ARBONIA

Uputstvo o kršenju zaštite podataka
(dodatak za uputstvo o zaštiti podataka od 16. juna 2020.)

16. Jun 2020

ARBONIA

ARBONIA

1. Opšte

Ovaj postupak za prijavljivanje kršenja zaštite podataka važi dodatno pored uputstva o zaštiti podataka Arbonia AG i njegovih kompanija koncerna (u daljem tekstu «Arbonia»). Ovo uputstvo je dopunjeno IT strategijom i IT bezbednosnom strategijom koncerna Arbonia, kao i njihovim osnovnim principima poverljivosti, integriteta i dostupnosti.

Brojne zemlje, a posebno Opšta uredba o zaštiti podataka (GDPR) definišu propise o zaštiti fizičkih lica u pogledu obrade podataka o ličnosti i obavezu prijavljivanja prekršaja zaštite podataka nadležnom nadzornom organu.

Sledeća tri događaja ili incidenata u vezi bezbednosti podataka («Incident u vezi bezbednosti podatak») ispunjavaju uslove za prijavu kršenja zaštite podataka:

- neovlašćeno prosleđivanje podataka o ličnosti trećoj strani (bezbednosni incident),
- neovlašćeni pristup treće strane ličnim podacima (kršenje zaštite podataka) ili
- gubitak podataka o ličnosti (curenje podataka)

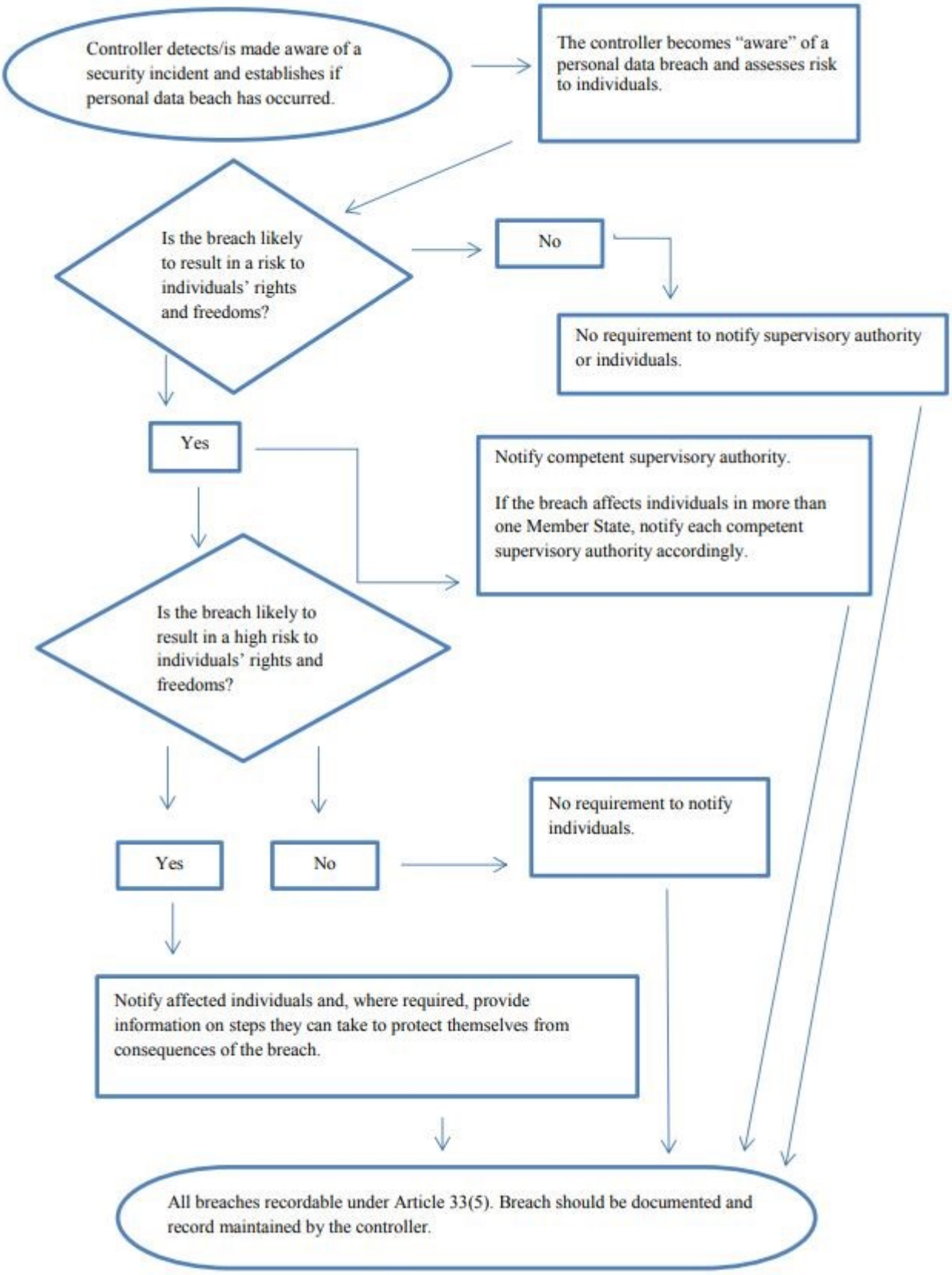
Pri tome kao incidente u vezi bezbednosti podataka treba uzeti u obzir sve događaje za koje postoji opravdana sumnja da se podaci o ličnosti nezakonito evidentiraju, prikupljaju, menjaju, kopiraju, prenose i koriste. Ovo se može odnositi na radnje trećih lica ili zaposlenih.

