BINDANDE FÖRETAGSBESTÄMMELSER FÖR PERSONUPPGIFTSANSVARIGA

Sammanfattning

Detta koncerndirektiv är en uppsättning av Bindande Företagsbestämmelser för Personuppgiftsansvariga (hädanefter kallade "**C-BCR**"), som reglerar alla internationella överföringar av Personuppgifter mellan Ericssonföretag som är BCR-medlemmar.

Integritet, transparens och ansvar präglar Ericssonkoncernens verksamhet. Vi värdesätter vårt ansvar att respektera rätten till dataskydd och att införa lämpliga standarder för dataskydd vid Behandling av Personuppgifter.

Kraven som anges i C-BCR är utformade för att hjälpa Ericssonkoncernen att uppfylla kraven i EU:s allmänna dataskyddsförordning 2016/679 (GDPR) och för att tillhandahålla lämpliga skyddsåtgärder för överföring av Personuppgifter mellan alla BCR-medlemmar globalt.

Tillämplighet
C-BCR gäller för alla BCR-medlemmar, inklusive deras Anställda och Extern arbetskraft som är involverad i Behandlingen av Personuppgifter eller i utvecklingen av interna verktyg eller tjänster som används för att behandla Personuppgifter där en BCR-medlem agerar som Personuppgiftsansvarig (enskilt eller tillsammans med en annan BCR-medlem) eller som Personuppgiftsbiträde för en annan BCR-medlem (internt Personuppgiftsbiträde).

Dessa bestämmelser är tillämpliga på Behandling av Personuppgifter som helt eller delvis företas på automatisk väg samt på annan Behandling än automatisk av Personuppgifter som ingår i eller kommer att ingå i ett register.

Syfte
Att skydda den personliga integriteten och att säkerställa en säker Behandling av Personuppgifter är av yttersta vikt för Ericssonkoncernen, särskilt i samband med globala överföringar av Personuppgifter.

Främja rätten till privatliv och yttrandefrihet

I enlighet med Ericssons affärsetiska kod respekterar och främjar Ericsson mänskliga rättigheter i hela vårt arbete, inklusive genom att tillhandahålla tillgång till kommunikation och information runt om i världen.

Ericssons grundläggande övertygelse är att vår hårdvara, mjukvara samt att våratjänster och lösningar medför en positiv förändring för människor. Samtidigt arbetar Ericsson för att mildra och minimera risken för eventuellt missbruk av vår teknik.

Vi gör detta genom att genomföra due diligence kopplat till våra säljuppdrag för att bedöma, förebygga och mildra potentiella negativa effekter avseende mänskliga rättigheter. Ericsson är också en stark förespråkare för yttrandefrihet och integritetsskydd Detta inbegriper att påtala om

nya lagstiftande, administrativa, licens- eller brottsbekämpande reglerkan ha en negativ inverkan på enskilda personers yttrandefrihet eller deras rätt till integritet.

Som en del av åtagandet att värna integritet och säkerhet bedriver Ericssonkoncernen sin verksamhet i enlighet med gällande lagar och förordningar om dataskydd. C-BCR bidrar till att tydligt definiera de regler som gäller för alla BCR-medlemmars Behandling av Personuppgifter för att säkerställa en konsekvent och hög skyddsnivå för Personuppgifter i samband med överföringar mellan BCR-medlemmar.

Innehåll

1. Direktiv

1.1 Introduktion

Begreppen i C-BCR har samma betydelse som de har i GDPR. Terminologitabellen i avsnitt 11 innehåller definitioner av de huvudsakliga begreppen.

GDPR kräver att överföring av Personuppgifter till länder utanför EU/EES som inte har en adekvat nivå av dataskydd ska ges lämpliga skyddsåtgärder för att skydda integriteten, individers grundläggande rättigheter och friheter samt utövandet av rättigheter.

C-BCR är ett sätt att tillhandahålla lämpliga skyddsåtgärder. De kan användas för att lagligt överföra (inklusive bevilja åtkomst till) Personuppgifter mellan olika juridiska personer inom samma företagsgrupp. C-BCR bidrar till att säkerställa att samma skyddsnivå för Personuppgifter appliceras av alla BCR-medlemma. Ericssonkoncernen har implementerat ett koncernövergripande program för regelefterlevnad av dataskydd och har utsett (i) ett koncernövergripande Dataskyddsombud ("GDPO") och (ii) en Group Privacy Head/Chief Privacy Officer, vars respektive team är involverade i tillsynen och säkerställandet av efterlevnad samt genomförandet av Ericssons Integritetspolicy.

Chief Privacy Officer och integritetsteamet samt, i förekommande fall GDPO:s team, ansvarar för tillsynen av Ericssons Integritetspolicy och rapporterar till den högsta ledningsnivån inom Ericsson. Chief Privacy Officer eller GDPO kan informera den högsta ledningsnivån om det uppstår några frågor eller utmaningar under utförandet av deras uppgifter. Dessutom finns det en Head of Product Privacy som arbetar specifikt med inbyggt dataskydd och produktintegritetsfrågor och dedikerade resurser som arbetar specifikt med HR-frågor.

1.2 Bindande karaktär

1.2.1 Skyldighet att beakta C-BCR

Alla BCR-medlemmar, inklusive deras Anställda och Externa arbetskraft, har en skyldighet att beakta C-BCR.

Ericssonkoncernens interna policyer lyfter fram styrelsens och koncernledningens åtagande att säkerställa att C-BCR följs.

Alla BCR-medlemmar, inklusive deras Anställda **och** Externa **arbetskraft, har en skyldighet att endast behandla** Personuppgifter **på instruktion från den** Personuppgiftsansvarige **BCR-medlemmen, inklusive** säkerhets- och konfidentialitetsåtgärder**.**

1.2.2 Bindande verkan för BCR-medlemmar

För att vara bundna av C-BCR har BCR-medlemmarna ingått ett Koncerninternt Avtal. Varje ändring, revidering, rättelse eller tillägg till C-BCR ska automatiskt gälla för varje BCR-medlem.

Ingen dataöverföring kan göras i enlighet med C-BCR från ett Ericssonföretag till ett annat förrän det mottagande Ericsson-företaget har undertecknat det Koncerninterna Avtalet och blivit BCR-medlem.

1.2.3 Bindande verkan för Anställda och Extern arbetskraft

C-BCR är bindande för Anställda och Extern arbetskraft. Alla som arbetar inom Ericssonkoncernen måste bekräfta att de har läst och förstått Ericssons affärsetiska kod, som de måste följa. Dessutom måste Anställda och Extern arbetskraft underteckna individuella sekretessavtal. Den affärsetiska koden innehåller en föreskrift om att följa Ericssonkoncernens policyer, direktiv och instruktioner samt lokala direktiv och instruktioner, av vilka C-BCR är en. Underlåtenhet att göra detta kan leda till disciplinära åtgärder, inklusive uppsägning och/eller civilrättsligt och straffrättsligt ansvar.

I enlighet med Ericssons affärsetiska kod skyddar Ericsson Personuppgifter och stödjer globala ansträngningar för att bevara dessa. Ericsson följer globala integritetsprinciper och tillämpliga lagar, inklusive GDPR. Ericsson har också dessa C-BCR och avtal som reglerar hur vi behandlar och delar data.

1.3 Materiellt tillämpningsområdet för C-BCR

C-BCR gäller för all överföring av Personuppgifter mellan BCR-medlemmar, inklusive överföringar till BCR-medlemmar utanför EU/EES.

Ericssonkoncernen behandlar i första hand Personuppgifter som rör Anställda, Extern arbetskraft, besökare, aktieägare, kundrepresentanter, leverantörer, kandidater och andra affärsrelaterade tredje parter. Behandlingen förekommer inom Ericssonkoncernen av de olika Ericssonbolagen; inklusive men inte begränsat till interna enheter, geografiska organisationer och följande koncernfunktioner:

(a) Human Resources (personalfunktion)

(b) Finans

(c) Juridik och regelefterlevnad

(d) Företagsrevision

(e) Säkerhet

(f) Inköp

(g) Försäljning

(h) Marknadsföring

Information relaterad till typen av de Personuppgifter som överförs och Behandlingstyper beskrivs i bilaga 2.Ericssonkoncernens interna dataflöden är globala till sin natur, vilket återspeglar den sammanlänkade och internationella närvaron av affärsverksamheten. Den största delen av Personuppgifterna exporteras dock av Ericsson AB i Sverige till Ericssonkoncernens interna supportcenter i Kina, Indien, Filippinerna, Mexiko, Rumänien, Spanien och USA. Överföringar sker huvudsakligen i form av fjärråtkomst till servrar belägna inom EES.

2. Principer för dataskydd

2.1 Laglig och rättvis Behandling

BCR-medlemmar ska endast behandla Personuppgifter på ett lagligt och rättvist sätt och när det är tillåtet att göra det i enlighet med en rättslig grund enligt tillämpliga dataskyddslagar. Nedan följer en uttömmande lista över alla rättsliga grunder för Behandling som BCR-medlemmarna avser att förlita sig på.

(a) Den Registrerade har otvetydigt gett sitt samtycke till Behandlingen;

(b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den Registrerade är part eller för att vidta åtgärder på begäran av den Registrerade innan ett avtal ingås;

(c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den

(d) Personuppgiftsansvarige Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den Registrerade eller för en annan fysisk person.

(e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den Personuppgiftsansvariges myndighetsutövning; eller

(f) Behandlingen är nödvändig för ändamål som rör den Personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den Registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av Personuppgifter, särskilt när den Registrerade är ett barn.

