ARBONIA

Uputstvo o rukovanju podacima (Uputstvo o zaštiti podataka)

16. Jun 2020

ARBONIA

SADRŽAJ

ARBONIA

1 SVRHA I CILJ

Radi ispunjavanja zakonskih i ugovornih obaveza neophodno je vršiti prikupljanje i obradu podataka o ličnosti. Pri tome se obavezno moraju poštovati važeći propisi o zaštiti podataka u odgovarajućim zemljama. Ovo uputstvo pokazuje na koji način Arbonia AG i kompanije koncerna (u daljem tekstu: „Arbonia“) ili pojedinačna kompanija koncerna (u daljem tekstu: „kompanija koncerna“) rukuju podacima o ličnosti. Propisane odredbe važe kao minimalni standardi. Ukoliko lokalni Zakon o zaštiti podataka predviđa strože propise, oni se moraju poštovati. Za primenu ovog uputstva se takođe moraju poštovati svi lokalni propisi.

Svrha ovog uputstva o rukovanju podacima („Uputstvo o zaštiti podataka“) je utvrđivanje, primena, održavanje i stalno poboljšanje usaglašenosti zaštite podataka, u skladu sa zahtevima Opšte uredbe o zaštiti podataka o ličnosti Evropske unije 2016/679 (**Opšta uredbu o zaštiti podataka o ličnosti**) i svih drugih važećih lokalnih propisa o zaštiti podataka (pod zajedničkim nazivom **važeći zakoni o zaštiti podataka**) od strane koncerna Arbonia.

Nepoštovanje važećih zakona o zaštiti podataka izlaže koncern Arbonia riziku narušavanja ugleda i visokim novčanim kaznama (npr. do 4 % globalnog prometa prema Opštoj uredbi o zaštiti podataka o ličnosti). Osim toga, naši kupci i zaposleni mogu biti izloženi određenim rizicima u pogledu zaštite podataka, kao što su krađa identiteta i finansijski gubici. Poštovanje važećih zakona o zaštiti podataka nam pomaže da održimo poverenje u organizaciju Arbonia i osiguramo uspešno poslovanje.

Svrha ovog uputstva o zaštiti podataka je da pruži okvir za takvu usklađenost zaštite podataka unutar koncerna Arbonia. To naročito ima za cilj primenu osnovnih principa za obradu podataka o ličnosti (**Osnovni principi zaštite podataka**), koji su navedeni u odeljku 6 i koji su odgovorni za kompanije koncerna Arbonia, ukoliko one prema Opštoj uredbi o zaštiti podataka o ličnosti deluju kao odgovorno lice, reguliše neophodnost primene adekvatnih tehničkih i organizacionih mera i prijavljivanje incidenata u vezi sa zaštitom podataka kao minimalni standard za sve kompanije koncerna Arbonia i važi za sve zaposlene koncerna Arbonia, kao i za članove Upravnog odbora Arbonia AG.

Pored toga, pruža okvir za dodatne zahteve koji se primenjuju na odgovorna lica i obrađivače naloga u skladu sa Opštom uredbom o zaštiti podataka o ličnosti (ili sličnim primenljivim zakonima o zaštiti podataka), kao što je opisano u odeljku 7.

2 ZNAČENJA POJMOVA I DEFINICIJE

Za potrebe ovog uputstva o zaštiti podataka primenjuju se sledeća značenja pojmova i definicije:

Anonimizirani podaci znače da lični identitet niko nikada ne može da prati ili da bi se lični identitet mogao pratiti samo uz neprimereno ulaganje vremena, troškova i rada.

Važeći zakoni o zaštiti podataka predstavljaju Opštu uredbu o zaštiti podataka o ličnosti Evropske unije 2016/679 (**GDPR**) ili sve druge važeće nacionalne zakone o zaštiti podataka koji obuhvataju slične propise.

Vlasnik poslovnog procesa u skladu sa ovim Uputstvom o zaštiti podataka predstavlja nadležno fizičko lice koje je odgovorno za obradu podataka o ličnosti i odgovarajuću IT aplikaciju.

Saglasnost predstavlja saglasnost lica čiji se podaci obrađuju, dakle svako dobrovoljno izražavanje volje za određeni slučaj, koje je kao informacija i nedvosmisleno dato u obliku izjave ili druge nedvosmislene potvrdne radnje kojom se lice čiji se podaci obrađuju izjašnjava da je saglasno sa obradom svojih podataka o ličnosti.

Odgovorno lice predstavlja svako fizičko i pravno lice, državni organ, agenciju ili drugo telo koje samostalno ili u saradnji sa drugima definiše svrhe i sredstva za obradu podataka o ličnosti.

Incident u vezi bezbednosti podataka predstavlja događaj za koji 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.

Lice čiji se podaci obrađuju predstavlja fizičko lice koje je identifikovano ili se može identifikovati. Fizičko lice koje se može identifikovati je osoba koja se može identifikovati direktno ili indirektno, naročito dodeljivanjem identifikacije kao što je ime, identifikacioni broj, podaci o lokaciji, identifikacija mreže ili jedne, odn. nekoliko posebnih karakteristika, koje izražavaju fizički, fiziološki, genetski, psihološki, ekonomski, kulturni ili socijalni identitet ovog fizičkog lica.

Obrađivač naloga je fizičko ili pravno lice, državni organ, ustanova ili drugo telo koje vrši obradu podataka o ličnosti po nalogu odgovornog lica.

Spisak procesa obrade predstavlja evidenciju obrade podataka pod nadležnošću odgovornog lica. Ovaj spisak sadrži sledeće informacije: (i) ime i podatke o kontaktu odgovornog lica i, ako je primenljivo, zajedničkog odgovornog lica, predstavnika odgovornog lica i lokalnog koordinatora za zaštitu podataka; (ii) svrhe obrade; (iii) opis kategorija lica čiji se podaci obrađuju i kategorije ličnih podataka; (iv) kategorije primalaca čiji su podaci o

ličnosti obelodanjeni ili će biti obelodanjeni, uključujući primaoce u trećim zemljama; (v) ako je primenjivo, prenos podataka o ličnosti u treću zemlju, uključujući naziv treće zemlje i dokumentaciju o odgovarajućim garancijama; (vi) predviđeni rokovi za brisanje različitih kategorija podataka o ličnosti; (vii) opšti opis tehničkih i organizacionih mera bezbednosti.

Poverenik za zaštitu podataka ili koordinator za zaštitu podataka ili DSK predstavlja osobu opisanu u odeljku 5.

