejeti take tehnične izvedbene ukrepe.

(5) Področje uporabe te uredbe je omejeno na obveščanje o kršitvi varnosti osebnih podatkov, zato ne določa tehničnih izvedbenih ukrepov glede člena 4(2) Direktive 2002/58/ES v zvezi z obveščanjem naročnikov v primeru posebnega tveganja za kršitev varnosti omrežja.

(6) Iz prvega pododstavka člena 4(3) Direktive 2002/58/ES sledi, da bi ponudniki morali pristojni nacionalni organ obvestiti o vseh kršitvah varnosti osebnih podatkov. Zato ponudnik ne bi smel prosto presojati o tem, ali bo pristojnemu nacionalnemu organu poslal obvestilo ali ne. Vendar pa to zadevnemu pristojnemu nacionalnemu organu ne sme preprečiti prednostne obravnave določenih kršitev tako, kot je po njegovem mnenju skladno z zakonodajo, ki se uporablja, in sprejemanja ukrepov, potrebnih za preprečitev preobsežnega ali nezadostnega poročanja o kršitvah varnosti osebnih podatkov.

(7) Primerno je zagotoviti sistem za obveščanje pristojnega nacionalnega organa o kršitvah varnosti osebnih podatkov, ki bo ob izpolnjevanju določenih pogojev sestavljen iz različnih faz, od katerih bo vsaka imela določene časovne omejitve. Namen tega sistema je zagotoviti karseda hitro in podrobno obveščanje pristojnega nacionalnega organa, pri čemer pa se ne bo oviralo ponudnikovih prizadevanj za preiskavo kršitve in sprejetje ukrepov, potrebnih za omejitev kršitve ter odpravo njenih posledic.

([1]) UL L 201, 31.7.2002, str. 37.
([2]) UL L 281, 23.11.1995, str. 31.

(8) Samo sum kršitve varnosti osebnih podatkov ali samo odkritje incidenta brez zadostnih razpoložljivih informacij, ne glede na to, ali si je ponudnik za to prizadeval po svojih najboljših močeh, ne zadostujeta, da bi se za namene te uredbe štelo, da je bila odkrita kršitev varnosti osebnih podatkov. V zvezi s tem je treba paziti zlasti na razpoložljivost informacij iz Priloge I.

(9) Zadevni pristojni nacionalni organi bi v okviru uporabe te uredbe morali med seboj sodelovati, kadar bi šlo za kršitve varnosti osebnih podatkov, ki imajo čezmejne razsežnosti.

(10) V tej uredbi ni dodatnih specifikacij v zvezi z evidenco kršitev varnosti osebnih podatkov, ki jo morajo voditi ponudniki, saj njeno vsebino že dovolj natančno določa člen 4 Direktive 2002/58/ES. Kljub temu pa se ponudniki za določitev oblike evidence lahko sklicujejo na to uredbo.

(11) Vsi pristojni nacionalni organi bi morali zagotoviti varno elektronsko sredstvo, prek katerega bi lahko ponudniki pošiljali obvestila o kršitvah varnosti osebnih podatkov v skupni obliki zapisa na podlagi standarda, kot je XML, pri čemer bi taka obvestila vključevala informacije iz Priloge I v ustreznih jezikih, da se vsem ponudnikom v Uniji omogoči uporaba podobnega postopka obveščanja, ne glede na njihovo lokacijo ali kraj kršitve varnosti osebnih podatkov. V zvezi s tem bi Komisija morala olajšati izvajanje varnih elektronskih sredstev tako, da bi po potrebi sklicala sestanke s pristojnimi nacionalnimi organi.

(12) Pri oceni verjetnosti, da bo kršitev varnosti osebnih podatkov negativno vplivala na osebne podatke ali zasebnost naročnika ali posameznika, bi bilo treba upoštevati zlasti naravo in vsebino zadevnih osebnih podatkov, zlasti kadar ti podatki zadevajo finančne informacije, kot so podatki o kreditnih karticah in podatki o bančnem računu, posebne vrste podatkov iz člena 8(1) Direktive 95/46/ES, ter nekatere podatke, ki so izrecno povezani z zagotavljanjem storitev na področju telefonije ali interneta, tj. podatke z elektronske pošte, podatke o lokaciji, internetne dnevniške datoteke, zgodovino brskanja po spletu in razčlenjene sezname klicev.

