S

Binding Corporate Rules
BCR

voor bedrijfsentiteiten van de Siemens-groep
en andere aansluitende bedrijven
voor de bescherming van persoonsgegevens

1. Inleiding

Hoofddoel van deze bindende bedrijfsrichtlijnen of Binding Corporate Rules (BCR's) is het verzekeren dat in alle bedrijfsentiteiten van de Siemens-groep en andere aansluitende bedrijven een adequaat beschermingsniveau wordt voorzien voor de overdracht van persoonsgegevens bij de bedrijfsactiviteiten van een deelnemend bedrijf gevestigd in een land van de Europese Economische Ruimte (EER-land) of in een land waar er een adequaat gegevensbeschermingsniveau is voorzien, zoals bevestigd door een besluit van de Europese Commissie, aan andere bedrijfsentiteiten van de Siemens-groep en/of andere aansluitende bedrijven.

Hiertoe is het van cruciaal belang geharmoniseerde normen tot stand te brengen inzake de bescherming van de persoonlijke levenssfeer en gegevensbeveiliging voor de verwerking van de betreffende persoonsgegevens, zoals bedoeld door de EU-Richtlijn betreffende gegevensbescherming, om te verzekeren dat er een adequaat gegevensbeschermingsniveau en voldoende garanties voorzien zijn, zoals bedoeld door de EU-Richtlijn betreffende het recht op de bescherming van de persoonlijke levenssfeer en de uitoefening van gerelateerde rechten.

Deze BCR's creëren een algemeen en universeel geldend regelgevingkader voor de verwerking en behandeling van alle persoonsgegevens met betrekking tot medewerkers, klanten, leveranciers, actuele of toekomstige bedrijfspartners en andere betrokken identificeerbare personen door bedrijfsentiteiten van de Siemens-groep of andere aansluitende bedrijven

- in zoverre deze persoonsgegevens werden overgedragen door een deelnemend bedrijf gevestigd in een EER-land of gevestigd in een land waar een adequaat gegevensbeschermingsniveau voorzien is, zoals bevestigd door een besluit van de Europese Commissie, aan een deelnemend bedrijf gevestigd buiten de EER; en
- voor de verwerking en behandeling van persoonsgegevens door deelnemend bedrijven in een EER-land of in een land met een adequaat gegevensbeschermingsniveau, zoals bevestigd door een besluit van de Europese Commissie.

De onderhavige BCR's weerspiegelen de status en de huidige internationale eisen inzake gegevensbescherming van kracht op het ogenblik van het in voege treden van de BCR's, in het bijzonder de eisen van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG, de betreffende werkdocumenten van Werkgroep Artikel 29 voor de bescherming van persoonsgegevens en de principes van de Internationale Conferentie van de commissarissen voor gegevensbescherming (hieronder de "Madrid-resolutie" genoemd) van 5 november 2009.

2. Toepassingsgebied van de BCR's

Alle bedrijfsentiteiten van de Siemens-groep en andere aansluitende bedrijven wereldwijd vallen binnen de omvang van de BCR's.

De BCR's zijn enerzijds van toepassing op de verwerking en behandeling van alle persoonsgegevens overgedragen van een bedrijfsentiteit van de Siemens-groep of een ander aansluitend bedrijf gevestigd in een EER-land of in een land waar er een adequaat gegevensbeschermingsniveau is voorzien, zoals bevestigd door een besluit van de Europese Commissie, aan een bedrijfsentiteit van de Siemens-groep of een ander aansluitend bedrijf gevestigd buiten de EER. Ze zijn anderzijds ook van toepassing op de verwerking en behandeling van persoonsgegevens door deelnemende bedrijven gevestigd in een EER-land of in een land waar er een adequaat gegevensbeschermingsniveau is voorzien, zoals bevestigd door een besluit van de Europese Commissie.

De BCR's verzekeren de bescherming van alle persoonsgegevens van medewerkers, klanten, leveranciers, aandeelhouders en alle andere – actuele of toekomstige – contracterende partijen en bedrijfspartners van een bedrijfsentiteit van de Siemens-groep of een ander aansluitend bedrijf gevestigd in een EER-land of in een land waar er een adequaat gegevensbeschermingsniveau is voorzien, zoals bevestigd door een besluit van de Europese Commissie, in zoverre deze gegevens

overgedragen worden aan een deelnemend bedrijf buiten de EER en laatstgenoemd bedrijf ze verwerkt of behandelt.

3. Definities

De in deze BCR's gebruikte termen worden gedefinieerd als volgt:

- **BCR**: de onderhavige bindende bedrijfsrichtlijnen of Binding Corporate Rules en de hierin vervatte regelgeving;
- **CDPO**: de Chief Data Privacy Officer van Siemens AG;
- **Toestemming**: een vrij gegeven en geïnformeerde wilsuiting waarbij de betrokken identificeerbare persoon zich akkoord verklaart met de verwerking en behandeling van zijn/haar persoonsgegevens[1];
- **Verantwoordelijke voor de verwerking**: de juridisch onafhankelijke bedrijfsentiteit die het doel en de middelen voor gegevensverwerking bepaalt. Afhankelijke filialen, bedrijfslocaties en permanente vestigingen maken deel uit van de verantwoordelijke entiteit;
- **Klanten en leveranciers**: natuurlijke en rechtspersonen waarmee een bedrijfsrelatie bestaat of gepland is;
- **Betrokken identificeerbare persoon**: elke geïdentificeerde of identificeerbare natuurlijke persoon wiens gegevens verwerkt of behandeld worden. Een betrokken identificeerbare persoon is iedereen die, rechtstreeks of onrechtstreeks, kan worden geïdentificeerd bijv. door verwijzing naar een identificatienummer; rechtspersonen kunnen in de omvang van de BCR's opgenomen worden door een overeenkomst hieromtrent tussen het bedrijf dat de gegevens overdraagt en de gegevensontvanger;
- **DPO**: de Data Privacy Officer, d.w.z. de door het deelnemende bedrijf aangestelde persoon met verantwoordelijkheid voor de implementatie en de naleving van de BCR,'s ;
- **DPE**: de Data Privacy Executive van een bedrijfsentiteit van de Siemens-groep; deze functie wordt door de CEO van de betreffende bedrijfsentiteit van de Siemens-groep uitgeoefend;
- **EER-land / EER-landen**: de lidstaten van de Europese Unie (EU) en alle andere ondertekenaars van het Verdrag over de Europese Economische Ruimte (EER);
- **Bedrijf of bedrijfsentiteit van de Siemens-groep**: Siemens Aktiengesellschaft en elke andere bedrijfsentiteit, in Duitsland of het buitenland, waarin Siemens Aktiengesellschaft, rechtstreeks of onrechtstreeks, een meerderheidsbelang heeft of de meerderheid van de stemrechten in handen heeft of beheert ("Geaffilieerde bedrijven");
- **LC CO DP / LC C DP**: de globale functie ter bescherming van de persoonlijke levenssfeer bij Siemens AG;
- **Deelnemend bedrijf**: een bedrijfsentiteit van de Siemens-groep waarvoor de implementatie van deze BCR's verplicht is, of een ander met Siemens geassocieerd bedrijf in Duitsland of het buitenland waarin Siemens AG of een geaffilieerd bedrijf een minderheidsaandeel heeft en dat zich, met de goedkeuring van Siemens AG, vrijwillig akkoord heeft verklaard de regelgeving van de BCR's na te leven door een aansluitingsovereenkomst te sluiten ("andere aansluitende bedrijven");
- **Persoonsgegevens**: alle informatie met betrekking tot een betrokken identificeerbare persoon;
- **De verwerking of behandeling van persoonsgegevens of gegevensverwerking/-behandeling**: elke handeling of elk geheel van handelingen uitgevoerd met persoonsgegevens, al dan niet automatisch, zoals verzameling, opslag, retentie, aanpassing, wijziging, lezing, opzoeking, gebruik, openbaring door verzending, blokkering, verwijdering of vernietiging.
- **Gegevensverwerker**: natuurlijke of rechtspersoon die persoonsgegevens verwerkt of behandelt namens een verantwoordelijke entiteit
- **Derde**: elke natuurlijke of rechtspersoon of een andere entiteit dan de betrokken identificeerbare persoon, gegevensverwerker of verantwoordelijke entiteit;