Podaci o ličnosti predstavljaju sve informacije (uključujući podatke o ličnosti u posebnim kategorijama) koje se odnose na lice čiji se podaci obrađuju, dakle koji se odnose na fizičko lice koje je identifikovano ili se može identifikovati, kao što su ime, datum rođenja, adresa e-pošte, religija, podaci o lokaciji, podaci o mreži (IP adresa, podaci o lokaciji itd.), identifikacioni brojevi (broj socijalnog osiguranja, broj lične karte itd.), fizičke karakteristike (pol, boja kože, kose, očiju itd., podaci o kupcima i još mnogo toga) koji podležu važećoj odredbi o zaštiti podataka.

Proces ili **obrada** predstavlja bilo koji proces ili bilo koji niz takvih procesa koji se izvršava sa ili bez pomoći automatskog postupka u vezi sa podacima o ličnosti, kao što su prikupljanje, evidentiranje, organizacija, arhiviranje, čuvanje, prilagođavanje ili promena, očitavanje, slanje upita, upotreba, obelodanjivanje prenosom, distribucija ili stavljanje na raspolaganje na drugi način, upoređivanje ili povezivanje, ograničavanje, brisanje ili uništavanje.

Pseudonimizacija predstavlja obradu podataka o ličnosti na takav način, da podaci o ličnosti više ne mogu biti dodeljeni određenom licu čiji se podaci obrađuju bez primene dodatnih informacija, pod uslovom da se te dodatne informacije čuvaju odvojeno i podležu tehničkim i organizacionim merama koje garantuju da se podaci o ličnosti ne mogu dodeliti fizičkom licu koje je identifikovano ili se može identifikovati.

Podaci o ličnosti posebnih kategorija predstavljaju podatke o rasnom ili etničkom poreklu, političkom mišljenju, verskim ili filozofskim pogledima, krivičnim presudama, članstvu u sindikatu, zdravlju ili seksualnoj orijentaciji lica čiji se podaci obrađuju ili genetske podatke, biometrijske podatke u svrhu jednoznačne identifikacije fizičkog lica.

Treće zemlje su sve države koje ne spadaju u zemlje Evropske unije ili Evropskog ekonomskog prostora ili zemlja sa odgovarajućim nivoom zaštite podataka koji Komisija EU smatra odgovarajućim (vidi listu zemalja sa odgovarajućim nivoom zaštite podataka: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Treće lice predstavlja svakog drugog osim lica čiji se podaci obrađuju, dakle odgovorno lice ili obrađivača naloga (uključujući poslovne partnere, podugovarače, kreditne agencije i druge), kao i osobe koje su ovlašćene za obradu podataka o ličnosti pod direktnom nadležnošću odgovornog lica ili obrađivača naloga. Prilikom obrade podataka o ličnosti na

osnovu dozvole, prema Zakonu o zaštiti podataka obrađivači naloga pravno ne predstavljaju treća lica, jer su zakonski pridodati odgovornom licu.

3 OBIM

3.1 Organizacioni obim

Ovo uputstvo o zaštiti podataka važi za sve kompanije koncerna Arbonia, za sve zaposlene koncerna Arbonia i za sve članove Upravnog odbora Arbonia AG. Ono se pravno obavezujuće mora primenjivati u svakoj kompaniji koncerna.

3.2 Zakoni, odredbe, standardi i uputstva

Ovo uputstvo o zaštiti podataka obuhvata zahteve Opšte uredbe o zaštiti podataka o ličnosti i međunarodno priznate osnovne principe zaštite podataka, bez zamene postojećeg nacionalnog zakona. Ono dopunjuje nacionalno važeće zakone o zaštiti podataka. U slučaju sukoba sa ovim uputstvom o zaštiti podataka ili u slučaju strožih zahteva od ovog uputstva, relevantni nacionalni zakon ima prioritet. Sadržaj ovog uputstva o zaštiti podataka mora se poštovati takođe i u slučaju da ne postoji odgovarajuće nacionalno zakonodavstvo.

Ukoliko je ovo uputstvo o zaštiti podataka u suprotnosti sa odredbama u određenoj zemlji, onda se specifične odredbe ovog uputstva o zaštiti podataka u dogovoru sa Head Legal & Compliance mogu preuzeti u lokalnom uputstvu. Međutim, osnovni sadržaj i svrha relevantnih odredbi se ne mogu menjati.

4 REGULATORNA OSNOVA

Ovo uputstvo za zaštitu podataka se zasniva na Opštoj uredbi o zaštiti podataka o ličnosti i globalno prihvaćenim osnovnim principima zaštite podataka.

ARBONIA

5 ULOGE I NADLEŽNOSTI

- U nadležnost direktora kompanije koncerna[1] spada:
  1. apsolutna garancija da odgovarajuće pravno lice ispunjava svoje zakonske obaveze u vezi sa obradom podataka o ličnosti.
  2. garancija ispunjavanja zahteva iz ovog uputstva o zaštiti podataka (uključujući i obaveštavanje u slučaju incidenata u oblasti bezbednosti podataka).
  3. garancija da se „Spisak procesa obrade" na nivou kompanije koncerna popunjava i održava od strane vlasnika poslovnog procesa.
  4. Imenovanje lokalnog poverenika za zaštitu podataka (interno ili eksterno) (u nastavku „Poverenik za zaštitu podataka"), ukoliko se to zahteva lokalno važećom odredbom o zaštiti podataka i da o toj imenovanoj osobi sredinom svake godine obavesti Head Legal & Compliance i Internal Audit.
  5. imenovanje lokalnog menadžera za zaštitu podataka (u nastavku „koordinator za zaštitu podataka"), ukoliko važeća lokalna odredba o zaštiti podataka ne zahteva formalnog lokalnog poverenika za zaštitu podataka. O ovoj imenovanoj osobi sredinom svake godine treba obavestiti Head Legal & Compliance i Internal Audit.

- Lokalni koordinator za zaštitu podataka, odn. poverenik za zaštitu podataka koga je odredio direktor kompanije koncerna[2] mora da:
  1. vrši nadzor usklađenosti sa ovim uputstvom o zaštiti podataka i uputstvima odgovornog lica ili obrađivača naloga u vezi sa zaštitom podataka o ličnosti, uključujući prenos nadležnosti i odgovarajuće provere.
  2. informiše, savetuje i nadgleda odgovorno lice ili obrađivača naloga i zaposlene koji izvršavaju obaveze obrade u skladu sa ovim uputstvom o zaštiti podataka.
  3. na zahtev daje savete o proceni uticaja na zaštitu podataka u vezi podataka o ličnosti i nadgleda njihove rezultate, kao i da daje odgovore na druga pitanja u vezi sa podacima o ličnosti koji su mu dodeljeni u skladu sa ovim uputstvom o zaštititi podataka.
  4. vrši nadzor „Spiska procesa obrade", koji vodi odgovarajuća kompanija koncerna i koju popunjava vlasnika poslovnog procesa, da ga održava ažurnim i da sredinom svake godine potvrđuje celovitost i ažurnost spiska direktoru i Head Legal & Compliance.
  5. služi kao kontakt osoba za Head Legal & Compliance i da ih redovno obaveštava o odgovornosti, rizicima i problemima u vezi sa zaštitom podataka o ličnosti.
  6. pruža podršku odgovornom IT licu za IT aplikaciju prilikom provere i odobravanja novih IT aplikacija za obradu podataka o ličnosti na nivou kompanije koncerna i svake IT aplikacije za obradu posebnih kategorija podataka o ličnosti u pogledu zaštite podataka.