Odmah, ali najkasnije u roku od 24 sata nakon saznanja o takvom incidentu u vezi bezbednosti podataka unutar koncerna Arbonia mora se izvršiti prijava u skladu sa tačkom 2 o definisanim ulogama i odgovornostima i tačkom 3 matrice dodeljivanja «Uloga i odgovornosti».

Svaka prijava nacionalnom nadzornom organu u vezi sa bezbednosnim incidentom zahteva prethodnu informaciju ili odobrenje od strane Breach Notification Committee. Generalno važi: Incidenti u vezi bezbednosti podataka, koji su relevantni za lokalne aplikacije ili kompanije koncerna se prijavljuju od strane odgovarajućeg lokalnog poverenika za zaštitu podataka ili koordinatora za zaštitu podataka i o prijavi se informiše Breach Notification Committee. Incidenti u vezi bezbednosti podataka, koji su relevantni za zajednički korišćene usluge ili aplikacije se centralno prijavljuju od strane Breach Notification Committee.

ARBONIA

Sledeći dijagram toka prikazuje obaveze prijavljivanja:



ARBONIA

2. Uloge i nadležnosti

U procesu «**Postupak prijavljivanja incidenta u vezi bezbednosti podataka**» su važne sledeće uloge:

- **Inicijator/zaposleni:**
  Svi zaposleni moraju odmah informisati svog pretpostavljenog, lokalnog poverenika za zaštitu podataka ili koordinatora za zaštitu podataka u slučaju sumnje na incident u vezi bezbednosti podataka.

- **Lokalni poverenik za zaštitu podatka ili koordinator za zaštitu podataka („DSK"):**
  Ova uloga preuzima proveru prijavljenog incidenta u vezi bezbednosti podataka, kao i koordinaciju izveštavanja o kršenju zaštite podataka/izveštavanje o incidentima u vezi bezbednosti podataka. Kompanije koncerna takođe mogu da prenesu ovu funkciju posebno obučenom timu (takozvani „tim za zaštitu podataka").

  Ova uloga je odgovorna za popunjavanje internog obrasca o kršenju zaštite podataka koji je sadržan u Dodatak 2.

  Ukoliko su lokalne aplikacije, jedne od kompanija koncerna ili više kompanija koncerna kojima podršku pruža ista IT organizacija pogođeni incidentom u vezi bezbednosti podataka, ova uloga je odgovorna za izveštavanje nadzornog organa, dopis licu čiji se podaci obrađuju i donošenje odluke o korektivnim merama. O prijavi i preduzetim merama se porad toga mora informisati Breach Notification Committee, kao i Corporate IT.

  U slučaju da je nekoliko kompanija koncerna kojima podršku pružaju različite IT organizacije pogođeno incidentom u vezi bezbednosti podataka, ova uloga u roku od 36 sati mora da pruži neophodna objašnjenja i prosledi obrazac iz Dodatka 2 Breach Notification Committee-u. Pored toga, ova uloga mora dodatno da navede da li se preporučuje eksterna prijava nacionalnom ili vodećem centralnom nacionalnom nadzornom organu ili ne.