(13) Ponudniku bi bilo treba v posebnih okoliščinah dovoliti, da preloži obvestilo naročniku ali posamezniku, kadar bi lahko obvestilo naročniku ali posamezniku ogrozilo ustrezno preiskavo o kršitvi varnosti osebnih podatkov. Izjemne okoliščine v zvezi s tem so lahko med drugim kriminalne preiskave in druge kršitve varnosti osebnih podatkov, ki ne štejejo za resne zločine, vendar bi bilo primerno preložiti obvestilo o njih. V vsakem primeru bi moral pristojni nacionalni organ za vsak posamezen primer ob upoštevanju okoliščin oceniti, ali se strinja s preložitvijo obvestila ali ga zahteva.

(14) Ponudniki bi zaradi neposrednega pogodbenega razmerja s svojimi naročniki morali imeti njihove kontaktne podatke, vendar ni nujno, da so te informacije na voljo za druge posameznike, na katere je negativno vplivala kršitev varnosti osebnih podatkov. V takem primeru bi bilo treba ponudniku dovoliti, da te posameznike obvesti najprej prek oglasov v pomembnih nacionalnih ali regionalnih sredstvih javnega obveščanja, kot so časopisi, in jim nato čim prej pošlje ločeno obvestilo, kot je določeno v tej uredbi. Ponudnik torej ni zavezan k obveščanju prek medijev, temveč se mu to dovoli, če tako želi, kadar je še v procesu ugotavljanja, na katere posameznike je kršitev vplivala.

(15) Informacije o kršitvi bi se morale nanašati na kršitev in ne bi smele biti povezane z informacijami o drugi temi. Navedba informacij o kršitvi varnosti osebnih podatkov na običajnem računu se na primer ne bi smela obravnavati kot ustrezen način obveščanja o kršitvi varnosti osebnih podatkov.

(16) Ta uredba ne določa posebnih ukrepov za tehnološko zaščito, na podlagi katerih je mogoče odstopanje od obveznega obveščanja naročnikov ali posameznikov o kršitvah varnosti osebnih podatkov, ker se lahko kršitve sčasoma spremenijo zaradi tehnološkega napredka. Vendar bi bilo treba Komisiji v skladu s sedanjo prakso omogočiti objavo okvirnega seznama takih posebnih ukrepov za tehnološko zaščito.

(17) Samo šifriranje ali zgoščevanje ne bi smelo biti zadostna podlaga za utemeljene trditve ponudnikov, da so na splošno izpolnili obveznost na področju splošne varnosti iz člena 17 Direktive 95/46/ES. Ponudniki bi morali v zvezi s tem izvajati tudi ustrezne organizacijske in tehnične ukrepe za preprečevanje, odkrivanje in blokiranje kršitev varnosti osebnih podatkov. Ponudniki bi morali upoštevati vsa ostala tveganja, ki lahko nastanejo po izvedbi varnostnih ukrepov, da se ugotovijo področja, na katerih bi lahko prišlo do kršitve varnosti osebnih podatkov.

(18) Kadar ponudnik za opravljanje dela storitve vključi drugega ponudnika, na primer v zvezi s funkcijami obračunavanja ali upravljanja, se od navedenega drugega

ponudnika, ki ni v neposrednem pogodbenem razmerju s končnim uporabnikom, ne bi smelo zahtevati izdajanje obvestil v primeru kršitve varnosti osebnih podatkov. Namesto tega bi morala opozoriti in obvestiti ponudnika, s katerim je v neposrednem pogodbenem razmerju. To bi moralo veljati tudi v kontekstu zagotavljanja storitev elektronskih komunikacij na veleprodajni ravni, kadar ponudnik na veleprodajni ravni običajno ni v neposrednem pogodbenem razmerju s končnim uporabnikom.

(19) Direktiva 95/46/ES določa splošni okvir za varnost osebnih podatkov v Evropski uniji. Komisija je predstavila predlog za uredbo Evropskega parlamenta in Sveta, ki bi nadomestila Direktivo 95/46/ES (uredba o varstvu podatkov). Predlagana uredba o varstvu podatkov bi za upravljavce podatkov uvedla zahtevo obveščanja o kršitvah varnosti osebnih podatkov, in sicer na podlagi člena 4(3) Direktive 2002/58/ES. Trenutna uredba Komisije je v celoti skladna s tem predlaganim ukrepom.

(20) Predlagana uredba o varstvu podatkov v Direktivo 2002/58/ES vnaša tudi omejeno število tehničnih prilagoditev, ki upoštevajo preoblikovanje Direktive 95/46/ES v uredbo. Komisija bo preučila materialne pravne posledice, ki jih bo nova uredba povzročila v Direktivi 2002/58/ES.

