

Offentlig version

Capgemini Bindende virksomhedsregler (BCR)

For dataansvarlig- &
databehandleraktiviteter





Indholdsfortegnelse

Introduktion	2
Definitioner.....	3
1. Anvendelsesområder for BCR.....	5
1.1 Materielt anvendelsesområde	5
1.2 Geografisk anvendelsesområde	6
2. Bindende virkning af BCR.....	6
2.1 Bindende virkning for Capgeminiselskaber.....	6
2.2 Bindende virkning for Capgemini medarbejdere	6
2.3 Bindende virkning i forhold til Dataansvarlige	7
3. Implementering af databeskyttelsesprincipper i Capgemini.....	7
4. Intern og ekstern behandling og underdatabehandling	14
5. Gennemsigtighed	15
6. De Registreredes håndhævelsesrettigheder	17
7. Procedure for håndtering af anmodninger fra de Registrerede	19
8. Capgemini Databeskyttelsesorganisation	20
9. Databeskyttelsesbevidsthed og undervisning	20
10. Privacy by design	21
11. Revisioner i forhold til BCR	23
12. Capgemini ansvar i tilfælde af brud på BCR.....	24
13. Jurisdiktion.....	25
14. Gældende Persondataret og potentiel konflikt med BCR	25
15. Samarbejdsforpligtelser	26
16. Nem adgang til BCR	27
17. Opdateringer af BCR.....	27
Appendiks 1 Capgemini Behandlingsaktiviteter.....	28
Appendiks 2 Capgemini Databeskyttelsesorganisation	31
Appendiks 3 Procedure for håndtering af anmodninger fra de Registrerede	32



Introduktion

Capgemini er en førende global leverandør af rådgivning, teknologiservices og digital transformation. Virksomheden er i front, når det kommer til innovation for at kunne realisere sine kunders potentiale inden for cloud, digital og platforme. Baseret på 50 års erfaring og dyb industrispecifik ekspertise, gør Capgemini organisationer i stand til at realisere deres forretningsmæssige ambitioner via en række ydelser fra strategi til drift. Capgemini behandler på denne baggrund store mængder personoplysninger.

Capgemini er dedikeret til at beskytte alle personoplysninger, som er betroet os som en del af vores aktiviteter som dataansvarlig og som databehandler. Som en international koncern med selskaber i mere end 40 lande, er det vigtigt for Capgemini, at alle informationer flyder frit og sikkert. At sikre et passende beskyttelsesniveau med hensyn til de personoplysninger, der overføres inden for koncernen, er en af årsagerne til, at Capgemini har valgt at implementere disse bindende virksomhedsregler (**BCR**), som første gang blev godkendt af den franske databeskyttelsesmyndighed, CNIL, i marts 2016. Dette er af højeste vigtighed, da databeskyttelse og datasikkerhed fra et juridisk perspektiv er essentiel for enhver del af Capgemini-koncernen. De økonomiske og omdømmemæssige risici er høje.

Af denne årsag bør Capgeminis BCR ikke betragtes alene som en mekanisme for overførsel af data, men snarere som en strukturel ramme, der definerer vores tilgang til princippet om ansvarlighed i behandlingen af personoplysninger.

Capgeminis BCR definerer ikke alene de principper, som skal følges, når der behandles personoplysninger, men specificerer også de procedurer, som er designet til at sikre Capgeminis overholdelse af persondatarettelig lovgivning, herunder i særdeleshed databeskyttelsesforordningen 2016/679 (**GDPR**).



Definitioner

De begreber, der anvendes i dette dokument, er defineret som følger:

”**Behandling**” betyder enhver aktivitet eller række af aktiviteter, med eller uden brug af automatisk behandling, som Persondata eller en samling af Persondata gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

”**Binding Corporate Rules**” eller ”**BCR**” (på dansk, ”bindende virksomhedsregler”) betyder en databeskyttelsespolitik der er overholdt af en dataansvarlig eller databehandler for en overførsel eller en række af overførsler til en dataansvarlig eller databehandler i et eller flere tredjelande inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet. De udgør dette dokument med appendiks.

”**Capgemini**” eller ”**Gruppen**” betyder alle de enheder ejet og/eller kontrolleret direkte eller indirekte af Capgemini SE.

”**Capgemini kunde**” betyder enhver fysisk eller juridisk enhed til hvilken Capgemini leverer services, på baggrund af en aftale.

”**Capgemini medarbejder**” eller ”**Medarbejder**” betyder enhver nuværende, tidligere eller fremtidig medarbejder hos Capgemini, inklusive vikaransatte og praktikanter.

”**Capgemini selskab(er)**” betyder enhver enhed der er del af Gruppen og som er bundet af disse BCR.

”**Cybersecurityorganisationen**” betyder den globale funktion der udarbejder og administrerer de globale sikkerhedspolitikker; og overholdelse fra Business Units og Global Business Lines. Cybersecurityorganisationen udgøres af et netværk af Cybersecurity Officers, udpeget for hver Business Unit.

”**Dataansvarlig**” betyder den fysiske eller juridiske enhed, offentlige myndighed, institution eller et andet organ, der alene eller sammen med andre afgør formål og hjælpemidler til Behandlingen af Persondata.

”**Databehandler**” betyder en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler Persondata på vegne af den Dataansvarlige.

”**Databeskyttelsesforordningen**” eller ”**GDPR**” betyder Forordning (EU) 2016/679 fra det Europæiske Parlament og Rådet af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

”**Databeskyttelsesrådgiver**” eller ”**DPO**” betyder den udpegede Capgemini medarbejder, der har ekspertviden om databeskyttelsesret og -praksis, dedikeret til at rådgive, informere og overvåge overholdelse af Gældende Lov, og som er del af Databeskyttelsesorganisationen beskrevet i afsnit 8.

”**Databrud**” betyder et brud på sikkerheden, der fører til en hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til Persondata, der er transmitteret, opbevaret eller på anden måde behandlet, hvad enten det er et resultat af et sikkerhedsbrud eller ej.

”**EU Standardkontraktklausuler**” eller ”**SCC**” betyder de kontraktuelle klausuler som den Europæiske Kommission har udstedt for at skabe ramme om dataoverførsler fra Dataansvarlige etableret i EØS til Dataansvarlige etableret uden for EØS (og fra Dataansvarlige etableret i EØS til Databehandlere etableret uden for EØS).

”**EØS-Capgemini selskab**” betyder ethvert Capgemini selskab beliggende i det Europæiske Økonomiske Samarbejdsområde (eller ”**EØS**”).

”**Forretningskontakt**” betyder en Capgemini leverandør, underleverandør, aktionær, kunde eller partner.



“**Gældende Persondataret**” betyder enhver persondataretlig regulering, som måtte finde anvendelse og i særdeleshed (i) Europa-Parlamentets og Rådets forordning af 2016-04-27 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679) (**GDPR**), og (ii) enhver anden lov eller regulering vedrørende behandling af personoplysninger, som måtte finde anvendelse.

“**Ikke-EØS-Capgeminiselskab**” betyder ethvert Capgeminiselskab beliggende uden for EØS.