[1] Za kompanije koncerna koje nisu operativno aktivne, ova odgovornost se utvrđuje odvojeno u dogovoru sa Head Legal & Compliance.
[2] Za kompanije koncerna koje nisu operativno aktivne, ova odgovornost se utvrđuje odvojeno u dogovoru sa Head Legal & Compliance.

7. u pogledu odobri prenos podataka o ličnosti u treću zemlju sa stanovišta zaštite podataka (vidi u nastavku takođe i tačku 14).
8. služi kao lokalna polazna tačka za nadzorni organ za pitanja u vezi obrade podataka, kao i da sarađuje sa nadzornim telom,
9. obrađuje upite zaposlenih koji su uključeni u obradu podataka o ličnosti.
10. odgovora na upite lica čiji se podaci obrađuju o informacijama u vezi podataka o ličnosti koje Arbonia poseduje o njima ili da u slučaju upita o nekoliko kompanija koncerna Arbonia obradu vrši u koordinaciji sa Corporate IT (vidi u nastavku takođe i tačku 7.4)
11. proverava i odobrava pripremljene, odn. prethodno proverene ugovore ili sporazume vlasnika poslovnog procesa sa obrađivačima naloga koji mogu da obrađuju podatke o ličnosti po nalogu koncerna Arbonia, kao što je opisano u odeljku 7.2.
12. vrši nadzor eksternih lokalnih poverenika za zaštitu podataka, ukoliko je neko takav angažovan.
13. Obaveštava o incidentima u oblasti bezbednosti podataka u skladu sa Data Breach Notification uputstvom (vidi u nastavku tačku 9, kao i „Arbonia Data Breach Policy“).

- IT-Board je zajedno sa Corporate IT nadležan za:
  1. definisanje važećih standarda za celi koncern, kao i opštih IT Controls (GITC), koje se moraju poštovati prilikom čuvanja podataka.

- Odgovarajuće nadležno IT odeljenje koje pruža podršku kompaniji koncerna je odgovorno za to da:
  1. pomoću odgovarajućih standarda, smernica i sprovođenjem opštih IT kontrola (GITC) osigura da sistemi, performanse i oprema koja se koristi za čuvanje podataka zadovoljavaju prihvatljive sigurnosne standarde (kontrola pristupa/brisanje podataka), pri čemu se moraju uzeti u obzir stanje tehnike, troškovi za implementaciju i vrsta, obim, kontekst i svrha obrade, kao i različite verovatnoće i ozbiljnost uticaja na prava i slobode fizičkih lica.
  2. nastoji da odgovorno lice i obrađivač naloga primenjuju adekvatne tehničke i organizacione mere kako bi se osigurao nivo zaštite koji odgovara riziku, kao što je predviđeno u odeljku 8.
  3. nakon konsultacija sa koordinatorom za zaštitu podataka, odn. poverenikom za zaštitu podataka proverava i odobrava nove IT aplikacije za obradu podataka o ličnosti sa stanovišta zaštite podataka.
  4. vrši redovne provere i skenove, kako bi se osiguralo da sigurnosni hardver i softver ispravno funkcionišu. Rezultati kontrola zaštite podataka moraju se prijaviti nadležnom povereniku za zaštitu podataka.
  5. vrši procenu bezbednosti podataka svih usluga trećih lica (npr. obrađivača naloga), koje kompanija razmatra za obradu podataka o ličnosti (na primer Cloud-Computing usluge itd.)
  6. Vodi spisak incidenata u oblasti bezbednosti podataka i da incidente u oblasti bezbednosti podataka prijavi Corporate IT-u.

7. koordiniše i odgovora na upite lica čiji se podaci obrađuju o informacijama u vezi podataka o ličnosti, koje kompanija koncerna Arbonia poseduje o licu čiji se podaci obrađuju zahvaljujući podršci odgovarajućeg IT odeljenja (vidi u nastavku takođe i tačku 7.4)
8. otkrivene incidente ili rizike u oblasti bezbednosti podataka prijavi analogno Data Breach Notification uputstvu (vidi u nastavku tačku 9, kao i „Arbonia Data Breach Policy“)

- Corporate IT u saradnji sa IT odeljenjem koje je nadležno za podršku nekoj od kompanija koncerna je nadležno za:
  1. sprovođenje redovnih provera i skenova, kako bi se osiguralo da sigurnosni hardver i softver ispravno funkcionišu. Rezultati kontrola zaštite podataka moraju se prijaviti nadležnom povereniku za zaštitu podataka.
  2. Vođenje centralnog spiska incidenata u oblasti bezbednosti podataka.
  3. Prijavljivanje otkrivenih incidenata ili rizika u oblasti bezbednosti podataka analogno Data Breach Notification uputstvu (vidi u nastavku tačku 9, kao i „Arbonia Data Breach Policy“).

- Internal Audit je nadležan za to da:
  1. prilikom sprovođenja revizija u skladu sa redovnim planom revizija u okviru provere zasnovane na riziku bude izvršena provera da li organizacione procedure odgovaraju bitnim zahtevima ovog uputstva o zaštiti podataka.

- Vlasnik poslovnog procesa je nadležan za to da:
  1. osigura da lokalni poverenik za zaštitu podataka bude adekvatno i blagovremeno uključen u sva pitanja koja su neophodna za procenu obrade podataka o ličnosti.
  2. pripremi, odn. prethodno proveri sve ugovore ili sporazume sa obrađivačima ugovora koji mogu da obrađuju podatke o ličnosti po nalogu koncerna Arbonia, kao što je opisano u odeljku 7.2.
  3. vrši nadzor „Spiska procesa obrade“, koji odgovarajuća kompanija koncerna vodi, popunjava i ažurira i svake godine krajem aprila koordinatoru za zaštitu podataka, odn. povereniku za zaštitu podataka potvrđuje celovitost i ažurnost unosa.
  4. pre implementiranja novih postupaka obrade podataka o ličnosti izvrši procenu rizika koji iz toga proizilaze u vezi ličnosti i osnovnih prava lica čiji se podaci obrađuju i da u slučaju verovatnoće visokog rizika unapred izvrši procenu uticaja na zaštitu podataka.