(21) Uporaba te uredbe bi morala biti pregledana tri leta po začetku veljave, njeno vsebino pa bi bilo treba preučiti v luči takrat veljavnega pravnega okvira, vključno s predlagano uredbo o varstvu podatkov. Pregled te uredbe bi moral biti, kjer bo to mogoče, povezan z vsemi prihodnjimi pregledi Direktive 2002/58/ES.

(22) Uporabo te uredbe se lahko med drugim oceni na podlagi katerih koli statističnih podatkov pristojnih nacionalnih organov o kršitvah varnosti osebnih podatkov, o katerih so bili ti organi obveščeni. Ti statistični podatki lahko zajemajo na primer informacije o številu kršitev varnosti osebnih podatkov, o katerih je bil obveščen pristojni nacionalni organ, številu kršitev varnosti osebnih podatkov, o katerih je bil obveščen naročnik ali posameznik, času, potrebnem za odpravo kršitve varnosti osebnih podatkov, ter o tem, ali so bili sprejeti ukrepi za tehnološko zaščito. Ti statistični podatki naj bi Komisiji in državam članicam zagotovili dosledne in primerljive podatke, pri čemer pa se ne sme razkriti niti identitete ponudnika, ki obvešča, niti identitete zadevnih naročnikov ali posameznikov. Komisija lahko v ta namen tudi organizira redna srečanja s pristojnimi nacionalnimi organi in drugimi zainteresiranimi stranmi.

(23) Ukrepi, predvideni s to uredbo, so v skladu z mnenjem Odbora za komunikacije –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Področje uporabe

Ta uredba se uporablja za obveščanje ponudnikov javno razpoložljivih elektronskih komunikacijskih storitev (v nadaljnjem besedilu: ponudnik) o kršitvah varnosti osebnih podatkov.

Člen 2

Obvestilo pristojnemu nacionalnemu organu

1. Ponudnik obvesti pristojni nacionalni organ o vseh kršitvah varnosti osebnih podatkov.

2. Kadar je to mogoče, ponudnik obvesti pristojni nacionalni organ o kršitvi najpozneje 24 ur po odkritju kršitve varnosti osebnih podatkov.

Ponudnik v obvestilo pristojnemu nacionalnemu organu vključi informacije iz Priloge I.

Kršitev varnosti osebnih podatkov bi bilo treba obravnavati kot kršitev, kadar je ponudnik zadostno osveščen o varnostnem incidentu, ki je privedel do ogrožanja osebnih podatkov, da lahko o njem smiselno poroča, kot se zahteva v skladu s to uredbo.

3. Ponudniku se dovoli, da pošlje prvo obvestilo pristojnemu nacionalnemu organu najpozneje 24 ur po odkritju kršitve varnosti osebnih podatkov, kadar niso na voljo vse informacije iz Priloge I in se zahteva nadaljnja preiskava kršitve varnosti osebnih podatkov. Ponudnik v to prvo obvestilo pristojnemu nacionalnemu organu vključi informacije iz oddelka 1 Priloge I. Ponudnik pošlje drugo obvestilo pristojnemu organu v najkrajšem možnem času oziroma najpozneje tri dni po prvem obvestilu. Ponudnik v to drugo obvestilo vključi informacije iz oddelka 2 Priloge I in po potrebi posodobi že navedene informacije.

Kadar ponudnik kljub preiskavam ne more zagotoviti vseh informacij v treh dneh po prvem obvestilu, ta ponudnik pristojni organ obvesti o vseh informacijah, ki jih ima na voljo v tem časovnem okviru, in pristojnemu organu predloži utemeljeno obrazložitev o razlogih za pozno obveščanje o preostalih informacijah. Ponudnik pristojni nacionalni organ čim prej obvesti o preostalih informacijah in po potrebi posodobi že navedene informacije.

4. Pristojni nacionalni organ zagotovi vsem ponudnikom s sedežem v zadevni državi članici varno elektronsko sredstvo za obveščanje o kršitvah varnosti osebnih podatkov ter informacije o postopkih za dostop do tega sredstva za obveščanje in njegovo uporabo. Komisija po potrebi skliče srečanja s pristojnimi nacionalnimi organi, da se olajša uporaba te določbe.

5. Kadar kršitev varnosti osebnih podatkov zadeva naročnike ali posameznike iz držav članic, ki niso država pristojnega organa, ki je bil obveščen o kršitvi varnosti osebnih podatkov, pristojni nacionalni organ obvesti druge zadevne nacionalne organe.

Zaradi lažje uporabe te določbe Komisija pripravi in vzdržuje seznam pristojnih nacionalnih organov in ustreznih kontaktnih točk.