“**Intra-Gruppeaftalen**” betyder den juridiske bindende aftale, der er designet til at gøre disse BCR bindende for Capgeminiselskaberne.

“**Konsekvensanalyse vedrørende databeskyttelse**” eller “**DPIA**” betyder en proces designet til at beskrive en behandling, vurdere dens nødvendighed og proportionalitet og hjælpe med at håndtere de risici for rettigheder og frihedsrettigheder for de fysiske personer, der resulterer fra behandlingen af Persondata ved at vurdere dem og fastlægge foranstaltninger til at adressere dem.

“**Medarbejderpersondata**” betyder Persondata relateret til en nuværende, tidligere eller fremtidig Capgemini medarbejder.

“**Overførsel**” betyder videregivelse, transmission eller processen med at stille Persondata til rådighed for enhver tredjepart.

“**Persondata**” betyder enhver information relateret til en identificeret eller identificerbar fysisk person (den “**Registrerede**”). En identificerbar fysisk person er en der kan blive identificeret, direkte eller indirekte, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kultur eller sociale identitet.

“**Registreret**” eller “**den Registrerede**” betyder enhver identificeret eller identificerbar fysisk person hvis Persondata bliver behandlet.

“**Serviceaftale**” betyder en skriftlig aftale mellem en Dataansvarlig og en Databehandler hvorved Databehandleren skal levere ydelser til den Dataansvarlige og hvilket medfører behandling af Persondata af Databehandleren under instruktion fra den Dataansvarlige.

“**Særlige Kategorier af Persondata**” betyder Persondata om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

“**Tilsynsmyndighed(er)**” betyder den offentlige myndighed der er ansvarlig for at føre tilsyn med anvendelsen af GDPR og/eller enhver Gældende Lov.



1. Anvendelsesområde for BCR

Disse BCR finder anvendelse på og skaber en ramme omkring alle overførsler indenfor Capgemini og driver Gruppens ansvarligheds-tilgang. Som resultat heraf udgør BCR den databeskyttelsespolitik, der definerer hvilke databeskyttelsesprincipper, Capgemini skal overholde.

Hvor relevant Gældende Persondataret kræver en højere grad af beskyttelse end de forpligtelser, der er defineret i disse BCR, tager sådan forrang over BCR.

1.1 Materielt anvendelsesområde

Disse BCR finder anvendelse på al Persondata der behandles indenfor Capgemini, hvad enten som Dataansvarlig eller som Databehandler.



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, behandler Capgemini Persondata for egne Medarbejdere og Forretningskontakter.

Formålet med sådan behandling er relateret til HR, intern og ekstern kommunikation, markedsføring, compliance, etc.

For en mere udførlig oversigt over Capgeminis behandlingsaktiviteter som Dataansvarlig, se Appendiks 1.



Databehandler-aktiviteter

I rollen som Databehandler, behandler Capgemini Persondata på vegne af Dataansvarlige og i henhold til deres instruktioner.

Capgemini tilbyder en lang række ydelser, inklusiv konsulentytelser der forbedrer ydeevnen af organisationer baseret på dybdegående forståelse af kundeindustrier og -processer; applikationsytelser der udtænker, udvikler, implementerer og vedligeholder IT applikationer omfattende integration; applikationsvedligeholdelsesaktiviteter, hosting; og teknologi- og ingeniørydelser der leverer assistance og support til interne IT teams i kundevirksomheder; og andre managed services der integrerer, administrerer og/eller udvikler fuldt eller partielt, kunders IT-infrastruktursystemer, transaktionsytelser og on demand-ydelser og/eller forretningsaktiviteter.

For en mere udførlig oversigt over Capgeminis behandlingsaktiviteter som Databehandler, se Appendiks 1.



1.2 Geografisk anvendelsesområde

Disse BCR omfatter al Persondata der overføres og viderebehandles inden for Gruppen, uagtet oprindelse heraf. Dette medfører i praksis, at de finder anvendelse på Persondata overført fra:

1. Et EØS-Capgeminiselskab til et andet EØS-Capgeminiselskab;
2. Et EØS-Capgeminiselskab til et ikke-EØS-Capgeminiselskab;
3. Et ikke-EØS-Capgeminiselskab til et EØS-Capgeminiselskab; og
4. Et ikke-EØS-Capgeminiselskab til et andet ikke-EØS-Capgeminiselskab.

De Capgeminiselskaber, der er bundet af disse BCR, er opført på Capgemini hjemmeside.

2. Bindende virkning af disse BCR

Hvert Capgeminiselskab, og dets Medarbejdere, er juridisk bundne af og forpligtede til at overholde disse BCR.

2.1 Bindende virkning for Capgeminiselskaber

I praksis giver hver Capgemini-enhed en fuldmagt til Capgemini International BV til at underskrive Intra-Gruppeaftalen på sine vegne således, at enhver Capgemini-enhed er effektivt bundet til at overholde disse BCR overfor hinanden. Ved at underskrive Aftalen, forpligter Capgemini-enheden sig til at overholde bestemmelserne i disse BCR og til at implementere dem inden for sin egen organisation.

For så vidt angår nyligt erhvervede Capgemini-enheder, beliggende uden for EØS, må ingen Persondata blive overført dertil, indtil de er effektivt bundet af disse BCR i overensstemmelse med ovenstående mekanisme.

2.2 Bindende virkning for Capgemini medarbejdere

Alle Capgemini medarbejdere er bundet af disse BCR via en specifik henvisning hertil i deres ansættelseskontrakter og/eller via den forpligtelse, som er indeholdt i alle ansættelseskontrakter, om at overholde Gruppepolitikker, hvilket inkluderer disse BCR.

Som nærmere beskrevet i afsnittene 9 og 16 i disse BCR, bliver Capgemini medarbejdere gjort opmærksomme på disse BCR og de medfølgende forpligtelser via intern kommunikation og undervisning. Capgemini medarbejdere bliver også gjort opmærksomme på, at non-compliance med disse BCR kan føre til sanktioner i henhold til relevant lokal lovgivning.



2.3 Bindende virkning i relation til Dataansvarlige

I rollen som Databehandler, påtager Capgemini sig at indgå Service Aftaler, der overholder kravene i GDPR's artikel 28.

I tillæg hertil påtager Capgemini sig at overholde disse BCR, hvilket skal gøres bindende via en specifik reference i Serviceaftalen.

I ethvert tilfælde skal den Dataansvarlige være i stand til at håndhæve disse BCR mod ethvert Capgeminiselskab for brud på disse BCR, selskabet har forårsaget, i henhold til bestemmelserne beskrevet i afsnit 12.

3. Implementering af databeskyttelsesprincipper i Capgemini

Capgemini er dedikeret og forpligtet til at overholde de databeskyttelsesprincipper der er fastlagt i disse BCR, uagtet Gældende Persondataret, medmindre sådan Gældende Persondataret medfører strengere krav end de, der fremgår af disse BCR. Alle disse principper bliver fremmet og implementeret i Capgemini gennem et sæt af privacy by design-politikker og undervisning.