2.2 Öppenhet

BCR-medlemmar ska endast behandla Personuppgifter på ett transparent sätt och ska informera de Registrerade om hur deras Personuppgifter kommer att användas. Informationen kommer vanligtvis att tillhandahållas genom en integritetspolicy.

Om en BCR-medlem inte erhåller Personuppgifterna den Registrerade, ska BCR-medlemmen förse den Registrerade med information inom en rimlig period efter att ha erhållit Personuppgifterna, men senast inom en månad, med beaktande av de specifika omständigheter

under vilka Personuppgifterna behandlas eller, om Personuppgifterna ska användas för kommunikation med den Registrerade, senast vid tidpunkten för den första kommunikationen till den Registrerade eller, om ett utlämnande till en annan mottagare förutses,, senast vid den tidpunkt då uppgifterna först lämnas ut för första gången. Denna regel är tillämplig såvida det inte finns en legitim grund för att inte göra det, såsom rättsliga förfaranden, beskattningsfrågor, förebyggande eller upptäckt av ett brott, där undanhållande av information är nödvändig för att skydda nationell säkerhet eller försvar, eller där det på annat sätt är tillåtet enligt lag. .

Information till Registrerade avseende BCR-medlemmars Behandling av Personuppgifter ska uppfylla kraven i GDPR.

2.3 Ändamålsbegränsning

BCR-medlemmar ska endast samla in Personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

2.4 Uppgiftsminimering och riktighet

BCR-medlemmar ska vidta nödvändiga åtgärder för att säkerställa att Personuppgifter är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, samt att uppgifterna är riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att Personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

2.5 Lagringsminimering

BCR-medlemmar får inte förvara Personuppgifter **i en form som möjliggör identifiering av den** Registrerade **under en längre tid än vad som är nödvändigt för de ändamål för vilka** Personuppgifterna **behandlas samt i enlighet med relevant nationell lagstiftning**.

2.6 Särskilda Kategorier av Personuppgifter

Särskilda Kategorier av Personuppgifter är föremål för särskilt rättsligt skydd enligt GDPR. I tillämpliga fall ska sådana kategorier av Personuppgifter och lämpliga säkerhetsåtgärder för Behandling av sådana uppgifter specifikt beskrivas av den berörda BCR-medlemmen. Särskilda Kategorier av Personuppgifter får endast behandlas med stöd av följande specifika rättsliga grunder:.

(a) Den Registrerade har gett sitt uttryckliga samtycke till Behandling av särskilda kategorier av Personuppgifter, förutom där tillämpliga förbjuder detta;

(b) Behandlingen är nödvändig för att den Personuppgiftsansvarige eller den Registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den

omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den Registrerades grundläggande rättigheter och intressen fastställs;

(c) Behandlingen är nödvändig för att skydda den Registrerades eller någon annan fysisk persons grundläggande intressen när den Registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke;

(d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att Behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och Personuppgifterna inte lämnas ut utanför det organet utan den Registrerades samtycke;

(e) Behandlingen avser Personuppgifter som på ett tydligt sätt har offentliggjorts av den Registrerade;

(f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk;

(g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse;

(h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, Behandling, social omsorg, och när Personuppgifterna behandlas av hälso- och sjukvårdspersonal som enligt nationell lagstiftning eller nationella bestämmelser som fastställts av nationella behöriga organ omfattas av tystnadsplikt eller av en annan person som också omfattas av motsvarande tystnadsplikt. .

(i) Behandlingen är nödvändig av hänsyn till allmänintresset på folkhälsoområdet, eller

(j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

BCR-medlemmar får endast behandla Personuppgifter som rör fällande domar i brottmål och lagöverträdelser när sådan Behandling är tillåten enligt EU:s eller medlemsstaternas lagstiftning..

2.7 Säkerhet, integritet och konfidentialitet

BCR-medlemmar ska följa Ericssonkoncernens standardsäkerhetsåtgärder som anges i tillämpliga styrdokument för koncernen, inklusive lämpliga tekniska och organisatoriska åtgärder. Sådana åtgärder är utformade för att skydda Personuppgifter mot t.ex. obehörig eller otillåten Behandling, oavsiktlig förlust, förstörelse eller skada.

Säkerhetsåtgärder kommer att utformas med vederbörlig hänsyn till de särskilda risker som Behandlingen medför. De kan omfatta:

(a) Pseudonymisering och/eller kryptering av Personuppgifter;

(b) Åtgärder som säkerställer förmågan att säkerställa kontinuerlig konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och tjänster;

(c) Åtgärder som säkerställer möjligheten att återställa tillgängligheten och åtkomsten till Personuppgifter i tid vid en fysisk eller teknisk incident; och

(d) Processer för regelbunden testning, bedömning och utvärdering av effektiviteten hos tekniska och organisatoriska åtgärder för att säkerställa säkerheten vid Behandlingen.
.

Åtkomsträttigheter till Personuppgifter beviljas individuellt på behovsbasis i enlighet med Ericssons Integritetspolicy. Anställda och Extern arbetskraft som har åtkomst till Personuppgifter ska uppfylla sekretesssåtaganden enligt gällande sekretessavtal.

Ericssons ledningssystem för informationssäkerhet är för närvarande globalt certifierat enligt ISO/IEC 27001.

All Behandling som utförs av externa eller interna Personuppgiftsbiträden eller underbiträden på uppdrag av en BCR-medlem måste omfattas av ett skriftligt Personuppgiftsbiträdesavtall. Ett sådant skriftligt avtal ska ange föremålet för, varaktigheten, arten och syftet med Behandlingen, typen av Personuppgifter och kategorier av Registrerade samt den Personuppgiftsansvariges skyldigheter och rättigheter. Det skriftliga avtalet ska också särskilt ange att Personuppgiftsbiträdet:

(a) behandlar Personuppgifterna endast enligt dokumenterade instruktioner från den Personuppgiftsansvarige;

(b) säkerställer att personer med behörighet att behandla Personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt;

(c) vidtar alla nödvändiga åtgärder för att bedöma och implementera lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken,

(d) inte anlitar ett underbiträde utan föregående skriftligt godkännande från den Personuppgiftsansvarige, och säkerställer, vid sådan auktorisation och vid anlitande av ett underbiträde, att samma skyldigheter gällande dataskydd som anges i det skriftliga avtalet med den Personuppgiftsansvarige åläggs underbiträdet genom ett avtal;

(e) ska hjälpa den Personuppgiftsansvariga genom lämpliga tekniska och organisatoriska åtgärder så att den Personuppgiftsansvariga kan fullgöra sin skyldighet att svara på begäran om utövande av den Registrerades rättigheter;

(f) bistår den Personuppgiftsansvarige med att säkerställa efterlevnad av skyldigheterna att (i) bedöma och implementera lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken; (ii) anmäla en Personuppgiftsincident till Tillsynsmyndigheten; (iii) informera Registrerade om en Personuppgiftsincident som sannolikt medför en hög risk för fysiska personers rättigheter och friheter; (iv) genomföra en Konsekvensbedömning avseende dataskydd; och (v) samråda med Tillsynsmyndigheten innan Behandling påbörjas, om en Konsekvensbedömning avseende dataskydd indikerar att Behandlingen skulle medföra en hög risk utan åtgärder från den Personuppgiftsansvarige för att minska risken;

(g) På den Personuppgiftsansvariges begäran raderar eller återlämnar alla Personuppgifter till den Personuppgiftsansvarige efter att tillhandahållandet av tjänster relaterade till Behandlingen har avslutats; och

(h) Tillhandahåller den Personuppgiftsansvarige all information som krävs för att påvisa efterlevnad av de skyldigheter som anges i punkterna (a)–(g) ovan och möjliggör samt bidrar till revisioner som genomförs av eller på uppdrag av den Personuppgiftsansvarige.

2.8 Skyldighet att samarbeta med den Personuppgiftsansvariga

BCR-medlemmar som agerar som interna Personuppgiftsbiträden måste följa koncerninterna instruktioner om Behandling, överföring, säkerhet, rapportering av Personuppgiftsincidenter samt uppsägning, och omedelbart informera säkerhetsfunktionen inom Ericsson-koncernen och den BCR-medlem som agerar som Personuppgiftsansvarig om efterlevnad inte kan uppnås.

BCR-medlemmar som agerar som interna Personuppgiftsbiträden har också en skyldighet att hjälpa BCR-medlemmar som agerar som Personuppgiftsansvariga att följa och visa efterlevnad av tillämpliga dataskyddslagar (t.ex. dess skyldighet att respektera den Registrerades rättigheter, att hantera klagomål eller att svara på förfrågningar och/eller utredningar från Tillsynsmyndigheterna).

2.9 Rapportering av Personuppgiftsincidenter

BCR-medlemmar ska rapportera en Personuppgiftsincident på följande sätt:

- när en BCR-medlem som agerar som Personuppgiftsbiträde blir medveten om en Personuppgiftsincident ska denna utan onödigt dröjsmål meddela Ericsson AB och GDPO eller Chief Privacy Officer, beroende på situationen, samt till den BCR-medlem som agerar som Personuppgiftsansvarig, och respektive DPO.. På samma sätt bör BCR-medlemmar som agerar som underbiträden informera Personuppgiftsbiträdet om en misstänkt eller upptäckt Personuppgiftsincident.

- utan onödigt dröjsmål och, om möjligt, senast 72 timmar efter det att ha blivit medveten om Personuppgiftsincidenten meddela den behöriga Tillsynsmyndigheten såvida det inte

är osannolikt att Personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter, och

- utan onödigt dröjsmål meddela Registrerade, om Personuppgiftsincidenten sannolikt kommer att leda till en hög risk för deras rättigheter och friheter.