- **Breach Notification Committee**:
  U slučaju da su lokalne aplikacije ili da je jedna od kompanija koncerna pogođena incidentom u vezi bezbednosti podataka, Breach Notification Committee obaveštava nadzorni organ preko odgovarajućeg lokalnog poverenika za zaštitu podataka ili koordinatora za zaštitu podataka o informacijama o licu čiji se podaci obrađuju i/ili preduzetim korektivnim merama.

  U slučaju da su zajednički korišćene usluge ili aplikacije pogođene incidentom u vezi bezbednosti podataka, Odbor osigurava da se nadzornom organu podnese prijava u zakonskom roku od 72 sata nakon otkrivanja incidenta u vezi bezbednosti podataka koristeći Data Breach Reports koji je sadržan u Dodatak 3. odlučuje o informisanju lica čiji se podaci obrađuju i o svim korektivnim merama.

  Odbor obezbeđuje uključivanje izvršnog direktora koncerna, rukovodioca odeljenja i generalnog direktora.

Breach Notification Committee (za detalje vidi Dodatak 1) čine sledeće osobe:
- Direktor informacionih tehnologija koncerna Arbonia (zamenik je Head of IT Infrastructure)
- Head Legal & Compliance (zamenik je Legal Counsel)
- ICT-Security Officer/Quality Manager (zamenik je Audit Manager)

Ukoliko su incidentom u vezi bezbednosti podataka pogođene zajednički korišćene usluge ili aplikacije pored toga se uključuje i sledeća osoba:
- Direktori informacionih tehnologija relevantnih kompanija koncerna

- **Corporate IT**:
  Corporate IT upravlja internim registrom kršenja bezbednosti podataka koncerna Arbonia, kako bi se u skladu sa nacionalnim zakonom ispunile sve obaveze prijavljivanja i osigurava usvajanje relevantnih pravila zastupanja kako bi obaveza prijavljivanja kršenja zaštite podataka u svakom trenutku bila ispunjena.

- **Nadzorni organ ili organ za zaštitu podataka**: Nadležni službeni organ za zaštitu podataka

3. Matrica dodeljivanja «Uloga i odgovornosti»

Sledeća tabela opisuje odgovornosti pojedinačnih uloga koje su uključene u proces. U okviru dodele uloga unutar kompanije koncerna se mora osigurati da postoji podela uloga i sprečavanje samonadgledanja.

Radove na okončanju nekog koraka pažljivo sprovodi i odobrava *odgovorno lice/nosilac odgovornosti*. Stručnjaci za određeni korak su navedeni u odeljku *Konsultant*. Trenutni napredak i izveštaj se dostavlja *Informisanima*.

	Odgovorno lice/nosilac odgovornosti	Konsultant	Informisani
(1) Utvrđeni incident u vezi bezbednosti podataka ili incident u vezi bezbednosti podataka na koji se sumnja se u roku od 24 sata od saznanja o incidentu u vezi bezbednost podataka prijavljuje DSK-u	Inicijator/zaposleni		DSK
(2) DSK preuzima koordinaciju prijave kršenja zaštite podataka/izveštavanje o incidentu u vezi bezbednosti podataka	DSK		
(3) DSK određuje da li je došlo do kršenja zaštite podataka o ličnosti i procenjuje rizik za lice čiji se podaci obrađuju. DSK popunjava interni obrazac o kršenju zaštite podataka.	DSK		

(4a) *Pogođene su samo lokalne aplikacije kompanije koncerna ili više kompanija koncerna kojima podršku pruža ista IT organizacija:* DSK mora da podnese prijavu nadzornom organu koristeći Data Breach Report koji je sadržan u Dodatak 3 o tome da li će lice čiji se podaci obrađuju biti obavešteno i dali će biti doneta odluka o korektivnim merama. DSK mora informisati Breach Notification Committee, kao i Corporate IT o prijavi i preduzetim merama. (4b) *Incidentom u vezi bezbednosti podataka je pogođeno više kompanija koncerna kojima podršku pružaju različite IT organizacije:* DSK mora u roku od 36 sati da pruži neophodna objašnjenja i prosledi obrazac iz Dodatka 2 Breach Notification Committee-u. Pored toga, Breach Notification Committee u vezi sa tim treba da navede da li se preporučuje eksterna prijava nacionalnom ili vodećem centralnom nacionalnom nadzornom organu ili ne.	DSK	Lokalni IT	Breach Notification Committee, Corporate IT
(5) Breach Notification Committee obezbeđuje uključivanje izvršnog direktora koncerna, rukovodioca odeljenja i generalnog direktora.	Breach Notification Committee	Izvršni direktor grupe, rukovodilac odeljenja, generalni direktor	
(6a) *Pogođene su samo lokalne aplikacije kompanije koncerna ili više kompanija koncerna kojima podršku pruža ista IT organizacija:* Breack Notification Committee uzima informacije u obzir (6b) *Incidentom u vezi bezbednosti podataka je pogođeno više kompanija koncerna kojima podršku pružaju različite IT organizacije:* Breach Notification Committee odobrava izveštavanje o kršenju zaštite podataka i osigurava da se incident u vezi bezbednosti podataka prijavi nadzornim organima u roku od 72 sata nakon koraka 1 i da se donese odluka o informisanju lica čiji se podaci obrađuju i o korektivnim merama.	Breach Notification Committee		DSK

