Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače

Dokument “Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače ENT Grupe” primjenjiv je za sve odnose s dobavljačima, u sklopu kojih Dobavljač obrađuje informacije ENT Grupe unutar vlastitog IT okruženja te osigurava da Informacija ostane zaštićena, kako u prijenosu između ENT Grupe i Dobavljača, tako i u posjedu Dobavljača, na razini koju zahtijeva ENT Grupa.

Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače ENT Grupe predstavljaju minimalne zahtjeve koje ispunjavaju Dobavljač, njegova povezana društva, podugovaratelji i njihovo Osoblje koji pružaju Usluge uime ENT Grupe, pri čemu Uslugama može biti obuhvaćena Obrada Informacija ENT Grupe, kako bi zadržali razinu predanosti zaštiti Informacija ENT Grupe zahtjevanu od strane ENT Grupe.

Dobavljač će zaštititi Informacije ENT Grupe na način da implementira primjenjive zahtjeve kako je predviđeno u ovom Dokumentu te dokaže strukturiran pristup informacijskoj sigurnosti i zaštiti podataka na način da se uskladi s posljednjom inačicom međunarodnog standarda ISO/IEC 27001 ili drugog priznatog standarda, ukoliko drukčije nije pismeno dogovoreno.

Komunikacija prema ENT Grupi u vezi sigurnosnih incidenata, izuzev zahtjeva iz ovog Dokumenta ili ostala pitanja iz područja sigurnosti moraju bit zaštićeni od neovlaštenog pristupa ili presretanja enkriptiranog sadržaja.

Pitanja iz područja sigurnosti potrebno je prijaviti putem adrese: ent.company@ericssonnikolatesla.com ili na kontakt adrese navedene u ugovorima.

Ovaj Dokument se redovito pregledava te će se ažurirati s vremena na vrijeme. ENT Grupa će, zajedno s Dobavljačem razmotriti navedene promjene te se u dobroj vjeri dogovoriti u vezi vremena i načina na koji će se Dobavljač uskladiti s istima.

1 Informacijska Sigurnost

a. Dobavljač će dokazati strukturiran pristup informacijskoj sigurnosti kroz usklađenost svojih aktivosti s posljednjom inačicom međunarodnog standarda ISO/IEC 27001, ISO/IEC 22301, odredbama EU GDPR Uredbe (Opće uredbe o zaštiti podataka), Zakona o kibernetičkoj sigurnosti kao i drugih važećih i priznatih industrijskih standarda iz područja informacijske sigurnosti .

1.1 Politika informacijske sigurnosti

a. Izvršno poslovodstvo će definirati smjernice te iskazati predanost informacijskoj sigurnosti kroz politiku visoke razine informacijske sigurnosti i program koji je primjenjiv u cijeloj kompaniji.
b. Politika informacijske sigurnosti pregledavat će se u planiranim vremenskim razdobljima (najmanje jednom u 24 mjeseca) ili u slučaju značajne izmjene kako bi se osigurala kontinuirana prikladnost, primjenjivost i učinkovitost. Dobavljač će objaviti promjene svojih sigurnosnih politika te obavijestiti ENT Grupu o svim planiranim promjenama svojih sigurnosnih politika. Promjene politika dobavljača koje oslabljuju sigurnosnu zaštitu ili proturječe ovom dokumentu neće biti dozvoljene.

1.2 Organizacija informacijske sigurnosti

a. Jedan ili više kvalificiranih Zaposlenika bit će odgovorni za Održavanje programa informacijske sigurnosti.
b. Dobavljač će održavati Raspodjelu Odgovornosti u svrhu sprečavanja pogreške ili prijevara na način da osigura minimalno dvije odgovorne osobe za zasebne dijelove zadataka, na način da nijedna pojedinačna uloga ili korisnik ne može pristupiti Informacijama ENT Grupe, modificirati ih ili ih koristiti bez autorizacije ili raspoznavanja.

1.3 Upravljanje rizicima

a. Dobavljač mora imati uspostavljen okvir/proces upravljanja rizicima koji identificira i rješava rizike informacijske sigurnosti.