Desuden, I rollen som Dataansvarlig, skal Capgemini overholde Gældende Persondataret. Når man agerer som Databehandler skal Capgemini informere den Dataansvarlige, hvis dennes instruktioner klart krænker Gældende Persondataret.

3.1 Klart, identificeret formål



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, må Capgemini kun behandle Persondata for udtrykkeligt angivne og legitime formål og der må ikke ske viderebehandling på en måde, der er uforenelig med disse formål.

I praksis betyder dette, at der skal fastlægges og udtrykkeligt defineres et formål for enhver behandling før Persondataene bliver indsamlet.

I tillæg hertil skal Capgemini sikre, at Persondata ikke viderebehandles på en måde, der er uforenelig med de formål, for hvilke de oprindeligt blev indsamlet.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini grundigt overholde den Dataansvarliges instruktioner, særligt i relation til de årsager, for hvilke Persondataene skal behandles.

I praksis betyder dette, at Capgemini skal overholde bestemmelserne i Serviceaftalen og ikke må behandle Persondataene for andre formål, medmindre dette er udtrykkeligt autoriseret af den Dataansvarlige, og i henhold til Gældende Persondataret.



3.2 Retsgrundlag



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini kun behandle Persondata hvis en af de følgende vilkår er opfyldt:

1. Behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler Capgemini.

F.eks. *formidle Persondata til skattemyndigheder.*

2. Behandlingen er nødvendig af hensyn til opfyldelse af en kontrakt, som den Registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den Registreredes anmodning forud for indgåelse af en kontrakt

F.eks. *i forbindelse med ansættelseskontrakter, hvor det vil være nødvendigt at behandle løn- og bankoplysninger for at kunne udbetale løn.*

3. Behandlingen er nødvendig for, at Capgemini eller en tredjemand kan forfølge en legitim interesse.

F.eks. *hvor Capgemini har en legitim interesse i at kende sine kunders præferencer for at kunne personalisere sine tilbud og ultimativt kunne tilbyde ydelser, der bedre rammer kundernes behov og forventninger.*

Før man baserer sit lovlige grundlag på en legitim interesse, skal Capgemini gennemføre en afvejning for at fastslå, om Capgeminis legitime interesser må stå tilbage i forhold til den Registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af Persondata.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini assistere den Dataansvarlige med implementering af de organisatoriske og tekniske foranstaltninger for at gøre det muligt for denne at overholde forpligtelsen til at have et retsgrundlag for behandlingsaktiviteterne.

I praksis kan det blive nødvendigt for Capgemini at assistere den Dataansvarlige med at implementere mekanismer for at indhente de Registreredes samtykke på vegne af den Dataansvarlige. Under alle omstændigheder, så vil sådan assistance være genstand for forhandlinger der skal afspejles i Serviceaftalen, der er indgået mellem Capgemini og den Dataansvarlige.

Capgemini skal ikke overtage ansvaret for at fastlægge, hvad der er det rette lovlige grundlag på vegne af den Dataansvarlige og hvad der er de passende tekniske og organisatoriske foranstaltninger der skal implementeres, for at implementere en samtykke-mekanisme.



4. Behandlingen er nødvendig for at beskytte den Registreredes eller en anden fysisk persons vitale interesser.

F.eks. hvor den Registrerede er fysisk eller psykisk ude af stand til at give samtykke til behandlingen og hvor den Registreredes sikkerhed eller helbred er i fare.

5. Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse og som Capgemini har fået pålagt.

F.eks. hvor en embedsmand fra en offentlig myndighed ansvarlig for kriminalitetsefterforskning beder Capgemini om at medvirke i en pågående undersøgelse.

Det er meget usandsynligt, at underafsnit 4) og 5) vil finde anvendelse for Capgemini.

6. Hvis ingen af de ovenstående retsgrundlag kan finde anvendelse på en konkret situation, kan Capgemini forsøge at få den Registreredes samtykke. For at være gyldigt, skal sådant et samtykke være afgivet frivilligt, specifikt, informeret og utvetydigt.

I praksis medfører dette, at Capgemini kun kan foretage en given Persondatabehandling hvis det kan påvises, at mindst et af ovenstående vilkår er opfyldt.

3.3 Dataminimering



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, må Capgemini kun indsamle og behandle Persondata som er strengt nødvendigt i relation til de på forhånd definerede formål.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini strengt overholde de instruktioner, som den Dataansvarlige giver.

I tillæg hertil, når der designes og udvikles et produkt eller en services der inkluderer behandling af Persondata, skal sådant produkt eller services blive udviklet således, at den



Dataansvarlig-aktiviteter

I praksis medfører dette, at når der designes et projekt der involverer behandling af Persondata, skal Capgemini fastslå hvilke Data der er strengt nødvendige for at opnå det påtænkte formål. Som resultat heraf må Capgemini ikke indsamle og opbevare ikke-essentiell Persondata blot for at have mulighed for at bruge sådan til et hypotetisk formål der måtte blive defineret i fremtiden.



Databehandler-aktiviteter

alene indsamler og behandler de Persondata, som er nødvendige for de(t) behandlingsformål, som den Dataansvarlige har fastsat.

I praksis betyder dette, at Capgemini skal samarbejde med og supportere den Dataansvarlige i at begrænse de Persondata det er nødvendig at indsamle, når design af applikationer eller systemer er en del af de ydelser der skal leveres. Dette skal dog ikke tolkes som en forpligtelse for Capgemini til selv at fastlægge, hvilke Persondata der skal indsamles, når der ageres på vegne af den Dataansvarlige.

3.4 Datakvalitet



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini sikre, at Persondata er korrekte og ajourførte igennem hele behandlings-livscyklussen.

I praksis betyder dette, at Capgemini skal tilbyde de Registrerede muligheder for at anmode om at få ukorrekte Persondata rettet, opdateret eller slettet som nærmere beskrevet i proceduren for håndtering af henvendelser fra Registrerede i Appendiks 3. I tillæg hertil skal Capgemini sikre, at det er teknisk muligt at



Databehandler-aktiviteter

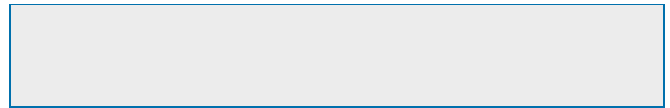
I rollen som Databehandler, skal Capgemini assistere den Dataansvarlige i at overholde dennes forpligtelser til at holde Persondata korrekte og ajourførte.

Det betyder, at Capgemini skal opdatere, rette eller slette Persondata efter anmodning fra den Dataansvarlige i det omfang dette er teknisk muligt og på de betingelser, der er aftalt i Serviceaftalen. I de tilfælde, hvor data er blevet videregivet til et Capgeminiselskab der agerer som underdatabehandler, vil dette blive orienteret om sådanne modifikationer.

I praksis skal Capgemini implementere de tekniske foranstaltninger der er nødvendige for at kunne efterkomme den Dataansvarliges instruktioner i relation til anmodning om at opdatere, rette eller slette Persondata.



slette eller rette Persondata efter anmodning fra de Registrerede.