(7) Obaveštavanje nadzornog organa pomoću Data Breach Report sadržanom u Dodatak 3, obaveštavanje lica čiji se podaci obrađuju i odluka o korektivnim merama, u slučaju da je potrebno.	DSK ili Breach Notification Committee		Nadzorni organ, lice čiji se podaci obrađuju
(8) Incident u vezi bezbednosti podataka se prijavljuje Corporate IT-u	DSK ili Breach Notification Committee		Corporate IT
(9) Corporate IT upravlja internim registrom kršenja bezbednosti podataka koncerna Arbonia, kako bi se u skladu sa nacionalnim zakonom ispunile sve obaveze prijavljivanja i osigurava usvajanje relevantnih pravila zastupanja kako bi obaveza prijavljivanja kršenja zaštite podataka u svakom trenutku bila ispunjena	Corporate IT		

Dodaci:

- Dodatak 1: Breach Notification Committee koncerna Arbonia
- Dodatak 2: Obrazac za prijavljivanje incidenta u vezi bezbednosti podataka (Breach Notification obrazac, «BNF»)
- Dodatak 3: Breach Notification Report («BNR») – za podnošenje eksterne prijave

ARBONIA

Dodatak 1: Breach Notification Committee koncerna Arbonia

Pozicija	Direktor informacionih tehnologija	E-pošta	breachnotification@arbonia.com
	Head Legal & Compliance	E-pošta	breachnotification@arbonia.com
	ICT-Security Officer/Quality Manager	E-pošta	breachnotification@arbonia.com

Zastupnik:

Pozicija	Head of IT Infrastructure	E-pošta	breachnotification@arbonia.com
	Legal Counsel	E-pošta	breachnotification@arbonia.com
	Audit Manager	E-pošta	breachnotification@arbonia.com

ARBONIA

Dodatak 2: Obrazac za prijavljivanje incidenta u vezi bezbednosti podataka (Breach Notification obrazac, «BNF»)

Lokalni poverenik za zaštitu podatka ili lokalni IT

Ime/prezime		Privredno pravno lice	
Broj telefona		E-pošta	
Datum prijave			

1) Opis IT bezbednosnog incidenta

- Šta se desilo?
  Kako je došlo do incidenta?
  Čime je izazvan IT bezbednosni incident?
  Koji sistemi/aplikacije su pogođeni?
  Da li treba očekivati negativne efekte na poslovne procese?
  Da li su identifikovane bilo kakve slabosti?

ARBONIA

2) Zemlje koje su pogođene kršenjem bezbednosti podataka:

3) Datum, vreme i mesto pojave IT bezbednosnog incidenta (TTMMJJJJ, HHMM) (procena, ukoliko nije poznato tačno vreme pojave)

4) Količina relevantnih podataka («MB», «GB», «TB»)

5) Datum i vreme utvrđivanja IT bezbednosnog incidenta

6) Mogući uzrok kršenja zaštite podataka?

- ❑ a) Interno
- ❑ b) Eksterno
- ❑ Incident (otkaz sistema)
- ❑ Nemar (ljudska greška)
- ❑ Zlonamerne aktivnosti (npr. krađa, ransomver, trojanac)
- ❑ Drugo (navesti):

7) Ukoliko je kršenje zaštite podataka bio rezultat zlonamerne aktivnosti: Čime je prouzrokovano?