Personuppgiftsincidenter bör dokumenteras (inbegripet omständigheterna kring Personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits).Sådan dokumentation bör på begäran göras tillgänglig för den behöriga Tillsynsmyndigheten.

Ericssonkoncernen har implementerat processer med obligatoriska instruktioner för att säkerställa att säkerhets, - personuppgifts- och relaterade incidenter rapporteras och hanteras på ett korrekt sätt för att undvika onödig skada och kostnad samt för att uppfylla lagar, regler och avtalsförpliktelser.

2.10 Begränsningar för överföring och vidareöverföring till externa Personuppgiftsbiträden och Personuppgiftsansvariga (som inte är medlemmar i Ericsson-koncernen)

BCR-medlemmar ska säkerställa att lämpliga skyddsåtgärder tillämpas för all överföring av Personuppgifter utanför EU/EES när så krävs. BCR-medlemmar får endast överföra Personuppgifter till externa Personuppgiftsansvariga och Personuppgiftsbiträden utanför EU/EES om minst ett av följande gäller:

(a) Mottagarlandet har av Europeiska kommissionen bedömts ge tillräckligt skydd.

(b) Överföringen omfattas av EU:s standardavtalsklausuler. Det är BCR-medlemmens ansvar att, vid behov och med hjälp av den tredje parten, bedöma om den skyddsnivå som krävs enligt EU-lagstiftningen beaktas i tredjelandet, för att avgöra om de garantier som ges i EU:s standardavtalsklausuler kan uppfyllas i praktiken. Om så inte är fallet måste den tredje parten vidta kompletterande åtgärder för att säkerställa en väsentligen likvärdig skyddsnivå som den som tillhandahålls i EU/EES, eller

(c) Andra lämpliga skyddsåtgärder, såsom ett juridiskt bindande och verkställbart instrument mellan offentliga myndigheter eller organ, standardklausuler för dataskydd som antagits av en Tillsynsmyndighet och godkänts av kommissionen, eller en godkänd uppförandekod eller certifieringsmekanism tillsammans med bindande och verkställbara åtaganden från den Personuppgiftsansvarige eller Personuppgiftsbiträdet i tredjeland att tillämpa lämpliga skyddsåtgärder, inklusive när det gäller Registrerades rättigheter..

Under särskilda omständigheter kan BCR-medlemmar överföra Personuppgifter till en tredje part utanför EU/EES utan att behöva vidta ovanstående åtgärder om något av följande villkor är uppfyllt:

(a) Den Registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den

Registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder;

(b) Överföringen är nödvändig för att fullgöra ett avtal mellan den Registrerade och BCR-medlemmen eller för att genomföra åtgärder som föregår ett sådant avtal på den Registrerades begäran;

(c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan BCR-medlemmen och en annan fysisk eller Juridisk Person i den Registrerades intresse;

(d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset..

(e) Överföringen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk;

(f) Överföringen är nödvändig för att skydda den Registrerades eller andra personers grundläggande intressen, när den Registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke; eller

(g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

Därutöver, om en överföring inte kan grundas på något av de villkor som anges ovan, får en överföring till ett tredjeland äga rum endast om överföringen inte är repetitiv, endast gäller ett begränsat antal Registrerade, är nödvändig för ändamål som rör BCR-medlemmens tvingande berättigade intressen och den Registrerades intressen eller rättigheter och friheter inte väger tyngre. BCR-medlemmen ska även ha bedömt alla omständigheter kring dataöverföringen och har på grundval av denna bedömning tillhandahållit lämpliga skyddsåtgärderavseendeskyddet av Personuppgifter. Den BCR-medlem som agerar som Personuppgiftsansvarig ska i sådana fall informera Tillsynsmyndigheten om överföringen samt informera den Registrerade om överföringen och de tvingande berättigade intressen som eftersträvas.

2.11 Begränsningar för överföringar till BCR-medlemmar

BCR-medlemmarna kommer att använda C-BCR:er som verktyg för överföringar endast efter att ha bedömt att lagstiftningen och praxis i det tredjeland dit överföringen sker, som gäller för Behandling av Personuppgifter av den BCR-medlem som agerar som Data Importör, inklusive eventuella krav på utlämnande av Personuppgifter eller åtgärder som möjliggör åtkomst för offentliga myndigheter, inte hindrar dem från att uppfylla sina skyldigheter enligt dessa C-BCR. Vid behov måste kompletterande kontraktuella, tekniska eller organisatoriska skyddsåtgärder genomföras av BCR-medlemmen i tredjeland för att säkerställa en likvärdig adekvat skyddsnivå som tillhandahålls i EU/EES. Där det krävs ytterligare skyddsåtgärder, utöver de som omfattas av C-BCR:erna, ska Ericsson AB, som ansvarig enhet, samt GDPO, Chief Privacy Officer, lokala

DPO:er, Privacy managers och andra relevanta funktioner informeras och involveras i en sådan bedömning.

Vid bedömningen av lagar och praxis i tredjeland som kan påverka efterlevnaden av de åtaganden som ingår i C-BCR:erna, ska BCR-medlemmarna särskilt beakta följande element::

(a) De särskilda omständigheterna för överföringarna eller en uppsättning av överföringar och för eventuella planerade vidareöverföringar inom samma tredjeland eller till ett annat tredjeland, inbegripet följande:

(i) ändamål för vilka Personuppgifterna överförs och behandlas;

(ii) Typer av juridiska personer som är involverade i Behandlingen (Importören och eventuella ytterligare mottagare av eventuell vidareöverföring).

(iii) ekonomisk sektor där överföringen eller gruppen av överföringar äger rum.

(iv) kategorier och format av de överförda Personuppgifterna;

(v) Plats för Behandlingen, inklusive lagring samt överföringskanaler som används och

(vi) överföringskanaler som används.

(b) De lagar och praxis i det tredjeland dit överföringen sker som är relevanta med hänsyn till omständigheterna kring överföringen, inklusive de som kräver utlämnande av data till offentliga myndigheter eller som tillåter åtkomst av sådana myndigheter, samt de som medger åtkomst till dessa data under transit mellan landet för Exportören och landet för Importören, tillsammans med de tillämpliga begränsningarna och skyddsåtgärderna. .

(c) Alla relevanta kontraktuella, tekniska eller organisatoriska skyddsåtgärder som vidtagits för att komplettera skyddsåtgärderna enligt C-BCR, inklusive åtgärder som vidtas under överföringen och Behandlingen av Personuppgifterna i destinationslandet.

Bedömningen ovan bygger på förutsättningen att lagar och praxis respekterar det väsentliga innehållet i de grundläggande rättigheterna och friheterna, och inte går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda de mål som anges i artikel 23.1 i GDPR samt inte strider mot C-BCR.

Om adekvata kompletterande åtgärder inte har kunnat vidtas kommer de aktuella överföringarna att förhindras eller avslutas.

BCR-medlemmarna måste dokumentera bedömningen och på begäran göra den tillgänglig för den behöriga Tillsynsmyndigheten. De bestämmelser som fastställts av Ericssonkoncernen för att utföra denna bedömning (t.ex. verktyg, instruktioner om utförande och utvärdering) måste följas.

3. De Registrerades rättigheter

Registrerade vars Personuppgifter behandlas av BCR-medlemmar har vissa dataskyddsrättigheter som de kan utöva på begäran. Dessa inkluderar:

(a) Rätten att bli ***informerad*** av den Personuppgiftsansvarige om Behandlingen av deras Personuppgifter, inklusive kategorier av Personuppgifter som Behandlingen gäller, ändamålen med den Behandling för vilken Personuppgifterna är avsedda samt den rättsliga grunden för Behandlingen, mottagarna eller de kategorier av mottagarare, att Personuppgifterna ska överföras till ett tredjeland eller en internationell organisation och grunden för en sådan överföring, perioden eller de kriterier som används för att fastställa perioden under vilken Personuppgifterna kommer att lagras; de Registrerades rättigheter; förekomsten av, betydelsen och de förutsedda följderna av automatiserat beslutsfattande; om den Registrerade är skyldig att tillhandahålla Personuppgifterna; och, när Personuppgifterna inte har erhållits från den Registrerade, varifrån Personuppgifterna kommer. Informationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. .

(b) Rätten att få bekräftelse från den Personuppgiftsansvarige huruvida deras Personuppgifter behandlas eller inte, och om så är fallet, ***tillgång*** till Personuppgifterna genom att förses med en kopia av de Personuppgifter som behandlas, tillsammans med information om ändamålen med Behandlingen, de kategorier av Personuppgifter som berörs, mottagarna eller kategorierna av mottagare av Personuppgifterna, perioden eller de kriterier som används för att fastställa perioden under vilken Personuppgifterna kommer att lagras; de Registrerades rättigheter; när Personuppgifterna inte har erhållits från den Registrerade, varifrån Personuppgifterna kommer; förekomsten av, betydelsen och de förutsedda följderna av automatiserat beslutsfattande; och lämpliga skyddsåtgärder när Personuppgifter överförs till ett tredjeland eller en internationell organisation. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

(c) Rätten att få felaktiga Personuppgifter ***rättade*** och, med hänsyn till ändamålen med Behandlingen, få ofullständiga Personuppgifter ***kompletterade***, bland annat genom att tillhandahålla ett kompletterande utlåtande. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

(d) Rätten att få Personuppgifter ***raderade*** när de inte längre är nödvändiga för de ändamål för vilka de samlades in eller på annat sätt behandlats, i händelse av ett återkallande av det samtycke som Behandlingen grundar sig i och där det inte finns

någon annan rättslig grund för Behandlingen, i händelse av invändning mot Behandlingen och det saknas berättigade skäl för Behandlingen; när Personuppgifterna har behandlats på ett olagligt sätt eller måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller medlemsstaternas nationella rätt som den Personuppgiftsansvarige omfattas av; eller när Personuppgifterna har samlats in i samband med erbjudandet av informationssamhällets tjänster. Rätten till radering gäller inte i den utsträckning Behandlingen är nödvändig för att utöva rätten till yttrande- och informationsfrihet; för att uppfylla en rättslig förpliktelse som kräver Behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den Personuppgiftsansvarige omfattas av, eller för att utföra en uppgift av allmänt intresse; för skäl av allmänt intresse på folkhälsoområdet eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål; eller för att upprätta, göra gällande eller försvara rättsliga anspråk. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. .