Člen 3

Obvestilo naročniku ali posamezniku

1. Kadar je verjetno, da bo kršitev varnosti osebnih podatkov negativno vplivala na osebne podatke ali zasebnost naročnika ali posameznika, ponudnik ne pošlje le obvestila iz člena 2, ampak o kršitvi obvesti tudi naročnika ali posameznika.

2. Verjetnost, da bo kršitev varnosti osebnih podatkov negativno vplivala na osebne podatke ali zasebnost naročnika ali posameznika, se oceni ob upoštevanju zlasti naslednjih okoliščin:

(a) narava in vsebina zadevnih osebnih podatkov, zlasti kadar podatki zadevajo finančne informacije, posebne vrste podatkov iz člena 8(1) Direktive 95/46/ES in podatke o lokaciji, internetne dnevniške datoteke, zgodovino brskanja po spletu, podatke z elektronske pošte in razčlenjene sezname klicev;

(b) verjetne posledice kršitve osebnih podatkov za zadevnega naročnika ali posameznika, zlasti kadar bi lahko zaradi kršitve prišlo do kraje ali zlorabe identitete, fizičnih poškodb, psihične stiske, poniževanja ali škodovanja ugledu, in

(c) okoliščine kršitve osebnih podatkov, zlasti kadar so podatki ukradeni ali ponudnik ve, da s podatki razpolaga nepooblaščena tretja oseba.

3. Naročnik ali posameznik je o odkritju kršitve varnosti osebnih podatkov obveščen brez nepotrebnega odlašanja, kot je določeno v tretjem pododstavku člena 2(2). To ni odvisno od uradnega obvestila pristojnim nacionalnim organom o kršitvi varnosti osebnih podatkov iz člena 2.

4. Ponudnik v obvestilo naročniku ali posamezniku vključi informacije iz Priloge II. Obvestilo naročniku ali posamezniku je napisano v jasnem in razumljivem jeziku. Ponudnik obvestila ne sme izrabiti kot priložnost za promocijo ali oglaševanje novih ali dodatnih storitev.

5. V izjemnih okoliščinah se ponudniku, če bi lahko obvestilo, poslano naročniku ali posamezniku, ogrozilo ustrezno preiskavo o kršitvi varnosti osebnih podatkov, dovoli, da po pridobitvi soglasja pristojnega nacionalnega organa obvestilo naročniku ali posamezniku preloži za toliko časa, dokler pristojni nacionalni organ ne oceni, da je o kršitvi varnosti osebnih podatkov mogoče obvestiti v skladu s tem členom.

6. Ponudnik naročnika ali posameznika o kršitvi varnosti osebnih podatkov obvesti prek komunikacijskih sredstev, ki zagotavljajo takojšen prejem informacij in ustrezno varnost na podlagi najsodobnejše tehnologije. Informacije o kršitvi se nanašajo na kršitev in niso povezane z informacijami o drugi temi.

7. Če ponudnik, ki je v neposrednem pogodbenem razmerju s končnim uporabnikom, v časovnem okviru iz odstavka 3 kljub ustreznim prizadevanjem ne more identificirati vseh posameznikov, na katere bi lahko kršitev varnosti osebnih podatkov negativno vplivala, lahko ponudnik te posameznike v navedenem časovnem okviru obvesti prek oglasov v pomembnejših nacionalnih ali regionalnih sredstvih javnega obveščanja v zadevnih državah članicah. Ti oglasi vključujejo informacije iz Priloge II, ki so po potrebi v zgoščeni obliki. V takem primeru si ponudnik še naprej ustrezno prizadeva za identifikacijo teh posameznikov in čimprejšnje obveščanje teh posameznikov o informacijah iz Priloge II.

Člen 4

Ukrepi za tehnološko zaščito

1. Z odstopanjem od člena 3(1) zadevnega naročnika ali posameznika ni treba obvestiti o kršitvi varnosti osebnih podatkov, če je ponudnik pristojnemu organu zadovoljivo dokazal, da je izvedel ustrezne ukrepe za tehnološko zaščito in da je te ukrepe izvedel v zvezi s podatki, ki jih zadeva kršitev varnosti. Zaradi takih ukrepov za tehnološko zaščito postanejo podatki nerazumljivi za vse osebe, ki nimajo dovoljenja za dostop do njih.