3.5 Dataopbevaringsbegrænsning



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, må Capgemini ikke opbevare Persondata længere end hvad der er nødvendigt i relation til de formål, for hvilke de blev indsamlet.

Dette betyder, at Capgemini skal definere dataopbevaringsperioden på forhånd og i henhold til formålet med Behandlingen, hvor følgende skal tages i betragtning og balanceres:

- De gældende juridiske krav;
- forretningskravene;
- hensyn til de Registrerede hvis Persondata bliver behandlet.

I praksis skal Capgemini, i ethvert projekt der involverer Behandling af Persondata, foretage en afvejning af det overordnede formål for projektet og dokumentere denne afvejning.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini sikre at, i henhold til bestemmelserne i Serviceaftalen og den Dataansvarliges instruktioner, Persondata bliver enten slettet eller returneret til den Dataansvarlige ved ophør eller efter anmodning fra den Dataansvarlige.

I praksis betyder dette, at Capgemini skal implementere de nødvendige tekniske og organisatoriske foranstaltninger til at sikre, at Persondata bliver enten slettet eller returneret til den Dataansvarlige, som nærmere aftalt mellem parterne i Serviceaftalen og/eller i henhold til den Dataansvarliges instruktioner.



3.6 Sikkerhed



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini implementere alle passende tekniske og organisatoriske foranstaltninger for at garantere sikkerheden for de Persondata, der er overdraget til dem og sikre mod ulovlig adgang, tab, destruktion eller ændring af Persondataene.

I praksis medfører dette, som et minimum, at Capgemini skal implementere de krav og god praksis, som defineret af Cybersecurityorganisationen.

I tilfælde af et Databrud skal Capgemini dokumentere Bruddet i en dertil indrettet protokol og orientere den relevante ledelse og DPO i henhold til den interne Databruds-procedure.

Hvor Databruddet sandsynligvis resulterer i en risiko for de Registreredes rettigheder eller frihedsrettigheder, skal Capgemini også orientere de(n) relevante Tilsynsmyndighed(er), i henhold til Gældende Persondataret, uden unødigt forsinkelse og ikke senere end 72 timer efter at være blevet opmærksom på det.

I tilfælde af, at Databruddet sandsynligvis vil indebære en høj risiko for de Registreredes rettigheder og frihedsrettigheder, skal Capgemini orientere dem.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini implementere passende tekniske og organisatoriske foranstaltninger, som aftalt med den Dataansvarlige, for at sikre en høj grad af sikkerhed for Behandlingen af de Persondata, der er overladt til dem af den Dataansvarlige.

I praksis betyder dette, at Capgemini skal implementere de i Serviceaftalen aftalte bestemmelser.

Desuden, i tilfælde af et Databrud, skal Capgemini notificere den Dataansvarlige uden unødigt forsinkelse og skal assistere denne i at håndtere Databruddet, som aftalt i Serviceaftalen.



3.7 Behandling af Særlige Kategorier af Persondata



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, må Capgemini kun behandle Særlige Kategorier af Persondata når det er strengt nødvendigt eller krævet juridisk.

Når der behandles Særlige Kategorier af Persondata, skal Capgemini implementere forstærkede tekniske og organisatoriske foranstaltninger for at sikre behandlingssikkerheden.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini behandle Særlige Kategorier af Persondata på vegne af den Dataansvarlige og i henhold til dennes anmodning.

Når der behandles særlige Kategorier af Persondata skal Capgemini implementere enhver forstærket teknisk og organisatorisk foranstaltning i henhold til den Dataansvarliges instruktioner og afhængigt af kommercielle forhandlinger, for at sikre Behandlingens sikkerhed.

3.8 Automatiseret individuel afgørelse

De Registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk Behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker de pågældende. Dette gælder dog ikke, hvis afgørelsen er:

1. nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den Registrerede og Capgemini (i rollen som Dataansvarlig);
2. hjemlet i EU-ret eller medlemsstaternes national ret, som den Dataansvarlige (Capgemini) er underlagt, og som også fastsætter passende foranstaltninger til beskyttelse af den Registreredes rettigheder og frihedsrettigheder samt legitime interesser eller, er;
3. baseret på den Registreredes udtrykkelige samtykke.



Dataansvarlig-aktiviteter

Capgemini skal bestræbe sig på at forklare de Registrerede den underliggende logik for enhver automatiseret behandling, de er genstand for.

I praksis skal dette ske i den informationsmeddelelse, der skal gives til de Registrerede som beskrevet i afsnit 6 i disse BCR.



Databehandler-aktiviteter

Capgemini skal følge den Dataansvarliges instruktioner og skal bestræbe sig på at gøre det muligt for den Dataansvarlige at overholde sin forpligtelse til at informere de Registrerede.



4. Intern og ekstern Behandling og underdatabehandling

4.1 Grundlæggende forpligtelse – Databehandlersaftale eller Klausul (“DP Clause”) i Serviceaftalen

Capgemini kan alene benytte Databehandlere eller underdatabehandlere, enten indenfor eller udenfor Gruppen, hvis sådanne Databehandlere eller underdatabehandlere kan give tilstrækkelige garantier om at implementere tekniske og organisatoriske foranstaltninger til at sikre, at Behandlingen sker i overensstemmelse med GDPR og principperne som beskrevet i disse BCR.

I praksis betyder dette at, når man benytter en tredjepart, så skal Capgemini indgå en Serviceaftale som beskriver vilkårene for behandlingsaktiviteterne. Serviceaftalen skal indeholde en DP Clause der som minimum afspejler, at Databehandleren eller underdatabehandleren:

- alene må behandle Persondata på dokumenteret instruks fra Capgemini – inklusiv i relation til Overførsel til et land uden for EØS;
- skal sikre, at personer autoriseret til at behandle Persondataene er forpligtede til fortrolighed;
- skal implementere tekniske og organisatoriske foranstaltninger for at sikre et passende niveau af beskyttelse af Persondataene;
- alene benytter en underdatabehandler med forudgående specifik eller generel godkendelse fra Capgemini og indgår en Serviceaftale med underdatabehandleren der pålægger denne de samme forpligtelser som beskrevet her;
- skal assistere Capgemini med dennes opfyldelse af sin forpligtelse til at besvare anmodninger fra de Registrerede;
- skal assistere Capgemini i at sikre overholdelse af sine forpligtelser i relation til sikkerhed for Behandlingen, udførelse af DPIA'er, rapportering af Databrud;
- efter Capgeminis valg og som aftalt i Serviceaftalen, enten sletter eller returnerer Persondata efter ophør af leverance af ydelserne i relation til Behandlingen;
- stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i GDPR, til rådighed for Capgemini og særligt tillader Capgemini at udføre revisioner;
- rapporterer ethvert Databrud til Capgemini uden unødigt forsinkelse.

I ethvert tilfælde, når man benytter en tredjepart, skal Capgemini gennemføre en vurdering af de databeskyttelses- og sikkerhedsgarantier som denne tredjepart forpligter sig til at implementere og overholde.