ARBONIA

6 OSNOVNI PRINCIPI ZAŠTITE PODATAKA ZA OBRADU PODATAKA O LIČNOSTI

Svaka kompanija koncerna koja prilikom obrade podataka o ličnosti obavlja aktivnosti kao odgovorno lice mora da obezbedi **dokaz o usklađenosti sa sledećih 6 (šest) osnovnih principa zaštite podataka:**

1. Obrada podataka o ličnosti može da se vrši samo ako može da se pruži dokaz o važećoj pravnoj osnovu u skladu sa primenljivim zakonima o obradi podataka i ako je relevantna osoba obaveštena o identitetu i podacima za kontakt odgovornog lica, vrsti i pravnoj osnovi za prikupljanje podataka o ličnosti, odgovarajućem periodu čuvanja i o svrsi za koju se podaci o ličnosti evidentiraju

2. Uvek voditi računa o svrsi za koju su podaci o ličnosti prikupljeni

3. Vršiti samo prikupljanje/obradu podataka o ličnosti koji su zaista neophodni

4. Čuvati samo korektne podatke o ličnosti i izbrisati netačne podatke o ličnosti

5. Podatke o ličnosti čuvati samo u zaista neophodnim zakonskim periodima čuvanja

6. Postupati poverljivo sa podacima o ličnosti i deliti samo ono što zaista mora biti podeljeno

6.1 Pravičnost, zakonitost i transparentnost

Obrada podataka o ličnosti se može vršiti samo u svrhe koje su izričito dozvoljene kao je opisano u nastavku; to se mora obavljati na transparentan način. Zbog toga se obrada podataka o ličnosti mora vršiti na zakonit i pravičan način i moraju se poštovati individualna prava lica čiji se podaci obrađuju. To može obuhvatati podatke o ličnosti koje je koncern Arbonia dobio direktno od lica čiji se podaci obrađuju (na primer popunjavanjem obrazaca ili stupanjem u komunikaciju sa nama putem pošte, telefona, e-pošte ili na drugi način), kao i podatke o ličnosti koje Arbonia dobija od trećeg lica.

Prema važećim zakonima o zaštiti podataka, u skladu sa Opštom uredbom o zaštiti podataka o ličnosti, podaci o ličnosti se mogu zakonito obrađivati na osnovu jednog od **pet zakonitih razloga** (**zakoniti razlozi**). Ovi razlozi obuhvataju:

1. **Ugovor:** Obrada podataka o ličnosti je neophodna za ispunjavanje ugovora u kome je ugovorna strana lice čiji se podaci obrađuju, ili je obrada neophodna za sprovođenje predugovornih mera koje se sprovode na zahtev lica čiji se podaci obrađuju, ili

2. **Saglasnost:** Obrada podataka o ličnosti zasniva se na saglasnosti (Opt-in-Modell) lica čiji se podaci obrađuju za jednu ili više specifičnih svrha. Saglasnost mora biti dokumentovana, ili

3. **Zakonska obaveza:** Obrada podataka o ličnosti zasniva se na zakonskoj obavezi koncerna Arbonia. Vrsta i obim obrade podataka moraju biti neophodni za zakonski dozvoljenu aktivnost obrade i u skladu sa važećim zakonskim uslovima, ili

4. **Javni interes:** Obrada je neophodna za obavljanje zadatka koji predstavlja javni interes, ili

5. **Legitimni poslovni interesi:** Obrada je srazmerna legitimnim poslovnim interesima koncerna Arbonia ili treće strane kojoj su podaci o ličnosti obelodanjeni, osim ako interesi ili osnovna prava i slobode lica čiji se podaci obrađuju ne prevazilaze te interese. Legitimni interesi su opšte pravne prirode (npr. naplata neisplaćenih potraživanja/kolektivni ugovor sa radničkim savetom/ostvarivanje prava/primena ili odbrana od pravnih zahteva u vezi sa licem čiji se podaci obrađuju) ili komercijalne prirode (npr. sprečavanje kršenja ugovora).

Transparentnost zahteva da lice čiji se podaci obrađuju mora biti obavešteno o načinu na koji će se postupati sa njihovim podacima o ličnosti. Zbog toga se generalno preporučuje prikupljanje podataka o ličnosti direktno od lica čiji se podaci obrađuju (a ne preko treće strane). Ukoliko se vrši obrada podataka o ličnosti, lice čiji se podaci obrađuju mora biti obavešteno o sledećem:

- ime i podaci za kontakt odgovornog lica i, ako je primenjivo, njegovog predstavnika u EU
- po potrebi podaci za kontakt koordinatora za zaštitu podataka odn. poverenika za zaštitu podataka
- svrha obrade podataka o ličnosti i pravni osnov za obradu,
- primaoci treće strane ili kategorije primalaca treće strane kojima se mogu prenositi podaci
- ako je primenljivo, informacije o obradi u trećoj zemlji i referenca o adekvatnim garancijama

6.2 Namenska svrha

Podaci o ličnosti mogu se obrađivati samo u svrhu koja je pre evidentiranja podataka o ličnosti saopštena licu čiji se podaci obrađuju. Naknadne izmene svrhe su moguće samo u ograničenom obimu i zahtevaju obrazloženje. Odgovorno lice mora da informiše lice čiji se podaci obrađuju o svrsi za koju Arbonia vrši obradu njegovih podataka o ličnosti kada Arbonia po prvi put prikuplja podatke o ličnosti ili što je pre moguće nakon toga. Prilikom svake obrade u reklamne svrhe ili za marketinške programe, lice čiji se podaci obrađuju mora dobiti pravo na prigovor za obradu svojih podataka o ličnosti i o tome mora biti izričito

obavešteno. U tom pogledu, svako odgovorno lice mora da implementira sistem za obradu žalbi koji osigurava Opt-Outs.

6.3 Minimizacija podataka

Vršiti samo obradu podataka o ličnosti koji su zaista neophodni. Pre obrade podataka o ličnosti mora se utvrditi da li je i u kojoj meri obrada podataka o ličnosti neophodna za postizanje svrhe zbog koje se vrši. Podaci o ličnosti se ne smeju unapred prikupljati i čuvati za potencijalne buduće svrhe, osim ako to ne zahteva ili dozvoljava nacionalni zakon.

