PROCEDURA U SLUČAJU POVREDE BEZBEDNOSTI PODATAKA O LIČNOSTI

1. UVOD

Ova procedura u slučaju povrede bezbednosti podataka o ličnosti („**procedura**") opisuje proces eskaliranja, prijavljivanja i evidentiranja pretpostavljenih ili stvarnih povreda bezbednosti podataka koje obuhvataju podatke o ličnosti (definisane ispod), a doneta je u skladu sa Zakonom o zaštiti podataka o ličnosti ("Sl. Glasnik br. 87/2018) koji počinje sa primenom od 21.08.2019. godine, uz osvrt na Opštu uredbu o zaštiti podataka o ličnosti (General Data Protection Regulation) koja može biti primenjena na kompaniju u slučajevima predviđenim pomenutom uredbom.

S tim u vezi, CRH (Srbija) d.o.o. kao članica CRH Grupe, čije je sedište na području Evropske Unije, usvaja ove smernice u celini.

Ova procedura se odnosi na društvo CRH (Srbija) d.o.o. Popovac („**kompanija**").

Svrha ove procedure je da obezbedi da kompanija upravlja povredom bezbednosti podataka o ličnosti (definisanom ispod) i da je brzo lokalizuje da bi se uticaj povrede bezbednosti podataka o ličnosti minimalizovao i da bi se blagovremeno ispunila obaveza o prijavljivanju povrede bezbednosti podataka o ličnosti nadzornom telu i/ili pojedincima koji su pogođeni povredom bezbednosti podataka.

2. ŠTA SU TO PODACI O LIČNOSTI?

Podaci o ličnosti su bilo koji podaci koji se odnose na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podatak o lokaciji, identifikator u elektronskim komunikacionim mrežama ili jedan, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta („**podaci o ličnosti**"). Osobu je moguće identifikovati ako se njen identitet razumno može utvrditi na osnovu podataka bez ulaganja nesrazmerno velikog truda. U primere podataka o ličnosti spadaju: ime, adresa, datum rođenja, broj telefona, broj računa, radno mesto, fotografija, IP adresa itd.

3. ŠTA JE TO POVREDA BEZBEDNOSTI LIČNIH PODATAKA?

ZZPL definiše povredu bezbednosti podataka o ličnosti kao „*povredu koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneseni, čuvani ili na drugi način obrađivani.*" („**povreda bezbednosti podataka o ličnosti**"). Primeri povrede bezbednosti podataka o ličnosti su: gubitak ili krađa laptopa ili mobilnog telefona koji sadrži podatke o ličnosti; slanje (nezaštićene) Excel datoteke sa podacima o ličnosti neovlašćenoj osobi; štampanje informacija o plati i ostavljanje odštampanog dokumenta u štampaču; hakovanje sistema koji sadrži podatke o ličnosti i/ili gubitak ili krađa datoteka itd.

Incident koji uključuje povredu bezbednosti podataka opisuje se kao „**Incident sa podacima**". Ako incident sa podacima ne uključuje podatke o ličnosti, ne radi se o povredi bezbednosti podataka o ličnosti. Pored toga, ne predstavljaju svi incidenti sa podacima koji uključuju podatke o ličnosti povrede bezbednosti podataka o ličnosti. Na primer, gubitak ili ugrožavanje podataka o ličnosti možda ne predstavlja povredu bezbednosti podataka o ličnosti u sledećim slučajevima: (i) podaci o ličnosti su šifrovani ili pretvoreni u anonimne; (ii) postoji kompletna i ažurirana rezervna kopija podataka o ličnosti i (iii) pristup podacima o ličnosti se nadgleda. U skladu sa time, odluka o tome da li neki incident sa podacima predstavlja povredu bezbednosti podataka o ličnosti donosi se za svaki slučaj zasebno.

4. KADA SE OVA PROCEDURA PRIMENJUJE?

Ako u incident sa podacima *nisu* uključeni podaci o ličnosti, ova procedura se ne primenjuje. Ako u incident sa podacima *jesu* uključeni podaci o ličnosti, moguće je da je došlo do povrede bezbednosti podataka o ličnosti i ova procedura se primenjuje. Ako postoji ikakva sumnja u vezi sa time da li je došlo do povrede bezbednosti podataka o ličnosti, kompanija odmah treba da zatraži savet od Pravne službe kako bi se situacija brzo procenila.