4.2 Yderligere forpligtelser i tilfælde af dataoverførsel til et tredjeland

I tillæg til implementering af ovenstående Databehandleraftale eller DP Clause skal Capgemini, når Behandling eller underdatabehandling medfører Overførsel til tredjelands, garantere, at der kan opnås et tilstrækkeligt beskyttelsesniveau, i henhold til kravene defineret nedenfor.



Dataansvarlig-aktiviteter

I praksis medfører dette, at hvor et EØS-Capgeminiselskab, der agerer som Dataansvarlig, overfører Persondata til et ikke-EØS-Capgeminiselskab, der agerer enten som en Dataansvarlig eller en Databehandler, så skal disse BCR finde anvendelse.

Hvor et EØS-Capgeminiselskab, der agerer som Dataansvarlig, overfører Persondata til en tredjepart placeret uden for EØS, der agerer enten som en Dataansvarlig eller en Databehandler, så skal Capgemini indgå de relevante EU Standardkontraktklausuler.

Hvor et ikke-EØS-Capgeminiselskab, der agerer som Dataansvarlig, overfører Persondata til en tredjepart placeret i et tredjeland, skal der muligvis implementeres et passende rammeværk for at overholde Gældende Persondataret eller andre juridiske forpligtelser. I tilfælde af sådan overførsel til et andet Capgeminiselskab, kan overførslen drage fordel af disse BCR og kan kræve implementering af yderligere garantier, for at overholde Gældende Persondataret.



Databehandler-aktiviteter

I praksis giver BCR et tilstrækkeligt sikkerhedsniveau for de overførte Persondata, når et EØS-Capgeminiselskab, der agerer som Databehandler på vegne af en Dataansvarlig etableret i EØS, overfører Persondata til et ikke-EØS-Capgeminiselskab.

Hvor et EØS-Capgeminiselskab, i rollen som Databehandler på vegne af en Dataansvarlig etableret i EØS, har til hensigt at overføre Persondata til et tredjeland placeret uden for EØS, skal parterne indgå de relevante EU Standardkontraktklausuler.

I ethvert tilfælde, i rollen som Databehandler, skal Capgemini, før der sker nogen Overførsel til et tredjeland, indhente den Dataansvarliges forudgående tilladelse.



5. Gennemsigtighed

I rollen som Dataansvarlig, skal Capgemini give de Registrerede alle de krævede informationer om Behandlingen af deres Persondata.

I praksis medfører dette, at hvor Persondata relateret til en Registreret bliver indsamlet direkte fra den Registrerede, skal Capgemini give den Registrerede følgende informationer:

- Identitet og kontaktdetaljer på det Capgeminiselskab, der agerer som Dataansvarlig;
- Kontaktdetaljer på den lokale DPO;
- Formålene med den Behandling Persondataene bliver indsamlet til samt retsgrundlaget for Behandlingen;
- Hvor Behandlingen er baseret på Capgeminis legitime interesser, en beskrivelse af de interesser Capgemini forfølger;
- Modtagere eller kategorier af modtagere, hvis nogen;
- Hvor relevant, det faktum, at Capgemini agter at overføre Persondata uden for EØS og eksistens eller fravær af en tilstrækkelighedsafgørelse fra EU Kommissionen, eller en reference til de fornødne eller passende garantier (dvs. BCR eller EU Standardkontraktklausuler) og hvor der kan fås en kopi heraf, eller hvor de er gjort tilgængelige;
- Det tidsrum, hvor Persondata vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum;
- Retten til at anmode om indsigt i og berigtigelse eller sletning af Persondata eller begrænsning af Behandling eller til at gøre indsigelse mod Behandling samt retten til dataportabilitet;
- Når Behandling er baseret på samtykke, retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af Behandlingen;
- Retten til at indgive en klage til en tilsynsmyndighed;
- Om meddelelse af Persondata er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den Registrerede har pligt til at give Persondataene og de eventuelle konsekvenser af ikke at give sådanne data;
- Forekomsten af automatiske afgørelser, herunder profilering, og oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan Behandling for den Registrerede.

Hvor Persondataene ikke er skaffet direkte fra den Registrerede, skal Capgemini stadig give den Registrerede ovenstående informationer såvel som beskrivelsen af kategorier af Persondata og kilden til de omhandlede Persondata. Capgemini skal give de angivne informationer til den Registrerede inden for en rimelig periode efter at have skaffet Persondataene. Hvis Persondataene bliver brugt til at kontakte den Registrerede, skal Capgemini give de angivne oplysninger i forbindelse med den første kommunikation.

I rollen som Databehandler, skal Capgemini assistere den Dataansvarlige med at opfylde sine forpligtelser om at informere de Registrerede.

I praksis medfører dette, at Capgemini skal give den Dataansvarlige detaljerede informationer om Behandlingen, og særligt om datamodtagere inklusiv de enheder, som Persondata kan blive overført til således, at den Dataansvarlige kan informere de Registrerede korrekt.



6. De Registreredes håndhævelsesrettigheder

De Registrerede kan, som tredjepartsbegunstigede, håndhæve bestemmelser fra disse BCR mod Cappgemini, som beskrevet nedenfor.



Dataansvarlig-aktiviteter

De Registrerede kan håndhæve de følgende elementer fra disse BCR mod Cappgemini i rollen som Dataansvarlig:

- Databeskyttelsesprincipperne beskrevet i afsnit 3, 4 og 5;
- Det faktum, at Cappgemini giver nem adgang til disse BCR, som beskrevet i afsnit 16;
- Rettigheder til adgang, berigtigelse, sletning, begrænsning, at gøre indsigelse mod Behandlingen samt retten til ikke at være genstand til afgørelser alene baseret på automatisk behandling, som tildelt de Registrerede, som beskrevet i afsnit 5;
- Forpligtelsen, for ethvert Cappgeminiselskab til, at orientere den kompetente Tilsynsmyndighed såvel som Cappgeminihovedkvarteret, i tilfælde af en konflikt mellem lokal lovgivning og disse BCR, som beskrevet i afsnit 14;
- Retten for de Registrerede til at klage via Cappgemini's interne klagemekanisme, som beskrevet i afsnit 7;
- Cappgemini's pligt til at samarbejde med Tilsynsmyndigheden, som beskrevet i afsnit 15;
- Retten for de Registrerede til at indgive en klage til den kompetente Tilsynsmyndighed og/eller til den kompetente domstol, som beskrevet i afsnit 7 og 13;



Databehandler-aktiviteter

De Registrerede kan håndhæve de følgende elementer fra disse BCR direkte mod Cappgemini i rollen som Databehandler:

- Pligten for Cappgemini til at respektere instruksen fra den Dataansvarlige om Behandlingen, som beskrevet i afsnit 2;
- Pligten for Cappgemini til at implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i underafsnit 3.6;
- Pligten til at orientere den Dataansvarlige i tilfælde af et Databrud, som beskrevet i underafsnit 3.6;
- Pligten for Cappgemini til alene at antage underdatabehandlere i overensstemmelse med GDPR's artikel 28, som beskrevet i afsnit 4;
- Pligten for Cappgemini til at samarbejde med og assistere den Dataansvarlige i at overholde og demonstrere overholdelse af GDPR, som beskrevet i afsnit 3 og 15;
- Det faktum, at Cappgemini giver nem adgang til disse BCR, som beskrevet i afsnit 16;
- Retten for de Registrerede til at klage via Cappgemini's interne klagemekanisme, som beskrevet i afsnit 7;
- Pligten for Cappgemini til at samarbejde med den kompetente Tilsynsmyndigheden for den Dataansvarlige, som beskrevet i afsnit 15;



Dataansvarlig-aktiviteter

- Forpligtelsen for hvert EØS-Capgeminiselskab, der overfører Persondata til et ikke-EØS-Capgeminiselskab på baggrund af BCR, til at acceptere ansvaret for ethvert brud af BCR af ikke-EØS-Capgeminiselskabet der har modtaget Persondataene, som beskrevet i afsnit 12;
- Det faktum, at i tilfælde af brud på BCR af et ikke-EØS-Capgeminiselskab, så er det op til det EØS-Capgeminiselskab, der har eksporteret Persondataene at påvise, at modtageren (dvs. ikke-EØS-Capgeminiselskabet) ikke har krænket BCR, som beskrevet i afsnit 12.



Databehandler-aktiviteter

- Retten for de Registrerede til at indgive en klage til den kompetente Tilsynsmyndighed og/eller til den kompetente domstol, som beskrevet i afsnit 7 og 13;
- Forpligtelsen for hvert Capgeminiselskab, der eksporterer Persondata uden for EØS, til at acceptere ansvar for ethvert brud på BCR af underdatabehandlere (intern eller eksternt i forhold til Capgemini) etableret uden for EØS, som har modtaget Persondataene, som beskrevet i afsnit 12;
- Det faktum, at det er op til det EØS-Capgeminiselskab, der har eksporteret Persondataene, at påvise, at underdatabehandleren placeret uden for EØS (dvs. modtageren af data) ikke brød BCR, som beskrevet i afsnit 12;
- De Registrerede kan håndhæve yderligere elementer mod Capgemini i rollen som Databehandler, hvis de ikke kan bringe et krav mod den Dataansvarlige på grund af, at denne er ophørt med at eksistere juridisk eller er blevet insolvent – og ingen efterfølgende enhed har påtaget sig de juridiske forpligtelser fra de Dataansvarlige via kontrakt eller ifølge lov;
- Pligten for Capgeminiselskaber, og deres medarbejdere, til at respektere BCR, som beskrevet i afsnit 2;
- Pligten for Capgemini til at skabe tredjepartsbegunstigende rettigheder for de Registrerede, som beskrevet i dette afsnit;
- Databeskyttelsesprincipperne som beskrevet i afsnit 3, 4 og 5;
- Forpligtelsen til at liste Capgeminiselskaberne, som beskrevet i afsnit 1, på Capgemini hjemmeside;



Dataansvarlig-aktiviteter



Databehandler-aktiviteter

- Forpligtelsen for hvert Capgeminiselskab til at orientere den Dataansvarlige, den kompetente Tilsynsmyndighed for den Dataansvarlige og Capgeminis hovedkvarter, i tilfælde af en konflikt mellem lokal lovgivning og disse BCR, som beskrevet i afsnit 14.

7. Procedure for håndtering af henvendelser fra de Registrerede



Dataansvarlig-aktiviteter

Capgemini har opsat en intern procedure for håndtering af henvendelser fra de Registrerede i rollen som Dataansvarlig, der er nærmere beskrevet i Appendiks 3. Den tillader de Registrerede at kontakte den lokale DPO, enten for at udøve deres rettigheder i relation til Behandlingen af deres Persondata eller til at klage over et brud på Gældende Persondataret.

Proceduren beskriver til de Registrerede hvor og hvordan de kan indgive en anmodning og/eller en klage, ventetiden for svaret på anmodningen eller klagen, konsekvenserne i tilfælde af afvisning af denne, konsekvenserne hvis anmodningen eller klagen anses for berettiget samt retten for den Registrerede til at indgive en klage til de kompetente domstole eller Tilsynsmyndigheder.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini omgående videresende enhver henvendelse fra de Registrerede der modtages, til den Dataansvarlige. Capgemini skal derefter afvente instruktioner fra den Dataansvarlige om hvordan der skal reageres, medmindre andet er aftalt mellem parterne i Serviceaftalen.

Selvom Capgemini opfordrer de Registrerede til at kontakte den Dataansvarlige direkte, tillader man stadig de Registrerede at sende anmodninger og/eller klager via den interne mekanisme, beskrevet i afsnit 3.



8. Capgeminis Databeskyttelsesorganisation

Databeskyttelsesrådgiveren, der er en del af Databeskyttelsesorganisationen, som angivet i Appendiks 2, overvåger den juridiske overholdelse af Gældende Persondataret for Capgeminiselskaberne inden for deres anvendelsesområde, rådgiver i alle forhold relateret til databeskyttelse, implementerer det globale databeskyttelsesprogram, håndterer eller rådgiver om Databrud og har et aktivt forhold til den lokale Tilsynsmyndighed.

Som en del af den Juridiske funktion, bliver de Globale, Regionale og Lokale Databeskyttelsesrådgivere understøttet i deres opgave af de lokale juridiske teams. Databeskyttelsesrådgiverne rapporterer kvartalsmæssigt til den lokale landebestyrrelse eller Executive Comity om privacy-relaterede forhold såsom kritiske Databrud, henvendelser fra de Registrerede, privacy-forhold i store handler etc.

I tillæg til denne regulatoriske rolle, så handler Gruppens, Regionale og Lokale DPO'er som forretningsfacilitatorer ved at validere Capgemini-tilgangen til databeskyttelse og datasikkerhed. Gruppens, den Regionale og Lokale DPO har også en nøglerolle i at hjælpe forretningen med at identificere nye forretningsmuligheder ved at identificere huller mellem de rent juridiske privacy-krav som Capgemini skal overholde og de krav fra kunder, der måtte berettigede til yderligere tilbud.

I praksis medfører dette, at Databeskyttelsesorganisationen bør konsulteres i alle nye projekter for at sikre, at sådanne nye projekter indkredser databeskyttelsesbegrænsninger i designfasen. I tillæg, for at understøtte forretningen yderligere, sørger Gruppe-DPO'en for at stille skabeloner og procedurer til rådighed for at sikre, at databeskyttelsesbegrænsninger bliver overvejet som udgangspunkt i de forskellige tilbud og services.

Databeskyttelsesrådgivernetværket er afsluttet af et netværk af Databeskyttelses-Champions, som repræsenterer hver Gruppe-funktion og hver Global Business Line. Disse Databeskyttelses-Champions er ikke del af den juridiske organisation men bliver udpeget fra Gruppefunktions- og Global Business Lines-repræsentanter for at sikre, at de juridiske indskrænkninger og Gruppe-retningslinjer bliver afspejlet i hvert niveau af organisationen. Mere vigtigt, så interagerer disse Databeskyttelses-Champions med Databeskyttelsesorganisationen for at sikre, at programmet på behørig vis integrerer forretningsbehov og forventninger.

