ASCENDUM PRIRUČNIK ZA ZAŠTITU PODATAKA

Ascendum Central Europe GmbH

Ascendum Baumaschinen Österreich GmbH

Ascendum Stavebne stroje Slovensko s.r.o.

Ascendum Stavebni stroje Czech s.r.o.

Ascendum Építőgépek Hungária Kereskedelmi Kft.

Ascendum građevinski strojevi Hrvatska d.o.o.

Ascendum Machinery s.r.l.

Pravna napomena

Informacije koje dobijete s priručnikom za zaštitu podataka, prilozi i primjerci ugovora nisu pravni savjeti niti su zamišljeni kao takvi. Pokušavamo pružiti kvalitetnu informaciju, ali ne dajemo nikakve tvrdnje, obećanja ili garancije o preciznosti, potpunosti ili adekvatnosti politike za zaštitu podataka, spomenutih ugovora i/ili spomenutih podataka. Kako pravni savjet mora biti prilagođen specifičnim okolnostima svakog slučaja i zakoni se stalno mijenjaju, ništa što je pruženo priručnikom za zaštitu podataka, prilozima i primjercima ugovora ne bi trebalo biti korišteno kao zamjena za savjet kompetentnog pravnog savjetnika. Nadalje, od presudne je važnosti napomenuti kako smo tražili najbolje primjere za vježbu na internetu, kopirali te dijelove informacija i prilagodili te dijelove informacija našim potrebama. Naše izvore informacija možete naći na listi referenca.

Međunarodni priručnik za zaštitu podataka i Pravila

Izjava Predsjednika i izvršnog direktora Ascendum Central Europe GmbH

Ascendum grupacija je posvećena usklađenju svojeg djelovanja s primjenjivim propisima svugdje gdje obavlja svoje poslovanje. To je presudno za naš kontinuirani uspjeh na sve više reguliranom globalnom tržištu, i isto tako odražava našu predanost da poslujemo u skladu s najvišim pravnim i etičkim standardima.

Kao tvrtka kćer kompanije bazirane u Portugalu s djelovanjem diljem svijeta, uključujući S.A.D., Ascendum je podložan regulaciji prava Sjedinjenih Američkih Država, država članica Europske Unije, i drugih država pokrivajući informacije koje obrađujemo u odnosu na naše zaposlenike, korisnike, dobavljače i druge.

Međunarodna Pravila zaštite podataka su namijenjena kako bi vam pomogla da shvatite ove propise. Premda specifične tehničke pretpostavke zakona prelaze primjenu ovih pravila, ove pretpostavke utvrđuju ujednačene standarde ponašanja za zaposlenike Ascenduma i njegovih podružnica unutar Grupe Srednje Europe koje obrađuju informacije pokrivene ovim propisima.

U Ascendumu, zahtijevamo potpunu usklađenost s ovim pravilima kako bi pomogli osigurati pridržavanje primjenjivim zakonima o privatnosti i sigurnosti podataka.

Zahvaljujem na vašoj pozornosti za ovu važnu temu.

Ascendum Central Europe GmbH

Dr. Thomas Michael Schmitz
Presjednik i izvršni direktor

TABLE OF CONTENTS

I. Ascendum Pravila za zaštitu podataka[1]

1.0 Svrha

Ova Pravila definiraju pretpostavke za osiguranje usklađenosti sa zakonima i propisima primjenjivim na Ascendum Central Europe Grupu pri korištenju i prijenosu osobnih podataka kroz cijelu Ascendum Central Europe Grupu.

2.0 Doseg

Ascendum Central Europe Grupa je posvećena usklađivanju s primjenjivim zahtjevima za privatnost i sigurnost podataka u zemljama u kojima Grupa i njene podružnice („Kompanija“) djeluju. Zbog različitosti među ovim nadležnostima, Kompanija je usvojila Pravila zaštite podataka koja stvaraju zajedničke središnje vrijednosti, pravila i procedure namijenjene postizanju skoro univerzalne usklađenosti koja su nadopunjena s alternativnim ili dodatnim pravilima ili implementacijskim postupcima primjenjivima u onim nadležnostima koje imaju specifične zahtjeve. Ova Pravila se primjenjuju na sve zaposlenike na puno i na nepuno radno vrijeme Ascenduma, zaposlenike podružnica koje su u većinskom vlasništvu Ascenduma, zaposlenike zajedničkih pothvata, i na sve dobavljače i prodavače koji prime osobne podatke od Ascenduma, koji imaju pristup osobnim podacima koje je Ascendum sakupio ili obradio, ili koji pružaju informacije Ascendumu, nevezano za geografsku lokaciju.

3.0 Pretpostavke

3.1 Ured za zaštitu podataka

Ascendumov program usklađenosti će nadzirati pojedinci sa značajnim ovlastima i neovisnošću. Kako bi naglasili našu predanost nadležnim vlastima i neovisnosti naših napora za nadzor usklađenosti i kako bi potaknuli efikasnost tih napora, Kompanija je uspostavila Koordinatora za obradu podataka.

3.1.1 Glavni koordinator za usklađenje Ascenduma će koordinirati Koordinatora zaštite podataka.
3.1.2 Obveze ovih koordinatora zaštite podataka su postavljene ovim Pravilima i implementiraju procedure koje će Ured za zaštitu podataka usvojiti, kao i bilo koje druge obveze naložene primjenjivim propisima koje će obavljati određeni koordinator zaštite podataka, uključujući najmanje sljedeće:
3.1.2.1 Određivanje postoji li obveza obavještavanja jednog ili više nadležnih tijela za zaštitu podataka temeljem trenutnih ili namjeravanih aktivnosti obrade podataka Kompanije.
3.1.2.2 Izvršavanje bilo koje obavijesti i održavanje takvih obavijesti u tijeku.
3.1.2.3 Dizajniranje i implementacija programa za osposobljavanje zaposlenika u odnosu na pravila i procedure zaštite podataka.
3.1.2.4 Ustanovljivanje procedura i standardnih ugovornih odredaba radi ostvarivanja usklađenosti s ovim Pravilima od prodavatelja, dobavljača, i trećih osoba koje prime osobne podatke od Ascenduma, koje imaju pristup osobnim podacima koje je prikupio ili obradio Ascendum, ili koji pružaju informaciju Ascendumu, nevezano za njihovu geografsku lokaciju.
3.1.2.5 Ustanovljivanje mehanizama za povremene revizije usklađenosti s ovim Pravilima, postupcima implementacije i primjenjivim popisima.
3.1.2.6 Ustavnovljivanje, održavanje, i korištenje sustava za brze i adekvatne odgovore na zahtjeve Ispitanika kojima koriste svoja prava.

[1] “Visteon (2013): Međunarodna pravila za zaštitu podataka, https://www.visteon.com/utils/media/privacy.pdf, zadnji put pristupljeno 27.04.2018, u 11:45”

3.1.2.7 Osiguravanje da se program usklađenosti Ascenduma održava ažurnim.
3.1.2.8 Informiranje starijih menadžera, djelatnika, i direktora Kompanije o potencijalnim korporativnim i osobnim građanskim i kaznenim sankcijama koje mogu biti određene protiv Kompanije i/ili njezinih zaposlenika zbog kršenja primjenjivih zakona o zaštiti podataka.

3.2 Načela zaštite podataka

Kompanija je usvojila sljedeća načela radi uređenja korištenja, sakupljanja i prijenosa osobnih podataka, osim za slučajeve kada je pojedinačno uređeno ovim Pravilima drugačije ili kada je to obvezatno na temelju primjenjivih zakona:
3.2.1 Osobni podaci će se obrađivati samo pošteno i zakonito.
3.2.2 Osobni podaci će se prikupljati samo za specifične, eksplicitne, zakonite i legitimne svrhe, i neće se dalje obrađivati ni na koji način koji nije kompatibilan s tim svrhama.
3.2.3 Osobni podaci će biti adekvatni, relevantni i neće prekoračivati potrebu u odnosu na svrhu za koju se prikupljaju i/ili obrađuju.
3.2.4 Osobni podaci će biti točni, cjeloviti i u tijeku što je u skladu sa svrhom za koju se prikupljaju i/ili obrađuju.
3.2.5 Osobni podaci se neće čuvati u obliku koji dopušta identifikaciju Ispitanika na dulje vremena od onoga koje je nužno za ostvarivanje dozvoljene svrhe.
3.2.6 Osobni podaci se neće prikupljati ni obrađivati osim ako:
3.2.6.1 je Ispitanik pružio valjani, informirani pristanak, vidi Odjel 3.3.;
3.2.6.2 je obrada nužna za ostvarivanje ugovora kojeg je ugovorna strana Ispitanik ili kako bi se poduzeli koraci na zahtjev Ispitanika prije stupanja u ugovorni odnos;
3.2.6.3 Obrada je nužna za usklađivanje s Ascendumovim pravnim obvezama;
3.2.6.4 Obrada je nužna kako bi se zaštitili presudni interesi Ispitanika;
3.2.6.5 Obrada je nužna za izvršavanje zadatka koji se provode u javnom interesu ili radi izvršavanja službene vlasti povjerene Kontroloru podataka ili trećoj osobi kojoj su podaci dani; ili
3.2.6.6 Obrada je nužna za legitimne interese Ascenduma ili treće osobe ili osoba kojima su podaci dani, osim ako osnovna prava i slobode Ispitanika prevladavaju nad tim interesima.
3.2.7 Osobni podaci će se skupljati i obrađivati u skladu s pravima Ispitanika, vidi Odjel 3.8.
3.2.8 Primjerene fizičke, tehničke i proceduralne mjere će se poduzeti kako bi se:
(i) spriječilo i/ili identificiralo neovlašteno ili nezakonito skupljanje, obrađivanje, prijenos osobnih podataka; i
(ii) spriječio slučajan gubitak ili uništenje, ili oštećenje osobnih podataka. Vidi Odjel 7.0.

3.3 Pristanci

3.3.1 Da bi bio valjan, pristanak mora biti informiran, izričit, i slobodno dan.
3.3.2 Ako se pristanak dobiva s ostalim pisanim izjavama, zahtjev za pristanak mora biti uočljiv.
3.3.3 Pristanak u odnosu na Osjetljive podatke mora se odnositi izričito na te podatke.
3.3.3.1 Pristanak mora biti opoziv.
3.3.3.2 Sustav pristanka će uključivati odredbe koje utvrđuju koje objave bi trebale ili morale biti učinjene kako bi se dobio valjan pristanak te koje dokumentiraju o vrijeme, metodu i sadržaj učinjenih objava, kao i valjanost, doseg, i volju danih pristanaka.

