Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače

UPUTE

1/00021-2849 Uhr Rev H

Uvod

Ericssonova Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače (BISPRS) predstavljaju minimalne zahtjeve koje ispunjavaju Dobavljač, njegova povezana društva, podugovaratelji i njihovo Osoblje koji pružaju Usluge uime Ericssona, pri čemu Uslugama može biti obuhvaćena Obrada Ericssonovih Informacija, kako bi zadržali razinu Ericssonove predanosti zaštiti Ericssonovih Informacija.

Ericssonovim Informacijama obuhvaćene su informacije koje pripadaju Ericssonu, Ericssonovim kupcima, ostalim trećim stranama koje imaju poslovne odnose s Ericssonom te druge informacije koje su dio Usluge/Usluga za Ericsson.

Dobavljač je dužan osigurati ispunjavanje i svih dodatnih zahtjeva u vezi sa sigurnošću i tajnošću koji su dio ugovornih sporazuma i primjenjivih zakona i propisa.

Ovaj se dokument redovito pregledava te će se povremeno ažurirati. Ericsson će s Dobavljačem pregledati takve izmjene te će se u dobroj vjeri dogovoriti kako će se (na koji način i/ili kojim sredstvima ili mjerama) i kada Dobavljač pridržavati ažuriranog sadržaja.

Sadržaj

1 Temeljna informacijska sigurnost i zahtjevi za privatnost za dobavljače

Dobavljač je dužan zaštititi Ericssonove Informacije provedbom primjenjivih kontrola kako su predviđene ovim Dokumentom u skladu s posljednjom inačicom međunarodne norme ISO/IEC 27002, osim ako nije drukčije dogovoreno u pisanom obliku.

Za potrebe obveze Dobavljača, „u skladu s" znači da Dobavljač mora redovito razmatrati sve kontrole uključene u navedenu normu i donositi savjesne odluke o tome treba li se konkretna kontrola primijeniti u cijelosti, djelomično ili se uopće ne treba primijeniti, ili moraju li se alternativne zaštitne mjere provoditi ili se već provode. Međutim, Dobavljač uvijek mora osigurati da Ericssonove Informacije nisu izložene riziku.

Obavješćivanje Ericssona o sigurnosnim incidentima, izuzećima od zahtjeva u ovome Dokumentu ili drugim problemima ili upitima povezanima sa sigurnošću moraju biti zaštićeni s pomoću šifriranja od neprimjerenog pristupa ili presretanja.

Incidente povezane sa sigurnošću potrebno je prijaviti na adresu: corporate.security.office@ericsson.com, dodijeljenu kontaktnu točku ili kako je drukčije određeno u ugovornim sporazumima.

Podrška u vezi s uporabom šifrirane e-pošte: Kako mogu sigurno komunicirati s Ericssonovim korisnicima putem e-pošte.

2 Informacijska sigurnost

2.1 Politika informacijske sigurnosti

a. Izvršno poslovodstvo dužno je odrediti smjernice za informacijsku sigurnost i pokazati svoju predanost informacijskoj sigurnosti. Treba postojati barem politika informacijske sigurnosti na visokoj razini i popratni program koji se primjenjuje u cijeloj kompaniji.

b. Politika informacijske sigurnosti pregledava se u planiranim vremenskim razdobljima ili ako dođe do znatnih promjena kako bi se zajamčila njezina neprekinuta stabilnost, prikladnost i djelotvornost.

2.2 Organizacija informacijske sigurnosti

a. Jednoj ili više kvalificiranih osoba iz Osoblja dodjeljuje se odgovornost održavanja programa informacijske sigurnosti.

b. Dobavljač održava Odvajanje/Razgraničenje Dužnosti kako bi se spriječile greške i prijevare jamčeći da su barem dvije osobe odgovorne za pojedinačne dijelove svakog zadatka kako nijedna uloga ili račun ne bi mogli pristupiti Ericssonovim Informacijama, izmijeniti ih ili upotrijebiti, a da se to ne dopusti ili ne otkrije.