- ❑ Trojanac
- ❑ Ransomver, Distributed Denial of Service
- ❑ Malver
- ❑ CEO-Fraud/krađa
- ❑ Ucena
- ❑ Phishing
- ❑ Drugo (navesti):

8) Koji je verovatni uticaj kršenja zaštite podataka?

- ❑ Obelodanjivanje podataka
- ❑ Krađa podataka
- ❑ Krađa identiteta ili lažni identitet

- ❑ Gubitak podataka
- ❑ Gubitak poverljivosti podataka o ličnosti
- ❑ Materijalna šteta
- ❑ Direktni finansijski gubici
- ❑ Prekid poslovanja
- ❑ Problemi sa odgovornošću
- ❑ Povreda ugleda
- ❑ Drugo (navesti)

9) Vrsta zloupotrebljenih/relevantnih/ukradenih podataka?

- ❑ Podaci koji nisu lični (npr. anonimni podaci)
- ❑ Podaci o ličnosti:
- Osetljivi podaci o ličnosti (npr. podaci o zdravlju, genetski podaci, itd., navesti):
- Podaci koji nisu osetljivi (navesti):

10) Kakvom vrstom IT podrške kompanija raspolaže?

- ❑ Interna
- ❑ Interna na nivou koncerna
- ❑ Eksterna

11) Koje su neposredne mere preduzete radi smanjivanja negativnog uticaja kršenja podataka?

- ❑ Isključivanje i/ili izolacija relevantnih kompjuterskih sistema
- ❑ Brisanje štetnog softvera
- ❑ Zamena uništene imovine ili oporavak izgubljenih podataka
- ❑ Forenzička istraga od strane eksternog veštaka
- ❑ Poboljšanje mera u vezi bezbednosti podataka
- ❑ Sprečavanje daljeg neovlašćenog pristupa sistemu
- ❑ Drugo (navesti):

12) Procena incidenta u vezi bezbednosti podataka

- ❑ Od velikog značaja
- ❑ Od malog značaja

ARBONIA

Kratko obrazloženje ili druga ocena:

13) Planirane mere za savladavanje IT bezbednosnih incidenata

Očekivani početak primene mere	Očekivani završetak mere	Opis planiranih mera

14) Procenjeni troškovi za savladavanje IT bezbednosnih incidenata

ARBONIA

Dodatak 3: Breach Notification Report («BNR») – za podnošenje eksterne prijave

Ove informacije su namenjene isključivo nadležnom organu za zaštitu podataka i ne smeju se prosleđivati trećoj strani.

I. Podaci o odgovornom licu

1) Odgovorno lice

Naziv firme	
Adresa	
Poštanski broj	
Zemlja	
Mesto	

2) Osoba za kontakt (za dobijanje dodatnih informacija)

Ime	
Adresa	
Poštanski broj	
Zemlja	
Mesto	
Funkcija	
Adresa e-pošte	
Br. telefona	

ARBONIA

3) Vrsta prijave

- ❑ kompletna prijava (polja u odeljcima II i III se popunjavaju u roku od 72 sata nakon saznanja o kršenju zaštite podataka)
- ❑ Prijava u dva koraka (polja u odeljku II se popunjavaju unutar roka za prijavljivanje od 72 sata, a polja u odeljku III u roku od četiri nedelje nakon saznanja o kršenju zaštite podataka)

II. Osnovne informacije o kršenju podataka

1) Poslovne aktivnosti pogođenog preduzeća

2) Veličina privrednog pravnog lica – Broj zaposlenih

- ❑ 1–250
- ❑ 250–749
- ❑ 750–1000
- ❑ > 1000

3) Veličina – Promet

4) Zemlja i kojoj je došlo do kršenja zaštite podataka

5) Zemlja u kojoj se nalazi glavno sedište preduzeća

6) Datum/vreme kršenja zaštite podataka

7) Datum/vreme utvrđivanja

8) Mogući uzrok kršenja zaštite podataka?

- ❑ a) Interno
- ❑ b) Eksterno
- ❑ Incident (otkaz sistema)
- ❑ Nemar (ljudska greška)

- ❑ Zlonamerne aktivnosti (npr. krađa, ransomver, trojanac)
- ❑ Drugo (navesti):

❑

9) Ukoliko je kršenje zaštite podataka bio rezultat zlonamerne aktivnosti: Čime je prouzrokovano?

- ❑ Trojanac
- ❑ Ransomver
- ❑ Distributed Denial of Service
- ❑ Malver
- ❑ CEO-Fraud/krađa
- ❑ Ucena
- ❑ Phishing
- ❑ Drugo (navesti):
- ❑

10) Koji je verovatni uticaj kršenja zaštite podataka?