3.4 Prijenosi trećim osobama

3.4.1 Osobni podaci se neće prenositi drugom tijelu, državi ili teritoriju, osim ako se ne provedu razumni i adekvatni koraci kako bi se održala potrebna razina zaštite podataka.
3.4.2 Osobni podaci se mogu prenositi trećim osobama samo zbog razloga koji su u skladu s ciljevima zbog kojih su podaci izvorno prikupljeni ili zbog drugih razloga koje zakon dopušta.
3.4.3 Svi Osjetljivi podaci preneseni izvan Kompanije ili preko javnih komunikacijskih mreža će se anonimizirati ili će se zaštititi od neovlaštenog pristupa korištenjem enkripcije.

3.4.4 Svi prijenosi Osobnih podataka trećim osobama radi daljnje obrade će biti podložni pisanim sporazumima. Ured zaštite podataka će, u suradnji s odvjetnicima, razviti standardne odredbe i uvjete koji se mogu koristiti u te svrhe.
3.4.5 Osobni podaci EU se neće prenositi u državu ili teritorij izvan Europskog Ekonomskog Područja osim ako se prijenos ne obavlja u državu ili teritorij za kojega je EU priznala da ima adekvatni nivo pravne zaštite za prava i slobode Ispitanika u odnosu na obradu osobnih podataka ili je prijenos učinjen u suglasnosti s jednim od mehanizama koje EU prepoznaje da pruža adekvatnu zaštitu kada se prijenosi obavljaju državama ili teritorijima koji nemaju adekvatnu razinu pravne zaštite.
3.4.5.1 Unatoč odredbama pododjela 3.4.4. i 3.4.5., Osobni podaci mogu se prenijeti gdjegod se primjenjuje sljedeće:
(a) Ispitanik je dao pristanak na predloženi prijenos;
(b) Prijenos je nužan za ispunjenje ugovora između Ispitanika i Kompanije, ili za provođenje predugovornih mjera poduzetih u odgovoru na zahtjev Ispitanika;
(c) Prijenos je nužan za završetak ili izvršenje ugovora sklopljenog u interesu Ispitanika između Kompanije i treće strane;
(d) Prijenos je nužan ili zakonski obvezan radi razloga od važnog javnog interesa, ili za ustanovljenje, provođenje ili zaštitu od pravnih zahtjeva;
(e) Prijenos je obvezan na temelju zakona;
(f) Prijenos je nužan kako bi se zaštitili presudni interesi Ispitanika; ili
(g) Prijenos je učinjen između registra koji je prema zakonima ili regulacijama namijenjen pružanju informacija javnosti i koji je otvoren za pristup javnosti ili bilo kojoj osobi koja može dokazati legitimni interes.

3.5 Prevencija novih ili proširenih neusklađenih aktivnosti

3.5.1 Ni jedno novo ili prošireno djelovanje prikupljanja ili obrade koje uključuje Osjetljive podatke se ne može poduzeti bez prijašnjeg prikupljanja odobrenja od Koordinatora zaštite podataka.
3.5.2 Kako bi se dobilo odobrenje, poslovna jedinica će pružiti Koordinatoru zaštite podataka informacije identificirane u formularu procjene obrade podataka i bilo koje druge informacije koje Koordinator zaštite podataka zatraži.
3.5.3 **Informacijsko tehnološki odjel Kompanije**, u suradnji s **Koordinatorom zaštite podataka,** će uspostaviti proceduru radi procjene utjecaja svake nove uporabe tehnologije na privatnost i sigurnost Osobnih podataka. **Informacijsko tehnološki odjel** će uključiti takvu procjenu za svaki tako predložen novi ili prošireni način uporabe tehnoloških resursa u svojem procesu revizije primjene i pružiti će takve procjene **Koordinatoru zaštite podataka**.
3.5.4 Zaposlenici na svim razinama Kompanije će primijeniti sljedeće smjernice prilikom izrade novih sustava, načina uporabe ili procesa koji uključuju Osobne podatke i/ili revidiraju ili proširuju trenutne aktivnosti koje uključuju prikupljanje ili obradu Osobnih podataka:
3.5.4.1 Prikupljanje i korištenje Osobnih podataka će se izbjegavati ili ograničiti kada god to bude razumno moguće.
3.5.4.2 Osobni podaci će se anonimizirati kada svrha prikupljanja podataka ili obrade podataka može biti ostvarena uz razumne troškove bez održavanja osobne identifikacije.
3.5.4.3 Svrha ili svrhe prikupljanja ili obrade Osobnih podataka će biti izričito identificirane od strane poslovne jedinice koja priprema bilo koji novi ili prošireni oblik aktivnosti ili funkciju prikupljanja i obrade podataka.
3.5.4.4 Osobni podaci se mogu iskoristiti samo u svrhe za koje su izvorno prikupljeni, kao i za povijesne, statističke, znanstvene ili pravno naložene svrhe, osim ako je Ispitanik dao pristanak ili ako je primjenjiva iznimka postavljena u Odjelu 3.2.6.

3.6 Obavijesti u trenutku prikupljanja podataka

3.6.1 Prikladne obavijesti će se izvršiti u vrijeme kada se zatraži od Ispitanika da dade svoj pristanak za prikupljanje ili obradu Osobnih podataka, i kada god se Osobni podaci prikupljaju.

3.6.2 Ispitanik mora biti obaviješten o specifičnim informacijama i/ili o njima mora biti obaviještena bilo koja druga osoba od koje se Osobni podaci prikupljaju u trenutku prikupljanja, osim ako Ispitanik nije već o tome bio obaviješten. Poslovna jedinica koja prikuplja informacije, u suradnji s Koordinatorom zaštite podataka, mora ustanoviti tehničke ili administrativne mjere za dokumentiranje činjenice da je Ispitanik već bio obaviješten i na koji način.
3.6.3 Naprijed navedeni zahtjevi za obavještavanje se neće primijeniti ondje gdje se obavijest nije mogla izvršiti na razuman način u skladu s razmjernim troškovima i trudom u odnosu na važnost predložene obrade, ili gdje primjenjivi propisi dozvoljavaju iznimku za pretpostavke za obavijest i/ili pristanak.
3.6.4 Ako ne dolazi do primjene iznimaka, sljedeće informacije moraju biti pružene Ispitaniku i/ili bilo kojoj drugoj osobi od koje se Osobni podaci dobivaju u vrijeme prikupljanja:
3.6.4.1 Ime i adresa Kontrolora podataka i, ako je imenovan, ime i adresa unutar-državnog zastupnika za privatnost podataka unutar države članice EU voditelja obrade podataka.
3.6.4.2 Svrha (svrhe) prikupljanja, obrade i prijenosa podataka.
3.6.4.3 Da li je izvor podataka pod obvezom pribaviti podatke i posljedice u slučaju da to ne napravi.
3.6.4.4 Identitete, ili bar kategorije, fizičkih i pravnih osoba koje će ili bi mogle primiti podatke.
3.6.4.5 Može li doći do prijenosa podataka izvan Europskog ekonomskog područja i, ako da, mogu li ti prijenosi biti u državu koja nije bila određena da ima adekvatne zakone o zaštiti podataka prema EU.
3.6.4.6 Uvjeti prijenosa, kao primjerice obavlja li se prijenos sukladno proceduri koju je odobrilo Vijeće rada, prema ugovoru koji utjelovljuje Primjere ugovornih odredbi EU Komisije, Procedure Sigurne luke S.A.D.-a ili neki drugi mehanizam.
3.6.4.7 Pravo Ispitanika da pristupi, dobije primjerak, izbriše i ispravi podatke i sredstva za ostvarivanje tih prava.
3.6.4.8 Koliko dugo Ascendum pretpostavlja da će se Osobni podaci zadržati.
3.6.4.9 Procedure dostupne za rješavanje bilo kakvih sporova oko obrade osobnih podataka Ispitanika.
3.6.4.10 Bilo koje druge informacije nužne radi garancije "poštene obrade". Primjerice, gdje se podatak namjerava koristiti na način koji nije očigledan Ispitaniku, a o kojem bi trebao biti obaviješten.
3.6.5 Ove obavijesti se trebaju dati što prije moguće, i po mogućnosti u trenutku prvog kontakta s Ispitanikom. U slučaju zaposlenika, obavijesti se trebaju dati u ugovoru o radu (ako postoji). Prikladne obavijesti bi trebale biti dane i u svakom formularu za prijavu na posao ili priručniku za zaposlenike. Obavijesti se moraju pružiti na način da se privuče pozornost na njih.
3.6.6 Obavijesti se mogu dati usmeno, elektronski, putem unutarnjeg sustava Kompanije ili pismeno. Ako se daju usmeno, osoba koja daje obavijesti mora koristiti odgovarajuće bilješke ili formular koji je unaprijed odobrio Koordinator zaštite podataka. Potvrda ili formular se treba zadržati zajedno sa suvremenim arhivom koji utvrđuje način, datum, sadržaj i metodu obavještavanja.
3.6.7 Ako se u početku daju neadekvatne obavijesti, dodatne obavijesti mogu biti učinjene naknadno, a način, datum, sadržaj i metoda ovih naknadnih obavijesti će biti zabilježen.

3.7 Izvori osobnih podataka

3.7.1 Osobni podatak će se prikupljati samo od Ispitanika osim ako narav poslovne svrhe nalaže skupljanje podataka od ostalih osoba ili tijela, ili ako prikupljanje od Ispitanika traži nerazmjeran trud, ili ako se prikupljanje podataka vrši pod hitnim okolnostima kako bi se zaštitili interesi Ispitanika ili kako bi se spriječili veliki gubici ili ozljede drugoj osobi.
3.7.2 Ako se Osobni podaci prikupljaju osobe koje nisu Ispitanik, Ispitanik mora biti obaviješten o sljedećim stvarima, osim ako Ispitanik nije primio potrebne informacije kroz druga sredstva, ili ako bi obavijest tražila nerazmjerni trud ili ako zakon izričito nalaže prikupljanje, obradu ili prijenos Osobnih podataka:
3.7.2.1 Činjenica prikupljanja, obrade ili prijenosa podataka koju izvršava Kontrolor podataka;
3.7.2.2 Priroda i svrha obrade;
3.7.2.3 Primatelji ili kategorije primatelja podataka;

3.7.2.4 Porijeklo podataka; i
3.7.2.5 Informacije određene u Odjelu 3.6.4. iznad.
3.7.3 Poslovna jedinica, u suradnji s Uredom za zaštitu podataka, će napraviti formular ili sustav kako bi zabilježili i automatizirali ovaj postupak u što većoj mogućoj mjeri.
3.7.4 Obavijest Ispitaniku treba nastupiti brzo, ali ni u kojem slučaju kasnije od 3 mjeseca od prvog prikupljanja podataka ili snimanja Osobnog podatka od Kompanije.