2.3 Sigurnost ljudskih resursa

a. Dobavljač je dužan imati postupak kojim jamči da je sve Osoblje koje ima pristup Ericssonovim Informacijama potpisalo Dobavljačev Ugovor o povjerljivosti.

b. Osoblje koje ima pristup Mrežnoj infrastrukturi i informacijama Ericssona dužno je potpisati potvrdu da je pročitalo i razumjelo Ericssonov dokument o povjerljivosti i uputama za pristup.

c. Dobavljač je dužan imati postupak uvođenja Osoblja u posao kojim je obuhvaćena provjera identiteta Osoblja te osobnih podataka i vještina koje navodi.

d. Dobavljač je dužan imati postupak raskida ugovora za Osoblje kojim je obuhvaćeno ukidanje prava pristupa, oduzimanje informatičke opreme, poništenje kartice za pristup kompaniji te obavijest o obvezama o povjerljivosti koje i dalje vrijede.

e. Osoblje koje ima pristup Ericssonovim Informacijama dužno je redovito prolaziti odgovarajuću obuku u području sigurnosti.

f. U slučaju da se Osoblje ne pridržava obveza u vezi s ovim Dokumentom poduzimaju se odgovarajuće disciplinarne mjere koje nametne Dobavljač.

2.4 Upravljanje imovinom

a. Dobavljač je dužan rukovati Ericssonovim Informacijama kao Povjerljivim informacijama.

b. Dobavljač je dužan koristiti se šifriranjem za prijenos Ericssonovih informacija, uključujući Ericssonove Informacije koje se prenose e-poštom.

c. Ericssonove Informacije ne smiju se prekomjerno pohranjivati, ispisivati, kopirati, objavljivati ili Obrađivati drugim sredstvima izvan svrhe za uporabu.

a. Ericssonove Informacije obrađuju se i pohranjuju logički odvojeno od informacija Dobavljača i informacija drugih kupaca.

b. Po završetku ili prekidu rada Dobavljača za Ericsson Dobavljač pročišćava i na siguran način uništava (ili na Ericssonov zahtjev vraća Ericssonu) sve kopije svih Ericssonovih Informacija, uključujući sve rezervne i arhivske kopije, u svakom elektroničkom ili neelektroničkom obliku.

2.5 Kontrola pristupa

a. Pristup Ericssonovim informacijskim sustavima ili mrežama iz mreže izvan Ericssonova nadzora za pojedine osobe ili tijela koji nisu dio Ericssona omogućuje se samo preko odobrene Veze treće strane koju pruža Ericsson.

b. Pristup Ericssonovim Informacijama ograničava se na pojedine članove Osoblja i kada je to neophodno.

c. Pristup sustavima i mrežama koji sadržavaju Ericssonove Informacije koristi se dvjema metodama provjere autentičnosti čimbenika.

d. Moraju postojati odabir lozinki i kontrole upravljanja za pristup Ericssonovim Informacijama kojima je obuhvaćeno sljedeće:

    i. provjera identiteta korisnika prije ponovnog postavljanja lozinke;

    ii. lozinke sadržavaju najmanje 8 znakova i imaju najmanje 3 od sljedećih četiriju vrsta znakova: – velika slova – mala slova – arapski brojevi (1, 2, … 9) – znakovi (posebni) koji nisu slovno-brojčani (npr. ?, |, %, $, # itd.) ili odgovarajući primjeri iz svjetskih jezika;

    iii. lozinke ne mogu biti istovjetne 5 prethodno korištenih lozinki u razdoblju od 12 mjeseci;

    iv. lozinke najdulje vrijede 90 dana;

    v. zadane, privremene ili prethodno postavljene lozinke postavljene su na jedinstvene vrijednosti i mijenjaju se odmah nakon prve uporabe;

    vi. ograničavanje opetovanih pokušaja pristupa blokiranjem identifikacije korisnika nakon najviše šest (6) pokušaja uz najkraće trajanje blokiranja od trideset (30) minuta;

    vii. ako je sesija neaktivna više od petnaest (15) minuta, zatražiti od korisnika da ponovno unese lozinku kako bi ponovno aktivirao terminal;

    viii. lozinke se nikada ne smiju prenositi, prikazivati ili ispisivati u čitkom obliku.