1.4 Sigurnost ljudskih resursa

a. Dobavljač je dužan provesti provjere prije zapošljavanja za sve svoje zaposlenike, u skladu s važećim zakonima. Dokumentacija o provedenim provjerama mora se čuvati i dostaviti ENT-u na zahtjev.
b. Osoblje Dobavljača koje ima pristup Informacijama ENT Grupe mora potpisati ugovor o povjerljivosti (NDA) sa ENT Grupom.
c. Osoblje Dobavljača koje ima pristup Mrežnoj infrastrukturi i informacijama ENT Grupe dužno je potpisati Izjavu o obvezi čuvanja poslovne tajne.
d. Dobavljač je dužan imati postupak uvođenja Osoblja u posao kojim je obuhvaćena provjera identiteta Osoblja te osobnih podataka i vještina koje navodi.
e. Dobavljač je dužan imati postupak raskida ugovora za Osoblje, kojim postupkom je obuhvaćeno ukidanje prava pristupa, oduzimanje informatičke opreme, poništenje kartice za pristup kompaniji te obavijest o obvezama o povjerljivosti koje i dalje vrijede.
f. Osoblje koje ima pristup Informacijama ENT Grupe dužno je redovito prolaziti odgovarajuću obuku iz područja sigurnosti i privatnosti.
g. U slučaju da se Osoblje ne pridržava obveza u vezi s ovim Dokumentom poduzet će se odgovarajuće disciplinske mjere koje će izreći Dobavljač.

1.5 Upravljanje imovinom

a. Dobavljač je dužan rukovati Informacijama ENT Grupe kao Povjerljivim informacijama i štititi ih u skladu sa zahtjevima navedenima u ovom dokumentu.
b. Informacije ENT Grupe neće se pohranjivati, štampati, kopirati, otkrivati ni obrađivati u mjeri većoj no što je potrebno za ispunjenje svrhe upotrebe istih.
c. Informacije ENT Grupe obrađivat će se i pohranjivati na logički odvojen način od informacija Dobavljača te ostalih klijenata.
d. Po završetku ili prekidu Dobavljačevog posla za ENT Grupu, Dobavljač će zbrinuti te na siguran način uništiti (ili na zahtjev ENT Grupe, vratiti ENT Grupi) sve kopije svih Informacija ENT Grupe, uključujući sve rezervne i arhivske kopije, u svakom elektroničkom ili neelektroničkom obliku

1.6 Kontrola pristupa

a. Pristup informacijskim sustavima ili mrežama ENT Grupe iz mreže izvan nadzora ENT Grupe za pojedine osobe ili tijela koji nisu dio ENT Grupe dopušten je samo preko vanjske veze odobrene od strane ENT Grupe

b. Pristup Informacijama ENT Grupe ograničava se na pojedine članove Osoblja te na temelju poslovne funkcije i neophodne potrebe pristupa.
c. Pristup sustavima i mrežama koji sadržavaju Informacije ENT Grupe moguć je samo uz minimalno dvofaktorsku provjeru autorizacije pristupa.
d. Pristup Informacijama ENT Grupe moguć je samo uz uvjet ugrađenih kontrola upravljanja i odabira lozinki.

Sustav 1

i. Lozinke moraju sadržavati najmanje 8, a najviše 64 znaka, bez zahtjeva za kompleksnost istih (velika/mala slova, broj, posebni znakovi, itd.) uz dopušteno korištenje svih znakova.
ii. Lozinke neće istjecati, osim u slučaju kad postoji sumnja da je lozinka ugrožena.
iii. Tijekom postupka odabira, lozinke će se provjeravati radi uzastopnih ili ponavljajućih znakova (npr. 12345678, aaaaaaaa itd.), konteksta, često korištenih lozinki, prethodnih prekršaja i riječi iz rječnika. Navedeno će biti zabranjeno.