6.4 Tačno i aktuelno

Podaci o ličnosti moraju biti tačni, potpuni i – ukoliko dođe do promena – ažurirani. Moraju se preduzeti odgovarajući koraci kako bi se osiguralo da se netačni ili nepotpuni podaci o ličnosti izbrišu, isprave, dopune ili ažuriraju. Svi koji rade sa podacima o ličnosti moraju u tu svrhu preduzeti odgovarajuće korake (na primer potvrđivanjem podataka kada se obavlja telefonski poziv sa licem čiji se podaci obrađuju ili uklanjanjem sačuvanog telefonskog broja iz baze podataka, ukoliko ga lice čiji se podaci obrađuju više ne koristi).

6.5 Ograničeni period zadržavanja

Podaci o ličnosti se mogu čuvati samo tokom vremena skladištenja koje je zaista potrebno. Podaci o ličnosti se moraju izbrisati čim više ne budu potrebni za predviđene svrhe ili se opozve saglasnost, odn. ukoliko su u suprotnosti sa upotrebom na osnovu legitimnog interesa i Arbonia ne može navesti prioritetnije legitimne razloge. U pojedinim slučajevima duži periodi skladištenja mogu nam omogućiti duže čuvanje podataka o ličnosti, ukoliko to zahteva zakon (npr. u skladu sa poreskim zakonima i zakonima o trgovini) ili ako su podaci o ličnosti potrebni za ostvarivanje, primenu ili odbranu pravnih zahteva.

6.6 Poverljivost i bezbednost podataka

Podacima o ličnosti se u svakom trenutku mora poverljivo postupati i deliti samo onako kako zaista moraju biti podeljeni. Princip „potrebne informacije“ se primenjuje tako da zaposleni i treća strana imaju pristup podacima o ličnosti samo ako i u onoj meri u kojoj je to neophodno za ispunjenje svrhe. To zahteva pažljivo izrađen koncept koji definiše specifična prava pristupa za svaki poslovni proces, uključujući primenu i odobravanje uloga i nadležnosti (koncept prava pristupa). Primaoci podataka o ličnosti moraju biti obavešteni o poverljivosti podataka o ličnosti i moraju **i moraju se obavezati sporazumom o neotkrivanju/sporazumom o poverljivosti** (to može biti deo ugovora o radu ili slično). Izuzetak: Primalac podleže profesionalnoj ili zakonskoj obavezi čuvanja poverljivosti podataka.

Podaci o ličnosti moraju biti zaštićeni odgovarajućim organizacionim i tehničkim merama kako bi se sprečio nezakonit pristup, nezakonita obrada ili obelodanjivanje, kao i nenamerni gubitak, izmena ili uništavanje (vidi odeljak 8).

ARBONIA

7 OSTALE OBAVEZE U SKLADU SA OPŠTOM UREDBOM O ZAŠTITI PODATAKA O LIČNOSTI ILI DRUGIM SLIČNIM VAŽEĆIM PROPISIMA O ZAŠTITI PODATAKA

7.1 Princip odgovornosti

Kompanija koncerna Arbonia koja podleže Opštoj uredbi o zaštiti podataka o ličnosti (ili sličnoj važećoj odredbi o zaštiti podataka) mora da obezbedi dokaz o usklađenosti sa važećim zakonima o zaštiti podataka (princip „odgovornosti"). Prema tome, ove kompanije koncerna pored opštih zahteva iz ovog uputstva o zaštiti podataka moraju primeniti i održavati kontinuitet sledećih tačaka, pri čemu direktor odgovarajuće kompanije koncerna mora da osigura apsolutnu primenu i održavanje kontinuiteta:

1. Lokalni koordinator za zaštitu podataka odn. lokalni poverenik za zaštitu podataka: Imenovanje posebnog lokalnog koordinatora za zaštitu podataka odn. poverenika za zaštitu podataka

2. Vođenje „Spiska procesa obrade": Mora se voditi i ažurirati popis o aktivnostima obrade podataka o ličnosti

3. Provera legitimnosti: Mora se proveriti zakonitost obrade podataka o ličnosti u skladu sa važećim zakonitim razlozima, naročito kada se vrši obrada podataka o ličnosti posebnih kategorija

4. Kontrola obrađivača naloga: Zaključivanje ugovora o obradi naloga sa obrađivačem naloga ili sa obrađivačem naloga za obezbeđivanje ili prijem podataka o ličnosti na osnovu dozvole u skladu sa članom 28 Opšte uredbe o zaštiti podataka o ličnosti.

5. U slučaju zajedničkih odgovornih lica za obradu se mora predvideti sporazum između zajedničkih odgovornih lica u skladu sa članom 26. Opšte uredbe o zaštiti podataka o ličnosti.

6. Zaposleni koncerna Arbonia moraju biti obavešteni o aktivnostima obrade podataka o ličnosti.

7.2 Pravila za obrađivača naloga (pre svega partnera za pružanje usluga)

Odgovorno lice radi samo sa ugovornim obrađivačima naloga koji nude dovoljne garancije da su preduzete odgovarajuće tehničke i organizacione mere, tako da se obrada podataka o ličnosti vrši u skladu sa zahtevima člana 28. Opšte uredbe o zaštiti podataka o ličnosti i garantuje zaštitu prava lica čiji se podaci obrađuju.

Za zajedničke usluge unutar koncerna Arbonia postoji sporazum koji dozvoljava prenos podataka o ličnosti, pod uslovom da u skladu sa važećim zakonima o zaštiti podataka postoje legitimni pravni razlozi za prenos ovih podataka o ličnosti.

7.2.1 Stavljanje podataka o ličnosti na raspolaganje obrađivaču naloga (odlazno)

Obrada podataka o ličnosti na osnovu dozvole znači da je pružalac usluga ovlašćen za obradu podataka o ličnosti bez prenosa odgovornosti za odgovarajući poslovni proces (tj. pružaoci usluga, Outsourcing usluge). U ovom slučaju, traba zaključiti ugovor o obradi naloga za obradu podataka o ličnosti sa spoljnim dobavljačima na osnovu dozvole. Odgovarajuća kompanija koncerna Arbonia odgovorna je i zadržava kompletnu odgovornost za korektno obavljanje obrade podataka o ličnosti od strane obrađivača naloga.

Odgovarajući vlasnik poslovnog procesa mora da obezbedi da trenutni model sporazuma za obradu naloga ili odgovarajući sličan ugovor koji pružalac usluga stavlja na raspolaganje, ispunjava zahteve iz člana 28. Opšte uredbe o zaštiti podataka o ličnosti, kako bi mogao da se koristi za naručivanje takvih pružalaca usluga. Pružalac usluga alternativno može dokumentovati svoju usklađenost sa zahtevima bezbednosti podataka podnošenjem odgovarajućeg i odobrenog EU sertifikata. Svako odstupanje od takvog sigurnosnog standarda mora da odobri povernik za zaštitu podataka odn. koordinator za zaštitu podataka u saradnji Corporate IT-om. Postojeći ugovori se moraju revidirati u roku od jedne godine od stupanja na snagu ovog uputstva o zaštiti podataka i sadržati ugovor o obradi naloga u pisanom obliku.