e. Za pristup Ericssonovim Informacijama trebaju postojati kontrole Upravljanja identitetom i pristupom kojima se pružaju metode za:

    i. uporabu jedinstvenih identiteta Korisnika;

    ii. dodjeljivanje prava pristupa i povlastica pristupa te upravljanje njima;

    iii. jamčenje da prava pristupa i povlastice pristupa ostanu odgovarajućima;

    iv. redovito provjeravanje jesu li zastarjela prava pristupa izbrisana – barem svakih 6 mjeseci, a za povlašteni pristup svaka 3 mjeseca.

f. Zapisi se čuvaju u obliku koji se može revidirati te kojim se pokazuje kojim se Ericssonovim Informacijama pristupalo, koje su se Informacije izmjenjivale, otkrivale ili uklanjale.

2.6 Šifriranje

a. Kontrole šifriranja upotrebljavaju se u skladu sa svim relevantnim sporazumima, zakonodavstvom i propisima.

b. Dobavljač ima mogućnost sigurne komunikacije s Ericssonom preko šifrirane e-pošte, koristeći se standardnim tehnikama šifriranja koje je definirala industrija.

c. Ericssonove Informacije zaštićene su uporabom tehnika šifriranja ili jednakovrijednim mjerama zaštite u pokretu i mirovanju.

d. Ključevima za šifriranje upravlja se centralno kako bi se zajamčilo da postoje postupci za stvaranje, distribuciju, pohranu, arhiviranje, povrat i uništenje.

e. Osnovne potvrde ne upotrebljavaju se u operativnom okruženju.

2.7 Fizička sigurnost i sigurnost okoliša

a. Fizički pristup zgradama Dobavljača ograničava se na pojedine članove Osoblja i kada je to neophodno.

b. Politika čistog stola provodi se kako bi se zaštitile Ericssonove Informacije i Imovina.

c. Fizički pristup mjestu gdje se vrše Usluge za Ericsson ograničen je uporabom pojedinačnih kartica za provlačenje ili beskontaktnih kartica ili drugih jednakovrijednih sustava te je ojačan PIN kodom.

d. Sustavom za fizički pristup mjestu gdje se vrše Usluge za Ericsson zapisuju se događaji povezani s fizičkim pristupom, kao što su datum, vrijeme, identitet kartice za provlačenje ili beskontaktne kartice, identitet vrata, je li pristup odbijen ili odobren.

2.8 Operativna sigurnost

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

a. Dobavljač registrira i održava inventar sastavnica informacijske tehnologije koje su dio Usluge.

b. Sustavima je dodijeljen dovoljan kapacitet za jamčenje neprekidne dostupnosti u slučaju sigurnosnog incidenta.

c. Sustavima se jamči da se primjenjuje i ažurira zaštita od zlonamjernih programa.

d. Zapisuju se sve radnje korisnika s povlasticama. Sve izmjene zapisa u tim dnevnicima koje napravi sustav, povlašteni ili krajnji korisnik moraju se moći otkriti. Dnevnici se također moraju redovito i neovisno pregledavati.

e. Informacije o važnim događajima povezanima sa sigurnošću zapisuju se 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 je to tehnički moguće.

f. Dnevnici se čuvaju najmanje 6 mjeseci i dostupni su Ericssonu na zahtjev.

g. Rezervne kopije izrađuju se i održavaju kako bi se zajamčili kontinuitet i očekivanja u pogledu isporuke.

h. Mora postojati postupak upravljanja osjetljivostima kako bi se odredili prioriteti osjetljivosti i kako bi se one ispravile na temelju prirode/ozbiljnosti osjetljivosti.

i. Mora postojati postupak upravljanja zakrpama kako bi se zajamčilo da se zakrpe pravodobno primjenjuju.