Sustav 2

i. Provjera identiteta korisnika prije svakog poništavanja lozinke.
ii. Lozinke se sastoje od najmanje 8 znakova te od najmanje 3 od sljedeće 4 vrste znakova: - velika i mala slova - mala slova - zapadni arapski brojevi (1, 2, ...9) - Nealfanumerički (posebni) znakovi (npr. ? |,%, $, #, itd.) ili ekvivalentnih (sličnih) međunarodnih jezičnih predstavnika..
iii. Lozinke ne mogu biti jednake zadnjim 15 prethodno korištenim lozinkama tijekom razdoblja od 12 mjeseci.
iv. Lozinke vrijede maksimalno 90 dana.
v. Predefinirane, privremene ili unaprijed postavljene lozinke postavljaju se na jedinstvene vrijednosti i mijenjaju se odmah nakon prve upotrebe.
vi. Ponovni pokušaji pristupa ograničeni su zaključavanjem korisničkog ID-a nakon ne više od deset (10) pokušaja s minimalnim trajanjem zaključavanja od četrdeset pet (45) minuta.
vii. Ako je sesija bila neaktivna više od petnaest (15) minuta, zatražite od korisnika da ponovno unese lozinku za ponovno aktiviranje terminala.
viii. Lozinke se nikada ne smiju prenositi, prikazivati ili ispisivati u jasnom tekstu.

e. Kontrole identiteta I pristupa Informacijama ENT Grupe obuhvaćaju:
i. upotrebu jedinstvenih User ID-ova (pristupnih podataka)
ii. odobravanje i administriranje prava pristupa i privilegija pristupa
iii. osiguranje prikladnih pristupnih prava i povlastica
iv. provjeru brisanja zastarjelih prava pristupa (najmanje svakih 6 mjeseci, a za privilegirani pristup najmanje svaka 3 mjeseca)
f. Zapisi se čuvaju u obliku koji se može revidirati te kojim se pokazuje kojim se Informacijama ENT Grupe pristupalo, koje su se Informacije izmjenjivale, otkrivale ili uklanjale.

1.7 Enkripcija

a. Kontrole enkripcije će se upotrebljavati sukladno sa svim relevantnim sporazumima, zakonodavstvom i propisima.
b. Dobavljač će imati mogućnost sigurne komunikacije s ENT Grupom preko kriptirane e-pošte, koristeći se standardnim tehnikama šifriranja koje je definirala industrija.
c. Informacije ENT Grupe biti će zaštićene upotrebom tehnika enkripcije ili ekvivalentnih mjera zaštite u prijenosu i u mirovanju.
d. Kriptografskim ključevima će se upravljati centralno kako bi se osiguralo da postoje procesi za generiranje, distribuciju, pohranu, arhiviranje, pronalaženje i uništavanje.
e. Korijenski certifikati ne smiju se koristiti u operativnom okruženju.

1.8 Fizička sigurnost I sigurnost okoliša

a. Fizički pristup zgradama Dobavljača će biti ograničen na pojedine članove Osoblja i samo kada je to neophodno.
b. Objekti za obradu informacija u kojima se obrađuju informacije ENT Grupe moraju biti nadzirani i pod kontrolom pristupa u svakom trenutku (24x7).
c. Politika čistog stola će se provoditi kako bi se zaštitile Informacije i Imovina ENT Grupe.
d. Fizički pristup mjestu gdje se vrše Usluge za ENT Grupu će se ograničiti uporabom pojedinačnih kartica za provlačenje ili beskontaktnih kartica ili drugih jednakovrijednih sustava te ojačan PIN kodom.
e. Kroz sustav za fizički pristup mjestu gdje se vrše Usluge za ENT Grupu će imati zapise o događajima povezanih s fizičkim pristupom, kao što su datum, vrijeme, identitet kartice za provlačenje ili beskontaktne kartice, identitet vrata, je li pristup odbijen ili odobren.

1.9 Sigurnost operacija

Sljedeći zahtjevi za Operativnu sigurnost primjenjivi su na Dobavljače koji pružaju Usluge kojima se podržava obrada Informacija ENT Grupe u proizvodnom okruženju.