[1] Bepaalde nationale wet- en regelgeving kan speciale eisen stellen aan deze toestemming, met mogelijke invloed op de geldigheid van de toestemming.

- **Overdracht van persoonsgegevens of gegevensoverdracht**: de openbaring van persoonsgegevens aan derden, de verzending van dergelijke gegevens aan derden, of het proces om dergelijke gegevens beschikbaar te maken aan derden in om het even welke vorm voor inspectie of opzoeking;

4. Belangrijke principes voor de verwerking en behandeling van persoonsgegevens

De volgende principes, in het bijzonder afgeleid van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG en de Madrid-resolutie van 5 november 2009, zijn van toepassing op de verwerking en behandeling van persoonsgegevens door de deelnemende bedrijven binnen de omvang van deze BCR's.

4.1 Legitimiteit & wettigheid van gegevensverwerking/-behandeling

De verwerking en behandeling van persoonsgegevens dient volledig conform de betreffende wettelijke bepalingen te gebeuren en met inachtname van de principes vastgelegd in deze BCR's.

Verwerking of behandeling is uitsluitend toegestaan indien minimaal aan een van volgende vereisten is voldaan:

- De betrokken identificeerbare persoon heeft uit vrije wil zijn/haar uitdrukkelijke toestemming gegeven; of
- De gegevensverwerking/-behandeling heeft tot doel een contractuele relatie of gelijkaardige vertrouwensrelatie tot stand te brengen met de betrokken identificeerbare persoon; of
- De gegevensverwerking/-behandeling is nodig om de rechtmatige belangen van de verantwoordelijke entiteit te vrijwaren en er geen redenen zijn om aan te nemen dat de identificeerbare persoon een groter legitiem belang heeft bij het uitsluiten van gegevensverwerking/-behandeling; of
- De gegevensverwerking/-behandeling is voorgeschreven of toegestaan door de nationale wet- en regelgeving van toepassing op de verantwoordelijke entiteit; of
- De gegevensverwerking/-behandeling is noodzakelijk voor de conformiteit met de wettelijke verplichtingen waaraan de verantwoordelijke entiteit onderworpen is; of
- De gegevensverwerking/-behandeling is, uitzonderlijk, noodzakelijk om het leven, de gezondheid of de veiligheid van de betrokken identificeerbare persoon te vrijwaren.

De verantwoordelijke entiteit dient eenvoudige, snelle en efficiënte procedures te voorzien waarmee de betrokken identificeerbare persoon op elk gegeven ogenblik zijn/haar toestemming weer kan intrekken.

4.2 Doel

Persoonsgegevens zullen uitsluitend verwerkt en behandeld worden voor de gespecificeerde, expliciete en rechtmatige doeleinden. In geen geval mogen persoonsgegevens verwerkt of behandeld worden op een manier die niet-compatibel is met de legitieme doeleinden waarvoor de persoonsgegevens werden verzameld. Deelnemende bedrijven zijn verplicht zich aan deze oorspronkelijke doeleinden te houden bij de opslag en verdere verwerking of behandeling van aan hen door een ander deelnemend bedrijf overgedragen gegevens; het doel van de gegevensverwerking en -behandeling mag alleen gewijzigd worden met de toestemming van de betrokken identificeerbare persoon of in zoverre toegestaan door de nationale wetgeving waaraan het deelnemende bedrijf dat de gegevens overdraagt onderworpen is.

4.3 Transparantie

Alle deelnemende bedrijven zullen persoonsgegevens transparant verwerken en behandelen. De betrokken identificeerbare personen wier persoonsgegevens verwerkt en behandeld worden door een deelnemend bedrijf krijgen de volgende informatie van het deelnemende bedrijf (in overleg met het overdragende bedrijf, indien van toepassing):

- Identiteit van de verantwoordelijke entiteit en van het overdragende bedrijf
- Categorieën van ontvangers of identiteit van de ontvangende entiteit
- Doel van de verwerking of behandeling

- Oorsprong van de gegevens (tenzij deze persoonsgegevens rechtstreeks bij de betrokken identificeerbare persoon worden verzameld)
- Recht op bezwaar tegen de verwerking of behandeling van persoonsgegevens van de betrokken identificeerbare persoon voor reclamedoeleinden
- Andere informatie in zoverre vereist om redenen van billijkheid, bijv.
    - recht op informatie, rechtzetting en verwijdering.

In zoverre de persoonsgegevens niet rechtstreeks bij de betrokken identificeerbare persoon verzameld worden, dient deze informatie - uitzonderlijk - niet voorzien te worden, indien deze niet-verstrekking van informatie noodzakelijk is om de rechten van de betrokken identificeerbare persoon of andere personen te beschermen, indien de betrokken identificeerbare persoon reeds geïnformeerd werd of indien dit disproportionele inspanningen met zich mee zou brengen.

4.4 Gegevenskwaliteit en gegevensbeheer

Persoonsgegevens dienen feitelijk correct te zijn en indien nodig moeten ze worden bijgewerkt. Er dienen gepaste maatregelen genomen te worden om ervoor te zorgen dat onjuiste of onvolledige gegevens verbeterd of verwijderd worden.

De gegevensverwerking en -behandeling wordt geleid door het principe van de gegevensefficiëntie. Doel is het verzamelen, verwerken en gebruiken van alleen die persoonsgegevens die echt vereist zijn, d.w.z. zo weinig mogelijk persoonsgegevens. Er wordt in het bijzonder gebruik gemaakt van de mogelijkheid van anonieme of pseudonieme gegevens, op voorwaarde dat de kost en de inspanning evenredig zijn met het gewenste doel. Statistische evaluaties of studies gebaseerd op geanonimiseerde of gepseudonimiseerde gegevens zijn niet relevant in het kader van de bescherming van de persoonlijke levenssfeer, op voorwaarde dat dergelijke gegevens niet gebruikt kunnen worden om de betrokken persoon te identificeren.

Persoonsgegevens die niet langer vereist zijn voor de bedrijfsdoeleinden waarvoor ze oorspronkelijk verzameld en bewaard werden, moeten worden verwijderd. Indien er wettelijk voorziene retentieperiodes gelden, worden de gegevens geblokkeerd in plaats van verwijderd.