Endelig, så skal det bemærkes, at Databeskyttelsesorganisationen arbejder tæt sammen med Gruppens Cybersecurity-Officer og Cybersecurityorganisationen.

9. Databeskyttelsesbevidsthed og undervisning

Capgemini har indført og implementeret obligatorisk databeskyttelsesundervisning for at sikre, at alle Capgeminimedarbejdere er bevidste om og forstår nøgleprincipper og krav i databeskyttelse, såvel som disse BCR.

Undervisningsprogrammet, som er defineret i et dertil indrettet internt Capgemini-dokument, er formuleret omkring følgende søjler:



- Generel undervisning: En fælles kerneviden der beskriver de relevante principper når der Behandles Persondata;
- Praktisk undervisning: Et overblik over eksisterende relevante politikker og processer;
- Funktionsundervisning: Tilpasset undervisning designet til at adressere behovet fra specifikke funktioner (såsom HR eller marketing, for eksempel).

I tillæg til den obligatoriske undervisning er Capgemini engageret i at fremme implementeringen af databeskyttelsesprincipper inden for Gruppens organisation via et sæt af privacy by design-politikker og kommunikationshandlinger dedikeret til at højne bevidstheden iblandt forskellige Capgemini-fællesskaber.

10. Privacy by design

I rollen som Dataansvarlig, så er hvert Capgeminiselskab ansvarligt for og i stand til at påvise overholdelse af disse BCR og Gældende Persondataet generelt.

I rollen som Databehandler, skal Capgemini levere de nødvendige informationer til den Dataansvarlige med henblik på at hjælpe denne med at overholde egne forpligtelser.

10.1 Fortegnelse over behandlingsaktiviteter



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini have og vedligeholde en skriftlig fortegnelse over behandlingsaktiviteter, indeholdende følgende information:

- Navn og kontaktoplysninger på det Capgeminiselskab, der agerer som Dataansvarlig, DPO'en og hvor relevant, den fælles Dataansvarlige;
- Formålene med Behandlingen;
- En beskrivelse af kategorierne af Registrerede og kategorierne af Persondata;
- De kategorier af modtagere, som Persondataene er eller vil blive videregivet til, herunder modtagere placeret uden for EØS



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini have og vedligeholde en fortegnelse af alle kategorier af Behandlingsaktiviteter udført på vegne af Dataansvarlige, indeholdende følgende:

- Navn og kontaktoplysninger på det Capgeminiselskab, der agerer som Databehandler og for hver Dataansvarlig, på vegne af hvilke Capgemini handler, såvel som på DPO'en;
- Behandlingskategorierne der udføres på vegne af den Dataansvarlige;
- Hvor relevant, Overførsler af Persondata til lande placeret uden for EØS, inklusive identifikation af sådanne lande;



Dataansvarlig-aktiviteter

- Hvor relevant, Overførsler af Persondata til lande placeret uden for EØS, herunder angivelse af disse lande

Capgemini skal efter anmodning gøre fortegnelsen tilgængelig til den relevante Tilsynsmyndighed.

I praksis benytter Capgemini et dedikeret værktøj for at overholde denne forpligtelse. Værktøjet gør det muligt digitalt at logge al Behandling af Persondata og at udtrække en komplet fortegnelse over Behandlinger for sine Dataansvarligaktiviteter.



Databehandler-aktiviteter

- Hvor muligt, en generel beskrivelse af de tekniske og organisatoriske foranstaltninger, der er implementeret.

Capgemini skal efter anmodning gøre fortegnelsen tilgængelig til den relevante Tilsynsmyndighed.

I praksis benytter Capgemini et dedikeret værktøj for at overholde denne forpligtelse. Værktøjet gør det muligt digitalt at logge al Behandling af Persondata og at udtrække en komplet fortegnelse over Behandlinger for sine Databehandleraktiviteter.

10.2 Konsekvensanalyse vedrørende databeskyttelse (DPIA)



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini overholde kravet om at gennemføre en DPIA, når en Behandling af Persondata udgør en risiko for rettigheder og frihedsrettighederne for en Registreret.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini assistere den Dataansvarlige med at overholde sin forpligtelse til at gennemføre en DPIA.



Dataansvarlig-aktiviteter

I praksis betyder dette, at Capgemini skal implementere en DPIA-politik, der er designet til at identificere de risici en Behandling har og, afhængigt af alvorligheden af sådanne risici, enten gennemføre en DPIA eller ej. Beslutningen om at gennemføre en DPIA baseres på adskillige faktorer, inklusiv de kriterier og lister, der er identificeret af Tilsynsmyndighederne.

DPIA-processen er beskrevet i en DPIA-politik og er formuleret omkring fire skridt:

1. Beskrivelsen af Behandlingen
2. Vurdering af nødvendighed og proportionalitet af Behandlingen
3. Risikovurdering
4. Risikomitigering.



Databehandler-aktiviteter

I praksis betyder dette, at Capgemini skal levere al relevant information om Behandlingen til den Dataansvarlige. Navnlig de tekniske og organisatoriske foranstaltninger brugt til at implementere Behandlingen, placeringen af Data, de implementerede sikkerhedsforanstaltninger (fysiske og tekniske) og, hvor relevant, detaljer om underdatabehandlere, etc.

Dette betyder ikke, at Capgemini skal gennemføre DPIA'en på vegne af den Dataansvarlige. Capgemini skal alene assistere den Dataansvarlige, uden at forpligte sig til at levere DPIA'en som sådan.

11. Revisioner relateret til BCR

Capgemini skal regelmæssigt gennemføre databeskyttelsesrevisioner, der omfatter alle aspekter af disse BCR og i henhold til vores BCR- og Databeskyttelsesrevisionsprogram.

Revisionerne skal gennemføres årligt enten af interne eller eksterne kvalificerede og uafhængige revisorer i henhold til en tidsplan, der er udviklet af Gruppe-DPO'en. I tillæg hertil, kan den Globale, de Regionale og de Lokale DPO'er anmode om, at der udføres yderligere revisioner. Sådanne revisioner kan omfatte specifikke applikationer, IT-systemer eller databaser, der behandler Persondata; eller kan blive gennemført for en hel geografi.

Revisionsrapporten, inklusiv de foreslåede oprettende handlinger for at adressere og mitigere risiciene, skal kommunikeres til Databeskyttelsesorganisationen og til topledelsen og skal gøres tilgængelig til de(n) kompetente Tilsynsmyndighed(er) efter anmodning.

I tillæg hertil, hvor Capgemini agerer som Databehandler, skal der gives accept til at blive revideret af Dataansvarlige i relation til specifikke Behandlingsaktiviteter udført på deres vegne. Betingelserne for sådanne revisioner skal fastlægges i Serviceaftalen.