3.8 Prava Ispitanika

3.8.1 Koordinator zaštite podataka će ustanoviti sustav kako bi omogućio i olakšao izvršavanje prava pristupa, sprječavanja, brisanja, protivljenja, ispravljanja Ispitanika i, gdje je to prikladno ili potrebno prema primjenjivim propisima, ustanovit će sustav radi davanja obavijesti o neprikladnoj izloženosti Osobnih podataka.
3.8.2 Ispitanici će biti ovlašteni dobiti sljedeće informacije o vlastitim Osobnim podacima na zahtjev postavljen u skladu s razumnim pravilima i procedurama koje su ustanovljene, i izložene u pisanom obliku, od strane Koordinatora zaštite podataka:
3.8.2.1 Da li je Kompanija spremila Osobne podatke koji se odnose na Ispitanika.
3.8.2.2 Da li je ikoji od podataka Osjetljiv podatak.
3.8.2.3 Izvor (izvori) podataka, ako su poznati.
3.8.2.4 Primatelji ili kategorije primatelja kojima su podaci dani ili mogli biti dani.
3.8.2.5 Svrha prikupljanja, obrade, korištenja i pohrane podataka.
3.8.2.6 Fizički primjerak podataka u razumljivom obliku.
3.8.3 Kompanija će pružiti svoj odgovor na zahtjev iz Odjela 3.8.2. unutar 40 dana od dana kada Kompanija primi pisani zahtjev Ispitanika i adekvatnu potvrdu da je podnositelj zahtjeva Ispitanik ili ovlašteni pravni zastupnik.
3.8.4 Ispitanici će imati pravo zahtijevati od Kompanije da ispravi ili nadopuni pogrešne, zavaravajuće, zastarjele ili nepotpune Osobne podatke.
3.8.5 Zahtjevi za pristup ili ispravak Osobnih podataka će biti usmjeren, prema izboru Ispitanika, menadžeru poslovne jedinice odgovorne za Osobni podatak ili Koordinatoru zaštite podataka.
3.8.6 Sve poslovne jedinice koje primaju zahtjev Ispitanika za pristup Osobnim podacima će o tome obavijestiti Koordinatora zaštite podataka.
3.8.7 Ured zaštite podataka će uspostaviti sustav za bilježenje svakog zahtjeva pod ovim Odjelom u trenutku zaprimanja i zabilježit će datum odgovora.
3.8.8 Ako Kompanija ne može u potpunosti odgovoriti na zahtjev unutar zapriječenog vremena, tada će odgovorna poslovna jedinica ili Ured za zaštitu podataka u svakom slučaju pružiti sljedeće informacije unutar zapriječenog vremena:

- Potvrdu primitka zahtjeva
- Obavijest o informacijama koje su pronađene do trenutka izdavanja obavijesti.
- Identifikaciju bilo koje od zahtijevanih informacija ili modifikaciju koju Kompanija neće pružiti, razloge za odbijanje, i procedure za žalbu na tu odluku unutar Kompanije, ako postoji ta mogućnost.
- Procjenu datuma do kojega će se preostali odgovori dati.
- Izjavu ili procjenu troškova koje će trebati platiti Ispitanik.
- Ime i kontakt informaciju od pojedinca koga Ispitanik može kontaktirati za nove obavijesti.

3.8.9 Kada pružanje informacija o Ispitaniku predstavlja davanje Osobnih podataka o drugom pojedincu, poslovna jedinica koja obrađuje takav zahtjev mora pregledati podatke i urediti ili zadržati informacije ako bi to bilo nužno ili prikladno za zaštitu prava te druge osobe.
3.8.10 Kompanija neće naplaćivati zaposlenicima za pružanje informacija navedenih iznad. **Koordinator zaštite podataka** može uspostaviti razumne naknade kako bi pokrio troškove odgovora na zahtjeve Ispitanika koji nisu zaposlenici.
3.8.11 Koordinator zaštite podataka može uspostaviti procedure kako bi razabrao i odbio napasno opterećujuće ili ponavljajuće zahtjeve Ispitanika ili one zahtjeve učinjene u njegovo ime.

3.9 Automatska odluka

Ako se poslovna jedinica upusti u bilo kakvo odlučivanje učinjeno isključivo na automatiziranoj primjeni unaprijed određenih pravila, Ispitanici moraju o tome biti obaviješteni. Ispitanici moraju imati mogućnost
(i) pregledati logiku koju koristi automatizirani sustav,
(ii) nadopuniti automatizirani sustav s dodatnim podacima i
(iii) zatražiti pregled automatizirane odluke od strane pojedinca.

3.10 Osjetljivi podaci

3.10.1 Osjetljivi podaci se ne mogu obrađivati osim ako:
3.10.1.1 Takvo obrađivanje nije posebno ovlašteno ili obavezno po zakonu
3.10.1.2 Ispitanik izričito na to pristane
3.10.1.3 Obrada je potrebna za preventivnu medicinu, medicinsku dijagnozu ili zdravstveni tretman; pod uvjetom da se podaci obrađuju po stručnjaku za zdravlje koji podliježe nacionalnim zakonima ili pravilima s obvezom profesionalne tajne ili po drugoj osobi s jednakom obvezom tajnosti. Ako se Kompanija oslanja na ovakvu medicinsku iznimku, svi ugovori sa zaposlenima i neovisnim ugovornicima koji će imati pristup Osjetljivim podacima moraju imati zahtjeve povjerljivosti jednake onima koji se nameću stručnjacima za zdravlje.
3.10.1.4 Ako je Ispitanik fizički ili pravno nesposoban za davanje suglasnosti, ali je obrada nužna radi zaštite presudnih interesa Ispitanika. Ova iznimka se može primijeniti, primjerice, gdje je hitna medicinska njega potrebna.
3.10.1.5 Podaci koji se odnose na kaznene prijestupe mogu biti obrađeni samo pod kontrolom službene vlasti
3.10.2 Ako se Kompanija oslanja na jednu od ovih iznimaka kako bi bila ovlaštena za obradu Osjetljivih podataka, iznimka na koju se poziva i osnova za iznimku treba biti zabilježena zajedno s podacima.

3.11 Izravno oglašavanje

Kada se Osobni podaci prenose radi izravnog oglašavanja, Ispitanik treba imati mogućnost „opt-outa“ od toga da se njegovi/njezini podaci koriste za takve svrhe u bilo kojoj fazi.

3.12 Osiguravanje kvalitete podataka

3.12.1 Svaka poslovna jedinica će poduzeti potrebne korake kako bi osigurala da Osobni podaci koje prikuplja ili obrađuje budu potpuni i točni u prvom stupnju. Podaci moraju biti točni i obnavljani na način da bi dali pravu sliku trenutne situacije o Ispitaniku.
3.12.2 Kompanija će ispraviti podatke za koje zna da su pogrešni, netočni, nepotpuni, dvojaki, navodeći ili zastarjeli, čak i ako Ispitanik ne zatraži ispravak. Netočni podaci moraju biti izbrisani i zamijenjeni točnima ili nadopunjenima.
3.12.3 Osobni podaci se moraju čuvati samo na razdoblje nužno za dopuštene svrhe. Kada se definira dopuštena svrha podataka, poslovna jedinica će ustanoviti krajnji rok ili datum revizije za tu određenu svrhu.
3.12.4 Osobni podaci trebaju biti izbrisani ako njihova pohrana krši pravila zaštite podataka ili ako znanje o podacima više nije potrebno Kompaniji ili ako je to u korist Ispitanika.
3.12.5 Osobni podaci trebaju biti zablokirani, prije nego budu izbrisani, ako zakon brani brisanje, ako bi brisanje umanjilo legitimne interese Ispitanika, ako brisanje nije moguće bez nerazmjernog truda obzirom na specifičan način skladištenja; ili ako Ispitanik osporava da su podaci točni i ne može se utvrditi jesu li točni ili netočni.

3.13 Obavijest o ispravku

Ako se Osobni podaci isprave, Kontrolor podataka mora obavijestiti bilo koga kome je podatak prenesen da je podatak ispravljen.

3.14 Proporcionalnost

Ova pravila će se primijeniti na razuman način, uz razmjeran trud i trošak u odnosu na važnost predloženih načina obrade i osjetljivosti podataka o kojima se radi.

4.0 Obavijest

Obavijest nadležnima za privatnost podataka u odnosu na Ascendumove aktivnosti obrade

Ascendum neće obrađivati Osobne podatke bez obavijesti nadležnim tijelima zaštite podataka u nadležnostima koje zahtijevaju takve podatke. Koordinator zaštite podataka će obavijesti držati ažurnima u svakom trenutku.

5.0 Korištenje trećih osoba za obradu podataka.

5.1 Pretpostavke za korištenje trećih osoba za obradu podataka. Kada se Kompanija oslanja na druge da joj pomogne u njenim aktivnostima obrade podataka, Kompanija će izabrati obrađivača podataka koji pruža dovoljno mjera osiguranja i poduzima razumne korake kako bi osigurao usklađenost s tim mjerama.

5.2 Pisani ugovori za treće osobe za obradu podataka. Ascendum će ući u pisani ugovorni odnos sa svakom osobom za obradu podataka obvezujući ga da se uskladi sa zahtjevima zaštite i sigurnosti podataka koja su nametnuta Ascendumu lokalnom legislativom.

5.3 Revizije za treće osobe za obradu podataka. Kao dio Ascendumovog unutarnjeg procesa revizije, Ascendum će obavljati redovite provjere trećih osoba za obradu podataka, posebice u odnosu na mjere sigurnosti.

6.0 Obavijest Direktorima, menadžerima, i službenicima o potencijalnim sankcijama za neusklađenost

Ured za zaštitu podataka će obavijestiti direktore, menadžere i ostale službenike Ascenduma da:
i) neusklađenost s relevantnom legislativom zaštite podataka može biti povod za kaznenu i građansku odgovornost, što može uključivati novčane kazne, kazne zatvora i naknadu štete; i
ii) mogu biti osobno odgovorni kada Ascendum prijestup počini s njihovim pristankom ili prešutnim pristankom ili se kršenje može pripisati bilo kakvom nemaru s njihove strane.