(e) Rätten att begära en ***begränsning*** av Behandlingen av Personuppgifter till specifika ändamål eller när riktigheten av Personuppgifterna ifrågasätts (under en period som möjliggör för den Personuppgiftsansvarige att verifiera riktigheten) eller när Behandlingen är olaglig och radering motsätts till förmån för begränsning av användningen eller när den Personuppgiftsansvarige inte längre behöver Personuppgifterna, men de fortfarande krävs av den Registrerade för att fastställa, utöva eller försvara rättsliga anspråk; eller när den Registrerade har invänt mot Behandlingen i avvaktan på verifiering av om den Personuppgiftsansvariges berättigade skäl väger tyngre än den Registrerades.. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. .

(f) Rätten att bli ***underrättad*** om rättelse eller radering av Personuppgifter eller begränsning av Behandlingen. Kommunikationen ska tillhandahållas i en en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

(g) Rätten att få de Personuppgifter som den Registrerade tillhandahållit den Personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa Personuppgifter till en annan Personuppgiftsansvarig (***dataportabilitet***), inklusive, ha rätt till överföring av Personuppgifterna direkt från en Personuppgiftsansvarig till en annan, när detta är tekniskt möjligt och där Behandlingen baseras på den Registrerades samtycke eller på grundval av att det är nödvändigt för att fullgöra ett avtal. Kommunikationen ska tillhandahållas i koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk..

(h) Rätten att ***göra invändningar mot*** Behandlingen av Personuppgifter, inbegripet profilering och direktmarknadsföring, om Behandlingen grundar sig på att den är nödvändig för att utföra en uppgift av allmänt intresse eller för ändamål som rör den Personuppgiftsansvariges eller en tredje parts legitima intressen. I ett sådant fall ska

den Personuppgiftsansvarige upphöra med att behandla Personuppgifterna om den inte kan påvisa avgörande berättigade skäl för Behandlingen som väger tyngre än den Registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk. I händelse av en invändning mot Behandlingen av Personuppgifter för direktmarknadsföringsändamål ska den Personuppgiftsansvarige alltid upphöra med att behandla Personuppgifterna. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk..

(i) Rätten att inte bli utvärderad eller föremål för beslut som enbart grundar sig på ***automatiserat individuellt beslutsfattande***, inklusive profilering, som har rättsliga följder för den Registrerade eller på liknande sätt i betydande grad påverkar den Registrerade, såvida inte Behandlingen grundar sig på den Registrerades uttryckliga samtycke, alternativt att Behandlingen är nödvändig för att ingå eller för att fullgöra ett avtal mellan den Registrerade och en Personuppgiftsansvarig eller är tillåten enligt unionsrätten eller en medlemsstats nationella rätt som den Personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den Registrerades rättigheter, friheter och berättigade intressen. Kommunikationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk och

(j) Rätten att lämna in ett klagomål till en Tillsynsmyndighet, enligt vad som anges i avsnitt 4.3, utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel.

BCR-medlemmar ska svara på alla frågor eller förfrågningar från Registrerade i samband med ovanstående och ska följa de Interna Klagomålsmekanismer som anges i avsnitt 7.

4. Verkställande av C-BCR – Rättigheter som berättigad tredjepart (tredjepartsberättigande)

4.1 Tillgång till information om rättigheter för berättigade tredjeparter

Alla Registrerade med rättigheter som berättigad tredje part (tredjepartsberättigade) ska förses med information om sina rättigheter avseende Behandlingen av deras Personuppgifter och om hur de kan utöva dessa rättigheter. Alla Registrerade ska också, på ett tydligt, begripligt och transparent sätt förses med aktuell information om omfattningen av de C-BCR, Ericsson-koncernens ansvar, dataskyddsprinciperna, lagligheten av Behandlingen, Personuppgiftsincidenter, begränsningen av vidareöverföringar och de Registrerades rättigheter. BCR:erna är en del av Ericssons Integritetspolicy och publiceras som sådana på intranätet för enkel och obegränsad åtkomst för alla inom Ericssonkoncernen.

För att säkerställa öppenhet och enkel åtkomst ska Ericsson AB se till att en kopia av C-BCR tillhandahålls alla Anställda och all Extern Arbetskraft via intranätet samt tillhandahålla dessa på Registrerades begäran. För att säkerställa öppenhet och enkel åtkomst till C-BCR för Registrerade utanför Ericssonkoncernen (dvs. som inte har tillgång till intranätet) ska dessutom

C-BCR finnas tillgängliga på Ericssonkoncernens webbplats https://www.ericsson.com/en/legal/privacy.

Alla Registrerade kan också begära en kopia av C-BCR genom att skicka ett e-postmeddelande till privacy.bcr@ericsson.com.

4.2 Verkställbara delar av C-BCR

De Registrerade ska ha rätt att verkställa följande delar av C-BCR i egenskap av tredjepartsberättigade:

(a) Principerna för dataskydd, Behandlingens laglighet samt säkerhet och Personuppgiftsincidentrapportering (avsnitt 2.1-2.10);

(b) Öppenhet och enkel tillgång till C-BCR (avsnitt 2.2 och 1.1);

(c) Rätt till information, åtkomst, rättelse, radering, begränsning, underrättelse om rättelse, radering eller begränsning, invändning mot Behandling, rätt att inte bli föremål för beslut som enbart grundar sig på automatiserad Behandling, inklusive profilering (avsnitt 3);

(d) Nationella lagar och praxis som påverkar efterlevnaden av C-BCR och i händelse av myndighetsförfrågningar om åtkomst (avsnitt 6.5 och 6.6);

(e) Rätt att klaga via Ericssonkoncernens Interna Klagomålsmekanism (avsnitt 7);

(f) Samarbetsskyldighet med Behöriga Tillsynsmyndigheter (avsnitt 6.3);

(g) Bestämmelser om ansvar och jurisdiktion (avsnitt 5);

(h) Laglig och rättvis Behandling (avsnitt 2.1);

(i) Säkerhet, integritet och konfidentialitet (avsnitt 2.7);

(j) Begränsningar för överföring och vidareöverföring till externa Personuppgiftsbiträden och Personuppgiftsansvariga (som inte är medlemmar i Ericsson-koncernen) (avsnitt 2.10);

(k) Skyldighet att informera de Registrerade om alla uppdateringar av C-BCR och av listan över BCR-medlemmar (avsnitt 9);

(l) Rätt till effektivt rättsmedel, prövning och ersättning (avsnitt 4.4); och

(m) Rättigheter för berättigade tredjeparter (avsnitt 1.1 och 4.1).

De Registrerades rättigheter som berättigade tredjeparter omfattas av de avsnitt som anges ovan och omfattar inte några andra avsnitt i C-BCR. Dessutom är tredje parts rättigheter relaterade till Personuppgifter som överförs från EU/EES till ett tredje land.

4.3 Rätt att inge klagomål

Den Registrerade ska ha rätt att inge klagomål till en Tillsynsmyndighet. Den Registrerade kan välja att lämna in ett sådant klagomål till Tillsynsmyndigheten i den medlemsstat där han eller hon har sin hemvist, arbetsplats eller där den påstådda överträdelsen skett.

Den Registrerade ska också ha rätt att lämna in ett klagomål till behörig domstol i en medlemsstat; antingen där BCR-medlemmen har ett verksamhetsställe eller där den Registrerade har sin hemvist.

4.4 Rätt till effektivt rättsmedel

Den Registrerade ska ha rätt till effektivt rättsmedel samt rätt till prövning och i förekommande fall ersättning vid överträdelse av någon av de verkställbara delarna av C-BCR enligt vad som anges i avsnitt 4.2.. BCR-medlemmarna accepterar att Registrerade kan företrädas av ett icke-vinstdrivande organ, förening eller sammanslutning som har bildats i enlighet med lagstiftningen i en medlemsstat, har stadgeenliga mål som är av allmänt intresse och som är verksam inom området för skydd av de Registrerades rättigheter och friheter i förhållandet till skyddet av deras Personuppgifter, där detta föreskrivs i medlemsstaternas lagstiftning.

5. Ansvar

5.1 Ansvar för överträdelser mot C-BCR som begås av BCR-medlemmar i EU/EES

Varje BCR-medlem i EU/EES tar ansvar för och samtycker till att vidta nödvändiga åtgärder för att avhjälpa bristande efterlevnad av de verkställbara delarna av C-BCR som anges i avsnitt 4.1 och åtar sig och att betala ersättning för eventuella materiella eller immateriella skador som uppstår till följd av en sådan BCR-medlems överträdelse av C-BCR.

BCR-medlemmen har bevisbördan för att visa att den inte är ansvarig för den påstådda överträdelsen av C-BCR. BCR-medlemmen är fri från ansvar om den kan bevisa att den Registrerade inte har lidit någon skada som BCR-medlemmen skulle vara skyldig att ersätta enligt GDPR.