4.5 Verdere gegevensoverdracht

De overdracht van persoonsgegevens van een deelnemend bedrijf (d.w.z. een bedrijfsentiteit van de Siemens-groep of ander aansluitend bedrijf) aan een niet-deelnemend bedrijf (d.w.z. een bedrijf dat niet gebonden is door de BCR's, met inbegrip van bedrijven met een minderheidsbelang die geen aansluitingsovereenkomst hebben gesloten en externe bedrijven) buiten de EER is alleen toegestaan onder de volgende voorwaarden:

- De ontvangende entiteit beschikt over een adequaat gegevensbeschermingsniveau voor persoonsgegevens zoals bedoeld door Artikel 25 van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG, bijv. door het sluiten van een EU-modelovereenkomst (modelcontractbepalingen voor de overdracht van persoonsgegevens 2010/87/EU, modelcontractbepalingen tussen Data Verantwoordelijke entiteits 2001/497/EC of 2004/915/EC) of door het sluiten van andere gepaste contractuele bepalingen tussen de overdragende en de ontvangende entiteit;
- De overdracht is toegestaan volgens de uitzonderingen gedefinieerd in Artikel 26 van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG;
- Als de ontvangende entiteit een gegevensverwerker is, dient bijkomend aan de voorwaarden vastgelegd in Artikel 16 en 17 van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG te worden voldaan.

4.6 Bijzondere categorieën van persoonsgegevens

Bijzondere categorieën van persoonsgegevens, met andere woorden informatie over de raciale of etnische afkomst van een persoon, de politieke, religieuze of filosofische overtuigingen, eventueel lidmaatschap van een vakbond, gezondheid of seksuele oriëntatie van een persoon mogen als algemeen principe niet verwerkt of behandeld worden.

Indien de verwerking of behandeling van bijzondere categorieën van persoonsgegevens noodzakelijk is, moet de expliciete toestemming van de betrokken identificeerbare persoon bekomen worden, tenzij,

- de betrokken identificeerbare persoon zich niet in een positie bevindt om zijn/haar toestemming te geven (bijv. medische noodsituaties) en de verwerking of behandeling noodzakelijk is om de vitale belangen van de betrokken identificeerbare persoon of een andere persoon te beschermen; of
- de verwerking of behandeling noodzakelijk is in verband met medische diagnose, preventieve geneeskunde, zorgverstrekking, behandeling of het beheer van gezondheidszorgdiensten waar gegevensverwerking en -behandeling uitgevoerd wordt door medisch personeel dat gebonden is door beroepsgeheim of door ander personeel onderworpen aan een gelijkaardige geheimhoudingsverplichting, of
- de betrokken identificeerbare persoon de betreffende gegevens reeds openbaar gemaakt heeft; of
- de verwerking of behandeling noodzakelijk is voor het tot stand brengen, laten gelden of zich verdedigen tegen juridische claims in rechtszaken, op voorwaarde dat er geen redenen zijn om aan te nemen dat de betrokken identificeerbare persoon een groter legitiem belang heeft bij het ervoor zorgen dat dergelijke gegevens niet verwerkt of behandeld worden; of
- de verwerking of behandeling uitdrukkelijk wettelijk is toegestaan volgens de geldende nationale wetgeving (bijv. voor de registratie/bescherming van minderheden), en er bijkomende garanties worden gegeven zoals bedoeld door de EU-Richtlijn betreffende gegevensbescherming 95/46/EG voor de verwerking of behandeling van de gegevens, met inbegrip van specifieke, adequate gegevensbeveiligingsmaatregelen.

De bevoegde gegevens-DPO van het deelnemende bedrijf zal geraadpleegd worden voor de verwerking van bijzondere categorieën van persoonsgegevens.

4.7 Automatische afzonderlijke beslissingen

Als persoonsgegevens verwerkt worden met het oog op automatische afzonderlijke beslissingen, moeten de legitieme belangen van de betrokken identificeerbare persoon door gepaste maatregelen verzekerd worden. Beslissingen met mogelijk negatieve juridische gevolgen of een belangrijke nadeel voor de betrokken identificeerbare persoon, kunnen niet uitsluitend genomen worden op basis van een automatische afzonderlijke procedure ontworpen voor de evaluatie van persoonlijke eigenschappen van een individu, d.w.z. beslissingen mogen niet exclusief op het gebruik van informatietechnologie gebaseerd zijn. Een uitzondering is alleen van toepassing indien de beslissing

- genomen is tijdens het sluiten of uitvoeren van een overeenkomst, op voorwaarde dat aan de vraag tot sluiten of uitvoeren van een overeenkomst ingediend door de identificeerbare persoon werd voldaan of dat er gepaste maatregelen werden genomen om zijn legitieme belangen te vrijwaren, zodat hij de gelegenheid krijgt zijn standpunt toe te lichten; of
- gemachtigd is door een wet waarin maatregelen worden vastgelegd voor de vrijwaring van de legitieme belangen van de betrokken identificeerbare persoon.

4.8 Gegevensbeveiliging

Verantwoordelijke entiteiten dienen de gepaste technische en organisatorische maatregelen te nemen om de vereiste gegevensbeveiliging te verzekeren, die persoonsgegevens beschermt tegen toevallige of onwettige verwijdering, niet-toegestaan gebruik, wijziging, verlies, vernietiging en tegen niet-toegestane openbaring of niet-toegestane toegang. Rekening houdend met de technische mogelijkheden en de implementatiekosten dienen dergelijke maatregelen een beveiligingsniveau te verzekeren overeenkomstig de risico's verbonden aan de verwerking en behandeling en de aard van de te beschermen gegevens. Bijzondere categorieën van persoonsgegevens verdienen bijzondere bescherming.

De te voorziene veiligheidsmaatregelen hebben in het bijzonder betrekking op computers (servers en werkstations), netwerken, communicatieverbindingen en toepassingen.

Om een adequaat niveau van technische en organisatorische maatregelen voor gegevensbescherming te verzekeren, werd de Corporate Information Security Guide (richtlijnen voor de beveiliging van bedrijfsgegevens) geïntroduceerd, bindend voor de volledige Siemens-groep krachtens CIT-rondzendbrief nr. 4/2009. De actuele versie van de Corporate Information Security Guide is beschikbaar op het intranet.

Specifieke maatregelen om een adequaat gegevensbeschermingsniveau voor persoonsgegevens te verzekeren omvatten aannamecontroles, systeemtoegangscontroles, gegevenstoegangscontroles, transmissiecontroles, invoercontroles, opdrachtcontroles, beschikbaarheidscontroles en scheidingscontroles.

Alle werkstations – met inbegrip van mobiele toestellen (bijv. laptops) – beschikken over een wachtwoordbeveiliging. Het Siemens-intranet beschikt over een firewall-systeem om de interne bedrijfsinformatie tegen niet-toegestane externe toegang te beschermen. De transmissie van persoonsgegevens via het eigen bedrijfsnetwerk wordt typisch versleuteld – in zoverre vereist door de aard en het beoogde doel van de betreffende persoonsgegevens.