7.0 Sigurnost podataka

7.1 Fizičke, tehničke i organizacijske mjere sigurnosti

7.1.1 Kompanija će usvojiti fizičke, tehničke, i organizacijske mjere kako bi osigurala sigurnost Osobnih podataka, uključivo i prevenciju njihova mijenjanja, gubitka, oštećenja, neovlaštene obrade ili pristupa, imajući na umu stanje tehnologije, prirodu podataka i rizike kojima su izloženi kroz ljudsku djelatnost ili fizičku ili prirodnu okolinu.
7.1.2 Adekvatne mjere sigurnosti trebaju uključivati sljedeće:
7.1.2.1 Kontrola ulaska: Prevencija neovlaštenih osoba da zadobiju pristup sustavima obrade podataka u kojima se obrađuju Osobni podaci.
7.1.2.2 Kontrola pristupa: Prevencija korištenja sustava obrade podataka od neovlaštenih osoba.
7.1.2.3 Kontrola prilaza: Prevencija osoba koje su ovlaštene koristiti sustav obrade podataka od prilaza podacima koji su izvan njihovih potreba i odobrenja. Ovo uključuje sprečavanje neovlaštenog čitanja, kopiranja, modificiranja ili micanja za vrijeme obrade i korištenja ili poslije pohrane.
7.1.2.4 Kontrola obavještavanja: Osiguravanje da Osobni podaci u tijeku elektronskog prijenosa tijekom transporta ili za vrijeme pohrane na nosaču podataka ne mogu biti pročitani, kopirani,

modificirani ili maknuti bez ovlaštenja, i pružanje mehanizma za provjeru kako bi se ustanovilo tko je ovlašten primiti ili tko je primio informacije.
7.1.2.5 Kontrola ulaznih informacija: Osiguravanje da se može naknadno provjeriti i utvrditi da li su i od koga Osobni podaci dirani, modificirani ili maknuti iz sustava obrade podataka.
7.1.2.6 Kontrola poslova: Osiguravanje da u slučaju naručene obrade Osobnih podataka, podaci mogu biti obrađivani samo u skladu s uputama Kontrolora podataka.
7.1.2.7 Kontrola dostupnosti: Osiguravanje da su Osobni podaci zaštićeni od neželjenog uništenja ili gubitka.
7.1.2.8 Kontrola korištenja: Osiguranje da se podaci prikupljeni u različite svrhe mogu obrađivati odvojeno i da će se tako i obrađivati.
7.1.2.9 Kontrola dugotrajnosti: Osiguravanje da se podaci ne drže dulje nego što je potrebno, uključivo i obvezivanje da se podaci preneseni na treće osobe vraćaju ili unište.

7.2 Ugovori o tajnosti sa zaposlenicima.
Sve osobe uključene u bilo kojem stadiju obrade Osobnih podatka trebaju izričito biti podvrgnute obvezi tajnosti koja se treba nastaviti i nakon što se radni odnos prekine.

8.0 Rješavanje sporova

8.1 Zaposlenici
8.1.1 Zaposlenici s upitima ili primjedbama oko obrade njihovih Osobnih podataka trebaju prvo raspraviti to s neposredno nadređenima. Ako Ispitanik ne želi postaviti upit ili primjedbu s neposredno nadređenim, ili ako nadređeni i Ispitanik nisu u mogućnosti postići zadovoljavajuće rješenje postavljenih problema, zaposlenik treba problem prijaviti u pisanom obliku **Koordinatoru za zaštitu podataka**.
8.1.2 Ako se problem ne može riješiti kroz konzultacije s zaposlenikovim nadređenim ili Koordinatorom za zaštitu podataka, riješit će se na sljedeći način:
8.1.2.1 Kroz Proceduru zajedničke odluke gdje se ona može primijeniti, ili kroz drugi sličan ne sudski postupak koji je uspostavljen primjenjivim radnim sporazumima, sporazumom sindikata ili odredbama statuta koje se mogu primijeniti na pojedine osobe.
8.1.2.2 U slučaju podataka ljudskih resursa koji se odnose na zaposlenike u Europskoj uniji, zaposlenik koji nije zadovoljan s rezultatima unutarnje revizije, prigovora i postupka žalbi (ili bilo kojeg drugog postupka za rješavanje pritužbi reguliranim ugovorom sa trgovinskom unijom) će biti upućen na državu ili nacionalno ovlašteno tijelo za zaštitu podataka ili rada u nadležnosti prema mjestu rada zaposlenika.

8.2 Osobe koje nisu zaposlenici.
Osobe koje nisu zaposlenici s upitima ili pritužbama oko obrade njihovih Osobnih podataka trebaju dati na znanje sporno pitanje Koordinatoru zaštite podataka u pisanom obliku. Svi sporovi koji se tiču obrade Osobnih podataka osoba koje nisu zaposlenici će se rješavati kroz arbitražu.

8.3 Žalbe.
Ako se problem ne riješi kroz konzultacije s nadređenim Ispitanika ili Koordinatorom zaštite podataka, ili kroz druge mehanizme pod postojećim ugovorima o radu, sporazumima sindikata ili odredbama statuta, tada Ispitanik može, prema svom izboru, tražiti obeštećenje kroz medijaciju, obvezujuću arbitražu, parničenje, ili prigovor ovlaštenom tijelu za zaštitu podataka koje ima nadležnost (kako je dozvoljeno primjenjivim pravom ili procedurom).

9.0 Osposobljavanje.

Svaka poslovna jedinica će pružiti osposobljavanje kako bi naučila ili ponovno naglasila procedure vezane za privatnost i sigurnost. Te procedure će se postaviti u pisanim smjernicama zaposlenicima i uključivat će najmanje sljedeće:

- Dužnost svakog zaposlenika da koristi i dopusti korištenje Osobnih podataka samo po naredbi ovlaštenih osoba i samo za ovlaštene svrhe;
- Načela zaštite podataka uspostavljena u Odjelu 3.2;
- Sadržaje ovih Pravila;
- Odnos između ovih pravila i ostalih Ascendumovih pravila, uključujući bez ograničenja ona navedena u odjelu 10.2.;
- Potrebu za ispravnim korištenjem formulara i postupaka prihvaćenih i uvedenih ovim Pravilima;
- Ispravno korištenje lozinkama, sigurnosnim tokenima i ostalim mehanizmima pristupa;
- Važnost ograničavanja pristupa Osobnim podacima, kao korištenje lozinkom zaštićenih čuvara ekrana, odjavljivanja kada se informacija ne koristi ili pazi po ovlaštenoj osobi;
- Sigurno skladištenje ručnih datoteka, ispisa i elektronskih medija pohrane;
- Općenitu zabranu prijenosa Osobnih podataka izvan interne mreže i fizičkog uredskog porstora;
- Pravilno rješavanje povjerljivih datoteka rezanjem, i slično;
- Posebni rizici povezani s pojedinim aktivnostima.

9.1 Osposobljavanje menadžera prvog i drugog reda

Ascendum Central Europe Grupa je posvećena usklađivanju s primjenjivim zahtjevima za zaštitu podataka i sigurnosti u državama u kojima ona i njihove podružnice ("Kompanija") djeluju.

Stoga Ascendum pruža za svoje menadžere prvog i drugog reda sljedeće treninge:

1. Profesionalni osnovni trening zaštite podataka
2. Godišnje upute za zaštitu podataka
3. Obnavljanje treninga zaštite podataka (ako je potrebno)

9.2 Osposobljavanje redovnih zaposlenika

Za redovne zaposlenike će se pružiti sljedeći treninzi za zaštitu podataka, ako zaposlenici rade s osjetljivim kadrovima:

1. Profesionalni osnovni trening zaštite podataka
2. Godišnje upute za zaštitu podataka
3. Obnavljanje treninga zaštite podataka (ako je potrebno)

10.0 Posebna pravila za pojedine države.

10.1 Specifična pravila države.

Ured zaštite podataka može objaviti smjernice koje se primjenjuju u pojedinim državama.

10.2 Integracija s ostalim Ascendum pravilima.

Ako je Ascendum izdao druga pravila specifično primjenjiva na pojedine države ili područja, ta pravila će imati prednost pred ovim Pravilima.

10.3 Ograničeni učinak pravila.

Ova Pravila neće biti tumačena niti konstruirana na način da ijednom pojedincu daje prava veća od onih na koje bi ta osoba imala pravo pod primjenjivim pravom i drugim obvezujućim sporazumima.

11.0 Mjerenje usklađenosti.

11.1 Procjena trenutne usklađenosti.

Koordinator zaštite podataka će ustanoviti raspored revizije o usklađenosti zaštite podataka i implementirati ju za sve poslovne jedinice. **Koordinator zaštite podataka,** će u suradnji s poslovnim jedinicama razraditi plan i program za ispravljanje bilo kakvih uočenih manjkavosti unutar fiksnog i razumnog vremena.

11.2 Godišnja revizija zaštite podataka.

Svaka poslovna jedinica će godišnje revidirati svoju zbirku podataka, obradu i sigurnosne postupke. Ova godišnja revizija će se sastojati od najmanje sljedećega:

11.2.1 Poslovna jedinica će ustanoviti koje Osobne podatke poslovna jedinica prikuplja ili namjerava prikupiti, svrhe prikupljanja i obrade podataka, sve dodatne dopuštene svrhe, stvarno korištenje podataka, postojanje i doseg bilo kojih pristanaka Ispitanika na takve aktivnosti, bilo koje pravne obveze vezane uz prikupljanje i obradu takvih podataka, i doseg, samodostatnost i implementaciju statusa sigurnosnih mjera.

11.2.2 Poslovna jedinica će odrediti koje Osobne podatke ima u ručnim sustavima koji predstavljaju „relevantne sustave arhiviranja“.

11.2.3 Poslovna jedinica će identificirati sve prijenosnike Osobnih podataka u njenom posjedu ili pod njenom kontrolom. Poslovna jedinica će odrediti gdje su prijenosnici locirani, svrhu prijenosa, koje fizičke, tehničke i proceduralne sustave su uspostavili kako bi održavali u najmanju ruku postojeću razinu zaštite podataka i kako bi spriječili ili kontrolirali buduće prijenose.

11.2.4 Informacije prikupljene u ovoj godišnjoj reviziji će biti dostavljene **Koordinatoru zaštite podataka** na pregled i poduzimanje prikladnih radnji uključivo, bez ograničenja, sljedeće:

- Izrada preporuka za unaprjeđenje pravila i procedura kako bi se unaprijedila usklađenost s ovim pravilima i primjenjivim pravom.

12.0 Implementacija.

12.1 Objava.

Ova pravila će biti dostupna zaposlenicima kroz Odjel ljudskih resursa ili putem drugih sredstava obavijesti koja sredstva Koordinator zaštite podataka utvrdi prikladnima.