5.2 Ansvar för överträdelser av C-BCR som begås av BCR-medlemmar utanför EU/EES

Ericsson AB tar ansvar för och samtycker till att vidta nödvändiga åtgärder för att avhjälpa BCR-medlemmars utanför EU/EES bristande efterlevnad av C-BCR samt att betala ersättning för eventuella väsentliga eller immateriella skador till följd av sådana BCR-medlemmars överträdelse av C-BCR. Ericsson AB:s ansvar i detta avseende omfattar endast Personuppgifter som har överförts enligt dessa C-BCR från EU/EES till tredje land. Alla anspråk från Registrerade omfattas av de nationella domstolarnas jurisdiktion och behöriga Tillsynsmyndigheterna i EU/EES. Den Registrerade kommer att ha samma rättigheter och effektiva rättsmedel mot Ericsson AB som om överträdelsen hade orsakats av Ericsson AB i Sverige. Om de Registrerade kan visa att de har lidit skada och lägga fram fakta som visar att det är sannolikt att skadan har uppstått på grund av

överträdelsen av C-BCR, ankommer det på Ericsson AB att bevisa att BCR-medlemmen utanför EU/EES inte var ansvarig för överträdelsen av de C-BCR som gav upphov till skadan, eller att någon sådan överträdelse inte ägde rum.

6. Krav för Ericssonkoncernen

6.1 Ansvarsskyldighet, register över Behandling och insatser för regelefterlevnad

Varje BCR-medlem som agerar som Personuppgiftsansvarig är ansvarig för och måste kunna visa efterlevnad av C-BCR (*ansvarsskyldighet*), bland annat genom implementering av lämpliga tekniska och organisatoriska åtgärder för att säkerställa inbyggt dataskydd och dataskydd som standard (avsnitt 2.7 och 6.2 av dessa C-BCR).

Varje BCR-medlem måste föra ett skriftligt register, i elektronisk form, över alla kategorier av personuppgiftsbehandling som överförts enligt dessa C-BCR. Denna dokumentation bör på begäran göras tillgänglig för de behöriga Tillsynsmyndigheterna.

För en BCR-medlem som agerar som Personuppgiftsansvarig bör registret innehålla namn och kontaktuppgifter för BCR-medlemmen, samt i tillämpliga fall, dess företrädare samt dataskyddsombudet, information om ändamålen med Behandlingen, en beskrivning av kategorierna av Registrerade och kategorierna av Personuppgifter, information om de kategorier av mottagare till vilka Personuppgifterna har lämnats ut eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer, inbegripet identifiering av tredjelandet eller den internationella organisationen och, när så krävs, dokumentation av lämpliga skyddsåtgärder. Registret ska också, när så är möjligt, innehålla information om de förutsedda tidsfristerna för radering av de olika kategorierna av Personuppgifter och en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits.

För en BCR-medlem som agerar som Personuppgiftsbiträde bör registret innehålla namn och kontaktuppgifter för den BCR-medlem som agerar som Personuppgiftsbiträde och för varje Personuppgiftsansvarige för vars räkning BCR-medlemmen agerar, och, i förekommande fall, dess företrädare och ett dataskyddsombud. information om de kategorier av Behandling som utförs för den Personuppgiftsansvariges räkning; i tillämpliga fall, information om överföring av Personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, om så krävs, dokumentation av lämpliga skyddsåtgärder vid sådana överföringar; samt, om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits.

Om en BCR-medlems Behandling av Personuppgifter som överförts enligt dessa C-BCR:er sannolikt kommer att resultera i en hög risk för fysiska personers rättigheter och friheter, ska BCR-medlemmen se till att en Konsekvensbedömning avseende dataskydd genomförs. Om en sådan Konsekvensbedömning avseende dataskydd visar att Behandlingen skulle visa att Behandlingen skulle leda till en hög risk om inte den Personuppgiftsansvarige vidtar åtgärder för att minska risken, bör den BCR-medlem som agerar som Personuppgiftsansvarig samråda med den behöriga Tillsynsmyndigheten/de behöriga Tillsynsmyndigheterna innan Behandlingen utförs.

6.2 Inbyggt dataskydd och dataskydd som standard

BCR-medlemmar ska implementera lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, som är utformade för att implementera dataskyddsprinciper på ett effektivt sätt och för att integrera nödvändiga skyddsåtgärder i Behandlingen för att uppfylla dataskyddskraven i GDPR och skydda de Registrerades rättigheter (*Inbyggt dataskydd*). Sådana åtgärder ska genomföras med beaktande av den senaste tekniken, kostnaden för genomförandet och Behandlingens art, omfattning, sammanhang och ändamål samt de risker av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter som Behandlingen medför (som beskrivs närmare i avsnitt 2.7).

BCR-medlemmar ska också genomföra lämpliga tekniska och organisatoriska åtgärder för att som standard säkerställa att endast Personuppgifter som är nödvändiga för varje specifikt ändamål behandlas (*dataskydd som standard*). Denna skyldighet gäller mängden insamlade Personuppgifter, Behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

6.3 Ömsesidig samverkan och samarbete med behöriga Tillsynsmyndigheter

BCR-medlemmar ska samarbeta och bistå varandra för att hantera en begäran eller ett klagomål från en Registrerad eller en utredning eller förfrågan av behöriga Tillsynsmyndigheter i EU/EES.

BCR-medlemmarna ska samarbeta med, acceptera att bli granskade och inspekterade, inklusive vid behov på plats, av de behöriga Tillsynsmyndigheterna samt ta hänsyn till och följa dessa behöriga Tillsynsmyndigheters råd och beslut i alla frågor som rör C-BCR:erna. Detta åtagande begränsar dock inte BCR-medlemmarnas rätt att bestrida sådana råd eller beslut i domstol eller andra tillämpliga instanser när det anses lämpligt och nödvändigt.

BCR-medlemmar ska på begäran förse de behöriga Tillsynsmyndigheterna all information om de Behandlingsaktiviteter som omfattas av C-BCR.

Eventuella tvister som rör de behöriga Tillsynsmyndigheternas utövande av tillsyn över efterlevnaden av C-BCR ska avgöras av domstolarna i den medlemsstat där Tillsynsmyndigheten är belägen, i enlighet med den medlemsstatens processrätt. BCR-medlemmarna samtycker till att underkasta sig dessa domstolars jurisdiktion.

6.4 Förhållandet mellan nationell lagstiftning och C-BCR

Om den lokala lagstiftningen, till exempel EU-lagstiftningen, kräver en högre skyddsnivå för Personuppgifter kommer den att ha företräde framför C-BCR. Under alla omständigheter ska Personuppgifter behandlas i enlighet med tillämpliga dataskyddslagar, inklusive lokala lagar och förordningar, särskilt artiklarna 5 och 6 i GDPR.

Ingenting i C-BCR ska hindra en BCR-medlem från att behandla Personuppgifter eller utföra någon annan åtgärd som annars skulle vara lagligen tillåten enligt GDPR.

6.5 Åtgärder i händelse av nationell lagstiftning som påverkar efterlevnaden av C-BCR

En BCR-medlem, som agerar som Dataimportör, måste skyndsamt underrätta Dataexportören och Ericsson AB om den, vid användning av dessa C-BCR:er som ett verktyg för överföringar och under hela C-BCR medlemskapet, har skäl att tro att den omfattas av eller har blivit föremål för lagar eller praxis som skulle hindra denne från att uppfylla sina skyldigheter enligt C-BCR:erna. Detta inkluderar situationer där en ändring av lagstiftningen i tredjelandet eller en åtgärd (t.ex. en begäran om utlämnande) påverkar efterlevnaden.

Vid verifieringen av en sådan anmälan bör den BCR-medlem som agerar som Dataexportör, tillsammans med Ericsson AB och kontakten för dessa C-BCR, åta sig att omedelbart identifiera kompletterande åtgärder (t.ex. tekniska eller organisatoriska åtgärder för att säkerställa säkerhet och konfidentialitet) som ska vidtas av BCR-medlemmen som agerar som Dataexportör och/eller Dataimportör, för att möjliggöra efterlevnad av C-BCR:erna. Detsamma gäller om en BCR-medlem som agerar som Dataexportör har skäl att tro att en BCR-medlem som agerar som dess Dataimportör inte längre kan fullgöra sina skyldigheter enligt dessa C-BCR:er.

Om BCR-medlemmen, i egenskap av Dataexportör, tillsammans med Ericsson AB och kontaktpersonen för dessa BCR:er enligt avsnitt 12, bedömer att C-BCR:erna – även med kompletterande åtgärder – inte kan efterlevas vid en överföring eller en uppsättning överföringar, eller om den instrueras av den behöriga Tillsynsmyndigheten, åtar de sig att avbryta den aktuella överföringen eller uppsättningen av överföringar, samt alla överföringar där samma bedömning och resonemang skulle leda till en liknande slutsats, till dess att efterlevnaden återigen säkerställs eller överföringen avslutas.

Efter ett sådant upphävande måste den BCR-medlem som agerar som Dataexportör upphöra med överföringen eller uppsättningen av överföringar om C-BCR:erna inte kan efterlevas och efterlevnaden av BCR inte återställs inom en månad efter upphävandet. I detta fall ska Personuppgifter som har överförts innan avbrytandet, och eventuella kopior av dessa, antingen återlämnas till BCR-medlemmen som agerar som Dataexportör eller förstöras i sin helhet, enligt dennes val.

Ericsson AB och kontaktpersonen för dessa BCR:er, som anges i avsnitt 12, kommer att informera alla andra BCR-medlemmar om den genomförda bedömningen och om dess resultat, så att de identifierade kompletterande åtgärderna kan tillämpas om samma typ av överföringar utförs av någon annan BCR-medlem. Om effektiva kompletterande åtgärder inte kan införas ska de aktuella överföringarna avbrytas eller avslutas.