5. KAKO DA INTERNO PRIJAVIM POVREDU BEZBEDNOSTI PODATAKA O LIČNOSTI?

Važno je da se sve stvarne ili pretpostavljene povrede bezbednosti podataka o ličnosti odmah prijave interno u okviru kompanije CRH u skladu sa sledećim koracima:

5.1 Prvo prijavljivanje

Kada osoba postane svesna stvarne ili pretpostavljene povrede bezbednosti podataka o ličnosti, to odmah treba prijaviti generalnom direktoru kompanije („**MD kompanije**") ili direktno Pravnoj službi. MD kompanije će odmah prijaviti bilo kakve stvarne ili pretpostavljene povrede bezbednosti podataka o ličnosti Pravnoj službi.

5.2 Planiranje odgovora

Ako je došlo do povrede bezbednosti podataka o ličnosti, MD kompanije ili njegov predstavnik će u saradnji sa Pravnom službom razviti plan odgovora na povredu bezbednosti podataka o ličnosti. U Prilogu A je naveden dijagram upravljanja povredom bezbednosti podataka o ličnosti.

Prilikom razvijanja relevantnog plana odgovora, tim za razmatranje incidenta uzima u obzir:

- informacije primljene u obaveštenju o povredi bezbednosti podataka o ličnosti
- neophodne radnje koje odmah treba preduzeti u cilju lokalizacije povrede bezbednosti podataka o ličnosti

- da li postoji zahtev da se o povredi bezbednosti podataka o ličnosti obavesti nadležani organ za zaštitu podataka o ličnosti – Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti („**Poverenik**") i, ako postoji, šta treba prijaviti
- potencijalne posledice povrede bezbednosti podataka o ličnosti po kompaniju i ugrožene pojedince
- mere koje kompanija u to vreme preduzima i/ili koje može da preduzme kako bi ublažila štetu po ugrožene pojedince
- način na koji će ugroženi pojedinci biti informisani o povredi bezbednosti podataka o ličnosti, ako je to prikladno u datim okolnostima, kao i mere koje pojedinci mogu da preduzmu kako bi ublažili dodatnu štetu
- da li postoji lična odgovornost ili odgovornost trećih lica zbog povrede bezbednosti podataka o ličnosti
- internu (i, po potrebi, spoljnu) komunikaciju i njeno vreme
- da li, osim Poverenika, treba informisati i druge zainteresovane strane i
- koje se pouke mogu izvući iz povrede bezbednosti podataka o ličnosti i koje se mere mogu primeniti kako bi se sprečilo da do nje ponovo dođe.

5.3 Da li je potrebno obavestiti Poverenika?

Ne mora se svaka povreda bezbednosti podataka o ličnosti prijaviti Povereniku. Rukovalac ima obavezu da obavesti Poverenika u slučaju da povreda podataka o ličnosti može da proizvede rizik po prava i slobode fizičkih lica. U svim ostalim slučajevima prijava nije obavezna.

Ako je potrebno prijaviti povredu bezbednosti podataka o ličnosti Povereniku, Pravna služba će prijaviti povredu bezbednosti podataka o ličnosti Povereniku nakon konsultacija sa MD-om kompanije i bez nepotrebnog odlaganja, ili, ako je to moguće, u roku od 72 časa od saznanja za povredu. Ako kompanija ne prijavi povredu u roku od 72 časa od saznanja za povredu dužan je da obrazloži razloge zbog kojih nije postupila u tom roku.

5.4 Rešavanje

Nakon slanja obaveštenja Povereniku i uvažavanja primedbi tog Poverenika, Pravna služba će se konsultovati sa MD-om kompanije kako bi se povredom bezbednosti podataka o ličnosti upravljalo i kako bi se ona rešila u skladu sa relevantnim planom odgovora na povredu bezbednosti podataka o ličnosti.

6. ŠTA TREBA PRIJAVITI POVERENIKU?