12.2 Datum stupanja na snagu.

Ova Pravila su usvojena 1. svibnja 2018. godine. **Koordinator zaštite podataka** će, u suradnji s **Poslovnim jedinicama**, razviti vremenski tijek i program za implementaciju ovih Pravila. Taj program implementacije će uključivati rješavanje bilo kojih sukoba između ovih Pravila i drugih postojećih pravila.

12.3 Revizije.

Ova Pravila se mogu revidirati u bilo kojem trenutku. Obavijesti o značajnim revizijama će biti pružene zaposlenicima kroz Odjel ljudskih resursa i ostalim osobama kroz prikladne mehanizme koje odabere **Koordinator zaštite podataka.**

13.0 Sponzor.

Sponzor ovih Pravila je **Koordinator zaštite podataka**. **Koordinator zaštite podataka** je odgovoran za održavanje i točnost ovih Pravila. Bilo koja pitanja vezana za ova Pravila trebaju biti usmjerena **Koordinatoru zaštite podataka.**

14.0 Čuvar.

Čuvar ovih Pravila je **Koordinator zaštite podataka**. Svaki menadžer poslovne jedinice je odgovoran za implementaciju Pravila. Sva pitanja vezana za implementaciju ovih pravila trebaju biti usmjerena **Koordinatoru zaštite podataka**.

15.0 Odvojivost.

Kada god je to moguće, svaki Odjel ovih Pravila će se tumačiti na način da bi bio valjan u odnosu na primjenjivo pravo, ali ako bilo koja odredba bude zabranjena ili nevaljana, takva odredba će se smatrati bez učinka samo u mjeri u kojoj je zabranjena odnosno nevaljana, bez da povlači nevaljanost ostatka te odredbe ili nevaljanost ostalih odredaba ovih Pravila.

16.0 Druga Ascendum pravila

- Ascendum pravila ponašanja
- Ascendum smjernice za pravo tržišnog natjecanja

17.0 Rječnik

17.1 Pristanak znači „bilo koji slobodno dan specificiran i informiran indicij volje kojim Ispitanik daje do znanja svoju suglasnost za obradu Osobnih podataka koji se odnose na njega.“ Riječi „daje do znanja“ znače da mora postojati neki oblik aktivne komunikacije između stranaka. U tom smislu, puko ne odgovaranje komunikaciji Ascenduma ne može imati značenje pristanka. Unatoč tome, pristanak se može zadobiti na više načina. Oni mogu uključivati odredbe u ugovorima o radu, kućice za popunjavanje na odgovorima za formulare prijave ili kupnje, i kućice za označavanje na online formularima gdje se unose Osobni podaci. U većini zemalja Europske Unije, pristanak obradi Osjetljivih osobnih podataka mora biti izričit i nedvosmislen. Ovo u pravilu znači da je potreban određen oblik specifičnog, aktivnog pristanka (vidi Odjel 17.7. „opt-in“ pristanak). Postoji veća raznolikost u nacionalnim pristupima kada dolazi do odlučivanja što ustanovljuje pristanak za obradu drugih vrsta Osobnih podataka. Neke nadležnosti koriste manje restriktivan pristup, i prihvaćaju koncept implicitnog pristanka (vidi Odjel 17.8 „opt-out“ pristanak“) u ograničenim okolnostima. Za svrhu Ascendumove usklađenosti, i u interesu jedinstvenih Pravila koja će biti prihvatljiva u svim državama izvan Europske Unije, Ascendum će pratiti „opt-in“ formu aktivnog pristanka. Pristanak je ograničen za specifične svrhe koje su objavljene pojedincu. Daljnje obavijesti i pristanak je potreban za nove aktivnosti obrade koje prekoračuju one za koje je pristanak izvorno dan. U kontekstu aktivnosti sakupljanja novih podataka za koje pristanak nije bio ranije dan, dodatni pristanak je potreban. Tako, ako su podaci prikupljeni pod izvornim pristankom naknadno nadodani ostalim podacima u svrhu prijenosa nadodanih podataka trećim osobama i/ili preko mora, izvorni pristanak vjerojatno nije pokrio ovu kasniju aktivnost, te zahtijeva dodatni pristanak specifičan za novo korištenje podataka. U slučaju Osjetljivih podataka, sva europska prava se slažu oko „opt-in“ pristupa. Pristanak Ispitanika mora biti dostavljen Ascendumu prije nego bilo koja obrada nastupi, osim ako se primjenjuje iznimka. One uključuju obradu podataka koju nalaže radno pravo, slučajeve u kojima je nemoguće da Ispitanik da suglasnost i slučajeve gdje su podaci koji se obrađuju javna informacija ili informacija uglavnom namijenjena za javnost. Pojedine države mogu pružiti dodatne iznimke iz razloga znatnog javnog interesa. Bilo koja obrada osjetljivih osobnih podataka koja nije potrebna za pravilno poslovno djelovanje Ascenduma mora biti izbrisana.

17.2 Podatak (bilo da ima ili nema veliko prvo slovo) kada se koristi u ovim Pravilima će značiti informaciju koja (alternativno):

- se obrađuje putem opreme koja djeluje automatski u odgovoru na upute koje su dane za tu svrhu;
- se snima s namjerom da će se obrađivati sredstvima takve opreme;
- se snima kao dio relevantnog sustava arhiviranja ili s ciljem da će sačinjavati dio relevantnog sustava arhiviranja;
- ne spada niti pod jedno od navedenoga, ali tvori dio lako pristupačnog zapisnika koji pokriva pojedinca. Podatak stoga uključuje bilo koji digitalni podatak kompjutora ili automatske opreme, i bilo koju ručnu informaciju koja je dio odnosnog sustava arhiviranja.

17.3 Voditelj obrade označava osobu koja (samostalno ili s drugima) određuje svrhe i način na koji se bilo koji Osobni podatak obrađuje ili će biti obrađen. Općenito, Ascendum će biti Kontrolor podataka, iako može postojati više od jednog kontrolora podataka unutar grupe tvrtki ako lokalni uredi, podružnice ili povezani uredi unutar grupe uživaju određenu razinu autonomije u odnosu na obradu osobnih podataka koje koriste.

17.4 Izvršitelj obrade označava bilo koju osobu, osim zaposlenika Kontrolora podataka, koja obrađuje podatke u ime Kontrolora podataka.

17.5 Ispitanik označava osobu na koju se podaci odnose. Ispitanici uključuju korisnike i korisnike interneta, pojedince na popisu kontakata/e-pošte ili marketinške baze podataka, zaposlenike, izvođače i dobavljače.

17.6 EU osobni podaci podrazumijevaju Osobne podatke koje prikuplja ili obrađuje subjekt osnovan u državi članici Europske unije ili koji je obrađen na opremi koja se nalazi u državi članici Europske unije, osim za obradu koja se sastoji isključivo od prijenosa osobnih podataka.

17.7 Opt-in se odnosi na sustav putem kojeg kontrolori podataka dobivaju specifičan pristanak od Ispitanika prije nego što se osobni podaci Ispitanika obrađuju ili na neki drugi način koriste za određenu svrhu.

17.8 Opt-out se odnosi na sustav putem kojeg kontrolori podataka smatraju da je pristanak dan, osim ako Ispitanik izričito ne odluči odbiti da se njegovi osobni podaci obrađuju ili na neki drugi način koriste za određenu svrhu od strane kontrolora podataka.

17.9 Osobni podatak označava podatke koji se odnose na živućeg pojedinca koji se može identificirati iz tih podataka ili od onih podataka i drugih informacija koje posjeduju ili je vjerojatno da će doći u posjed, Kontrolora podataka ili Obrađivača podataka.

17.10 Obrada obuhvaća široki spektar poslova koji se odnose na podatke, uključujući dobivanje, snimanje ili držanje podataka ili obavljanje bilo kakvih operacija ili skupa operacija na podacima, uključujući:

• Organizaciju, prilagodbu ili izmjenu;
• objavljivanje putem prijenosa, diseminacije ili na drugi način; i
• usklađivanje, kombinaciju, blokiranje, brisanje ili uništavanje.

17.11 Relevantni sustav arhiviranja označava bilo koji skup podataka koji se odnose na pojedince, bilo da se čuvaju u ručnim ili elektronskim datotekama, strukturiranim, bilo na temelju pojedinosti pojedinaca, ili prema kriterijima koji se odnose na pojedince, tako da su specifične informacije vezane za određenu osobu lako dostupne. Stoga se svaka digitalna baza podataka i/ili organizirane ručne

datoteke koje se odnose na potencijalno identificirane životne pojedince spadaju u doseg zakona i propisa o zaštiti podataka, dok baza podataka čistih statističkih ili financijskih podataka (koje se ne mogu izravno ili neizravno povezati s pojedincima koji se mogu identificirati) neće spadati u taj doseg.

17.12 Osjetljivi podaci označavaju Osobne podatke koji sadrže informaciju o Ispitaniku:

- Njegovoj rasi ili etničkom podrijetlu;
- Vjerskim uvjerenjima ili drugim uvjerenjima slične prirode;
- Političkim uvjerenjima;
- Fizičkom ili mentalnom zdravlju odnosno stanju;
- Spolnoj povijesti ili orijentaciji;
- Članstvu u trgovinskim sindikatima;
- Počinjenju ili navodnom počinjenju bilo kakvog prekršaja i povezanih sudskih postupaka.

17.13 Tehnologija

se treba tumačiti široko i uključuje bilo koji način prikupljanja ili obrade podataka, uključujući, bez ograničenja, računala i mreže, telekomunikacijske sustave, uređaje za snimanje videozapisa i zvuka, biometrijske uređaje, televiziju zatvorenog kruga itd.