4.9 Vertrouwelijkheid van gegevensverwerking/-behandeling

Alleen personeel dat bevoegd is en speciaal werd opgeleid om conform de privacybeschermingeisen te handelen, mag persoonsgegevens verzamelen, verwerken of gebruiken. De toegangsrechten voor de afzonderlijke medewerker zullen beperkt zijn overeenkomstig de aard en de omvang van zijn/haar specifieke activiteitendomein. De medewerker mag geen persoonsgegevens gebruiken voor privédoeleinden en mag ook geen persoonsgegevens overdragen of op een andere wijze beschikbaar stellen aan niet-bevoegde personen. Niet-bevoegde personen omvatten in deze context, bijvoorbeeld medewerkers die geen nood hebben aan deze persoonsgegevens om hun gespecialiseerde taken uit te voeren. De vertrouwelijkheidverplichting blijft ook gelden na de beëindiging van de tewerkstellingsrelatie van de betreffende medewerker.

4.10 Uitbesteding van de gegevensverwerking

Indien deelnemende bedrijven een ander bedrijf aanstellen om persoonsgegevens te verwerken, overeenkomstig de voorwaarden van de BCR's, dienen de volgende eisen nageleefd te worden:

- De gegevensverwerker dient door de verantwoordelijke entiteit zorgvuldig geselecteerd te worden; een gegevensverwerker zal geselecteerd worden ter verzekering van de noodzakelijke technische en organisatorische veiligheidsmaatregelen voor de gegevensverwerking en -behandeling conform de geldende wet- en regelgeving betreffende de bescherming van de persoonlijke levenssfeer;
- De verantwoordelijke entiteit verzekert en controleert regelmatig dat de gegevensverwerker volledig conform de overeengekomen technische en organisatorische beveiligingsmaatregelen handelt;
- De uitvoering van de uitbesteedde gegevensverwerking en -behandeling dient geregeld te worden in een schriftelijk of anders gedocumenteerde overeenkomst, waarin de rechten en plichten van de gegevensverwerker ondubbelzinnig gedefinieerd zijn;
- De gegevensverwerker dient contractueel gebonden te zijn aan de verwerking van gegevens ontvangen van de verantwoordelijke entiteit binnen het contractuele kader en in overeenstemming met de instructies vrijgegeven door de verantwoordelijke entiteit. De verwerking van de gegevens voor de eigen doeleinden van de gegevensverwerker of voor de doeleinden van derden moeten contractueel verboden worden;
- De verantwoordelijke entiteit behoudt de verantwoordelijkheid voor de legitimiteit van de verwerking en blijft het contactpunt voor de betrokken identificeerbare persoon.

5. Materiële rechten van de betrokken identificeerbare persoon

De betrokken identificeerbare personen hebben de hieronder vermelde onvervreemdbare rechten m.b.t. hun persoonsgegevens die door een deelnemend bedrijf verwerkt worden binnen de omvang van deze BCR's.

- De betrokken identificeerbare persoon kan vragen dat er in een verstaanbare vorm met hem wordt gecommuniceerd over zijn/haar verwerkte persoonsgegevens met betrekking tot de reden en het doel van de verwerking. De betrokken identificeerbare persoon heeft ook recht op informatie over de identiteit van de verantwoordelijke entiteit en, in geval van de overdracht van persoonsgegevens, heeft de betrokken identificeerbare persoon ook recht op informatie over de ontvangers of categorieën van ontvangers. Het recht op informatie omvat ook de logische structuur van de automatische verwerkingshandelingen, in zoverre dat dit betrekking heeft op automatische beslissingen. Indien voorzien door de geldende wetgeving, heeft de betrokken identificeerbare persoon geen recht op informatie indien dit aanzienlijk afbreuk zou doen aan de bedrijfsdoeleinden, in het bijzonder indien de openbaring van bedrijfsgeheimen en het belang van de vrijwaring van bedrijfsgeheimen prioriteit heeft op het belang van de betrokken identificeerbare persoon. Lokale wettelijke voorschriften kunnen het recht op informatie van de identificeerbare persoon beperken indien dit recht herhaaldelijk binnen een korte tijdsperiode wordt uitgeoefend, tenzij de identificeerbare persoon een legitieme reden heeft voor de herhaalde bevestiging van verzoeken om informatie. Het deelnemende bedrijf kan de betrokken identificeerbare persoon een redelijke vergoeding vragen voor het verstrekken van de informatie, in zoverre door de geldende nationale wetgeving toegestaan.
- De betrokken identificeerbare persoon kan om een rechtzetting vragen indien zijn/haar persoonsgegevens onjuist of onvolledig blijken te zijn.
- De betrokken identificeerbare persoon heeft het recht te vragen dat zijn/haar persoonsgegevens geblokkeerd worden indien het niet mogelijk is te bepalen of de gegevens correct of incorrect zijn.
- De betrokken identificeerbare persoon heeft het recht te vragen dat zijn/haar persoonsgegevens verwijderd worden indien de gegevensverwerking ondertussen onwettig is geworden of zodra de gegevens niet langer vereist zijn voor de verwerkingsdoeleinden. Gerechtvaardigde claims door de betrokken identificeerbare persoon voor verwijdering dienen binnen een redelijke periode te worden opgevolgd, in zoverre de wettelijk voorziene retentieperiode of contractuele verplichtingen de verwijdering niet in de weg staan. In geval van wettelijk voorziene retentieperiodes, kan de betrokken identificeerbare persoon eisen dat zijn/haar gegevens geblokkeerd worden i.p.v. verwijderd. Hetzelfde geldt indien het onmogelijk is de gegevens te verwijderen.
- De betrokken identificeerbare persoon heeft het recht bezwaar aan te tekenen tegen de verwerking van zijn/haar persoonsgegevens voor reclame- of voor marktonderzoekdoeleinden en/of in het kader van opiniepeilingen. De betrokken identificeerbare persoon zal worden geïnformeerd over zijn/haar recht kosteloos bezwaar aan te tekenen.
- De betrokken identificeerbare persoon heeft ook een algemeen recht bezwaar aan te tekenen tegen de verwerking van zijn/haar persoonsgegevens, indien wegens de persoonlijke situatie van de identificeerbare persoon, het legitieme belang van de identificeerbare persoon prioriteit heeft t.o.v. het legitieme belang van de verantwoordelijke entiteit bij de verwerking van de persoonsgegevens.
- De betrokken identificeerbare persoon kan bovenstaande rechten schriftelijk laten gelden t.o.v. het deelnemende bedrijf, de bevoegde DPO van het deelnemende bedrijf of de LC CO DP. Op de gerechtvaardigde vraag van de betrokken identificeerbare persoon dient binnen een redelijke termijn een antwoord te volgen van de entiteit aan wie de vraag gericht werd. Dit antwoord dient schriftelijk te zijn (e-mail volstaat).

6. Beschrijving van de gegevensoverdracht

Siemens heeft een complexe groepsstructuur met een groot aantal bedrijfsentiteiten en deelnemende bedrijven, waartussen voor tal van doeleinden persoonsgegevens uitgewisseld worden. De gegevensuitwisseling vindt plaats tussen deelnemende bedrijven gevestigd in een EER-land evenals met deelnemende bedrijven gevestigd buiten een EER-land.

De nood aan een dergelijke interne gegevensuitwisseling binnen de Siemens-groep heeft betrekking op de persoonsgegevens van medewerkers, klanten, leveranciers, aandeelhouders en

andere bedrijfpartners en contracterende partijen. Dit omvat – afhankelijk van de beoogde doeleinden – bijvoorbeeld de naam, GID (Global Identifier), geboortedatum, nationaliteit, burgerlijke stand, geslacht, contactgegevens, adresgegevens, accountgegevens, bankgegevens, religieuze overtuiging, informatie over onderwijs, kennis en vaardigheden, loopbaan, datum van indiensttreding, functieniveau, enz.