2.9 Sigurnost komunikacije

a. Sustavi koji sadržavaju Ericssonove Informacije zaštićeni su vatrozidom/vatrozidovima i primjereno očvrsnuti, tj. uklonjene su ili isključene programska oprema i funkcionalnosti koje se ne upotrebljavaju.

b. Mreže Dobavljača koje se upotrebljavaju za pristup Ericssonovim Informacijama ili Ericssonovim mrežama imaju 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 Ericssonove Informacije šifriraju se sukladno najboljoj praksi.

d. Dobavljač se koristi tehnologijom kako bi pretraživao kompanijsku e-poštu Dobavljača tražeći viruse i zlonamjerne kodove i poveznice te ažurira tu tehnologiju.

2.10 Stjecanje, razvoj i održavanje sustava

a. Operativna okruženja koja sadržavaju Ericssonove Informacije odvajaju se od razvojnog i ispitnog okruženja.

b. U ispitnim i razvojnim sustavima ne dozvoljava se uporaba Ericssonovih Informacija iz proizvodnog sustava.

2.11 Odnosi s podugovarateljima

a. Otkrivanje Ericssonovih Informacija trećoj strani, kao što je Podobrađivač treće strane, dopušta se samo uz prethodni pisani pristanak Ericssona i samo u svrhe utvrđene u ugovornim sporazumima s Ericssonom.

b. Podobrađivači treće strane ograničeni su samo na nužan pristup, uporabu, zadržavanje i otkrivanje Ericssonovih Informacija potrebnih za izvršenje ugovornih obveza.

c. Podobrađivačima treće strane daju se jasne upute o sigurnosnim mjerama za zaštitu Ericssonovih Informacija.

2.12 Upravljanje incidentima

a. Dobavljač je dužan imati dokumentiran postupak upravljanja sigurnosnim incidentima kako bi mogao otkriti incidente i postupati s njima.

b. Dobavljač prijavljuje potvrđene sigurnosne incidente ili manjkavosti u koje su uključene Ericssonove Informacije ili Usluge za Ericsson čim je to izvedivo ili kako je drukčije dogovoreno.

c. Pri bavljenju tim izvješćima Dobavljač u potpunosti surađuje s Ericssonom. Suradnja može obuhvaćati pružanje pristupa računalnim dokaznim podacima[1] za forenzičko vrednovanje.

2.13 Upravljanje kontinuitetom poslovanja

Sljedeći zahtjevi za Upravljanje kontinuitetom poslovanja primjenjivi su na Dobavljače koji pružaju Usluge kojima se podržava Ericssonova infrastruktura ili obrada Ericssonovih Informacija u proizvodnom okruženju.

a. Dobavljač provodi Plan poslovnog kontinuiteta (BCP) koji se ispituje na godišnjoj razini.

b. Dobavljač provodi Analizu učinka na poslovanje i Procjenu rizika (BIA/RA) kako bi utvrdio i ublažio moguće prijetnje i opasnosti kojima Ericssonove Informacije mogu biti izložene.

c. Dobavljač zapisuje, analizira i pregledava incidente u vezi s poslovnim kontinuitetom koji utječu na pružanje Usluge Ericssonu te pravodobno ili kako je drukčije dogovoreno izvješćuje Ericsson o njima.

[1] Dokazni podaci mogu se nalaziti na uređajima kao što su uredska stolna računala / radne stanice, prijenosna računala, mrežni datotečni poslužitelji, prijenosni memorijski uređaji, rezervne vrpce itd.).

