šolski center ptuj

Šolski center Ptuj
Volkmerjeva cesta 19
2250 Ptuj
Slovenija

Biotehniška šola
Ekonomska šola
Elektro in računalniška šola
Strojna šola
Višja strokovna šola
Medpodjetniški izobraževalni center

☎+386 (0)2 7871 700
🖷 +386 (0)2 7871 711
www.scptuj.si
infoscp@scptuj.si

Datum: 13. 7. 2020
Številka: 1152/2020-1

Navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov

V skladu s Pravilnikom o varstvu osebnih podatkov organizacije in v smislu izvajanja 33. in 34. člena Splošne Uredbe (GDPR) pripravljamo navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.[1]

Kot upravljavec ali obdelovalec mora organizacija za dokazovanje skladnosti s Splošno Uredbo (GDPR) imeti vzpostavljen učinkovit sistem za zaznavanje in sporočanje v primeru kršitev. Ta navodila predstavljajo del omenjenega sistema. Najpomembnejša obveza iz Splošne Uredbe (GDPR)nalaga, da je organizacija dolžna obvestiti nadzorni organ (Informacijskega pooblaščenca) o zaznanih kršitvah varstva osebnih podatkov, če je (vsaj) verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. **Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah.**

1. Kaj je kršitev varstva osebnih podatkov?

Kršitev varstva osebnih podatkov pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev **pomeni varnostni incident**, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Primeri, ki se obravnavajo kot varnostni incident, kot jih navaja Informacijski pooblaščenec, so npr.:

- dostop do osebnih podatkov s strani nepooblaščene osebe;
- posredovanje osebnih podatkov napačnemu naslovniku;
- izguba ali kraja računalniške opreme (prenosni računalnik, USB ključek, itd., ...), ki vsebuje osebne podatke;
- nepooblaščeno uničenje baz z osebnimi podatki;
- sprememba osebnih podatkov brez potrebnega dovoljenja;
- izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t.i. »izsiljevalski virus«) idr.

Zaposleni so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente in v skladu z pravilnikom in temi navodili ustrezno ravnati.

[1] Pri pripravi navodil smo upoštevali informacije Informacijskega pooblaščenca RS na spletni strani: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev/

2. Obveščanje vodstva organizacije

Nemudoma, ko zaposleni zasledijo, da se je v organizaciji zgodil varnostni incident, morajo nujno o tem **obvestiti nadrejenega delavca oziroma vodstvo organizacije**.

Priporočamo, da ima organizacija s strani vodstva določeno **kontaktno osebo**, ki bo v primeru varnostnega incidenta najprej dokumentirala kršitev varstva osebnih podatkov, nato skupaj z vodstvom evidentirala nadaljnje nujne ukrepe, obvestila ali se posvetovala s Pooblaščeno osebo za varstvo podatkov če je ta imenovana, ter izvajala nadaljnje korake vključno s prijavo kršitve Informacijskemu pooblaščenca.

Kontaktna oseba za vse primere kršitve varstva osebnih podatkov v organizaciji je: ga. Tamara Inkret, tajništvo zavoda ŠC Ptuj.

3. Obveščanje Pooblaščene osebe za varstvo podatkov

V primeru, da je organizacija imenovala Pooblaščeno osebo za varstvo podatkov (v nadaljevanju: » pooblaščena oseba«), jo mora vodstvo o zaznani kršitvi nemudoma obvestiti na dpo@datainfo.si. Vodstvo v primeru, da mora organizacija imeti imenovano Pooblaščeno osebo za varstvo podatkov, nemudoma **Pooblaščeni osebi pošlje obvestilo o zaznani kršitvi** . V skladu s Splošno Uredbo (GDPR) pooblaščena oseba namreč sodeluje z nadzornim organom (Informacijskim pooblaščencem) ter deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo.

POMEMBNO: Kako pravilno obvestiti pooblaščeno osebo o domnevni kršitvi varstva podatkov?

Informacijski pooblaščenec predlaga dve možnosti:

- prva možnost je, da pooblaščeno osebo obvestite priporočeno po pošti.
- druga možnost pa je obvestitev preko elektronske pošte. V tem primeru je potrebno vsebino/priponko elektronskega sporočila šifrirati in nato posredovati geslo v ločenem elektronskem sporočilu.

Pooblaščena oseba organizaciji pomaga izdelati **oceno verjetnosti in resnosti** posledic za pravice in svoboščine posameznikov. Verjetnost je povezana z možnostjo nastanka posledic, resnost pa s škodo, ki jo kršitev lahko povzroči posameznikom.

V primeru, da organizacija nima imenovane Pooblaščene osebe, vseeno priporočamo, da se vodstvo organizacije obrne po strokovno pomoč, predvsem zaradi ustrezne priprave ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov, npr. tako da na dpo@datainfo.si pošlje sporočilo o zaznani kršitvi.