Deze gegevens worden binnen Siemens-groep uitsluitend verwerkt en overgedragen binnen de omvang van de normale bedrijfsdoeleinden en met het oog op de interne administratie. De gegevensoverdracht gebeurt met het oog op aanwerving, HR-administratie en personeelsontwikkeling, voor compliance-doeleinden, voor de uitvoering en implementatie van opdrachten en projecten voor externe en interne klanten, voor de verwerking van aankoop- en werkorders met leveranciers en serviceproviders, voor de naleving van rapporteringplichten, voor de uitvoering van te betalen posten (accounts payable) of de inning van te vorderen posten (accounts receivable), voor boekhoudredenen, met het oog op interne communicatie, voor consolidatiedoeleinden en het poolen van IT-processen in bepaalde regio's voor kostenverlagingen, en ook in verband met de samenwerking en coördinatie van bedrijfsentiteiten binnen de groep op divisie- en regionaal niveau of op algemeen niveau in de loop van de globale bedrijfstransacties en -projecten.

7. Procedurele kwesties

7.1 Bindende aard van de BCR's

De BCR's zijn in hun geheel bindend.

7.1.1 Bindend voor bedrijfsentiteiten van de Siemens-groep en andere aansluitende bedrijven

De BCR's zijn aanvaard door Siemens Aktiengesellschaft (Siemens AG) en treden in voege door publicatie van een Corporate-rondzendbrief van Siemens.

De verantwoordelijkheid voor de implementatie van de BCR's in de deelnemende bedrijven ligt bij het Executive Management van het betreffende deelnemende bedrijf, waarbij de specifieke uitvoering gebeurt door de entiteit die binnen het bedrijf persoonsgegevens verwerkt als onderdeel van haar gespecialiseerde taak. In bedrijfsentiteiten van de Siemens-groep ligt de verantwoordelijkheid bij de CEO van de Siemens-bedrijfsentiteit in zijn/haar hoedanigheid van Data Privacy Executive (DPE).

Door hun bindende aard dienen de BCR's door alle bedrijfsentiteiten van de Siemens-groep en de andere aansluitende bedrijven in acht genomen te worden.

Om de acceptatie en implementatie van de BCR's te documenteren, in het geval van bedrijfsentiteiten van de Siemens-groep, zal het Executive Management van de betreffende bedrijfsentiteit een expliciete schriftelijke verbintenisverklaring tot naleving van de BCR's opstellen. Het opstellen van deze schriftelijke verbintenisverklaring maakt de BCR-richtlijnen bindend voor de bedrijfsentiteit van de Siemens-groep. De verbintenisverklaring dient door het Executive Management van de bedrijfsentiteit van de Siemens-groep ondertekend en naar LC C DP teruggezonden te worden. De verbintenisverklaring is als Bijlage 1 bij de BCR's gevoegd.

In principe moeten alle bedrijfsentiteiten van de Siemens-groep de verbintenisverklaring ondertekenen en de BCR's implementeren ten laatste twee jaar na publicatie van de betreffende Siemens Corporate-rondzendbrief (ervan uitgaande dat gedurende de overgangsperiode de bedrijfsentiteit ernaar zal streven de BCR's na te leven in de mate van het redelijk mogelijke), tenzij een bedrijfsentiteit van de Siemens-groep wegens een geldige reden vrijgesteld wordt van de implementatie van de BCR's (bijv. geldende wet- en regelgeving m.b.t. toezicht op de financiële en banksector, geen bedrijfsactiviteiten, geen medewerkers, geen verwerking van persoonsgegevens, onmiddellijke vereffening of desinvestering). Een vrijstellingsaanvraag moet via e-mail bij Siemens AG (LC C DP) worden ingediend door de betreffende bedrijfsentiteit van de Siemens-groep en met vermelding van de reden. LC C DP zal vervolgens over de gegrondheid van de aanvraag oordelen en de bedrijfsentiteit van de groep hiervan op de hoogte brengen.

Andere bedrijven dan de bedrijfsentiteiten van de Siemens-groep, waarin Siemens AG een rechtstreeks of onrechtstreeks belang heeft, kunnen vrijwillig een juridisch bindende verbintenis sluiten voor de naleving van de BCR-richtlijnen indien gewenst en Siemens AG (LC C DP) akkoord gaat met een dergelijke deelname (de “andere aansluitende bedrijven”). Siemens AG beslist naar eigen goeddunken of andere bedrijven dan de bedrijfsentiteiten van de Siemens-groep de gelegenheid krijgen vrijwillig aan het BCR-proces deel te nemen.

Om de acceptatie en de implementatie van de BCR's door andere aansluitende bedrijven te documenteren, wordt er een aansluitingsovereenkomst gesloten tussen Siemens AG (LC C DP) en het deelnemende bedrijf; de BCR's worden als bijlage bij de aansluitingsovereenkomst gevoegd. Na het sluiten van de aansluitingsovereenkomst zijn de BCR-richtlijnen afzonderlijk bindend voor het deelnemend bedrijf. Bijgevolg zal er voor dergelijke "andere aansluitende bedrijven" een overgangsperiode gelden om de naleving van de BCR's te realiseren en te verzekeren; deze zal niet langer zijn dan twee jaar vanaf de uitvoering van de Aansluitingsovereenkomst (ervan uitgaande dat gedurende de overgangsperiode de andere aansluitende bedrijven ernaar zullen streven de BCR's na te leven in de mate van het redelijk mogelijke). De tekst van de aansluitingsovereenkomst is als bijlage bij de BCR's gevoegd.

LC C DP houdt op het Siemens-intranet een elektronisch register bij van deelnemende bedrijven die streven naar de naleving van de bepalingen van de BCR's door ondertekening van een verbintenisverklaring of een aansluitingsovereenkomst. De meest recente versie van dit elektronische register (statusoverzicht) kan op elk gegeven ogenblik op de intranetpagina's van LC CO DP worden geraadpleegd. Het statusoverzicht omvat en identificeert ook die bedrijfsentiteiten die wegens een geldige reden uitzonderlijk vrijgesteld zijn van de ondertekening en implementatie van de BCR's. Het statusoverzicht registreert en identificeert ook de bedrijfsentiteiten die (nog) niet aan de verplichting tot acceptatie en implementatie van de BCR's voldoen.

Als een bedrijfsentiteit van de Siemens-groep (nog) geen verbintenisverklaring (tot naleving van de BCR's) heeft opgesteld, dient de legitimiteit van gegevensoverdrachten naar deze bedrijfsentiteit te worden herbekeken in elk afzonderlijk geval en te worden verzekerd door de gepaste speciale maatregelen overeenkomstig de eisen van artikels 25 en 26 van de EU-Richtlijn 95/46/EG. Dit is ook van toepassing op andere aansluitende bedrijven in zoverre deze nog geen aansluitingsovereenkomst hebben gesloten.