3 Tajnost podataka

Sljedeći zahtjevi u pogledu tajnosti podataka primjenjivi su u slučajevima kada Dobavljač Obrađuje Osobne podatke uime Ericssona. Tim se zahtjevima nadopunjuju zahtjevi koji se već odnose na Ericssonove Informacije. Tajnost podataka na lokalnoj razini uvijek se mora čuvati u kontekstu primjenjivih pravnih i ugovornih zahtjeva.

a. Izvršno poslovodstvo određuje smjernice za tajnost i pokazuje svoju predanost čuvanju tajnosti. Treba postojati barem politika privatnosti na visokoj razini koja se primjenjuje u cijeloj kompaniji te se ukupna odgovornost za tajnost dodjeljuje rukovoditelju najviše razine ili osobi na istovjetnoj razini upravljanja.

b. Dobavljač jamči zaštitu i tajnost Osobnih podataka u vezi s Uslugama u skladu s relevantnim zakonodavstvom i propisima o zaštiti podataka.

c. Osobni podaci, uključujući uređene ili Anonimizirane Osobne podatke, ne upotrebljavaju se ni u kakve druge svrhe osim u svrhu izvršavanja ugovornih sporazuma s Ericssonom.

d. Osobni podaci prikupljeni u različite svrhe obrađuju se zasebno.

e. Osobnim podacima ne pristupa se bez prethodnog odobrenja.

f. Ovlašteno Osoblje ima pristup samo najmanjoj količini Osobnih podataka potrebnih kako bi moglo izvršavati svoje poslovne obveze.

g. Osoblje koje ima pristup Osobnim podacima dužno je redovito prolaziti odgovarajuću obuku u području tajnosti podataka.

h. Osobni podaci zadržavaju se samo toliko dugo koliko je potrebno za izvršavanje navedenih svrha u ugovornim sporazumima s Ericssonom, ili kako se zahtijeva zakonom ili propisima, te se nakon toga na odgovarajući način vraćaju ili uklanjanju prema Ericssonovu izboru.

i. Uklanjanje Osobnih podataka zapisuje se kako bi se Ericssonu potvrdilo da je doista izvršeno takvo uklanjanje.

j. Ako se zakonom ili propisom sprječava povrat ili uklanjanje nekih ili svih Osobnih podataka, čuva se tajnost ili anonimnost tih Osobnih podataka i oni se više ne obrađuju. Ericsson mora biti obaviješten o postojanju takvih obveza odmah nakon što dobavljač postane svjestan njihova postojanja.

k. Osobni podaci ne smiju se prekomjerno pohranjivati, ispisivati, kopirati, objavljivati ili Obrađivati drugim sredstvima izvan svrhe za uporabu.

l. Osobi čiji se podaci obrađuju omogućen je pristup njezinim Osobnim podacima radi pregleda.

m. U slučaju da Osoba čiji se podaci obrađuju nema izravan pristup svojim Osobnim podacima, Osobni podaci prenose se Ericssonu kako bi se podržao bilo koji zahtjev Osobe čiji se podaci obrađuju, a bez odgovaranja na zahtjev osim ako nije ovlašten za to.

n. Netočni Osobni podaci ispravljaju se kada Osoba čiji se podaci obrađuju ili Ericsson uime Osobe čiji se podaci obrađuju podnese zahtjev za ispravak.

o. Sve dok je ispravnost podataka sporna, nije omogućena obrada podataka.

p. Otkrivanje Osobnih podataka trećoj strani, kao što je Podobrađivač treće strane, dopušta se samo uz prethodni pisani pristanak Ericssona i samo u svrhe utvrđene u ugovornim sporazumima s Ericssonom. Ericsson ima pravo procjenjivati ugovorne uvjete opisane u odjeljku 3.q.