Od ocene je odvisno, ali bo treba o kršitvi obvestiti Informacijskega pooblaščenca. Če je verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, mora organizacija o tem obvestiti Informacijskega pooblaščenca. Če ni verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, obveščanje ni potrebno.

Za **pripravo ocene mora** upravljavec najprej izvedeti, **kaj se je zgodilo**, oceniti kakšne so **potencialne škodljive posledice** za pravice in svoboščine posameznikov in sprejeti **ustrezne ukrepe** za odpravo posledic ali vsaj zmanjšanje tveganj.

4. Obvestilo Informacijskemu pooblaščencu

Upravljavec mora o kršitvi obvestiti Informacijskega pooblaščenca **brez odlašanja, najkasneje pa v 72 urah** po zaznani kršitvi. V primeru, da ste v organizaciji v vlogi obdelovalca, morate o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

V predvidenem času 72 ur včasih ni mogoče zagotoviti vseh potrebnih informacij o incidentu, kot to zahteva Splošna Uredba (GDPR), zato lahko upravljavec Informacijskemu pooblaščencu obvestilo o kršitvah posreduje po fazah, vendar brez odlašanja. Od upravljavca se pričakuje, da bo svoje obveznosti v zvezi s preiskovanjem varnostnih incidentov izvedel prioritetno in hitro. Ne glede na to, je treba v roku 72 ur podati vsaj informacijo o zaznani kršitvi, izsledki notranje preiskave pa se lahko posredujejo kasneje. Upravljavci naj razlog za zamudo pri podaji popolnega obvestila o kršitvah posebej obrazložijo.

Pri Informacijskem pooblaščencu so pripravili **neobvezen obrazec za podajo obvestila o kršitvi**, ki je dostopen na naslednji povezavi: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev-varnosti/#c1955 Omenjen obrazec pa je priložen tudi kot priloga temu navodilu.

Obrazec izpolnite v največji možni meri, pomembno je, da ob prijavi Informacijski pooblaščenec pridobi vsaj naslednje informacije, kot to zahteva Splošna Uredba (GDPR):

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov.
- kontaktne podatke pooblaščene osebe za varstvo podatkov.
- opis verjetnih posledic kršitve varstva osebnih podatkov.
- opis ukrepov, ki jih je upravljavec sprejel ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

5. Obvestilo posameznikom

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

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

Informacijski pooblaščenec navaja kot primer, nepooblaščen dostop do zdravstvenih podatkov pacientov določene **bolnišnice,** kjer je že zaradi **narave podatkov** tveganje za pravice in svoboščine pacientov visoko in bo verjetno treba posameznike o kršitvi obvestiti.

V vsakem primeru je smiselno, da se o ukrepu obveščanja posameznikov posvetujete s Pooblaščeno osebo..

Samo **obvestilo posameznikom** mora v jasnem in preprostem jeziku vsebovati vsaj:

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

6. Vpis v seznam obvestil o kršitvah

Priporoča se, da organizacija vodi seznam obvestil o kršitvah. Pri Informacijskem pooblaščencu priporočajo vodenje dokumentacije tudi o tistih zaznanih kršitvah, ki niso bile sporočene nadzornemu organu ali posameznikom.

Seznam obvestil o kršitvah naj vsebuje vsaj naslednje podatke:

- datum kršitve
- datum seznanitve s kršitvijo
- datum obvestila Informacijskemu pooblaščencu (v kolikor je bilo uradno obvestilo potrebno)
- interna številka dokumenta / obvestila
- kratek opis kršitve
- opis ukrepov

7. Neukrepanje ob zaznani kršitvi

Informacijski pooblaščenec navaja, da neukrepanje ob zaznavi kršitev varstva osebnih podatkov in neobveščanje nadzornega organa, ko je to potrebno, predstavlja samostojno kršitev po Splošni Uredbi (GDPR), za katero je predpisana globa do 10 milijonov evrov oz. do 2% letnega prometa. Upravljavca lahko doleti kazen za kršitev in kazen, če ni izpolnil zahteve po obveščanju. Temu se dodajo tudi popravljalni ukrepi, ki jih lahko nadzorni organ naloži upravljavcu skladno s členom 58 Splošne Uredbe (GDPR). Zato morate zagotoviti učinkovit interni postopek javljanja kršitev, ki bo omogočil pravočasno zaznavo in sporočanje kršitev z vsemi potrebnimi informacijami o varnostnem incidentu.

V Ptuju, dne 13. 7. 2020

Odgovorna oseba organizacije

direktor
mag. Oton Mlakar, univ. dipl. inž. el.