Povereniku se u prijavi mora obavestiti o:

- prirodi povrede bezbednosti podataka o ličnosti, uključujući vrste podataka o ličnosti i približan broj lica na koje se podaci odnose, kao i približan broj podataka o ličnosti čija je bezbednost povređena;
- imenu i kontak podacima CRH osobe za kontakt od koje je moguće dobiti dodatne informacije o povredi bezbednosti podataka o ličnosti, ili informacije o drugom načinu na koji se mogu dobiti podaci o povredi;
- mogućim posledicama povrede;
- merama koje je rukovalac preduzeo ili čije je preduzimanje predloženo u vezi sa povredom, uključujući i mere koje su preduzete u cilju umanjenja štetnih posledica;
- merama koje ugroženi pojedinci mogu da preduzmu kako bi ograničili štetne posledice povrede bezbednosti podataka o ličnosti;

7. OBAVEŠTENJE O POVREDI BEZBEDNOSTI PODATAKA O LIČNOSTI ZA UGROŽENE POJEDINCE

Ugroženog pojedinca treba informisati samo ako povreda bezbednosti podataka o ličnosti može da dovede do „visokog stepena rizika" po prava i slobode lica na koje se podaci odnose. Prijavljivanje povrede bezbednosti podataka o ličnosti ugroženim pojedincima odvijaće se u skladu sa relevantnim planom odgovora.

- Obaveštenje koje se šalje ugroženim pojedincima treba da sadrži najmanje: (i) ime i kontakt podatke CRH osobe za kontakt od koje je moguće dobiti dodatne informacije o povredi bezbednosti podataka o ličnosti, ili informacije o drugom načinu na koji se mogu dobiti podaci o povredi (ii) informacije o prirodi i opsegu povrede bezbednosti podataka o ličnosti; (iii) opis utvrđenih i pretpostavljenih posledica koje će povreda bezbednosti podataka o ličnosti imati po te podatke (iv) mere koje je kompanija preduzela ili koje namerava da preduzmeu vezi sa povredom, uključujući i mere koje su preduzete u cilju umanjenja štetnih posledica;

Pojedincima nije potrebno slati obaveštenje u sledećim slučajevima: (a) kompanija je primenila odgovarajuće tehničke, organizacione i kadrovske mere zaštite zahvaljujući kojima su podaci o ličnosti nečitljivi osobama koje im neovlašćeno pristupaju, na primer putem upotrebe šifrovanja, kriptozaštite ili drugih mera; (b) kompanija je naknadno preduzela mere kojima je obezbedila da povreda podataka o ličnosti, sa visokim rizikom za prava i slobode lica na koje se podaci odnose više ne može da proizvede posledice i (c) ako bi obaveštavanje lica na koje se podaci odnose predstavljalo nesrazmeran utrošak vremena i sredstava, tada je obaveza rukovaoca da putem javnog obaveštavanja ili na drugi delotvoran način obezbedi pružanje obaveštenja licu na koje se podaci odnose.

8. REGISTAR POVREDE BEZBEDNOSTI PODATAKA

Kompanija će da kreira i vodi registar u kojem će da evidentira sve povrede bezbednosti podataka o ličnosti. Pravna služba će voditi pomenuti registar povreda bezbednosti podataka o ličnosti o kojima ga obaveštava kompanija (svaki se naziva „**registar**").

Svrha registra povreda bezbednosti podataka o ličnosti jeste: (i) da pruži pouku o povredi bezbednosti podataka o ličnosti i načinu na koji je ona rešena; (ii) da po potrebi pruži precizne odgovore na pitanja dobijena od ugroženih pojedinaca i/ili Poverenika i (iii) da pruži rezime Povereniku ukoliko se to zatraži.

Za svaku povredu bezbednosti podataka o ličnosti u registar se evidentiraju sledeće informacije:

- datum i vreme prijavljivanja povrede bezbednosti podataka o ličnosti
- ime i kontakt informacije lica čija su prava povređena
- činjenice i informacije o prirodi povrede bezbednosti podataka o ličnosti
- osoba kojoj je povreda bezbednosti podataka o ličnosti prijavljena i zašto i
- radnje preduzete nakon otkrivanja povrede bezbednosti podataka o ličnosti (kao što su mere kojima se sprečava da ponovo dođe do povrede bezbednosti podataka o ličnosti itd.).

Kompanija će čuvati registar povreda bezbednosti podataka o ličnosti prijavljenih Povereniku u periodu od najmanje pet godina.

U Popovcu, 15.08.2019.miltom godine

CRH (Srbija) DOO

Milan Ilić
Izvršni direktor

Maja Stojiljković
Izvršni direktor

Prilog I

Dijagram procedure u slučaju povrede bezbednosti podataka o ličnosti

Ako imate pitanja ili su vam potrebna dodatna uputstva, obratite se HR službi ili Licu za zaštitu podataka o ličnosti. Pravna služba može da vas posavetuje u vezi sa tumačenjem ove procedure.