- ❑ Obelodanjivanje podataka
- ❑ Krađa podataka
- ❑ Krađa identiteta ili lažni identitet
- ❑ Gubitak podataka
- ❑ Gubitak poverljivosti podataka o ličnosti
- ❑ Materijalna šteta
- ❑ Direktni finansijski gubici
- ❑ Prekid poslovanja
- ❑ Problemi sa odgovornošću
- ❑ Povreda ugleda
- ❑ Drugo (navesti)

11) Vrsta zloupotrebljenih/relevantnih/ukradenih podataka?

- ❑ Osetljivi podaci o ličnosti (npr. podaci o zdravlju, genetski podaci, itd., navesti):

- ❑ Podaci koji nisu osetljivi (navesti):

12) Kakvom vrstom IT podrške kompanija raspolaže?

- ❑ Interna
- ❑ Interna na nivou koncerna
- ❑ Eksterna

ARBONIA

13) Koje su neposredne mere preduzete radi smanjivanja negativnog uticaja kršenja podataka?

- ❑ Isključivanje i/ili izolacija relevantnih kompjuterskih sistema
- ❑ Brisanje štetnog softvera
- ❑ Zamena uništene imovine ili oporavak izgubljenih podataka
- ❑ Forenzička istraga od strane eksternog veštaka
- ❑ Poboljšanje mera u vezi bezbednosti podataka
- ❑ Sprečavanje daljeg neovlašćenog pristupa sistemu
- ❑ Drugo (navesti):

ARBONIA

III. Dopunske informacije za kompletnu prijavu

Popuniti u roku od maksimalno četiri nedelje nakon saznanja o kršenju zaštite podataka i proslediti organu za zaštitu podataka – Posetite i veb lokaciju odgovornog organa za zaštitu podataka u slučaju da nadležni organ za zaštitu podataka stavlja na raspolaganje specifični obrazac za dostavu prijave

1) **Datum/vreme prestanka efekata napada**

[sat minut dan mesec godina]

2) **Procenjena finansijska šteta**

3) **Koliko zapisa podataka o ličnosti je zloupotrebljeno/pogođeno/ukradeno?**

4) **Dali su informisana lica čiji se podaci obrađuju?**

❑ Da
❑ Ne

5) **Koliko je lica čiji se podaci obrađuju informisano?**

6) **Procenjeni finansijski gubici**

❑ Troškovi za prijavljivanje/obaveštavanje
❑ Finansijska šteta
❑ Poboljšanje mera u vezi bezbednosti podataka, a posebno:

7) **Šta je urađeno ili planirano za sprečavanje ponavljanja incidenta?**

❑ Provera i revizija postupka za prikupljanje podataka
❑ Provera i revizija postupka za obradu podataka
❑ Provera i ponovna procena «obrađivača naloga» (ukoliko je primenljivo)
❑ Šifrovanje sačuvanih podataka
❑ Nisu preduzete nikakve mere u vezi bezbednosti podataka
❑ Druge

ARBONIA

8) Šta je bio uzrok za kršenje zaštite podataka?

- ❑ a) Interno
- ❑ b) Eksterno

- ❑ Incident (otkaz sistema)
- ❑ Nemar (ljudska greška)
- ❑ Zlonamerne aktivnosti (npr. krađa, ransomver, trojanac)
- ❑ Drugo (navesti):

9) U slučaju da je poznato: Ko je bio napadač?

10) U slučaju da je poznato: U slučaju zlonamernog napada, kakva se motivacija krije iza kršenja zaštite podataka?

11) U slučaju da je poznato: Koji softver je korišćen u slučaju zlonamerne aktivnosti?

- ❑ Malver
- ❑ Ransomver
- ❑ Phishing
- ❑ SQL-Injection napad
- ❑ Cross-Site Scripting (XSS)
- ❑ Denial of Service (DoS)
- ❑ Session Hijacking
- ❑ Ponovna upotreba informacija za prijavljivanje
- ❑ Drugo (navesti)

Potpisi:

Mesto	Datum	Potpis

ARBONIA

Dva potpisa
[u slučaju lokalne prijave nadzornom organu dva lokalna potpisa]
[u slučaju centralne prijave nadzornom organu dva lokalna potpisa od strane Corporate-a]