18.0 Primjeri

18.1 Primjer A –Koordinator zaštite podataka – glavni službenik za usklađivanje

Glavni službenik za usklađivanje – Ascendum Worldwide:

tbd

Koordinator za zaštitu podataka – Ascendum CEG:

tbd

II. Proceduralni imenik zaštite podataka

1. Ascendum Central Europe GmbH – Ascendum Baumaschinen Österreich GmbH

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

2. Ascendum Stavebne stroje Slovensko s.r.o.

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

3. Ascendum Stavebni stroje Czech s.r.o.

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

4. Ascendum Építőgépek Hungária Kereskedelmi Kft.

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

5. Ascendum građevinski strojevi Hrvatska d.o.o.

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

6. Ascendum Machinery s.r.l.

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne
1	Proces apliciranja	24.9.2017	09.02.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne
2	Pristupanje	24.9.2017	09.02.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da
3	Postupak održavanja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da
4	Postupak razvoja zaposlenika	24.9.2017	09.02.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne
5	Program evaluacije i tumačenja podataka	24.9.2017	09.02.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne
6	Postupak specijalne koristi	24.9.2017	09.02.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne

7. Javni proceduralni imenik

Zakonom o zaštiti podataka propisano je da Koordinator zaštite podataka mora staviti sljedeće informacije na raspolaganje:

1. Naziv nadležnog tijela
2. Voditelj nadležnog tijela
3. Adresa odgovorne vlasti
4. Namjena svrhe prikupljanja, obrade ili uporabe podataka
5. Opis grupa zainteresiranih osoba i kategorija podataka ili podataka u tom smislu
6. Primatelji ili kategorije primatelja, koji se mogu obavijestiti o podacima
7. Standardni rokovi za brisanje podataka
8. Planirani prijenos podataka u treće zemlje

Javni proceduralni imenik pripremit će se za svaku tvrtku unutar Ascendum Central Europe Grupe i bit će objavljen na sljedećim web stranicama:

www.ascendum.at

www.ascendum.hr

www.ascendum.hu

www.ascendum.cz

www.ascendum.sk

www.ascendum.ro

Detaljni proceduralni imenik molimo da pronađete na sljedećem LINK-u:

Primjerak austrijskog javnog proceduralnog imenika:

Javni proceduralni imenik

Zakon o zaštiti podataka (DSG) nalaže da će Koordinator zaštite podataka učiniti sljedeće podatke dostupnima sukladno članku 26 DSG:

1. Ime odgovorne vlasti:
Ascendum Central Europe GmbH (CEG)
Ascendum Baumaschinen Osterreich GmbH (ABO)

2. Čelnik odgovornog tijela
CEG: Predsjednik i izvršni director: Dr. Thomas Michael Schmitz
ABO: Direktor uprave: Dr. Thomas Michael Schmitz

3. Adresa odgovornog tijela:
Ascendum Central Europe GmbH, Grafenholzweg 1

III. Zaštita podataka – ugovori usluge privatnosti podataka

1. Ugovor o uslugama prema općoj uredbi o zaštiti podataka

Detaljan ugovor o uslugama sukladno općoj uredbi o zaštiti podataka možete naći na sljedećem LINK-u:

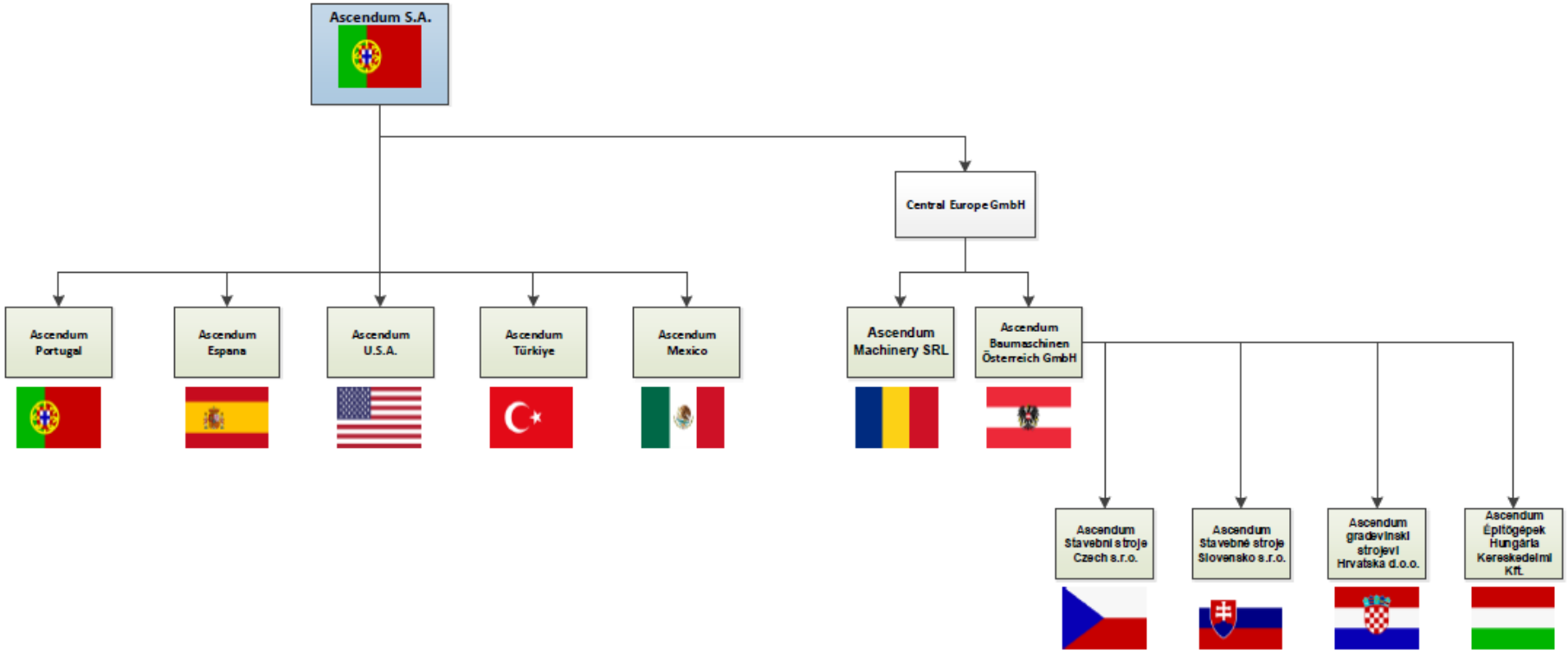
Ugovor o uslugama prema općoj uredbi o zaštiti podataka
zaključen između
….
….
….
….
u daljnjem tekstu „Kompanija“
….
….
….
….
u daljnjem tekstu „Dobavljač“

Aneks
Ovaj aneks uređuje obveze Stranaka vezane za zaštitu podataka koja je posljedica širine obrade osobnih podataka u ime kako je definirano u detalje u Sporazumu
….
Odnosit će se na sve aktivnosti unutar dosega Sporazuma i vezane uz Sporazum, u odnosu na kontekst u kojem Dobavljač, njegovi zaposlenici ili podizvođači mogu doći u doticaj s osobnim podacima Kompanije i podacima koje vrijedi zaštititi

Ugovor o uslugama prema općoj uredbi o zaštiti podataka mora se prilagoditi potrebama određenog ugovora s bilo kojim dobavljačem ili bilo kojom drugom osobom koja radi s podacima osoblja Ascendum grupe.

2. Ugovor o privatnosti podataka – zaštiti podataka unutar Kompanije

Preusmjeravajući se na sljedeću organizacijsku strukturu Ascendum grupe širom svijeta, stvoren je ugovor o zaštiti podataka i podacima o zaštiti podataka među tvrtkama kako bi se osigurala pravna i pravilna obrada svih podataka o osoblju pod Ascendum Central Europe Group.



Detaljan Ugovor o privatnosti podataka – zaštiti podataka unutar Kompanije možete naći na sljedećem LINK-u:

IV. Vodič za postupanje u slučaju povrede podataka[2]

Provjerite jesu li državne vlasti za zaštitu podataka imale bilo kakve rokove do kada nacionalno društvo mora obavijestiti nacionalna tijela za zaštitu podataka o ozbiljnim povredama podataka. Treba uzeti u obzir sljedeće čimbenike prilikom odlučivanja hoće li se prijaviti povreda državnim tijelima za zaštitu podataka:

1.0 Procedura

Ovaj plan odgovora na kršenje podataka (Plan odgovora) određuje postupak koji osoblje Ascenduma treba poštivati u slučaju da kod Ascenduma dođe do povrede podataka ili u slučaju sumnje da je došlo do povrede podataka.

Do povrede podataka dolazi kada se osobni podaci (definirani u I. 17.9 Osobni podaci) gube ili su podvrgnuti neovlaštenom pristupu, izmjeni, korištenju ili otkrivanju ili nekoj drugoj zlouporabi. Osobni podaci odnose se na podatke koji identificiraju ili razumno identificiraju pojedinca.

Također će doći do povrede podataka kada se zaštićeni podaci Ascenduma protupravno koriste ili otkrivaju. "Zaštićeni podaci Ascenduma" obuhvaćaju širi raspon informacija od "osobnih podataka" jer uključuje informacije o svim entitetima, a ne samo o pojedincima.

Iako se proces naveden u ovom Planu odgovora odnosi na sve povrede podataka, važno je napomenuti da u nekim slučajevima odredbe o tajnosti mogu postaviti strože standarde Ascendumu od onih sadržanih u ovom Planu odgovora. Dakle, ako povreda uključuje "zaštićene informacije Ascenduma", plan odgovora i zakonodavstvo moraju se razmatrati zajedno.

Također je važno napomenuti da su razna nacionalne tijela za zaštitu podataka zabrinuta samo zbog povreda osobnih podataka. Povrede podataka koje uključuju "zaštićene informacije Ascenduma" koje nisu "osobne informacije" ne moraju biti prijavljene različitim državnim tijelima.

Sukladnost s Planom odgovora osigurat će da Ascendum pravodobno može zadržati, procijeniti i reagirati na povrede podataka u zadanom vremenu kako bi ublažio potencijalnu štetu pogođenih osoba.

Ovaj plan:

a. utvrđuje uloge i odgovornosti osoblja;
b. utvrđuje kontakt podatke odgovarajućeg osoblja u slučaju povrede podataka; i
c. navodi postupak koji će se slijediti u slučaju povrede podataka

1.1 Ascendum djelatnik obavještava direktora

Odmah obavijestite svog direktora o sumnji na povredu podataka. Snimite i savjetujte svog ravnatelja o vremenu i datumu otkrivanja sumnje postojanja povrede, o vrsti informacija koje su uključene, o uzroku i opsegu povrede te o kontekstu informacija o kojima je riječ i o povredi.

[2] "Australska komisija za neprofitne i dobrotvorne (AU), https://www.acnc.gov.au/ACNC/Publications/Procedure_PDFs/OP_databreach.aspx?TemplateType=P , zadnji put pristupljeno 27.04.2018, u 11:45"

1.2 Direktor procjenjuje povredu

Direktor mora procijeniti i utvrditi je li došlo do povrede podataka. Ako direktor ima bilo kakvu sumnju da je došlo do povrede, direktor mora odmah obavijestiti odvjetnika i izvršnog direktora.