q. Prije nego što Dobavljač prenese Osobne podatke Podobrađivaču treće strane, Dobavljač osigurava da su odgovornosti Dobavljača i Podobrađivača treće strane jasno opisane i provedene kao dio komercijalnog ugovora. Na osnovi pojedinačnog slučaja analiziraju se uvjeti navedeni u nastavku:

    i. jasan sporazum da je Ericsson ili Nadzornik podataka ili Obrađivač podataka te da su Dobavljač i Podobrađivač treće strane Podobrađivači podataka;

    ii. jasan sporazum da Dobavljač ima pravo revidirati Podobrađivača treće strane u pogledu tajnosti podataka;

    iii. jasna definicija što čini Osobne podatke;

    iv. jasna definicija primjenjivog zakona / primjenjivih zakona za obradu Osobnih podataka i prijenos tih informacija preko granice;

    v. jasne upute kada i gdje se očekuje da Podobrađivač treće strane prijavi Narušavanje tajnosti;

    vi. jasne upute o sigurnosnim mjerama za zaštitu tajnosti, uključujući prikladne tehničke i organizacijske mjere za zaštitu Osobnih podataka na istoj razini zaštite koju pruža Ericsson ili razini višoj od te.

r. Podobrađivači treće strane ograničeni su samo na nužan pristup, uporabu, zadržavanje i otkrivanje Osobnih podataka potrebnih za izvršenje ugovornih obveza.

s. Osobni podaci ne prenose se u zemlju koja nije zemlja državljanstva Osobe čiji se podaci obrađuju niti im se pristupa iz te zemlje bez prethodnog pisanog pristanka Ericssona.

t. Dnevnici se vode na način koji se može revidirati, pokazujući koji su Osobni podaci preneseni u koje zemlje.

u. Poduzimaju se razumne mjere kako bi se zajamčilo da su Osobni podaci točni i precizni.

v. Dobavljač je dužan imati postupak za prijavljivanje Incidenata u vezi s tajnošću i/ili Narušavanja i rukovanje njima te rješavanje upita, pritužbi i sporova.

w. Dobavljač prijavljuje Ericssonu potvrđena Narušavanja tajnosti što je prije moguće ili kako je drukčije dogovoreno u pisanom obliku. Pri bavljenju tim izvješćima Dobavljač u potpunosti surađuje s Ericssonom.

x. Ako je to zatraženo zakonom, Dobavljač je suglasan surađivati s vladinim tijelom ili agencijom koji se bave tajnošću podataka; međutim, prije takve suradnje potrebno je obavijestiti Ericsson.

4 Sukladnost

a. Obučeno Osoblje redovito provodi unutarnje revizije i/ili procjene Dobavljača koje se odnose na sigurnost i tajnost, a rezultati se vrednuju radi mogućih korektivnih mjera.

b. Nakon 30-dnevnog zahtjeva Ericssona Dobavljač može pokazati usklađenost s ovim dokumentom i bilo kojim drugim zahtjevima u pogledu sigurnosti i tajnosti ili mjerama koje su dogovorene s Ericssonom. Utvrđena neusklađenost rješava se prema dogovoru strana.

5 Definicije

U svrhe ovoga dokumenta sljedeće riječi i izrazi imaju značenja koja im se pripisuju u nastavku osim ako bi se kontekstom očito zahtijevalo drukčije.

Anoniman	Elementi Osobnih podataka uklonjeni su kako se preostalim informacijama ne bi moglo identificirati pojedinca ili ako bi za identifikaciju trebala nerazmjerna količina vremena, troškova i napora. Također se označava kao „deidentificiran” i „anonimiziran”.
Nadzornik podataka	Fizička ili pravna osoba, javno tijelo, agencija ili neko drugo tijelo koje, samo ili zajedno s drugima, određuje svrhe i sredstva obrade Osobnih podataka.
Obrađivač podataka	Fizička ili pravna osoba, javno tijelo, agencija ili neko drugo tijelo koje obrađuje Osobne podatke uime Nadzornika podataka.
Osoba čiji se podaci obrađuju	Identificirana osoba ili osoba koja se može identificirati, a na koju se odnose određeni Osobni podaci. To je netko tko može biti identificiran, izravno ili neizravno, posebno upućivanjem na identifikacijski broj ili jedan ili više konkretnih čimbenika (fizički, fiziološki, psihički, ekonomski, kulturni, socijalni).
Imovina Ericssona	Informacijska imovina i Fizička imovina koja je povjerena Dobavljaču ili je dio usluge.
Ericssonove Informacije	Informacije koje pripadaju Ericssonu, Ericssonovim kupcima, ostalim trećim stranama koje imaju poslovne odnose s Ericssonom te druge informacije koje su dio Usluge. Ericssonove Informacije obuhvaćaju Osobne podatke.