BCR-medlemmar som agerar som Dataexportörer åtar sig att fortlöpande övervaka, och när så är lämpligt i samarbete med BCR-medlemmar som agerar som Dataimportörer, utvecklingen i de tredjeländer till vilka Dataexportörerna har överfört Personuppgifter som kan påverka den ursprungliga bedömningen av skyddsnivån och de beslut som fattats i enlighet därmed avseende sådana överföringar. .

6.6 Dataimportörens skyldigheter vid begäran om tillgång från myndigheter

Utan att det påverkar skyldigheten för den BCR-medlem som agerar som Dataimportör att

informera Dataexportören om sin oförmåga att uppfylla åtagandena i C-BCR (se avsnitt 2.11 och 6.5 ovan) ska BCR-medlemmen som agerar som Dataimportör:

(a) omedelbart underrätta Dataexportören och, om möjligt, den Registrerade (vid behov med hjälp av Dataexportören) om denne:

(i) tar emot en rättsligt bindande begäran från en offentlig myndighet enligt lagstiftningen i destinationslandet eller i ett annat tredjeland om utlämnande av Personuppgifter som överförts i enlighet med C-BCR:erna; En sådan underrättelse ska innehålla information om vilka Personuppgifter som begärs, den begärande myndigheten, den rättsliga grunden för begäran och det svar som lämnats.

(ii) får kännedom om att offentliga myndigheter har direkt tillgång till Personuppgifter som överförts i enlighet med C-BCR:erna enligt lagstiftningen i destinationslandet; en sådan underrättelse ska innehålla all information som Dataimportören har tillgång till.

(b) om det är förbjudet att underrätta Dataexportören och/eller Registrerade, göra sitt yttersta för att få ett undantag från ett sådant förbud i syfte att förmedla så mycket information som möjligt och så snart som möjligt, och dokumentera sina bästa ansträngningar för att kunna visa detta på begäran av Dataexportören.

(c) med jämna mellanrum förse den BCR-medlem som agerar som Dataexportör med så mycket relevant information som möjligt om de mottagna förfrågningarna (i synnerhet antalet förfrågningar, typ av begärda uppgifter, begärande myndighet eller myndigheter, huruvida begäranden har bestridits och resultatet av sådana bestridanden osv.). Om Dataimportören helt eller delvis förbjuds att förse Dataexportören med ovannämnda information ska denne utan onödigt dröjsmål informera Dataexportören om detta.

(d) bevara ovannämnda information så länge som Personuppgifterna omfattas av de skyddsåtgärder som tillhandahålls av C-BCR, och ska på begäran göra den tillgänglig för den behöriga Tillsynsmyndigheten.

(e) granska lagligheten i begäran om utlämnande, särskilt om den ligger inom de befogenheter som den begärande offentliga myndigheten har tilldelats, och bestrida begäran om den efter en noggrann bedömning kommer fram till att det finns rimliga skäl att anse att begäran är olaglig enligt lagstiftningen i destinationslandet, tillämpliga skyldigheter enligt internationell rätt, principen om internationell hövlighet. Dataimportören ska, under samma förutsättningar, söka möjligheter att överklaga.

(f) Vidbestridandet av en begäran ska Dataimportören ansöka om interimistiska åtgärder i syfte att suspendera begärans verkningar till dess att den behöriga rättsliga myndigheten har fattat beslut i sak. Dataimportören ska inte lämna ut de begärda Personuppgifterna förrän det krävs enligt tillämpliga processuella regler.

(g) dokumentera sin rättsliga bedömning och eventuella invändningar mot begäran om utlämnande och, i den utsträckning det är tillåtet enligt lagstiftningen i destinationslandet, göra dokumentationen tillgänglig för Dataexportören. Dataimportören kommer också att på begäran göra bedömningen tillgänglig för de behöriga Tillsynsmyndigheterna.

(h) tillhandahålla den minsta mängd information som är tillåten när man svarar på en begäran om utlämning, baserat på en rimlig tolkning av begäran.

En överföring av Personuppgifter från en BCR-medlem till en offentlig myndighet får inte i något fall vara massiv, oproportionerlig eller godtycklig på ett sätt som går utöver vad som är nödvändigt i ett demokratiskt samhälle.

7. Interna klagomålsmekanismer

7.1 Klagomål

Alla Registrerade kan utöva sina rättigheter enligt C-BCR och lämna in ett klagomål mot en BCR-medlem genom att använda den klagomålsmekanism som beskrivs i detta avsnitt 7.

En Registrerad som vill lämna in ett klagomål eller en begäran till en BCR-medlem uppmanas att göra det genom att skicka ett e-postmeddelande till privacy.bcr@ericsson.com, eller genom att kontakta Chief Privacy Officer på Ericsson, Torshamnsgatan 21164 80 Stockholm, Sverige. I, länder där det finns lokala kontakter för integritetsrelaterade frågor, kan Registrerade skicka ett e-postmeddelande till sådan lokal kontakt eller kontakter enligt följande länk: https://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdf.

Sådana klagomål eller förfrågningar ska behandlas i enlighet med Ericssonkoncernens verktyg och processer och, för BCR-medlemmar som agerar som Personuppgiftsbiträden, kommuniceras till den relevanta BCR-medlemmen som agerar som Personuppgiftsansvarig utan onödigt dröjsmål.

Ericssonkoncernen kommer hantera klagomål från Registrerade i enlighet med följande procedur:

(a) När klagomål tas emot kommer de att hanteras av Ericssons integritetsrådgivare, inklusive GDPO och/eller relevant dataskyddsombud. Den Registrerade kommer att informeras om åtgärder som vidtagits med anledning av klagomålet utan onödigt dröjsmål och alltid inom en (1) månad. En förlängning med upp till två (2) ytterligare månader kan beviljas på grund av omfattningen eller komplexiteten hos en viss begäran/begäranden. I sådana fall ska den Registrerade informeras om dröjsmålet inom en (1) månad från mottagandet. Vid inlämnande av ett klagomål ska den Registrerade få en bekräftelse och en förväntad tidsram för hantering av klagomålet.

(b) Den Registrerade ska informeras om konsekvenserna vid dröjsmål med svaret samt om klagomålet avvisas eller om klagomålet anses vara motiverat. Den Registrerade

ska också informeras om de rättsmedel som finns tillgängliga om den Registrerade inte är nöjd med svaret, såsom rätten att lämna in ett krav till relevant(a) domstol(ar) och/eller Tillsynsmyndigheter. Denna rätt är dock inte beroende av att den Registrerade först har använt klagomålshanteringsprocessen.

7.2 Rapportera incidenter

Alla Anställda är skyldiga att rapportera alla misstänkta eller observerade säkerhets- och personuppgiftsincidenter genom att rapportera in dem till SIMS (Security Management Incidents System). Detta säkerställer att incidenthanteringsprocessen initieras korrekt. När en ny incident loggas i SIMS tilldelas den automatiskt till ärendehanterare baserat på rapportörens placering.

Den tilldelade handläggaren ansvarar för att bedöma om incidenten faller inom dennes ansvarsområde. Om så inte är fallet ska ärendet vidarebefordras till lämplig organisation. Ärendehanteraren har till uppgift att bearbeta och hantera säkerhetsincidenter, samt eskalera dem vid behov.

Det globala dataskyddsombudet (GDPO), Chief Privacy Officer, Data Protection Officer (DPO) (https://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdfhttps://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdf) eller Privacy Advisor kommer att hjälpa BCR-medlemmen att utvärdera incidentens allvarlighetsgrad och rekommendera nästa steg. BCR-medlemmen måste följa de krav som anges i avsnitt 2.9.

7.3 Vidta åtgärder

De Registrerade har rätt att väcka talan vid domstol eller lämna in ett klagomål till en Tillsynsmyndighet i enlighet med vad som anges i avsnitt 7.1. I dessa situationer ska Registrerade som är Anställda i Ericssonkoncernen och som får information om åtgärden från eller på uppdrag av den Registrerade eller Tillsynsmyndigheten skicka ett e-postmeddelande om talan eller klagomålet till privacy.bcr@ericsson.com

8. Efterlevnad och tillsyn av efterlevnad

8.1 Revisionsprogram

Ericssonkoncernen har implementerat ett program som förutsätter regelbundna revisioner och om det finns indikationer på bristande efterlevnad för att säkerställa efterlevnad av C-BCR. Revisionsprogrammet omfattar alla aspekter av C-BCR (t.ex. applikationer, IT-system, databaser som behandlar Personuppgifter eller vidareöverföringar, beslut som fattas med avseende på obligatoriska krav enligt nationell lagstiftning som strider mot C-BCR, granskning av de avtalsvillkor som används för överföringar från Ericssonkoncernen till Personuppgiftsansvariga eller Personuppgiftsbiträden, korrigerande åtgärder, etc.), inklusive metoder och handlingsplaner som

säkerställer att korrigerande åtgärder har genomförts. Alla aspekter av C-BCR:erna kommer inte att övervakas varje gång en BCR-medlem revideras, men alla aspekter av C-BCR:erna övervakas med lämpliga regelbundna intervall för den BCR-medlemmen.

GDPO beslutar om den årliga revisionsplanen för C-BCR:erna. På grundval av de risker som den Behandling som omfattas av C-BCR utgör för de Registrerades rättigheter och friheter har det fastställts att regelbundna revisioner ska utföras minst en gång per år. BCR-medlemmar kan också bli föremål för särskilda, ad hoc-revisioner om det finns indikationer på bristande efterlevnad av C-BCR eller om det på annat sätt begärs av en Privacy Officer eller funktion, annan enhet inom ramen för deras integritethantering eller någon annan behörig funktion i organisationen.