1.3 Izvršni direktor (i ostali relevantni direktori) procjenjuju ozbiljnost povrede

U nekim slučajevima manje povrede se mogu razriješiti na razini direktora. Ako se na razini direktora rješavaju manje povrede, moraju se zabilježiti sljedeći podaci:

a. opis povrede ili sumnje na povredu;
b. radnje koje poduzima ravnatelj ili član osoblja Ascenduma kako bi se riješio povreda ili sumnja na povredu;
c. ishod tog djelovanja;
d. potpis izvršnog direktora da se ne traži daljnja akcija; i
e. potvrdu da je incident zabilježen u Ascendumovom zapisniku incidenata povreda podataka.

Zapis se mora spremiti s mapom ispod sljedećeg LINK-a:

Ako je povreda ozbiljna, mora se odmah proslijediti Ekipi za odgovor na povrede podataka

1.4 Ekipa za odgovor na povredu podataka

kontakt osobe:

Koordinator zaštite podataka:

Austria
tbd, +43 664 / 851 0669,

Ekipa za odgovor uključuje:

Pravna služba:

Austria
Pressl Endl Heinrich Bamberger Rechtsanwälte GmbH
Dr. Christoph Bamberger, +43 662 / 82 70 70, office@pehb.at
Dr. Johannes Neumann, +43 662 / 82 70 70, office@pehb.at

Informatički tehničari:

Austria
Leonhard Haberpointner, +43 664 / 967 24 23, leonhard.haberpointner@ascendum.at
Franz Wallinger, +43 664 / 921 3602, franz.wallinger@ascendum.at

Komunikacije:

Austria
Matthias Auer, +43 664 / 260 34 29, matthias.auer@ascendum.at
Johannes Böckl, +43 664 / 851 06 69, johannes.boeckl@ascendum.at

Hrvatska
Gordana Božiček, +38 5 16 59 4336, gordana.bozicek@ascendum.hr
Mirza Jurić, +38 5 16 59 4330, mirza.juric@ascendum.hr

Nije nužno da svi članovi tima za odgovor budu uključeni u sve odgovore na povrede podataka. Međutim, ako je uprava bila pogođena ili je bila uključena u povredu ili gdje uprava može pomoći u ublažavanju štete uzrokovane povredama, u odgovor se mora uključiti navedeni ili delegirani primarni ili sekundarni kontakt.

2.0 Proces:

Nakon što se predmet proslijedi ekipi za odgovor, mora se slijediti postupak naveden u nastavku. Ekipa za odgovore mora raditi u dogovoru s Izvršiteljima u odgovoru na povredu. Svaka povreda se mora rješavati od slučaja do slučaja, poduzimajući procjenu rizika koji su uključeni i korištenje te procjene rizika kao osnova za odlučivanje o aktivnostima koje će se poduzeti u danim okolnostima.

Postoje četiri ključna koraka koje valja razmotriti kada se reagira na povredu ili sumnju na povredu. Općenito, koraci 1-3 se trebaju provoditi istodobno ili u uskom slijedu.

Korak 1: Ograničiti povredu i napraviti preliminarnu procjenu
Korak 2: Procijeniti rizike povezane s povredom
Korak 3: Obavijest
Korak 4: Spriječiti buduće povrede

2.1 Korak 1: Ograničiti povredu i napraviti preliminarnu procjenu

Nakon što je otkrivena povreda podataka, potrebno je poduzeti radnje kako bi se odmah spriječila. Na primjer, zaustaviti neovlašteno postupanje, povratiti zapise ili isključiti sustav koji je probijen.

Pokrenite preliminarnu procjenu

Brzo se pokrenite i postavite nekoga da vodi početnu istragu. Ta osoba mora biti odgovarajuće kvalificirana i imati dovoljno ovlasti za provođenje početne istrage. U nekim slučajevima, to može biti član Ekipe za odgovor. U drugim slučajevima, to će biti osoba koja je najprikladnije kvalificirana za provođenje početne istrage (kako su odredili članovi Ekipe odgovora).

U nekim situacijama bit će potrebno sastaviti ekipu koja uključuje predstavnike odgovarajućih područja Ascenduma za provođenje preliminarne procjene.

Prilikom izrade preliminarne procjene treba obratiti pažnju na sljedeća pitanja:

a. Koje informacije povreda obuhvaća?
b. Koji je bio uzrok povrede?
c. Koja je razina povrede?
d. Koje su štete (na pogođene osobe) koje bi mogle biti uzrokovane povredom?
e. Kako se povreda može ograničiti?

2.2 Korak 2: Procijeniti rizike povezane s povredom

Sljedeći čimbenici su važni pri procjeni rizika:

a. Vrsta uključenih informacija
    i) Jesu li to osobni podaci ili zaštićeni podaci Ascenduma?

ii) Stvara li vrsta podataka koja je oštećena veći rizik od štete?
iii) Tko je pogođen povredom?

b. Odredite kontekst zahvaćenih informacija i povreda
i) Koji je kontekst informacija koje su uključene?
ii) Koje su stranke stekle neovlašteni pristup zahvaćenim informacijama?
iii) Je li bilo drugih povreda koje bi mogle imati kumulativni učinak?
iv) Kako se informacije mogu koristiti?

c. Utvrdite uzrok i opseg povrede
i) postoji li rizik trajnih povreda ili daljnje izloženosti informacija?
ii) Postoje li dokazi o krađi?
iii) Jesu li informacije adekvatno šifrirane, anonimne ili na drugi način nisu dostupne?
iv) Koji je bio izvor povrede? (rizik od zla može biti manji ako je izvor povrede slučajan, a ne namjeran)
v) Jesu li podaci povraćeni?
vi) Koji su koraci već poduzeti kako bi ublažili štetu?
vii) Je li to sustavni problem ili izolirani incident?
viii) Koliko je osoba pogođeno povredom?

d. Procijenite rizik štete pogođenih osoba
i) Tko je primatelj informacija?
ii) kakva šteta osobama može proizaći iz povrede?

e. Procijenite rizik od drugih šteta
i) druge moguće štete, uključujući i našu organizaciju koja je pretrpjela povredu. Na primjer:
(1) gubitak povjerenja javnosti
(2) narušenje reputacije
(3) Pravna odgovornost
(4) Kršenje odredbi o tajnosti

Temeljita procjena rizika pomoći će Ascendumu u određivanju odgovarajućeg tijeka akcije.

2.3 Korak 3: Obavijest

Odlučivanje hoće li se obavijestiti pojedince ili subjekte koji su pogođeni. Općenito, ako kršenje podataka stvara pravi rizik od teške štete nekoj osobi, oštećenu osobu treba obavijestiti. Ključno razmatranje je da li je obavijest neophodna kako bi se izbjegla ili ublažila ozbiljna šteta pogođenoj osobi.

Razmotrite sljedeće čimbenike:
a. Koji je rizik od teške štete osobi kako je utvrđeno u koraku 2?
b. Koja je mogućnost osobe da izbjegne ili ublaži moguću štetu ako se obavijesti o povredi (uz korake koje je poduzela organizacija)?
c. Čak i ako osoba ne bi mogla poduzeti korake kako bi popravila situaciju, jesu li informacije ugrožene osjetljive ili je vjerojatno da bi izazivale ponižavanje ili neugodnost?
d. Koje su zakonske i ugovorne obveze obavještavanja i koje su posljedice obavijesti?

Postupak obavještavanja
Općenito, obavijest se treba obaviti čim je to razumno moguće. Međutim, u nekim slučajevima, odgoda može biti potrebna. Obavijest bi trebala biti izravna - telefonom, pismom, e-poštom ili osobno, zahvaćenim pojedincima.

Neizravna obavijest, bilo putem web stranica, objavljenih obavijesti ili medija, može se obaviti samo ako izravna obavijest može uzrokovati daljnju štetu, ako je cijena previsoka ili ako podaci o kontaktu za pogođene osobe nisu poznati.

Pojedinosti za uključivanje u obavijest
Sadržaj obavijesti ovisi o specifičnoj povredi i metodi obavijesti. Međutim, Ascendum preporučuje da obavijesti sadrže sljedeće informacije:
a. opis incidenta;
b. vrsta informacija uključenih;
c. odgovor na povredu;
d. pomoć koja se pruža pogođenim osobama;
e. drugi izvori informacija namijenjeni za zaštitu od krađe identiteta ili smetnji s privatnošću
f. Kontakt podatke o Ascendumu;
g. je li prekršaj prijavljen regulatoru ili drugim vanjskim kontaktima;
h. pravne posljedice (npr. odredbe o tajnosti);
i. kako pojedinci mogu podnijeti žalbu Ascendumu; i
j. kako pojedinci mogu podnijeti žalbu Ascendumu (gdje su informacije osobni podaci).

Ostale obavijesti
Također može biti prikladno obavijestiti ostale treće strane, kao što su:

a. nacionalna tijela za zaštitu podataka.
b. Policija
c. Davatelji osiguranja.
d. Tvrtke s kreditnim karticama, financijske institucije.
e. Stručna ili druga regulatorna tijela.
f. Ostale unutarnje ili vanjske strane koje još nisu prijavljene.
g. Dobavljači, potrošači koji imaju izravan odnos s izgubljenim/ukradenim informacijama.

Nacionalna tijela za zaštitu podataka snažno potiču tvrtke da prijave ozbiljnije povrede podataka koje uključuju osobne podatke. Treba uzeti u obzir sljedeće čimbenike prilikom odlučivanja hoće li se povreda prijaviti državnim tijelima za zaštitu podataka:

a. bilo koji važeći zakon koji može zahtijevati obavijest;
b. vrstu osobnih podataka uključenih i postoji li pravi rizik od ozbiljne štete proizašle iz povrede;
c. da li je povredom pogođen veliki broj ljudi;
d. jesu li informacije u potpunosti povraćene bez daljnjeg otkrivanja;
e. jesu li obaviješteni pojedinci koji su pogođeni; i
f. ako postoji opravdano očekivanje da OAIC može primiti pritužbe/upite o povredau.

2.4 Korak 4: Sprečavanje budućih povreda.

Nakon poduzimanja neposrednih koraka za ublažavanje rizika povezanih s povredom, Ascendum mora uzeti vremena kako bi istražio uzrok povrede. Izvršni direktor Ascenduma mora biti obaviješten o ishodu istrage, uključujući preporuke:
a. kako poduzeti odgovarajuće promjene u pravilima i postupcima ako je potrebno;
b. po potrebi revidirati prakse izobrazbe osoblja; i
c. ako je potrebno, ažurirati Plan odgovora.

3.0 Kontrolni popis za prva 24 sata[3]

1. Snimite datum i vrijeme kada je otkrivena povreda, kao i trenutni datum i vrijeme kada počinju napori za odgovor, tj. kada je netko iz Ekipe za odgovore upozoren na povredu.