De verbintenis tot naleving van de BCR's kan beëindigd worden door terugtrekking, annulering of opzegging door Siemens AG of door het deelnemende bedrijf. Het verlies van de status van bedrijfsentiteit van de Siemens-groep betekent niet automatisch het einde van de verplichtingen voortvloeiend uit de BCR's. In dergelijke situaties is de opzegging van de BCR's door Siemens AG of de (voormalige) bedrijfsentiteit van de Siemens-groep echter wel noodzakelijk. In geval van terugtrekking/annulering van de verbintenisverklaring of van de verklaring tot sluiting van een aansluitingsovereenkomst of in geval van de opzegging van de BCR's, zullen de verplichtingen voortvloeiend uit de BCR's met betrekking tot de verwerkte of behandelde persoonsgegevens tot aan de terugtrekking, annulering of opzegging blijven gelden en tot deze gegevens door het betreffende bedrijf effectief verwijderd zijn conform de geldende wet- en regelgeving.

7.1.2 Bindend voor medewerkers van deelnemende bedrijven

De medewerkers van deelnemende bedrijven zijn ook gebonden door de BCR-richtlijnen. De CEO van het betreffende deelnemend bedrijf is verplicht de gepaste maatregelen te nemen om ervoor te zorgen dat de BCR's juridisch bindend zijn voor de medewerkers. Zodoende worden de BCR's, aangezien ze in een Siemens Corporate-rondzendbrief gepubliceerd worden, op dezelfde wijze bindend voor alle medewerkers (wat van land tot land kan verschillen) als bij alle andere Siemens Corporate-rondzendbrieven, in het bijzonder door middel van ethische gedragscode van Siemens of Siemens Business Conduct Guidelines (BCG), waardoor de naleving door de medewerkers van alle betreffende Siemens-rondzendbrieven en beleidsrichtlijnen verplicht wordt gesteld.

De BCR-richtlijnen en alle andere voorschriften betreffende de bescherming van de persoonlijke levenssfeer gelden ook altijd voor de medewerkers van de deelnemende bedrijven.

De deelnemende bedrijven informeren hun medewerkers dat niet-naleving van de BCR-richtlijnen in disciplinaire maatregelen of arbeidsrechtelijke sancties (bijv. formele waarschuwing, ontslag) tegen de medewerkers kan resulteren.

7.1.3 Bindend voor betrokken identificeerbare personen

Bepaalde richtlijnen van de BCR's zijn ook bindend voor de betrokken identificeerbare personen, krachtens de rechten van derdebegunstigden. De richtlijnen in de volgende secties verlenen voordelen aan derden: Secties 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 5, 7.1.3, 7.6, 7.9, 7.10 en 8.

De betrokken identificeerbare personen hebben de mogelijkheid een klacht in te dienen wegens niet-naleving van de betreffende BCR-richtlijnen door een deelnemend bedrijf, hetzij tegen het deelnemende bedrijf of tegen Siemens AG (LC CO DP). Meer informatie over eventueel verhaalsrecht en de interne klachtenprocedure worden in Sectie 7.6 van deze BCR's beschreven evenals in een afzonderlijk document m.b.t. de klachtenprocedure (Complaint Management Concept).

Hiernaast hebben de betrokken identificeerbare personen het recht de naleving van de bovenvermelde rechten van derdebegunstigden door een deelnemend bedrijf af te dwingen, door indiening van een klacht bij de bevoegde gegevensbeschermingsinstantie of door andere rechtsmiddelen aan te wenden via de bevoegde rechtbanken. De betrokken identificeerbare personen kunnen voor de geleden schade schadevergoeding eisen.

De betrokken identificeerbare personen hebben de mogelijkheid een dergelijke klacht in te dienen

- bij de bevoegde rechtbank voor het deelnemende bedrijf dat de gegevens heeft overgedragen; of
- bij de bevoegde rechtbank voor het hoofdkwartier van Siemens AG; of
- bij de bevoegde gegevensbeschermingsinstantie.

Dit betekent dat bij vaststelling van een inbreuk op de BCR-richtlijnen door een deelnemend bedrijf buiten de EER, de rechtbanken en overheidsinstanties binnen de EER ook bevoegd zijn. De betrokken identificeerbare persoon kan t.o.v. het deelnemende bedrijf dat de aansprakelijkheid heeft aanvaard dezelfde rechten laten gelden, alsof de inbreuk door een deelnemend bedrijf gevestigd binnen een EER-land gepleegd werd.

De bevoegdheid van de rechtbanken en overheidsinstanties binnen de EER, zoals hierboven beschreven, is niet van toepassing indien de gegevensontvanger gevestigd is in een land buiten de EER, maar over een adequaat gegevensbeschermingsniveau beschikt, zoals bevestigd door een besluit van de Europese Commissie.

Om te verzekeren dat de betrokken identificeerbare personen ook wettelijk afdwingbare rechten van derdebegunstigden genieten in die landen waar de toekenning van rechten van derdebegunstigden in het BCR-document mogelijk niet volstaat, zal Siemens AG – in zoverre noodzakelijk – hiertoe bijkomende contractuele overeenkomsten sluiten met de betreffende deelnemende bedrijven. Een clausule m.b.t. derdebegunstigden waarin de noodzakelijke rechten aan de betrokken identificeerbare personen worden toegekend, is opgenomen in de verbintenisverklaring die bedrijfsentiteiten van de Siemens-groep ondertekenen ter bevestiging van hun acceptatie en implementatie van de BCR's. Hetzelfde geldt voor de aansluitingsovereenkomst die de andere aansluitende bedrijven met Siemens AG sluiten.

7.2 Bekendmaking van de BCR's

De BCR's en de clausule m.b.t. derdebegunstigden zijn voor de betrokken identificeerbare personen makkelijk en voortdurend toegankelijk. De betrokken identificeerbare personen kunnen contact opnemen met de bevoegde DPO van het deelnemende bedrijf of kunnen als alternatief rechtstreeks contact met Siemens AG opnemen. Siemens AG zal de BCR's permanent en op gepaste wijze voor de betrokken identificeerbare personen beschikbaar stellen, in het bijzonder door publicatie van de actuele versie van de BCR's op de Siemens-website, momenteel te vinden op http://www.siemens.com.

7.3 Implementatie van de BCR's in de deelnemende bedrijven

Het Executive Management van een deelnemend bedrijf – of de CEO van een deelnemende bedrijfsentiteit van de Siemens-groep in zijn/haar hoedanigheid als DPE – is verantwoordelijk voor de correcte implementatie en naleving van de BCR's. Het Executive Management van het deelnemende bedrijf kan deze taak delegeren – zonder de verantwoordelijkheid te delegeren – aan de DPO.

Siemens heeft een wereldwijd netwerk van DPO's tot stand gebracht. Bij de opstelling van de verbintenisverklaring tot naleving van de BCR's of de sluiting van de aansluitingsovereenkomst van de BCR's, zal elk deelnemend bedrijf een bevoegde DPO aanduiden en de contactgegevens van de DPO aan LC C DP bezorgen. Het deelnemende bedrijf zal LC C DP onverwijld op de hoogte brengen van eventuele wijzigingen van de identiteit van de DPO.

De DPO rapporteert eenmaal per jaar aan het Executive Management van het betreffende deelnemende bedrijf en rapporteert regelmatig – maar minimaal eenmaal per jaar – aan de CDPO van Siemens AG. De DPO rapporteert onder andere ook over de mate waarin de BCR's in het specifieke deelnemende bedrijf geïmplementeerd worden.