a. Dobavljač će registrirati i održavati inventar sastavnica informacijske tehnologije koje su dio Usluge.
b. Sustavi će biti osigurani s dovoljnim kapacitetom zbog osiguravanja neprekidne raspoloživosti u slučaju sigurnosnog incidenta.
c. Sustavi će osigurati zaštitu od zlonamjernih programa i biti će redovito ažurirani
d. Zapisuju se sve radnje povlaštenih korisnika. Sve izmjene zapisa u tim dnevnicima koje napravi sustav, povlašteni ili krajnji korisnik moraju biti prepoznatljive. Dnevnici zapisa se također moraju redovito i neovisno pregledavati.
e. Informacije o važnim sigurnosnim događajima će biti zapisane u dnevnicima, uključujući vrste događaja kao što su neuspješna prijava, pad sustava, promjene prava pristupa i svojstva događaja kao što su datum, vrijeme, identitet Korisnika, naziv datoteke i IP adresa, gdje god je to tehnički moguće.
f. Dnevnici će se čuvati najmanje 6 mjeseci i biti dostupni ENT Grupi na zahtjev.
g. Rezervne kopije će biti načinjene i održavane kako bi se zajamčili kontinuitet i očekivanja u pogledu isporuke.
h. Postupak upravljanja ranjivostima mora postojati kako bi se odredili prioriteti ranjivosti i kako bi se one ispravile na temelju prirode/ozbiljnosti ranjivosti.
i. Postupak upravljanja zakrpama mora postojati kako bi se zajamčilo da se zakrpe pravodobno primjenjuju.
j. Dobavljač mora provoditi testiranje penetracije sustava i infrastrukture koji se koriste za podršku suradnji s ENT Grupom najmanje jednom godišnje, primjenjujući najbolju praksu u industriji.
k. Dobavljač mora uskladiti vrijeme na svim relevantnim sustavima za obradu informacija s jednim referentnim izvorom vremena.
l. Dobavljač mora implementirati očvršćivanje sustava (hardening) u skladu s trenutačnim najboljim praksama na sve sustave
m. Dobavljač mora osigurati da su informacije i aplikacije/sustavi ENT Grupe odvojeni od dobavljačevih vlastitih ili sustava i podataka drugih korisnika odgovarajućim fizičkim, tehničkim i/ili logičkim mjerama.
n. Razvojna, testna i produkcijska okruženja koja sadrže informacije ENT Grupe moraju biti logički i gdje je moguće fizički odvojena međusobno.
o. Dobavljač ne smije koristiti informacije ENT Grupe u bilo kakvim sustavima umjetne inteligencije osim ako to nije izričito dogovoreno u sklopu Ugovora.

1.10 Sigurnost komunikacija

a. Sustavi koji sadrže Informacije ENT Grupe zaštićeni su vatrozidom/vatrozidovima i primjereno ojačani, tj. uklonjeni ili isključeni SW i funkcionalnosti koje se ne upotrebljavaju.
b. Mreže Dobavljača koje se upotrebljavaju za pristup Informacijama ili mrežama ENT Grupe će imati sigurnosne kontrole koje mogu pružiti zaštitu od neovlaštenog presretanja prometa ili ometanja uporabom vatrozidova, otkrivanja/sprečavanja nedopuštenog ulaska itd.
c. Bežične mrežne veze kojima se prenose Informacije ENT Grupe će biti kriptirane sukladno najboljoj praksi.
d. Dobavljač mora implementirati rješenje za sigurnost e-pošte u skladu s najboljom praksom u industriji, radi zaštite od zlonamjernih napada kao što su malware, lažno predstavljanje putem e-pošte, phishing napadi i spam.
e. Dobavljač će koristiti tehnologiju kako bi pretraživao kompanijsku e-poštu Dobavljača tražeći viruse i zlonamjerne kodove i poveznice te ažurirati tu tehnologiju.

1.11 Nabava, razvoj i održavanje sustava

Sljedeći zahtjevi informacijske sigurnosti primjenjuju se na Dobavljače koji pružaju usluge razvoja ili prilagodbe softvera ili hardvera, uključujući obradu informacija ENT Grupe:

a. Dobavljač mora imati dokumentiranu metodologiju životnog ciklusa razvoja softvera (SDLC)
b. Izvorni i/ili objektni kod sustava mora biti zaštićen od neovlaštenog pristupa. Prava pristupa repozitoriju izvornog koda moraju se periodično pregledavati i biti ograničena na ovlaštene zaposlenike.
c. Operativna okruženja koja sadržavaju Informacije ENT Grupe će biti odvojena od razvojnog i testnog okruženja.
d. U testnim i razvojnim sustavima nije dozvoljena uporaba Informacija iz proizvodnog sustava ENT Grupe.
e. Dobavljač mora osigurati da su softver i/ili drugi proizvodi koji obrađuju informacije ENT Grupe bez svih poznatih sigurnosnih ranjivosti ili drugih sigurnosnih nedostataka.
f. Na zahtjev ENT Grupe, Dobavljač mora otkriti sav softver trećih strana/dodatke (vlasničke ili otvorenog koda) koji se koriste u razvoju softvera koji podržava obradu informacija ENT Grupe.
g. Dobavljač mora slijediti dokumentirane postupke upravljanja promjenama za podnošenje zahtjeva, testiranje i odobravanje promjena vezanih uz aplikacije i infrastrukturu.

1.12 Odnosi s podizvođačima

a. Otkrivanje Informacija ENT Grupe trećoj strani, kao npr. drugom Izvršitelju obrade, dopušta se samo uz prethodni pisani pristanak ENT Grupe i samo u svrhe utvrđene u ugovornima s ENT Grupom.
b. Drugi Izvršitelji obrade ograničeni su samo na nužan pristup, uporabu, zadržavanje i otkrivanje Informacija ENT Grupe potrebnih za izvršenje ugovornih obveza.
c. Drugim izvršiteljima obrade daju se jasne upute o sigurnosnim mjerama za zaštitu Informacija ENT Grupe.
d. Dobavljač mora procijeniti rizik povezan s novim podizvođačima prije njihovog ugovaranja te mora imati uspostavljen proces upravljanja rizicima trećih strana.

e. Dobavljač mora redovito pratiti, pregledavati i revidirati usklađenost podizvođača sa Zahtjevima

1.13 Upravljanje incidentima

a. Dobavljač je dužan imati dokumentirani postupak upravljanja sigurnosnim incidentima kako bi mogao otkriti incidente i postupati s njima. Dobavljač prijavljuje potvrđene sigurnosne incidente ili manjkavosti u koje su uključene Informacije ENT Grupe ili Usluge za ENT Grupu unutar 24 sata ili kako je drukčije dogovoreno. Sigurnosne incidente potrebno je prijaviti na ent.company@ericssonnikolatesla.com, određenoj kontakt osobi ili kako je navedeno u ugovorima.
b. Dobavljač će u potpunosti surađivati sa ENT Grupom u smislu rješavanja navedenih prijava. Zbog forenzičke procjene, suradnja može obuhvaćati pružanje pristupa podacima temeljenim na računalnim dokazima.

1.14 Upravljanje kontinuitetom poslovanja

Sljedeći zahtjevi za Upravljanje kontinuitetom poslovanja primjenjuju se na Dobavljače koji pružaju Usluge kojima se podržava infrastruktura ENT Grupe ili obrada Informacija ENT Grupe u proizvodnom okruženju.

a. Dobavljač će implementirati Plan kontinuiteta poslovanja koji se ispituje na godišnjoj razini.
b. Dobavljač provodi Analizu učinka na poslovanje i Procjenu rizika kako bi utvrdio i ublažio moguće prijetnje i opasnosti kojima Informacije ENT Grupe mogu biti izložene.
c. Dobavljač zapisuje, analizira i pregledava incidente u vezi s poslovnim kontinuitetom koji utječu na pružanje Usluge ENT Grupi te pravodobno ili kako je drukčije dogovoreno izvješćuje ENT Grupu o njima.

1.15 Sigurnost lanca opskrbe softverom

Dobavljač mora specificirati i dokumentirati softverske komponente trećih strana koje se koriste, zajedno s njihovim verzijama, uključujući komponente otvorenog koda i vlasničke komponente, te ENT Grupi dostaviti popis sastavnica softvera (Software Bill of Materials – SBOM) koji je u skladu sa specifikacijom SPDX V2.2.1 / ISO 5962:2021 kao i sa SBOM specifikacijom za dobavljače za sav softver (bilo da se isporučuje kao samostalan proizvod ili ugrađen u hardver) koji se isporučuje ili stavlja na raspolaganje ENT Grupi.