7.2.2 Primanje podataka o ličnosti od strane obrađivača naloga (ulaz)

Ukoliko treća strana prenese podatke o ličnosti kompaniji koncerna Arbonia, mora se osigurati da podaci o ličnosti (i) mogu da se koriste u predviđene svrhe, (ii) da se prikupljaju na legitimnim osnovama (preporučuje se pribavljanje pismene potvrde) i da (iii) postoji ugovor o obradi naloga koji je u skladu sa članom 28. Opšte uredbe o zaštiti podataka o ličnosti.

7.3 Prekogranični prenos podataka o ličnosti

U slučaju prekograničnog prenosa podataka o ličnosti, moraju biti ispunjeni odgovarajući nacionalni zahtevi za obelodanjivanje podataka o ličnosti u inostranstvu. U skladu sa Opštom uredbom o zaštiti podataka o ličnosti, prenos podataka o ličnosti se može vršiti unutar EU, Evropskog ekonomskog prostora ili u zemlju za koju je Evropska komisija utvrdila da ispunjava odgovarajuće garancije, kako bi se obezbedio adekvatan nivo zaštite podataka. Takav prenos podataka ne zahteva posebno odobrenje. Evropska komisija je između ostalog klasifikovala Švajcarsku kao zemlju koja pruža adekvatnu zaštitu (vidi aktuelnu listu zemalja: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Prenos podataka o ličnosti u treću zemlju je dozvoljen samo ako postoje odgovarajuće dodatne garancije. To znači da ako primalac može dokazati da održava standard zaštite podataka koji odgovara ovom uputstvu o zaštiti podataka npr. i) postoje obavezujuća pravila kompanije, ii) zaključene su standardne ugovorne klauzule EU za obradu naloga u trećim zemljama sa podugovaračima i ostalim podizvođačima [3], iii) postoje pravila ponašanja koje je odobrilo nadzorno telo, iv) pružalac usluga je radi postizanja dovoljnog nivoa zaštite podataka uključen u sistem sertifikacije koji je akreditovan od strane EU ili v) postoje pojedinačni sporazumi između odgovornog lica i obrađivača naloga i dozvola odgovornog nadzornog organa, kao i obaveštavanje lica čiji se podaci obrađuju o tome. Ova obaveza ne važi ukoliko se prenos zasniva na zakonskoj obavezi. Za takav prenos potrebno je odobrenje koordinatora za zaštitu podataka, odn. poverenika za zaštitu podataka.

Ako se podaci o ličnosti prenose u okviru koncerna Arbonia, kompanija koncerna koja uvozi podatke o ličnosti dužna je da sarađuje po pitanju svih zahteva nadzornog organa u državi u kojoj nalazi sedište kompanije koja izvozi podatke i da se pridržava svih primedbi nadzornog organa u vezi obrade prenetih podataka o ličnosti.

7.4 Postupanje sa zahtevom za informacijom od strane lica čiji se podaci obrađuju

Lica čiji se podaci obrađuju imaju pravo da podnesu formalni zahtev za informacije o detaljima podataka o ličnosti koje koncern Arbonia poseduje i mogu zahtevati sledeće:

Pravo na obaveštavanje o:

- svrhama obrade;
- kategorijama podataka o ličnosti koji se obrađuju;
- primaocima ili kategorijama primalaca kojima su podaci o ličnosti obelodanjeni ili će biti obelodanjeni, posebno u slučaju primalaca u trećim zemljama ili međunarodnim organizacijama;
- u slučaju da je moguće, planiranom trajanju za koje će se podaci o ličnosti čuvati ili, ako to nije moguće, kriterijumima za određivanje ovog trajanja;
- postojanju prava na ispravku ili brisanje relevantnih podataka o ličnosti ili na ograničenje obrade od strane odgovornog lica ili pravo na prigovor protiv obrade;
- postojanju prava na žalbu nadzornom organu;
- svim dostupnim informacijama o poreklu podataka, ukoliko podaci o ličnosti nisu prikupljeni direktno od lica čiji se podaci obrađuju;
- postojanju automatizovanog donošenja odluka, uključujući profilisanje;
- ukoliko se podaci o ličnosti prenose u treću zemlju ili međunarodnu organizaciju, lice čiji se podaci obrađuju ima pravo da bude obavešteno o odgovarajućim garancijama.

[3] Vidi odluku Komisije od 5. februara 2010. o standardnim ugovornim klauzulama za prenos podataka o ličnosti obrađivačima naloga u trećim zemljama u skladu sa Direktivom 95/46/EG Evropskog parlamenta i saveta, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

Pravo na ispravku:

- Lice čiji se podaci obrađuju ima pravo da zahteva da odgovorno lice odmah ispravi odgovarajuće netačne podatke o ličnosti. Uzimajući u obzir svrhe obrade, lica čiji se podaci obrađuju ima pravo da zahteva dopunu nepotpunih podataka o ličnosti – takođe i dodatnom izjavom.

Pravo na brisanje („Pravo na zaborav"):

- Lice čiji se podaci obrađuju ima pravo da zahteva od odgovornog lica da odmah izbriše relevantne podatke o ličnosti, a odgovorno lice je dužna da podatke o ličnosti odmah izbriše ukoliko je postoji jedan od sledećih razloga:
    1. Podaci o ličnosti više nisu potrebni u svrhe za koje su prikupljeni ili obrađivani drugi način;
    2. Subjekt podataka opoziva saglasnost na kojoj se zasnivala obrada u skladu sa članom 6, stav 1, slovo a Opšte uredbe o zaštiti podataka o ličnosti ili sa članom 9, stav 2, slovo a Opšte uredbem o zaštiti podataka o ličnosti, a ne postoji nikakva druga pravna osnova za obradu;
    3. Lice čiji se podaci obrađuju je u skladu članom 21, stav 1 Opšte uredbe o zaštiti podataka o ličnosti uložilo prigovor protiv obrade i ne postoje prioritetniji legitimni razlozi za obradu, ili lice čiji se podaci obrađuju ulaže prigovor protiv obrade u skladu sa članom 21, stav 2 Opšte uredbe o zaštiti podataka o ličnosti;
    4. Obrada podataka o ličnosti je vršena nezakonito;
    5. Brisanje podataka o ličnosti je neophodno kako bi se ispunila zakonska obaveza u skladu sa zakonom odgovarajuće države članice kojoj podleže odgovorno lice;
    6. Podaci o ličnosti su prikupljeni u vezi sa uslugama koje nudi informatičko društvo u skladu sa članom 8, stav 1 Opšte uredbe o zaštiti podataka o ličnosti.