De CDPO van Siemens AG rapporteert eenmaal per jaar aan de Raad van Bestuur (Managing Board) van Siemens AG. Dit rapport omvat in het bijzonder de mate van implementatie van de BCR's in alle deelnemende bedrijven.

De CDPO is de Chief Data Privacy Officer van Siemens AG en werd aangesteld door middel van een bestuursmededeling ondertekend door de CEO en de General Counsel van Siemens AG. De CDPO staat aan het hoofd van LC CO DP, de unit die de operationele verantwoordelijkheid draagt voor het Siemens-programma ter bescherming van de persoonlijke levenssfeer en de implementatie van de privacybepalingen, in het bijzonder door opleidingsmaatregelen en monitoring (met inbegrip van incidentbeheer en risicoanalyses). Als hoofd van deze unit wordt de CDPO ondersteund door de medewerkers die hij selecteert, en die vervolgens aan hem rapporteren.

7.4 Monitoring van de BCR-naleving

De BCR-naleving door de deelnemende bedrijven is aan regelmatige evaluaties onderworpen, hoofdzakelijk door de DPO aangesteld door het Executive Management van het deelnemende bedrijf. Het Executive Management van het deelnemende bedrijf ondersteunt de DPO bij de uitoefening van zijn/haar taken en betrekt hem/haar bij eventuele klachten ingediend door de betrokken identificeerbare personen wegens de niet-naleving van de BCR's.

In geval van ernstige inbreuken op het beleid ter bescherming van de persoonlijke levenssfeer en bij problemen van fundamentele aard, zal de DPO de CDPO van Siemens AG raadplegen en zijn/haar advies en beslissingen in acht nemen bij het remediëren van inbreuken en problemen m.b.t. beleid ter bescherming van de persoonlijke levenssfeer.

LC CO DP heeft het recht willekeurige controles van het werk van de DPO uit te oefenen m.b.t. de implementatie en naleving van de BCR's in het deelnemende bedrijf, hetzij door een schriftelijke zelfevaluatie door de DPO te vragen of als onderdeel van gesprekken. De inhoud van deze gesprekken zal door LC CO DP worden gedocumenteerd.

Elk deelnemend bedrijf dat gegevens overdraagt, heeft in specifieke situaties het recht de gegevensbewerking/-behandeling bij het ontvangende bedrijf te evalueren. Zodoende zal het overdragende bedrijf de geverifieerde rechten van de identificeerbare personen laten gelden, en ondersteuning bieden aan de betrokken identificeerbare personen, die wegens schendingen van de verplichtingen opgelegd door deze BCR's werden benadeeld bij de uitoefening van hun rechten t.o.v. het verantwoordelijke bedrijf.

7.5 Training en opleiding

Een cruciaal aspect voor de correcte implementatie van de BCR's is de gepaste verstrekking van informatie en instructies aan medewerkers. Dit omvat het informeren van medewerkers dat inbreuken op de BCR's mogelijk strafrechtelijke of arbeidsrechtelijke gevolgen kunnen hebben evenals gevolgen op het vlak van burgerrechtelijke aansprakelijkheid.

Siemens AG biedt specifieke informatie en speciale training- en opleidingsprogramma's aan over de BCR's met het oog op het verzekeren van de adequate informatie en opleiding en training voor de medewerkers van een deelnemend bedrijf m.b.t. de correcte behandeling en bescherming van persoonsgegevens inzake de implementatie van de BCR's. De training- en opleidingsprogramma's zijn specifiek gericht op medewerkers die voortdurend of regelmatig persoonsgegevens behandelen of verwerken. Voor deze medewerkers is deelname aan de training- en opleidingscursussen verplicht. Training- en opleidingscursussen over de BCR's worden op regelmatige intervallen herhaald.

De informatie- en training- en opleidingsprogramma's omvatten bijvoorbeeld het aanbieden van webtrainingen (WBT), gepaste presentaties en opleidingsmateriaal voor zelfstudie, opleidingsprogramma's in klasverband en de organisatie van workshops op maat van specifieke medewerkers.

De succesvolle deelname door medewerkers aan training- en opleidingsprogramma's dient te worden gedocumenteerd.

Meer informatie hierover vindt u in een gedetailleerd training- en opleidingsconcept.

7.6 Klachtenprocedure

Identificeerbare personen kunnen altijd contact opnemen met de bevoegde dienst voor klachtenafhandeling bij Siemens AG (LC CO DP; voor contactgegevens, zie Sectie 9) of de bevoegde DPO van het deelnemende bedrijf, met klachten over inbreuken op de BCR's door een deelnemend bedrijf of met mogelijke vragen. De betrokken identificeerbare persoon ontvangt onmiddellijk een bevestiging van de ontvangst van de klacht door de gecontacteerde entiteit, waarna de klacht binnen drie (3) maand na ontvangst afgehandeld moet worden. Dit tijdskader kan redelijkerwijze worden overschreden in geval van vertragingen die niet aan de bedrijfsentiteit van de Siemens-groep of een ander aansluitend bedrijf toe te schrijven zijn, bijv. indien de betrokken identificeerbare persoon het nalaat tijdig noodzakelijke informatie te verstrekken.

De medewerkers betrokken bij de klachtenafhandeling in de bevoegde dienst voor klachtenafhandeling genieten een zekere mate van autonomie voor de uitoefening van deze functie.

Het deelnemende bedrijf en LC CO DP dienen bij een onderzoek mee te werken met de gegevensbeschermingsinstanties van het betreffende land en hun oordeel in acht te nemen.

Verdere details – het soort klacht, de responstijd, verdere procedures volgend op de aanvaarding en/of afwijzing van de klacht, bijkomende rechtsmiddelen – worden vastgelegd in een afzonderlijk Complaint Management Concept dat in een afzonderlijke bijlage bij de BCR's wordt gevoegd.

7.7 BCR-audit

Naast andere bestaande interne audit- en controlesystemen in de Siemens-bedrijvengroep, heeft Siemens een afzonderlijk BCR-auditprogramma ingevoerd om te verzekeren dat er een adequaat gegevensbeschermingsniveau voorzien is, zoals vereist door de BCR-richtlijnen, dat door de deelnemende bedrijven regelmatig wordt geëvalueerd. Dergelijke BCR-audits dienen regelmatig of op verzoek van de CDPO van Siemens AG uitgevoerd te worden; ze zullen door de Siemens-auditorganisatie (F A) uitgevoerd worden met ondersteuning van de Siemens-gegevensbeschermingsorganisatie (bijv. gegevensbeschermingsexperts) of een externe auditor. Indien nodig kan een BCR-audit ook geïnitieerd worden door de interne auditorganisatie van Siemens (F A), door het auditcomité van Siemens AG, door het Executive Management of het auditcomité van het deelnemende bedrijf of door de informatiebeveiligingsorganisatie (GS IT ISEC).

De BCR-audit omvat alle aspecten van de BCR's. Als uit een BCR-audit blijkt dat er corrigerende maatregelen genomen dienen te worden om een inbreuk op de BCR's te remediëren, zal de CDPO controleren of de vereiste corrigerende maatregelen geïmplementeerd worden.

De CDPO van Siemens AG, het verantwoordelijke lid van de Raad van Bestuur van Siemens AG en het Executive Management van het deelnemende bedrijf dat de audit ondergaat, zullen het volledige BCR-auditrapport ontvangen. De resultaten van de BCR-audit worden op verzoek

beschikbaar gesteld aan de betreffende gegevensbeschermingsinstanties (d.w.z. de instanties van de EER-landen van waaruit de persoonsgegevens werden overgedragen aan het bedrijf dat de audit ondergaat).