Osobni podaci	Osobni podaci znači sve informacije koje se mogu povezati s identificiranom živom fizičkom osobom ili osobom koja se može identificirati („osoba čiji se podaci obrađuju”) ili kako je drukčije određeno zakonom, propisom ili ugovornim sporazumom. Osoba koja se može identificirati, izravno ili neizravno, posebno upućivanjem na identifikacijski broj ili jedan ili više čimbenika koji su specifični za njezin fizički, fiziološki, psihički, ekonomski, kulturni ili socijalni identitet. Pojmovi „informacije koje omogućavaju identificiranje osobe”, „Osobni podaci”, „privatne informacije”, „osjetljivi Osobni podaci”, „posebne kategorije podataka” i „zakonito zaštićene informacije” često se upotrebljavaju naizmjenično kako bi se uputilo na informacije koje se odnose na pojedince. Pojmovi „podaci o kupcu” i „informacije o pretplatniku” obično se upotrebljavaju za upućivanje na informacije koje se odnose na pretplatnike ili druge krajnje korisnike.
Osoblje	Svaka osoba koja obavlja neki posao za Ericsson uime Dobavljača.
Narušavanje tajnosti	Neovlašten pristup, uporaba ili otkrivanje Osobnih podataka na način koji nije dopušten zakonom, propisom ili ugovorom, a kojim se kompromitira sigurnost i tajnost Osobnih podataka i kojim se stvara znatan rizik od krađe identiteta, prijevare ili štete koja se može nanijeti osobi.
Incident u vezi s tajnošću	Neovlašten pristup, uporaba ili otkrivanje Osobnih podataka ili neki sličan pojam koji se odnosi na situacije u kojima osobe osim ovlaštenih korisnika, i u svrhe osim ovlaštene svrhe, imaju pristup ili mogući pristup Osobnim podacima. Ne smatraju se svi Incidenti u vezi s tajnošću Narušavanjima tajnosti.
Obrada	Obrada Osobnih podataka znači svaka radnja ili niz radnji koje se izvode nad Osobnim podacima, bilo automatskim sredstvima ili ne (na primjer: prikupljanje, zapisivanje, prilagodba ili izmjena, dohvat, savjetovanje, uporaba, otkrivanje prenošenjem, brisanje ili uništavanje itd.).

Usluga	Isporuka dobara ili usluga Ericssonu koju vrši Dobavljač.
Podugovaratelj	Poslovni partneri, proizvođači i pružatelji eksternaliziranih usluga.
Dobavljač	Trgovačko društvo koje je primilo narudžbenicu od Ericssona i pružat će Usluge.
Veza treće strane	Pristup pojedinih osoba ili tijela koja nisu dio Ericssona Ericssonovim informacijskim sustavima ili mrežama iz mreže izvan Ericssonova nadzora. Rješenje Veze treće strane primjenjuje se uvijek kad poslovni subjekt Ericssona želi uspostaviti IS/IT okruženje između vanjskoga trgovačkog društva i mreže ECN u Ericssonu sukladno Poslovnom sporazumu između Ericssona i drugih vanjskih strana. **Napomena:** Mora postojati valjani Poslovni sporazum za Vezu treće strane koji će se primjenjivati.
Podobrađivač treće strane	Podobrađivač treće strane dobavljač je koji obrađuje Ericssonove Informacije uime Dobavljača.