Pravo na ograničenje obrade:

- Lice čiji se podaci obrađuju ima pravo da zahteva od odgovornog lica da ograniči obradu ukoliko je ispunjen jedan od sledećih uslova:
- ako lice čiji se podaci obrađuju osporava ispravnost podataka o ličnosti za period koji omogućava odgovornom licu da proveri tačnost podataka o ličnosti:
- ukoliko se obrada podataka vrši nezakonito i lice čiji se podaci obrađuju odbije brisanje podataka o ličnosti i umesto toga zahteva ograničenje upotrebe podataka o ličnosti;
- ukoliko odgovornom licu podaci o ličnosti više nisu potrebni za potrebe obrade, ali su licu čiji se podaci obrađuju potrebni za podnošenje zahteva, ostvarivanje ili odbranu pravnih zahteva,
- ukoliko je lice čiji se podaci obrađuju uložilo prigovor na obradu u skladu sa članom 21, stav 1, sve dok se ne utvrdi da li legitimni razlozi odgovornog lica premašuju razloge lica čiji se podaci obrađuju.

Od lica čiji se podaci obrađuju treba zatražiti da svoj zahtev preda u pismenoj formi ili e-poštom, ili poštom, i da ga dostavi na adresu relevantnom lokalnom povereniku. Lokalni poverenik za zaštitu podataka mora licu čiji se podaci obrađuju bez odlaganja da pruži informacije, ali u svakom slučaju u roku od mesec dana nakon prijema zahteva. Ovaj rok se može produžiti za još dva meseca, ukoliko je to potrebno uzimajući u obzir složenost i broj zahteva. U roku od jednog meseca nakon prijema zahteva koordinator za zaštitu podataka ili poverenik za zaštitu podataka odgovornog lica obaveštava lice čiji se podaci obrađuju o produženju roka, zajedno sa razlozima kašnjenja. Za lice čiji se podaci obrađuju ne smeju nastati nikakvi troškovi u vezi zahteva o informacijama koje kompanija koncerna Arbonia ima o njemu, osim ukoliko su upiti lica čiji se podaci obrađuju očigledno neosnovani ili suvišni, naročito usled ponovnog podnošenja. Upiti lica čiji se podaci obrađuju koji su upućeni na nekoliko kompanija koncerna Arbonia se radi koordinacije i odgovora moraju proslediti Corporate IT-u.

7.5 Sprovođenje procene uticaja na zaštitu podataka

Ukoliko postoji verovatnoća da će planirani novi oblik obrade podataka o ličnosti, posebno kada se koriste nove tehnologije, usled vrste, obima, okolnosti svrhe obrade, predstavljati visok rizik za prava i slobode lica čiji se podaci obrađuju, prethodno se mora izvršiti procena posledica predviđenih postupaka obrade radi zaštite podataka o ličnosti.

Pre implementiranja novih postupaka obrade se zbog toga mora izvršiti procena rizika koji iz toga proizilaze u vezi ličnosti i osnovnih prava lica čiji se podaci obrađuju. U slučaju novih IT aplikacija, ovo mora uzeti u obzir u okviru postupka odobravanja. Ukoliko se na osnovu prve procene može zaključiti da će planirani, novi oblik obrade podataka o ličnosti verovatno dovesti do visokog rizika za lice čiji se podaci obrađuju, mora se izvršiti procena uticaja na zaštitu podataka.

Upite u vezi neophodnosti odn. tokom obavljanja procene uticaja na zaštitu podataka, treba upućivati lokalnom koordinatoru za zaštitu podataka, odn. lokalnom povereniku za zaštitu podataka. Nakon sprovođenja, o proceni uticaja na zaštitu podataka, treba obavestiti lokalnog koordinatora za zaštitu podataka, odn. lokalnog poverenika za zaštitu podataka, kako bi se od njega dobilo mišljenje.

Ukoliko procena uticaja na zaštitu podataka pokaže da bi obrada rezultirala visokim rizikom za lice čiji se podaci obrađuju i ako se ne preduzmu mere za suzbijanje rizika, nadzorni, pre implementacije novog postupka obrade se mora konsultovati nadležan nadzorni organ.

8 BEZBEDNOST PODATAKA O LIČNOSTI

Podaci o ličnosti se moraju zaštititi od nezakonitog pristupa i nezakonite obrade ili obelodanjivanja, kao i nenamernog gubitka ili uništavanja. Ovo važi bez obzira na to da li se podaci o ličnosti obrađuju elektronskim putem ili na papiru.

Odgovorno lice i obrađivač naloga moraju da primenjuju adekvatne tehničke i organizacione mere kako bi se podaci zaštitili od nezakonite obrade. Ove mere moraju da se zasnivaju na (i) najboljim postupcima obrade, (ii) rizicima obrade i (iii) potrebi zaštite podataka o ličnosti (utvrđenih postupkom za klasifikaciju informacija); oni po potrebi, između ostalog, uključuju:

(a) pseudonimizaciju i šifrovanje podataka o ličnosti;

(b) sposobnost da se dugoročno osigura poverljivost, integritet, dostupnost i opteretivost sistema i usluga u vezi sa obradom;

(c) sposobnost brzog vraćanja dostupnosti i pristupa podacima o ličnosti u slučaju fizičkog ili tehničkog incidenta;

(d) postupak za redovnu proveru, procenu i evaluaciju efikasnosti tehničkih i organizacionih mera kojima se garantuje sigurnost obrade.

Tehničke i organizacione mere za zaštitu podataka o ličnosti su deo internog upravljanje informacionom sigurnošću i moraju se stalno prilagođavati tehničkom razvoju i organizacionim promenama.

Bezbednosne procedure mogu da uključuju najmanje:

- Kontrole pristupa: Treba prijaviti svaku nepoznatu osobu koja se nađe u područjima sa kontrolisanim pristupom.

- Bezbedne fioke ili ormari na zaključavanje: pisaći stolovi i ormari trebaju ostati zaključani ukoliko sadrže poverljive informacije bilo koje vrste. Podaci o ličnosti su uvek poverljive informacije. Zaposleni treba da osiguraju da se papir i odštampani primerci sa podacima o ličnosti ne ostavljaju na opšte vidljivom mestu, kao na primer u štampaču. Ako se podaci o ličnosti sa autorizacijom čuvaju na mediju za razmenu podataka (kao što je CD, memorijski stik ili DVD), moraju se držati zaključani kada nisu u upotrebi.
- Metode za odlaganje: Ukoliko više nisu potrebni, papirne dokumente treba usitniti i bezbedno odložiti. Ovo se odnosi i na podatke o ličnosti, koji se obično čuvaju elektronski, ali su odštampani.