De bevoegde gegevensbeschermingsinstantie heeft het recht een eigen BCR-audit van een deelnemend bedrijf uit te voeren. De overheidsinstantie kan ofwel zelf de BCR-audit uitvoeren of deze door een erkende onafhankelijke auditor laten uitvoeren. Een dergelijke officiële BCR-audit beperkt zich uitsluitend tot de naleving van BCR's door het deelnemende bedrijf. Er zal zoals nodig rekening gehouden worden met eventuele beperkingen als gevolg van vertrouwelijkheidovereenkomsten of bedrijfs- en handelsgeheimen.

Meer informatie over de BCR-audit vindt u in een afzonderlijk BCR-auditconcept.

7.8 Bijwerking & wijzigingsbeheer van de BCR's

Siemens behoudt zich het recht voor de BCR's op elk gegeven ogenblik te wijzigen en/of bij te werken. Dergelijke bijwerkingen van de BCR's kunnen in het bijzonder noodzakelijk blijken als gevolg van veranderende wettelijke eisen, belangrijke wijzigingen van de structuur van de groep of officiële vereisten opgelegd door de bevoegde gegevensbeschermingsinstanties.

Belangrijke wijzigingen aan de BCR's zullen in bepaalde omstandigheden een nieuwe goedkeuring vereisen. Alle andere wijzigingen aan de BCR's zijn mogelijk zonder nieuwe goedkeuring door de bevoegde gegevensbeschermingsinstanties.

LC C DP houdt een lijst van alle wijzigingen/bijwerkingen van de BCR's bij sinds de BCR's van kracht werden. LC C DP houdt ook een regelmatig bijgewerkte lijst van alle deelnemende bedrijven bij die effectief door de BCR's gebonden zijn (statusoverzicht, zie Sectie 7.1.1). De overdracht van persoonsgegevens aan een nieuw toegevoegd deelnemend bedrijf is pas toegestaan nadat deelnemende bedrijf de naleving van de BCR's kan verzekeren en een effectieve verbintenisverklaring tot naleving van de BCR's heeft opgesteld of een aansluitingsovereenkomst (m.b.t. de BCR's) heeft gesloten en de correct ondertekende overeenkomst aan LC C DP heeft terugbezorgd.

LC C DP brengt op verzoek, maar minstens eenmaal per jaar, de bevoegde gegevensbeschermingsinstantie op de hoogte van eventuele wijzigingen aan de BCR's of aan het statusoverzicht. Deze meldingen bevatten een korte toelichting van de redenen ter rechtvaardiging van de wijzigingen.

7.9 Wederzijdse ondersteuning en samenwerking met de gegevensbeschermingsinstanties

Siemens AG en de deelnemende bedrijven zullen in goed vertrouwen samenwerken en elkaar ondersteunen in geval van vragen of klachten van identificeerbare personen met betrekking tot de niet-naleving van de BCR's.

Siemens AG en de deelnemende bedrijven zullen in het kader van de implementatie van de BCR's bovendien ook in vertrouwen met de bevoegde gegevensbeschermingsinstanties samenwerken. Ze zullen BCR-gerelateerde vragen van de gegevensbeschermingsinstantie(s) binnen een gepast tijdskader en op gepaste wijze beantwoorden en het advies en de beslissingen van de bevoegde gegevensbeschermingsinstantie met betrekking tot de implementatie van de BCR's opvolgen.

7.10 Verhouding tussen de BCR's en lokaal geldende wet- en regelgeving

De legitimiteit van de verwerking of behandeling van persoonsgegevens wordt op basis van de lokaal geldende wet- en regelgeving beoordeeld. In zoverre de lokaal geldende wet- en regelgeving een hoger beschermingsniveau voor persoonsgegevens stipuleert dan deze BCR's, zal de gegevensverwerking/-behandeling overeenkomstig de geldende wet- en regelgeving gebeuren. Elk deelnemend bedrijf dient voor zichzelf na te gaan (bijv. via de DPO of de juridische afdeling) wat de betreffende lokaal geldende wet- en regelgeving is (bijv. wetgeving betreffende de bescherming van de persoonlijke levenssfeer) en dient de naleving ervan te verzekeren. Indien de lokaal geldende wet- en regelgeving een lager beschermingsniveau voor de bescherming van persoonsgegevens voorziet dan de BCR's, zijn de onderhavige BCR's van toepassing.

Indien de verplichtingen resulterend uit de lokaal geldende wet- en regelgeving tegenstrijdig zijn met de BCR's, zal het deelnemende bedrijf LC C DP onverwijld op de hoogte stellen. LC C DP zal het gemelde conflict in het statusoverzicht (zie Sectie 7.1.1) opnemen.

LC C DP zal vervolgens alle deelnemende bedrijven die eerder gegevens aan het deelnemende bedrijf hebben overgedragen informeren over de gemelde tegenstrijdigheid tussen de BCR's en de lokale wetgeving. LC C DP informeert ook de bevoegde gegevensbeschermingsinstantie over de tegenstrijdigheid tussen wet- en regelgeving en de bindende bedrijfsrichtlijnen en zoekt, samen met de gegevensbeschermingsinstantie en het deelnemende bedrijf, naar een praktische oplossing die de principes van de EU-Richtlijn betreffende gegevensbescherming 95/46/EG zoveel mogelijk benadert.

8. Aansprakelijkheid

Siemens AG aanvaardt de aansprakelijkheid voor niet-naleving van de BCR's door deelnemende bedrijven gevestigd buiten de EER. Siemens AG staat in voor de monitoring van de BCR-naleving door deelnemende bedrijven gevestigd buiten de EER en verzekert dat de deelnemende bedrijven gevestigd buiten de EER de noodzakelijke corrigerende maatregelen te nemen om inbreuken van de BCR's te remediëren.

Siemens AG garandeert verder de uitbetaling van schadevergoedingen bij aangetoonde inbreuken op de BCR's en de resulterende schending van de rechten van een betrokken identificeerbare persoon.

De bewijslast hiervoor ligt bij Siemens AG. Siemens AG dient aan te tonen dat er geen inbreuk op de BCR's heeft plaatsgevonden of dat het deelnemende bedrijf gevestigd buiten de EER niet verantwoordelijk is voor de inbreuk op de BCR's waarop de schadeclaim van de identificeerbare persoon gebaseerd is.

9. Contact

De betrokken identificeerbare personen kunnen eventuele vragen of bekommernissen met de DPO van het betreffende deelnemende bedrijf of met de algemene verantwoordelijke voor privacybescherming van Siemens AG bespreken:

Siemens AG

LC CO DP

St.-Martin-Str. 76

D-81541 München

E-mail: datenschutz@siemens.com

Siemens Intranet website: https://intranet.privacy.siemens.com

Internet: http://www.siemens.com

10. Bijlagen

Bijlage 1: Verbintenisverklaring voor bedrijfsentiteiten van de Siemens-groep

Bijlage 2: Aansluitingsovereenkomst voor andere aansluitende bedrijven

Bijlage 3: Lijst van deelnemende bedrijven

Bijlage 4: BCR-klachtenbeheer