OSNOVNA ŠOLA JOŽETA GORJUPA KOSTANJEVICA NA KRKI
Gorjanska cesta 2
8311 Kostanjevica na Krki

Navodila zaposlenim za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov

Uvod

V skladu s Pravilnikom o varstvu osebnih podatkov organizacije in v smislu izvajanja členov 33 in 34 Splošne uredbe (GDPR) ter zakonov, ki urejajo varstvo osebnih podatkov, smo pripravili navodila za ravnanje in ukrepanje v primeru kršitve varstva osebnih podatkov.[1]

Za dokazovanje skladnosti s Splošno uredbo (GDPR) moramo imeti vzpostavljen učinkovit sistem za zaznavanje in sporočanje v primeru kršitev varstva osebnih podatkov. Dolžni smo obvestiti Informacijskega pooblaščenca RS o zaznanih kršitvah varstva osebnih podatkov, če je (vsaj) verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. **Obvestilo moramo 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.

[1] Pri pripravi navodil smo upoštevali informacije Informacijskega pooblaščenca RS na spletni strani: https://www.ip-rs.si/

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

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**.

Kontaktna oseba za primere kršitve varstva osebnih podatkov v organizaciji je: MELITA SKUŠEK, ravnateljica.

V primeru varnostnega incidenta bo kontaktna oseba dokumentirala kršitev varstva osebnih podatkov, evidentirala nadaljnje nujne ukrepe ali obvestila ter izvajala nadaljnje korake vključno s prijavo kršitve Informacijskemu pooblaščencu RS. Ob zaznani kršitvi se bo nemudoma posvetovala z osebo, pooblaščeno za varstvo podatkov (v nadaljevanju: »pooblaščena oseba«).

Vsi zaposleni so dolžni kontaktni osebi pomagati pri zbiranju informacij o dogodku in se truditi čim prej omejiti oz. odpraviti škodljive posledice.

3. Obvestilo Informacijskemu pooblaščencu

Kadar smo upravljavec osebnih podatkov, moramo o kršitvi obvestiti Informacijskega pooblaščenca **brez odlašanja, najkasneje pa v 72 urah** po zaznani kršitvi. V primeru, da smo v vlogi pogodbenega obdelovalca in obdelujemo osebne podatke za naročnika, moramo v najkrajšem možnem času po zaznani kršitvi o kršitvi obvestiti upravljavca (naročnika).

Kadar v predvidenem času 72 ur ni mogoče zagotoviti vseh potrebnih informacij o incidentu, kot to zahteva Splošna uredba (GDPR), lahko upravljavec Informacijskemu pooblaščencu obvestilo o kršitvah posreduje po fazah, vendar brez odlašanja. Od nas se pričakuje, da bomo svoje obveznosti v zvezi s preiskovanjem varnostnih incidentov izvedli prioritetno in hitro. V primeru zamude roka 72 ur moramo razlog za zamudo posebej obrazložiti.

Obvestilo za Informacijskega pooblaščenca vsebuje 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 predvidenih ukrepov za ublažitev tveganj za kršitve.

Obvestilo lahko vsebuje tudi druge pomembne informacije.

4. Obvestilo posameznikom

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

Pred odločitvijo o obveščanju posameznikov bomo preučili mnenja in smernice Informacijskega pooblaščenca RS.

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

- kontaktne podatke pooblaščene osebe (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.

5. Evidenca varnostnih incidentov

Vodili bomo posebno evidenco varnostih kršitev in spremljajočo dokumentacijo, tudi takšnih kršitev, 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 (če obstaja),
- kratek opis kršitve,
- opis ukrepov.

6. Neukrepanje ob zaznani kršitvi

Neukrepanje ob zaznani kršitvi varstva osebnih podatkov in neupravičena opustitev obvestila Informacijskemu pooblaščencu RS nadzornega organa, ko je to potrebno, predstavlja samostojno kršitev po Splošni uredbi (GDPR) in Zakonu o varstvu osebnih podatkov ZVOP-2, za katero je predpisana globa.

7. Obveščanje pooblaščene osebe za varstvo podatkov

Vodstvo in/ali kontaktna oseba **nemudoma pošlje obvestilo o zaznani kršitvi pooblaščeni osebi za varstvo podatkov**.

V skladu s Splošno uredbo (GDPR) pooblaščena oseba sodeluje z Informacijskim pooblaščencem RS ter deluje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo.

8. Končna določba

To navodilo je obvezno za vse zaposlene in se uporablja od 1. 4. 2023 dalje.

V Kostanjevici na Krki, 17. 3. 2023

Odgovorna oseba:
Melita Skušek, ravnateljica

Melita Skušek, ravnateljica

Digitalno podpisal Melita Skušek, ravnateljica
Datum: 2023.03.27 13:17:54 +02'00'