2 Tajnost podataka

Sljedeći zahtjevi u pogledu tajnosti podataka primjenjivi su u slučajevima kada Dobavljač obrađuje Osobne podatke u ime ENT Grupe. Tim se zahtjevima nadopunjuju zahtjevi koji se već odnose na Politiku privatnosti ENT Grupe. Tajnost podataka na lokalnoj razini uvijek se mora čuvati u kontekstu primjenjivih pravnih i ugovornih zahtjeva.

a. Izvršno poslovodstvo Dobavljača određuje smjernice za tajnost i pokazuje svoju predanost čuvanju tajnosti. Dobavljač treba imati politiku privatnosti visoke razine koja se primjenjuje u cijeloj kompaniji te se ukupna odgovornost za tajnost dodjeljuje rukovoditelju najviše razine ili osobi na istovjetnoj razini upravljanja. Uloge i odgovornosti povezane s obradom osobnih podataka trebaju biti jasno definirane i raspodijeljene. Dobavljač će objaviti promjene svojih sigurnosnih politika te obavijestiti ENT Grupu o svim planiranim promjenama svojih sigurnosnih politika. Promjene politika dobavljača koje oslabljuju sigurnosnu zaštitu ili proturječe ovom dokumentu neće biti dozvoljene.

b. Dobavljač će osigurati zaštitu i tajnost Osobnih podataka u vezi s Uslugama u skladu s propisima o zaštiti Osobnih podataka, te internim dokumentima i uputama ENT Grupe.
c. Osobni podaci, neće se koristiti ni u kakve druge svrhe osim u svrhu izvršavanja ugovora s ENT Grupom.
d. Dobavljač neće prenositi Osobne podatke s radnih stanica na vanjske uređaje za pohranu (npr. USB, DVD, vanjski tvrdi diskovi).
e. Prema potrebi, Dobavljač će pseudoanonimizirati Osobne podatke ili primijeniti druge adekvatne mjere zaštite (enkripcija i sl.).
f. Osobnim podacima neće se moći pristupiti bez prethodne autorizacije.
g. Ovlašteno osoblje imat će pristup samo najmanjoj količini Osobnih podataka nužnoj za izvršavanje svoje radne dužnosti. Treba izbjegavati upotrebu uobičajenih korisničkih računa. U slučajevima kada je to potrebno, treba osigurati da svi korisnici zajedničkog računa imaju iste uloge i odgovornosti.
h. Osoblje s pristupom Osobnim podacima mora prolaziti odgovarajuće obuke o privatnosti podataka najmanje jednom godišnje ili češće ako to ENT Grupa opravdano zahtijeva (npr. u slučaju incidenata, provođenja promjena i ažuriranja privatnosti /sigurnosti i slično).
i. Dobavljač mora uspostaviti postupke za redovito ispitivanje, procjenu i ocjenu učinkovitosti tehničkih i organizacijskih mjera kako bi se osigurala sigurnost Obrade. Procesi će se testirati, a testovi će se dokumentirati najmanje jednom godišnje.
j. Po potrebi, ENT Grupa obaviti će inspekciju razine zaštite Osobnih podataka kod Dobavljača te zahtijevati moguće prilagodbe/poboljšanja.
k. Osobni podaci čuvat će se samo onoliko dugo koliko je potrebno radi ispunjavanja navedenih svrha u ugovornim ugovorima s ENT Grupom ili u skladu sa zakonom ili propisima, a nakon toga će se na odgovarajući način vratiti ili zbrinuti po izboru ENT Grupe.
l. Uklanjanje Osobnih podataka će biti evidentirano kako bi se ENT Grupi potvrdilo da je došlo do takvog uklanjanja.
m. Ako je vraćanje ili uklanjanje nekih ili svih osobnih podataka spriječeno zakonom ili propisom, osobni podaci bit će povjerljivi ili anonimizirani i više se neće aktivno obrađivati. ENT Grupa će se obavijestiti ako takve obveze postoje odmah po saznanju Dobavljača.
n. Osobni podaci neće se pohranjivati, tiskati, kopirati, otkrivati te neće biti korišteni u drugom načinu obrade izuzev onog koji je potreban za ispunjenje Svrhe.
o. Dobavljač će slijediti upute ENT Grupe i pomagati ENT Grupi u ispunjavanju zahtjeva za ostvarivanje prava Ispitanika prema važećim zakonima i propisima.
p. U slučaju da Dobavljač primi zahtjev od Ispitanika, takav će se zahtjev prenijeti ENT grupi bez nepotrebnog odgađanja. Dobavljač neće odgovarati na zahtjeve Ispitanika bez naloga i autorizacije ENT Grupe.
q. Netočni osobni podaci ispravit će se u skladu s uputama ENT Grupe.
r. Otkrivanje osobnih podataka trećoj strani, poput Drugog izvršitelja obrade, dopušteno je samo uz prethodno pismeno odobrenje ENT Grupe u svrhe utvrđene u ugovoru s ENT Grupom ili u uputama ENT Grupe, sve sukladno važećim propisima o zaštiti podataka. Ako Drugi izvršitelj obrade ne ispuni svoje obveze u pogledu zaštite podataka, Dobavljač ostaje u potpunosti odgovoran ENT Grupi za izvršavanje obveza Drugog izvršitelja obrade.
s. Prije nego što Dobavljač prenese osobne podatke na Drugog izvršitelja obrade, Dobavljač će osigurati da su odgovornosti Dobavljača i Drugog izvršitelja obrade jasno opisane i dogovorene u komercijalnom ugovoru koji utvrđuje iste obveze zaštite podataka kao i ugovor između Dobavljača i ENT Grupe. ENT Grupa imat će pravo procijeniti uvjete takvog ugovora. Uvjeti navedeni u nastavku dodaju se ugovoru i sadrže zahtjeve iz čl. 28/3 Opće uredbe o zaštiti osobnih podataka EU 2016/679 (GDPR), između ostalog:
    i. Jasna ugovorna definicija da je ENT Grupa ili Voditelj obrade podataka ili izvršitelj obrade podataka, a dobavljač i drugi izvršitelj Obrade su izvršitelji obrade ili drugi izvršitelji obrade.
    ii. Jasan ugovorna definicija da Dobavljač i ENT Grupa imaju pravo procjene drugog izvršitelja obrade s obzirom na privatnost podataka.
    iii. Jasna definicija Osobnih Podataka.