2. Upozorite i aktivirajte sve u Ekipi za odgovor, uključujući vanjske resurse, kako biste započeli s izvršavanjem vašeg procesa.

3. Osigurajte prostore oko područja na kojem je došlo do povrede podataka radi očuvanja dokaza.

4. Zaustavite dodatni gubitak podataka. Stavite pogođene strojeve izvan mreže, ali nemojte ih isključiti niti ispitivati kompjutere dok ne stigne tim forenzičara.

5. Dokumentirajte sve što je do sada poznato o povredi: Tko ju je otkrio, tko je to izvijestio, kome je prijavljeno, tko još zna za to, kakva je vrsta povrede, što je ukradeno, kako je ukradeno, koji sustavi su pogođeni , koji uređaji nedostaju itd.

6. Intervjuirajte one koji su uključeni u otkrivanje kršenja i bilo koga tko bi mogao znati o tome. Dokumentirajte svoju istragu.

7. Pregledajte protokole koji se odnose na širenje informacija o povredi svih sudionika u ovoj ranoj fazi.

8. Procijenite prioritete i rizike na temelju onoga što znate o povredi.

9. Dovedite svoju tvrtku forenzičara da započne temeljitu istragu.

10. Obavijestite policiju, ako je potrebno, nakon konzultacija s pravnim savjetnikom i višim menadžmentom.

[3] "Experian Innovation (2012): Vodič za odgovor na povreda podataka, https://iapp.org/media/pdf/knowledge_center/Data_Breach_Response_Guide.pdf, zadnji put pristupljeno 27.04.2018, u 11:45 sati."

V. Imenik za brisanje za zaštitu podataka[4]

Osnovna regulacija zaštite podataka temelji se na načelima dobrog upravljanja informacijama. To daje ljudima specifična prava u vezi s njihovim osobnim podacima i postavlja određene obveze našoj organizaciji koja je odgovorna za njihovu obradu.

Brisanje osobnih podataka je važna aktivnost u zaštiti podataka. Osobni podaci koji se obrađuju u bilo koju svrhu ili svrhe ne smiju se čuvati duže nego što je potrebno u tu svrhu ili u te svrhe.

U nekim slučajevima organizacije mogu biti zakonom zatražene da izbrišu osobne podatke pojedinca.

„Dobra je praksa da ljudima jasno damo do znanja što će se dogoditi s njihovim informacijama kada zatvore svoj račun, prekinu sporazum o zapošljavanju - tj. hoće li se podaci izbrisati nepovratno ili jednostavno deaktivirati ili arhivirati. Imajte na umu da ako arhivirate osobne podatke, pravila zaštite podataka, uključujući prava na pristup Ispitanika, se i dalje primjenjuju na njih. Ako korisnicima ponudite opciju za brisanje osobnih podataka koje unose, brisanje mora biti stvarno, tj. sadržaj se ne smije ni na koji način moći povratiti, na primjer, pristupanjem URL-u s te web lokacije. Loša je praksa dati korisniku dojam da je brisanje apsolutno, a zapravo nije. "

1.0 Fizičko brisanje

Sigurno je da bi naša organizacija trebala biti apsolutno razumljiva kada pojedincima govori o tome što znači brisanje i što se zapravo događa s osobnim podacima nakon što se izbrišu.
Ova smjernica namijenjena je rješavanju problema organizacije kod obavješćivanja ljudi da su njihovi osobni podaci izbrisani kada su, zapravo, podaci samo arhivirani i mogu se ponovno vratiti.
Također je namijenjena poticanju organizacija da stavljaju zaštitne mjere na informacije koje su izbrisane, ali su još uvijek u posjedu organizacije. Ova smjernica odražava naš opći stav o brisanju i bit će relevantna za sve tvrtke unutar naše Grupe koje trebaju brisati ili žele brisati osobne podatke.

2.0 Brisanje i arhiviranje

Postoji značajna razlika između brisanja podataka nepovratno, arhiviranja podataka na strukturiran, dohvatljiv način ili zadržavanja kao slučajnih podataka u neispražnjenoj elektronskoj otpadnoj košari. Informacije koje se arhiviraju, primjerice, podliježu istim pravilima o zaštiti podataka kao i "žive" informacije, iako informacije koje su u stvarnosti inertne su daleko manje vjerojatne da će imati nepošteno ili štetno djelovanje na pojedinca od informacija koje su žive.

Međutim realan je pristup, u smislu prepoznavanja da brisanje podataka iz sustava nije uvijek jednostavna stvar i da je moguće staviti informacije „izvan upotrebe“, a da se problemi usklađenosti s podacima o zaštiti podataka mogu "privremeno obustaviti" pod uvjetom da su određene zaštitne mjere ustanovljene:

- podaci su izbrisani bez namjere da ih kontrolori podataka ponovno koriste ili ponovno pristupaju podacima, ali koji još uvijek mogu postojati u elektroničkom eteru. Na primjer, mogu biti na čekanju da budu prebrisani s drugim podacima.

[4] “ICO Information Commissioner´s Office (2014) https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf, posljednji puta pristupljeno 27.04.2018, u 11:45 sati”

- ove informacije više nisu žive. Kao takve, pitanja o usklađenosti s podacima o zaštiti podataka više se ne primjenjuju. (Paralelna situacija može biti vrećica isjeckanog papirnog otpada, iako je moguće ponovno sastaviti informacije iz fragmenata, to bi bilo izuzetno teško i malo je vjerojatno da bi organizacija imala namjeru to učiniti.)
- podaci koji su trebali biti izbrisani, ali se i dalje održavaju u živom sustavu, jer iz tehničkih razloga nije moguće izbrisati te podatke bez brisanja drugih podataka koji se nalaze u istoj seriji.
- U takvim slučajevima organizaciji koja drži informacije se može zakonom zabraniti da ih upotrebljava na isti način na koji bi mogli upotrebljavati žive informacije. To se može dogoditi ako je sud naložio brisanje podataka koji se odnose na određenu osobu, ali to se ne može učiniti bez brisanja podataka o drugim pojedincima koji se nalaze u istoj seriji.

3.0 Stavljanje informacija „izvan upotrebe“

Državna tijela za zaštitu podataka će se uvjeriti da su informacije "stavljene izvan upotrebe", ako nisu izbrisane, pod uvjetom da ih kontrolor podataka koji ih drži:

- ne može, ili neće pokušati, koristiti osobne podatke kako bi donio informiranu odluku u odnosu na bilo kojeg pojedinca ili na način koji na bilo koji način utječe na pojedinca;
- ne daje drugoj organizaciji pristup osobnim podacima;
- okružuje osobne podatke uz odgovarajuću tehničku i organizacijsku sigurnost; i
- se obvezuje na trajno brisanje informacija ako ili kada to postane moguće.

4.0 Brisanje, Arhiviranje i/ili stavljanje informacija “izvan upotrebe”

Pronađite proceduralni direktorij - izbrišite imenik ispod sljedećeg **LINK-a**:

Opis obrade				Djelatnici	Svrha	Prijenos izvan EU?	Osjetljivi podaci	Vremenski rok za brisanje	tehničke mogućnosti
Broj aktivnosti obrade	ime	Datum stvaranja	Posljednje ažuriranje	Kontrolor	Glavna svrha obrade	Da/Ne	Da/Ne	vremenski raspored	Mjera
1	Proces apliciranja	24.9.2017	21.3.2018	Ascendum Central Europe	Tražiti i naći adekvatne kandidate	Ne	Ne	6 mjeseci nakon apliciranja	izbrisat
2	Pristupanje	24.9.2017	21.3.2018	Ascendum Central Europe	Pripreme za pristupanje, pripreme za ugovor o radu	Ne	Da	7 godina nakon završetka ugovora o radu - blokirano	arhiviranje i stavljanje informacija izvan upotrebe
3	Postupak održavanja podataka	24.9.2017	21.3.2018	Ascendum Central Europe	Održavati osobne podatke unutar potrebnih sustava	Ne	Da	7 godina nakon završetka ugovora o radu - blokirano	arhiviranje i stavljanje informacija izvan upotrebe
4	Postupak razvoja zaposlenika	24.9.2017	21.3.2018	Ascendum Central Europe	Razvoj zaposlenika s vanjskim obrazovnim institucijama	NE	Ne	Vanjske obrazovne institucije imaju odgovornost izbrisati osobne podatke nakon završetka programa razvoja zaposlenika	ugovor o usluzi
5	Program evaluacije i tumačenja podataka	24.9.2017	21.3.2018	Ascendum Central Europe	Evaluacija podataka, usporedba razvoja, interpretacija	Ne	Ne	ugovor unutar Kompanije	Ugovor unutar Kompanije
6	Postupak specijalne koristi	24.9.2017	21.3.2018	Ascendum Central Europe	Dodatno mirovinsko osiguranje, Dionice zaposlenika	Ne	Ne	ugovor između osiguravatelja i zaposlenika	ugovor o usluzi

VI. Priručnik održavanja i provjere kvalitete osobnih podataka

Koordinator za zaštitu podataka provodi postupke i dužnosti i može usvojiti te mjere i dužnosti jer su promjene potrebne primjenjivim zakonom. Često, ali najmanje jednom godišnje, koordinator za zaštitu podataka provjerava sve postupke i mjere. Nove mjere i programe za osposobljavanje zaposlenika o pravilima i postupcima zaštite podataka predočuje i objavljuje koordinator zaštite podataka.

VI. Dnevnik provjere kvalitete zaštite podataka

Dnevnik				
Broj	**Datum**	**Zahtjev - Povreda podataka - Aktivnosti obrade**	**Mjera - Opis mjere**	**Datum zaključenja**

VII. Popis referenca

"Visteon (2013): Međunarodna pravila za zaštitu podataka, https://www.visteon.com/utils/media/privacy.pdf, posljednji put pristupljeno 27.04.2018, u 11:45"

"Experian Innovation (2012): Vodič za odgovor na povreda podataka, https://iapp.org/media/pdf/knowledge_center/Data_Breach_Response_Guide.pdf, posljednji put pristupljeno 27.04.2018, u 11:45"

" Australska komisija za neprofitne i dobrotvorne (AU), https://www.acnc.gov.au/ACNC/Publications/Procedure_PDFs/OP_databreach.aspx?TemplateType=P , posljednji put pristupljeno 27.04.2018, u 11:45"

"ICO Information Commissioner´s Office (2014) https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf, posljednji put pristupljeno 27.04.2018, u 11:45"