Revisionerna kommer att genomföras av, eller under ledning av, GDPO. Åtgärder har utformats för att garantera och skydda GDPO:s självständighet och oberoende när det gäller utförandet av de uppgifter som är knutna till dessa revisioner för att säkerställa att intressekonflikter inte uppstår. Externa revisorer kan anlitas för att utföra revisioner när så är lämpligt för att uppfylla resurskrav och/eller för att säkerställa oberoende. Dessutom kan koncernfunktionen Corporate Audit när som helst granska alla aspekter av efterlevnaden av det interna ramverket för styrning, inklusive C-BCR.

Resultaten av revisionerna tillsammans med framsteg med att åtgärda revisionsfynd ska kommuniceras till följande: (i) ledningen och styrelsen för den BCR-medlem som är föremål för revisionen, (ii) Privacy Officer eller Privacy funktionen och (iii) styrelsen för Ericssonkoncernens Ansvariga Medlem.

Behöriga Tillsynsmyndigheter kan på begäran få tillgång till resultaten av eventuella revisionsrapporter från BCR-medlemmar. BCR-medlemmar ska omedelbart informera GDPO och samarbeta fullt ut och öppet med den behöriga Tillsynsmyndigheten samt utan onödigt dröjsmål för att uppfylla en sådan begäran.

8.2 Utbildningsprogram

Enligt Ericssons Integritetspolicy ska lämpliga och uppdaterade utbildningar att tillhandahållas och behöva genomföras kontinuerligt av Anställda och Extern Arbetskraft som har permanent eller regelbunden tillgång till Personuppgifter eller är involverade i insamlingen av Personuppgifter eller i utvecklingen av verktyg eller tjänster som används för att behandla Personuppgifter. Detta inkluderar utbildning som är specifik för C-BCR:erna. Utbildningsprogrammet inkluderar obligatorisk integritetsutbildning för alla nyanställda och Extern Arbetskraft, som därefter genomförs vart tredje år. Dessutom tillhandahålls riktad utbildning för specifika funktioner såsom Human Resources och Sourcing. Utbildningen omfattar bland annat förfaranden för att hantera myndigheters begäran om tillgång till Personuppgifter.

Chief Privacy Officer, GDPO, DPO:er och andra Anställda med integritetsansvar hos BCR-medlemmen har ansvaret för att upprätta, upprätthålla och distribuera lämplig utbildning om integritet, inklusive om C-BCR:erna.

8.3 Styrning och ansvar

Styrning av C-BCR ska vara en del av Ericssons Integritetspolicy.

Ericssonkoncernen har utsett en Chief Privacy Officer, en GDPO och DPO:er där så krävs enligt tillämpliga regelverk, och BCR:s medlemmar har dessutom utsett specifika personer såsom Data Protection Advisors, Privacy Managers och Advisors, samt Privacy Officers med ansvar för att övervaka efterlevnaden av C-BCR. Dessa roller har det högsta ledningsstödet för att utföra sina uppgifter. Chief Privacy Officer, GDPO och utsedda DPO:er, samt andra som arbetar med integritetsskydd, kan kontaktas direkt. Ericssonkoncernen har åtagit sig att offentliggöra deras kontaktuppgifter.

Med beaktande av de Personuppgifter som behandlas i samband med personalfrågor har Ericssonkoncernen utsett särskilda integritetsresurser som arbetar specifikt med dessa frågor.

Ytterligare ansvarsområden som är specifika för C-BCR:erna är bland annat följande:

(a) GDPO, Chief Privacy Compliance Officer, utsedda Dataskyddsombud och nätverket av integritetsrådgivare ska övervaka efterlevnaden av dessa C-BCR och ge råd om implementeringen av C-BCR:erna

(b) GDPO ska säkerställa att C-BCR:ernas regelefterlevnadsrevisioner genomförs regelbundet. GDPO ska dessutom säkerställa att revisionsresultaten åtgärdas på ett korrekt sätt och i rätt tid.

(c) GDPO har ansvaret för att samordna och ordna tillgång till databehandlingsanläggningar om den behöriga Tillsynsmyndigheten begär en revision av regelefterlevnad av C-BCR.

(d) HR-funktionen ansvarar för att säkerställa att Personuppgifter i personalprocesser och verktyg hanteras i enlighet med C-BCR.

(e) Legal and Compliance ansvarar för att säkerställa att Personuppgifter iv juridiska samt regelefterlevnadsprocesser hanteras i enlighet med C-BCR.

(f) Säkerhet (Security) ansvarar för att säkerställa att Personuppgifter i säkerhetsprocesser och verktyg hanteras i enlighet med C-BCR.

(g) Ekonomiavdelningen ansvarar för att säkerställa att Personuppgifter i ekonomiprocesser och verktyg hanteras i enlighet med C-BCR.

(h) IT-avdelningen ansvarar för att integritetskontroller utformas i interna IT-program och system i förväg.

(i) Inköp (Sourcing) ansvarar för att säkerställa att integritetskontroller och dataöverföringsavtal är en del av avtal med tredjepartsleverantörer.

9. Uppdatering av C-BCR

C-BCR:erna måste hållas uppdaterade för att återspegla den aktuella situationen (t.ex. för att ta hänsyn till ändringar i regelverket, relevanta rekommendationer från Europeiska Dataskyddsstyrelsen (EDPB) eller Ericssonkoncernens struktur).

Ericssonkoncernen ska rapportera alla ändringar i C-BCR:erna (inklusive ändringar i listan över BCR-medlemmar) till alla BCR-medlemmar utan onödigt dröjsmål med hjälp av Ericssonkoncernens interna kommunikationsprocess, inklusive intranätet.

Ericssonkoncernen ska också, utan onödigt dröjsmål och i förväg, underrätta Tillsynsmyndigheterna, via den Ansvariga Tillsynsmyndigheten, om alla väsentliga ändringar av C-BCR som kan vara skadliga för skyddsnivån som erbjuds av C-BCR:erna eller väsentligt påverka dem (t.ex. ändringar i det sätt på vilket de är bindande). Underrättelsen ska innehålla en kortfattad redogörelse för skälen till uppdateringen, varefter Tillsynsmyndigheten bedömer om de ändringar som gjorts kräver ett nytt godkännande.

Uppdateringen av C-BCR:erna eller av förteckningen över BCR-medlemmar i bilaga 1 är möjliga utan att ett godkännande behöver ansökas om på nytt, förutsatt att

(a) Ericssonkoncernen har en fullständigt uppdaterad lista över BCR-medlemmar och håller reda på och registrerar alla uppdateringar av reglerna och tillhandahåller nödvändig information till de Registrerade eller behöriga Tillsynsmyndigheterna på begäran;

(b) Ingen överföring av Personuppgifter görs till en ny BCR-medlem förrän den nya BCR-medlemmen är effektivt bunden av C-BCR:erna och kan uppfylla kraven.

(c) Om en ändring eventuellt skulle kunna påverka skyddsnivån enligt C-BCR eller i betydande grad påverka C-BCR (dvs. ändringar av dess bindande karaktär) ska ändringen skyndsamt meddelas de berörda Tillsynsmyndigheterna via den Ansvariga Tillsynsmyndigheten och

(d) Eventuella ändringar av C-BCR eller av förteckningen över BCR-medlemmar i bilaga 1 rapporteras en gång om året till de berörda Tillsynsmyndigheterna via den Ansvariga Tillsynsmyndigheten, med en kort förklaring av skälen till uppdateringen. En sådan årlig uppdatering ska innehålla en bekräftelse på att Ericsson AB har tillräckliga tillgångar, eller har vidtagit lämpliga åtgärder för att kunna betala ersättning för skada till följd av brott mot C-BCR.

Den Ansvariga Tillsynsmyndigheten bör underrättas en gång om året även om inga ändringar av C-BCR:erna har gjorts. En sådan årlig underrättelse ska även innehålla en bekräftelse av att Ericsson AB har tillräckliga tillgångar eller har vidtagit lämpliga åtgärder för att kunna betala ersättning för skada till följd av brott mot C-BCR.

Det är Chief Privacy Officer:s ansvar att hålla en fullständigt uppdaterad lista över BCR-medlemmarna, dokumentera eventuella uppdateringar av C-BCR:erna och tillhandahålla

nödvändig information till de Registrerade och, på begäran, till behöriga Tillsynsmyndigheter.

10. Bristande efterlevnad och uppsägning av C-BCR

För att säkerställa efterlevnad av C-BCR måste alla BCR-medlemmar iaktta följande:

(a) Säkerställa att ingen överföring görs till en BCR-medlem om inte BCR-medlemmen är effektivt bunden av C-BCR:erna och kan säkerställa efterlevnad;

(b) Dataimportören måste skyndsamt informera Dataexportören om denne av någon anledning inte kan efterleva C-BCR:erna, inklusive de situationer som beskrivs närmare i avsnitt 6.5 ovan;

(c) Om Dataimportören bryter mot C-BCR:erna eller inte kan efterleva dem bör Dataexportören avbryta överföringen.

(d) Dataimportören ska, enligt Dataexportörens val, omedelbart återlämna eller radera de Personuppgifter (inklusive eventuella kopior av dessa) som har överförts i enlighet med C-BCR:erna i sin helhet, om

(i) Dataexportören har avbrutit överföringen och efterlevnaden av dessa C-BCR inte har återställts inom rimlig tid, och i vilket fall som helst inom en månad efter avbrytandet eller

(ii) Dataimportören väsentligt eller ihållande bryter mot C-BCR; eller

(iii) Dataimportören underlåter att följa ett bindande beslut av en behörig domstol eller Tillsynsmyndighet avseende sina skyldigheter enligt C-BCR.