iv. Jasna definicija mjerodavnih zakona za obradu osobnih podataka i za prijenos takvih podataka preko međunarodne granice.
v. Jasne upute o tome kada i gdje se očekuje da će drugi izvršitelj obrade prijaviti kršenje privatnosti.
vi. Jasne upute o sigurnosnim mjerama za zaštitu privatnosti, uključujući odgovarajuće tehničke i organizacijske mjere za zaštitu osobnih podataka na istoj ili višoj razini zaštite koju pruža ENT Grupa.

t. Drugi izvršitelji obrade bit će ograničeni samo na potreban pristup, upotrebu, zadržavanje i otkrivanje osobnih podataka potrebnih za ispunjavanje ugovornih obveza.
u. Zapisi će se čuvati na način koji se može revidirati, pokazujući koji su osobni podaci preneseni u koje zemlje. Dobavljač bi trebao imati registar IT resursa koji se koriste za obradu osobnih podataka u ime ENT Grupe (hardver, softver i mreža).
v. Dobavljač će imati uspostavljen postupak za prijavljivanje i rješavanje povreda privatnosti, kao i rješavanje upita, žalbi i sporova.
w. Dobavljač će prijaviti kršenja privatnosti o kojima dobavljač sazna ENT Grupi odmah, bez nepotrebnog odgađanja ili ako je drugačije pismeno dogovoreno. Dobavljač će u potpunosti surađivati s ENT Grupom u radu s tim izvješćima.
x. Ako je to zakonski potrebno, dobavljač će se složiti da će surađivati s državnim tijelom ili agencijom povezanom s privatnošću podataka, međutim prije takve suradnje nužno je obavijestiti ENT Grupu.