2. Podatki se obravnavajo kot nerazumljivi, če:

(a) so varno šifrirani s standardiziranim algoritmom, če ključ za dešifriranje podatkov ni bil ogrožen zaradi katere koli kršitve varnosti in če je bil ključ za dešifriranje podatkov ustvarjen tako, da ga s tehnološkimi sredstvi, ki so na voljo, ne more ugotoviti nobena oseba, ki nima dovoljenja za dostop do ključa, ali

(b) so bili nadomeščeni z zgoščeno vrednostjo, izračunano s standardizirano zgoščevalno funkcijo z uporabo šifrirnega ključa, če ključ za zgoščevanje podatkov ni bil ogrožen zaradi katere koli kršitve varnosti in če je bil ključ za zgoščevanje podatkov ustvarjen tako, da ga s tehnološkimi sredstvi, ki so na voljo, ne more ugotoviti nobena oseba, ki nima dovoljenja za dostop do ključa.

3. Komisija lahko po posvetovanju s pristojnim nacionalnim organom prek delovne skupine iz člena 29, Evropsko agencijo za varnost omrežij in informacij ter Evropskim nadzornikom za varstvo podatkov v skladu s sedanjo prakso objavi okvirni seznam ustreznih ukrepov za tehnološko zaščito iz odstavka 1.

Člen 5

Vključitev drugega ponudnika

Kadar se za opravljanje dela elektronskih komunikacijskih storitev najame drugega ponudnika, ki ni v neposrednem pogodbenem razmerju z naročniki, navedeni drugi ponudnik v primeru kršitve varnosti osebnih podatkov o tem nemudoma obvesti ponudnika, ki ga je najel.

Člen 6

Poročanje in pregled

Komisija v roku treh let po začetku veljavnosti te uredbe pripravi poročilo o uporabi te uredbe, njeni učinkovitosti ter njenem vplivu na ponudnike, naročnike in posameznike. Na podlagi ugotovitev iz navedenega poročila Komisija opravi pregled te uredbe.

Člen 7

Začetek veljavnosti

Ta uredba začne veljati 25. avgusta 2013.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 24. junija 2013

Za Komisijo
Predsednik
José Manuel BARROSO

PRILOGA I

Vsebina obvestila pristojnemu nacionalnemu organu

Oddelek 1

Identifikacija ponudnika

1. Naziv ponudnika.

2. Identiteta in kontaktni podatki uradne osebe za varnost podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij.

3. Ali zadeva prvo ali drugo obvestilo.

Osnovne informacije o kršitvi varnosti osebnih podatkov (ki se po potrebi dopolnijo v poznejših obvestilih)

4. Datum in čas incidenta (če sta znana; po potrebi se lahko navedeta približna datum in čas) in odkritja incidenta.

5. Okoliščine kršitve varnosti osebnih podatkov (npr. izguba, kraja, kopiranje).

6. Narava in vsebina zadevnih osebnih podatkov.

7. Tehnični in organizacijski ukrepi, ki jih je ponudnik izvedel (ali jih bo izvedel) v zvezi z zadevnimi osebnimi podatki.

8. Vključitev drugih ponudnikov (če je ustrezno).

Oddelek 2

Dodatne informacije o kršitvi varnosti osebnih podatkov

9. Povzetek incidenta, ki je povzročil kršitev varnosti osebnih podatkov (vključno s fizično lokacijo kršitve in zadevnim pomnilniškim medijem):

10. Število zadevnih naročnikov ali posameznikov.

11. Možne posledice in možni negativni učinki za naročnike ali posameznike.

12. Tehnični in organizacijski ukrepi ponudnika za ublažitev možnih negativnih učinkov.

Morebitna dodatna obvestila naročnikom ali posameznikom

13. Vsebina obvestila.

14. Uporabljena komunikacijska sredstva.

15. Število obveščenih naročnikov ali posameznikov.

Morebitna čezmejna vprašanja

16. Kršitev varnosti osebnih podatkov, ki zadeva naročnike ali posameznike v drugih državah članicah.

17. Obvestilo drugim pristojnim nacionalnim organom.

PRILOGA II

Vsebina obvestila naročniku ali posamezniku

1. Naziv ponudnika.

2. Identiteta in kontaktni podatki uradne osebe za varnost podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij.

3. Povzetek incidenta, ki je povzročil kršitev varnosti osebnih podatkov.

4. Ocenjeni datum incidenta.

5. Narava in vsebina zadevnih osebnih podatkov iz člena 3(2).

6. Verjetne posledice kršitve varnosti osebnih podatkov za zadevnega naročnika ali posameznika iz člena 3(2).

7. Okoliščine kršitve varnosti osebnih podatkov iz člena 3(2).

8. Ukrepi ponudnika za odpravo kršitve varnosti osebnih podatkov.

9. Ukrepi, ki jih priporoča ponudnik za ublažitev možnih negativnih učinkov.