Dataimportören ska intyga raderingen av uppgifterna till Dataexportören. Tills uppgifterna har raderats eller återlämnats, ska Dataimportören fortsätta att säkerställa efterlevnad av C-BCR:erna. .

Om lokala lagar som gäller för Dataimportören förbjuder återlämning eller radering av de överförda Personuppgifterna, ska Dataimportören garantera att den fortsätter att säkerställa efterlevnad av C-BCR:erna och endast behandlar uppgifterna i den utsträckning och så länge som krävs enligt den lokala lagen. För situationer där tillämpliga lokala lagar och/eller praxis påverkar efterlevnaden av C-BCR:erna, se avsnitt 2.11 och 6.5 ovan. En BCR-medlem som agerar som Dataimportör, och som inte längre är bunden av C-BCR:erna, får behålla, återlämna eller radera de Personuppgifter som mottagits enligt C-BCR:erna, enligt överenskommelse med BCR-medlem som agerar som Dataexportör. Om BCR-medlemmarna är överens om att Personuppgifterna får behållas av Dataimportören, måste skyddet upprätthållas i enlighet med kapitel V i GDPR..

11. Terminologi

Term	Definition
BCR-medlemmar	Avser alla Ericssonföretag när de har blivit parter i det Koncerninterna Avtalet och därmed är bundna av de C-BCR som anges i avsnitt 1.2.2. En förteckning över BCR-medlemmar och deras kontaktuppgifter finns i Bilaga 1.
C-BCR	Hänvisar till dessa bindande företagsbestämmelser (Binding Corporate Rules) för Personuppgiftsansvariga.
Personuppgiftsansvarig	Avser en fysisk eller Juridisk Person, offentlig myndighet, institution eller något annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för Behandlingen av Personuppgifter.
behörig Tillsynsmyndighet	Hänvisar till EU/EES-Tillsynsmyndigheten för dataskydd som är behörig för Dataexportören.
Personuppgiftsincident	Avser en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till Personuppgifter som överförs, lagras eller på annat sätt behandlas.
Dataexportör	Avser en Personuppgiftsansvarig (eller, där det är tillåtet, ett Personuppgiftsbiträde) som är etablerad inom EU/EES och som överför Personuppgifter till en Dataimportör.
Dataimportör	Avser en Personuppgiftsansvarig eller ett Personuppgiftsbiträde som befinner sig i ett tredjeland och som tar emot Personuppgifter från Dataexportören.

Konsekvensbedömning avseende dataskydd	Avser en bedömning av hur den planerade Behandlingen påverkar skyddet av Personuppgifter, i enlighet med artikel 35 i den Allmänna Dataskyddsförordningen.
Registrerade	Avser en identifierad eller identifierbar fysisk person som specifika Personuppgifter avser. Det är en person som kan identifieras, direkt eller indirekt, särskilt genom hänvisning till en identifierare som ett namn, personnummer, platsdata, en onlineidentifierare eller till en eller flera faktorer som är specifika för den fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identiteten hos den fysiska personen.
Europeiska dataskyddsstyrelsen (EDPB)	Hänvisar till europeiska dataskyddsstyrelsen.
EES	Hänvisar till europeiska ekonomiska samarbetsområdet. EES består av EU:s medlemsstater samt Island, Liechtenstein och Norge.
Anställda	Avser personer som är Anställda av en BCR-medlem.
Ericsson-företag	Avser en Juridisk Person (inklusive någon av dess filialer) som direkt eller indirekt kontrolleras av LM Ericsson, och vars finansiella rapporter ingår i Ericsson-koncernens koncernredovisning.
Ericssonkoncernen	Avser koncernen Ericsson.
Ericssonkoncernens Ansvariga Medlem	Avser Ericsson AB.

Ericssons Integritetspolicy	En uppsättning direktiv eller instruktioner som gäller för alla Anställda och Extern arbetskraft och som rör integritetsfrågor [https://www.ericsson.com/en/legal/privacy/privacy-policy] och styrande Ericssons integritetsprinciper [https://www.ericsson.com/en/legal/privacy].
EU	Avser Europeiska unionen, dess medlemsstater.
Extern arbetskraft	Avser tillfällig arbetskraft (t.ex. konsulter, oberoende entreprenörer, frilansare osv.), dvs. personer som inte faktiskt är Anställda av någon BCR-medlem.
GDPO (GDPO)	Avser Koncernens dataskyddsombud. GDPO är en del av koncernfunktionen Legal Affairs and Compliance.
Allmänna Dataskyddsförordningen (GDPR)	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på Behandling av Personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). och eventuella ändringar och förordningar av detta.
Koncerninternt Avtal	Hänvisar till det koncerninterna avtalet (intern referens GFLA-23:000524 Uen "Internal Group Agreement relating to Ericsson Binding Corporate Rules for Controllers"), som innehåller ett specifikt åtagande som bekräftar den bindande verkan av C-BCR.
Ansvarig Tillsynsmyndighet	Hänvisar till Integritetsskyddsmyndigheten (IMY).

Juridisk Person	Avser en förening, ett bolag, ett handelsbolag eller liknande som har rättslig ställning enligt lag och har rättskapacitet att ingå avtal eller kontrakt, åta sig skyldigheter, stämma och bli stämd i eget namn samt att hållas ansvarig för sina handlingar.
Personuppgifter	Avser all information som rör en identifierad eller identifierbar fysisk person (d.v.s. en Registrerad, enligt definitionen ovan).
Behandling	Avser varje åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring
Personuppgiftsbiträde	Avser den fysiska eller juridiska person, offentliga myndighet, institution eller annat organ som behandlar Personuppgifter för den Personuppgiftsansvariges räkning. I det här dokumentet är Personuppgiftsbiträdet vanligtvis en BCR-medlem som behandlar data på uppdrag av en BCR-medlem som agerar som Personuppgiftsansvarig.
Process för hantering av säkerhetsincidenter (SIMS)	Avser Ericssonkoncernens process för att planera och ha beredskap för säkerhetsincidenter, upptäcka, rapportera och bedöma säkerhetsincidenter och sårbarheter, reagera på säkerhetsincidenter samt ta lärdom av och göra förbättringar om en säkerhetsincident har inträffat.

Särskilda Kategorier av Personuppgifter	Avser Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och Behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. .
Tillsynsmyndighet/Tillsynsmyndigheter	Avser den oberoende myndighet/de myndigheter i varje EU/EES-land som har ansvar för att övervaka tillämpningen av GDPR, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med Behandling och för att underlätta det fria flödet av Personuppgifter inom EU. Vissa medlemsstater kan ha flera myndigheter som har sådana ansvarsområden.

12. Kontakt för dessa C-BCR:er

Cheif Privacy Officer

Privacy.bcr@ericsson.com

Ericsson

Torshamnsgatan 21

164 80 Stockholm, Sverige

13. Bilagor och referenser

13.1 Bilagorna

Bilaga 1 BCR-medlemmar

Bilaga 2 Personuppgifter som överförs

13.2 Referenser

- Koncernpolicy, Affärsetiska kod Vår kompass - Guide för affärsetik - Internt (ericsson.com)
- Lista överdataskyddsombud data-protection-officers.xlsx (ericsson.com)
- Informationsdokument Integritetspolicy för Ericssons Anställda och Extern arbetskraft Integritetspolicy för Personuppgifter som behandlas av Ericsson - Internt

Bilaga 1

Enligt lista publicerad på Privacy - Ericsson.

Bilaga 2

1. Typ och kategorier av Personuppgifter som överförs

Ericssonkoncernen behandlar följande huvudkategorier av Personuppgifter:

1. Anställda: namn, akademiska och yrkesmässiga uppgifter, kontaktuppgifter, personnummer, anställningsinformation, ersättning, bankkontoinformation, nödkontakter etc.

2. Extern arbetskraft: namn, akademiska och yrkesmässiga uppgifter, kontaktuppgifter, personnummer, ersättning, bankkontoinformation etc.

3. Besökare i BCR-medlemmars lokaler: kontaktuppgifter, information om kameraövervakning osv.

4. Aktieägare: namn, kontaktuppgifter, aktieinnehav m.m.

5. Kundrepresentanter: namn, arbetstitel, kontaktuppgifter etc.

6. Leverantörer: namn, kontaktuppgifter etc.

7. Arbetssökande/kandidater: namn, kontaktuppgifter, personnummer, akademiska och yrkesmässiga uppgifter och annan information relaterad till rekryteringsprocessen.

8. Andra tredje parter: namn, kontaktuppgifter etc.

2. Syften med Behandlingen

BCR-medlemmarna behandlar huvudsakligen Personuppgifterna för de ändamål som anges nedan:

1. Passersystem/Faciliteter

2. Personalhantering (HR)

3. Kandidater (rekrytering)

4. Kunder (inklusive marknadsförings- och kommunikationsändamål)

5. Säkerhetsincidenter

6. Rättsliga förfaranden och avtal

7. Kameraövervakning

8. Visselblåsning (inklusive utredningsverksamhet)
9. Kontakter
10. Leverantörer

3. Typer av Behandling

De typer av Behandlingsaktiviteter som utförs inkluderar, men är inte begränsade till: insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållandet på annat sätt, justering eller sammanföring, begränsning, radering eller förstöring.

4. Överföring till tredje land

Ericssonkoncernens verksamhet är global och Personuppgifter kan överföras av och mellan alla BCR-medlemmar (se bilaga 1).