3 Usklađenost

a. Unutarnje revizije i/ili procjene dobavljača u vezi sa sigurnošću i privatnošću redovito će provoditi obučeno osoblje, a nalazi će se ocjenjivati radi mogućih korektivnih radnji.
b. U roku od 30 dana od zahtjeva ENT grupe, dobavljač će morati moći dokazati sukladnost s odredbama ovog Dokumenta i svim ostalim zahtjevima ili mjerama sigurnosti i privatnosti koji su dogovoreni s ENT Grupom.
c. Dobavljač će, na zahtjev ENT Grupe, dostaviti dokaze o usklađenosti podizvođača s ovim Zahtjevima.
d. Na zahtjev ENT Grupe, Dobavljač mora dostaviti sve rezultate penetracijskog testiranja i/ili ispitivanja ranjivosti ili omogućiti ENT Grupi provođenje penetracijskog testiranja i/ili ispitivanja ranjivosti na sustavima ili okruženjima kojima upravlja, a u kojima se obrađuju ili pohranjuju informacije ENT Grupe.
e. Dobavljač mora čuvati i štititi sve potrebne zapise kako bi dokazao usklađenost sa Zahtjevima.

4 Definicije

Za potrebe ovog dokumenta, sljedeće riječi i izrazi imat će značenje dodijeljeno im u nastavku, osim ako kontekst očito ne zahtijeva drugačije.

Anoniman	Elementi osobnih podataka nepovratno su uklonjeni tako da preostali podaci ne mogu identificirati pojedinca ili bi identifikacija zahtijevala nesrazmjerno puno vremena, troškova i truda.
Voditelj obrade podataka	Fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo koje, samostalno ili zajedno s drugima, određuje svrhe i sredstva obrade osobnih podataka.
Izvršitelj obrade podataka	Fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo koje obrađuje Osobne podatke u ime Voditelja obrade podataka.
Ispitanik	Identificirana ili utvrdiva osoba na koju se odnose osobni podaci. To je netko koga se može izravno ili neizravno identificirati, posebno pozivanjem na identifikacijski broj ili na jedan ili više specifičnih čimbenika (fizički, fiziološki, mentalni, ekonomski, kulturni, socijalni).
Imovina ENT Grupe	Informacijska imovina i fizička imovina koja je povjerena Dobavljaču ili je dio usluge.
Informacije ENT Grupe	Podaci u vlasništvu ENT Grupe, kupaca ENT Grupe, ostalih sudionika koji imaju poslovne odnose s ENT Grupom i ostale informacije koje su dio Usluge.
Osobni Podaci	Pod osobnim podacima podrazumijevaju se svi podaci koji se mogu povezati s identificiranom ili utvrdivom živom fizičkom osobom („Ispitanikom“) ili kako je drugačije određeno zakonom, propisom ili ugovornim sporazumom. Osoba koja se može identificirati može se identificirati, izravno ili neizravno, posebno pozivanjem na identifikacijski broj ili na jedan ili više čimbenika specifičnih za njezin fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet. Pojmovi „Osobni podaci”, „Podaci koji mogu osobno identificirati (PII)”, „Osobni podaci”, „privatni podaci”, „osjetljivi osobni podaci”, „posebne kategorije podataka” i „zakonski zaštićeni podaci” često se koriste naizmjenično za upućivanje na informacije koje se odnose na pojedince.

	Izrazi "podaci o kupcima" i "podaci o pretplatnicima" obično se koriste za upućivanje na podatke koji se odnose na pretplatnike ili druge krajnje korisnike.
Osoblje	Svaki pojedinac koji u ime dobavljača obavlja posao za ENT Grupu.
Kršenje privatnosti	Kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, promjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji se prenose, pohranjuju ili obrađuju na drugi način.
Obrada	Obrada osobnih podataka znači bilo koju operaciju ili skup operacija koja se izvršava na osobnim podacima, bilo automatskim sredstvima ili ne (na primjer: prikupljanje, snimanje, prilagodba ili izmjena, pronalaženje, savjetovanje, upotreba, otkrivanje prijenosom, brisanjem ili uništavanjem, itd.)
Usluga	Isporuka robe ili usluga od strane dobavljača ENT Grupi.
Podizvođač	Poslovni partneri, dobavljači i pružatelji outsourcing usluga .
Drugi izvršitelj obrade	Drugi izvršitelj obrade je dobavljač koji obrađuje informacije ENT Grupe u ime dobavljača.