- Podaci koji se čuvaju u elektronskom obliku: Podaci o ličnosti treba da budu zaštićeni lozinkama u skladu sa trenutnom smernicom za lozinke i nikada se ne smeju deliti

među zaposlenima. Ako se radi o elektronskom obliku, čuvanje i pristup podacima o ličnosti se mora vršiti na serverima IT sistema i u strukturiranim aplikacijama informacione tehnologije, umesto u nešifrovanom obliku na lokalnim računarima.

- Podaci o ličnosti koji su prikupljeni u elektronskom obliku i koje je na raspolaganje stavilo lice čiji se podaci obrađuju: Identitet lica čiji se podaci obrađuju mora biti verifikovan, po mogućnosti utvrđen dvostrukim postupkom prijavljivanja (tj. druga e-pošta za potvrdu navedene adrese e-pošte). Ako je pristup internet stranici ili aplikaciji ograničen na registrovane korisnike (tj. korisnički nalog), identifikacija i potvrda identiteta lica čiji se podaci obrađuju moraju da obezbede bezbednosnu zaštitu koja je srazmerna odgovarajućem sadržaju tokom pristupa.

- Opreznost prilikom deljenja podataka o ličnosti: Podaci o ličnosti se nikada ne smeju deliti neformalno. Važi princip „neophodnih informacija". Koncept klasifikacije i razdvajanja po poslovnom procesu, kao i primena uloga i odgovornosti je obavezan. Podaci o ličnosti se pre slanja moraju šifrovati u elektronskom obliku. Menadžer informacione tehnologije može objasniti na koji način se podaci o ličnosti šalju ovlašćenim eksternim osobama za kontakt.

- Pribavljanje uputstva: U slučaju da postoje pitanja ili nedoumice u vezi sa aspektom zaštite podataka ili obavezama prema ovom uputstvu o zaštiti podataka, potražite savet od svog direktnog pretpostavljenog, odgovarajućeg lokalnog poverenika za zaštitu podataka ili Legal & Compliance.

Opštea uredba o zaštiti podataka o ličnosti zahteva da se privatnost uzme u razmatranje što je pre moguće. Privatnost putem tehnološkog inženjeringa zahteva od organizacija da razmotre privatnost u ranim fazama tehnološkog inženjeringa i tokom procesa razvoja novih proizvoda, procesa ili usluga koji su povezani sa obradom podataka o ličnosti. Podrazumevana privatnost znači da kada sistem ili usluga obuhvata odluku pojedinca koliko podataka o ličnosti će deliti sa drugima, podrazumevana podešavanja treba da budu ta koja će pružiti maksimalnu zaštitu privatnosti. Zbog toga se svaka nova IT aplikacija podvrgava internom postupku odobravanja, pri čemu ta nova IT aplikacija u okviru evaluacije takođe mora proceniti i sa stanovišta zakona o zaštiti podataka.

9 PRIJAVLJIVANJE INCIDENATA U OBLASTI BEZBEDNOSTI PODATAKA

Mnogi važeći propisi o zaštiti podataka zahtevaju se incidenti u oblasti zaštite podataka prijave direktno zakonodavcu. Zbog toga se zahteva da se u skladu sa postupkom koji je opisan u uputstvu koncerna Arbonia za incidente u oblasti bezbednosti podataka („Arbonia Data Breach Policy"), svi incidenti u oblasti bezbednosti podataka odmah prijave nadležnom koordinatoru za zaštitu podataka ili povereniku za zaštitu podataka, bez obzira da li je pogođen lokalni sistem ili sistem koncerna. Ukoliko IT otkrije incidente ili rizike u oblasti bezbednosti podataka, oni se moraju prijaviti analogno Data Breach Notification uputstvu.

ARBONIA

Cilj je poštovanje obaveze prijavljivanja kršenja važećih obaveza zaštite podataka u prema važećim zakonima o zaštiti podataka (npr. u skladu sa Opštom uredbom o zaštiti podataka o ličnosti najkasnije 72 sata nakon dobijanja obaveštenja).

U takvom slučaju, se akcenat mora staviti na ispunjavanje odgovarajućih rokova za obaveštavanje o kršenju zaštite podataka i preduzimanju neposrednih mera kako bi se istražili incidenti i utvrdilo da li je zaista došlo do kršenja u pogledu podataka o ličnosti. Corporate IT mora da vodi internu listu bezbednosnih propusta u koncernu Arbonia, kako bi se u skladu sa nacionalnim zakonom mogle poštovati obaveze izveštavanja i osigurati primena relevantnih pravila zastupanja radi omogućavanja prijave kršenja u svakom trenutku. Pre prijavljivanja nacionalnom nadležnom organu mora se obavestiti Corporate IT ili odeljenje Legal and Compliance koncerna.

Moraju se strogo poštovati sva ostala uputstava Corporate IT i lokalnih IT odeljenja.

10 POSLEDICE U SLUČAJU NEPOŠTOVANJA

Usklađenost sa ovim uputstvom o zaštiti podataka je od izuzetne važnosti za koncern Arbonia i javni ugled koncerna Arbonia. Neadekvatna obrada podataka o ličnosti ili druga kršenja zakona o zaštiti podataka takođe mogu biti predmet krivičnog postupka u mnogim zemljama i dovesti do zahteva za naknadu štete. Unutar koncerna Arbonia kršenje pravila iz ovog uputstva o zaštiti podataka može za posledicu imati sankcije u skladu sa zakonom i/ili odgovarajućim ugovorom (o radu).

11 ODSTUPANJA

Odstupanja od odredaba ovog uputstva i dodataka dozvoljena su samo nakon konsultacija sa Head of Legal & Compliance.

12 INFORMACIJE

Informacije u vezi sa uputstvom o zaštiti podataka se mogu dobiti od Head of Legal & Compliance.

ARBONIA

13 STUPANJE NA SNAGU

Ovo uputstvo stupa na snagu 17. juna 2020. i zamenjuje uputstvo o postupanju sa podatima (Uputstvo o zaštiti podataka) od 5. decembra 2013.

Arbon, 16. Jun 2020

Arbonia AG

Alexander von Witzleben
Predsednik Upravnog odbora i izvršni direktor

Andrea Wickart
Head of Legal & Compliance/generalni sekretar

Dodaci ovom uputstvu o zaštiti podataka koncerna Arbonia:

Sledeći dodaci u svojoj ažurnoj verziji potvrđuju ovo uputstvo o zaštiti podataka:

- Uputstva o zahtevima lica čiji se podaci obrađuju i o brisanju podataka
- Uputstvo o kršenju zaštite podataka
- Izjava o zaštiti podataka za zaposlene

Ovaj dokument važi bez potpisa.