12. Capgemini's ansvar i tilfælde af brud på disse BCR



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal ethvert EØS-Capgeminiselskab, der eksporterer Persondata til et ikke-EØS-Capgeminiselskab være ansvarligt over de Registrerede, for ethvert brud på disse BCR, forårsaget af ikke-EØS-Capgeminiselskabet.

I alle andre tilfælde ((1) overførsler fra et EØS-Capgeminiselskab til et andet EØS-Capgeminiselskab; (2) overførsler mellem to ikke-EØS-Selskaber; eller (3) overførsler fra et ikke-EØS-Selskab til et EØS-Selskab) skal hvert Capgeminiselskab være ansvarligt for de brud på disse BCR, som det har forårsaget.

I praksis betyder dette, at det selskab, der i henhold til ovenstående bliver identificeret til at bære ansvaret, skal acceptere ansvaret for at betale kompensation og for at afhjælpe bruddet, hvor det har medført skade på en Registreret.

I tillæg, så er det op til Capgemini at vise, at det ikke forbrød sig mod disse BCR. I tilfælde af en Overførsel mellem et EØS-Capgeminiselskab og et ikke-EØS-Capgeminiselskab, hvis ikke-EØS-Capgeminiselskabet bliver bebrejdet for det påståede brud, så skal EØS-Capgeminiselskabet påvise, at ikke-EØS-Capgeminiselskabet ikke forbrød sig mod disse BCR.



Databehandler-aktiviteter

I rollen som Databehandler, kan den Dataansvarlige, og i visse tilfælde den Registrerede, som fremført i afsnit 6, håndhæve BCR mod ethvert Capgeminiselskab for brud som det har forårsaget.

Hvor et EØS-Capgeminiselskab overfører Persondata til et ikke-EØS-Capgeminiselskab, skal EØS-Capgeminiselskabet være ansvarligt for brud forårsaget af ikke-EØS-Capgeminiselskabet.

I alle andre tilfælde ((1) overførsler fra et EØS-Capgeminiselskab til et andet EØS-Capgeminiselskab; (2) overførsler mellem to ikke-EØS-Selskaber; eller (3) overførsler fra et ikke-EØS-Selskab til et EØS-Selskab) skal hvert Capgeminiselskab være ansvarligt for de brud på BCR som det har forårsaget.

I praksis betyder dette at, i tilfælde af et brud på BCR, så skal det eksporterende EØS-Capgeminiselskab bære ansvaret for at betale kompensation og for at afhjælpe bruddet på BCR, hvor et sådant brud har forårsaget skade på en Dataansvarlig og/eller til Registrerede.

I tillæg, så skal det være op til Capgemini at påvise, at man ikke forbrød sig mod BCR.



13. Jurisdiktion

I tilfælde af brud på en rettighed garanteret i henhold til disse BCR, opfordrer Cappgemini de Registrerede til at bruge den dedikerede klagehåndteringsprocedure beskrevet i afsnit 7.

De Registrerede er dog også berettigede til at indgive en klage til den kompetente Tilsynsmyndighed – som kan være enten den i det EU-medlemsland hvor de bor, hvor de arbejder or hvor den påståede krænkelse er sket.

I tillæg hertil, kan de Registrerede indgive en klage til en kompetent domstol.

Hvor Behandlingen er foretaget af et ikke-EØS-Cappgeminiselskab, kan de Registrerede indgive en klage for den kompetente domstol i henhold til Gældende Lov; medmindre ikke-EØS-Selskabet er omfattet af GDPR, i hvilket tilfælde ovenstående gælder.

14. Gældende Persondataret og potentiel konflikt med BCR

Hvor Gældende Persondataret kræver et højere niveau for beskyttelse for Persondata, skal det tage forrang over disse BCR. I alle tilfælde, så vil Persondata blive behandlet i overensstemmelse med Gældende Persondataret.



Dataansvarlig-aktiviteter

Hvor et Cappgeminiselskab, i rollen som Dataansvarlig, har grund til at formode at relevant lokal lovgivning forhindrer det i at opfylde dets forpligtelser i henhold til disse BCR, så skal det informere Cappgemini hovedkvarter såvel som organisationens DPO; medmindre man er forhindret heri af en retshåndhævende myndighed.

I tillæg hertil, hvis et Cappgeminiselskab er genstand for lokale juridiske krav, der har væsentlig uønskede bivirkninger på de garantier der tilvejebringes af BCR (inklusive bindende anmodninger om udlevering af Persondata), så skal det orientere den kompetente Tilsynsmyndighed; medmindre man er forhindret heri af en retshåndhævende myndighed. Cappgemini vil yde sin bedste indsats for at underrette den kompetente Tilsynsmyndighed og vil, i ethvert tilfælde, give Tilsynsmyndigheden årlig, generel information om de anmodninger om udlevering af Persondata, som man har modtaget.



Databehandler-aktiviteter

Hvor et Cappgeminiselskab, i rollen som Databehandler, har grund til at formode, at relevant lokal lovgivning forhindrer det i at opfylde dets forpligtelser i henhold til disse BCR, så skal det informere den Dataansvarlige, Cappgemini hovedkvarter såvel som DPO-organisationen og den Tilsynsmyndighed, der er kompetent for den Dataansvarlige; medmindre man er forhindret heri af en retshåndhævende myndighed.

I tillæg hertil, skal den Dataansvarlige orienteres om enhver juridisk bindende anmodning om udlevering af Persondata fra en retshåndhævende myndighed eller statssikkerhedsinstans, medmindre dette er forbudt.

I hvert tilfælde vil Cappgemini yde sin bedste indsats for at underrette den kompetente Tilsynsmyndighed, både for den Dataansvarlige og for sig selv og vil give dem information om anmodningen om udlevering.



15. Samarbejdsforpligtelser

Hvor Gældende Persondataret kræver et højere niveau for beskyttelse af Persondata, skal det tage forrang over disse BCR. I alle tilfælde vil Persondata blive behandlet i overensstemmelse med Gældende Persondataret.



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig, skal Capgemini samarbejde med Tilsynsmyndighederne.

I praksis betyder dette, at Capgemini skal efterleve anbefalinger fra de kompetente Tilsynsmyndigheder og acceptere at blive revideret af dem efter anmodning.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini samarbejde med og assistere den Dataansvarlige for at hjælpe denne med at overholde dennes forpligtelser under Gældende Persondataret.

I tillæg hertil skal Capgemini samarbejde med de(n) kompetente Tilsynsmyndighed(er) for den Dataansvarlige, i henhold til den Dataansvarliges instruktioner. Navnlig, så skal Capgemini følge Tilsynsmyndighedens anbefalinger og acceptere at blive revideret af dem, i relation til de Behandlingsaktiviteter der udføres på vegne af en specifik Dataansvarlig.



16. Nem adgang til BCR

En offentlig udgave af disse BCR er tilgængelig på Capgeminis hjemmeside såvel som på Capgeminis Intranet.



Dataansvarlig-aktiviteter

I rollen som Dataansvarlig skal Capgemini offentliggøre den offentlige version af disse BCR på selskabets Intranet og gennemføre en kommunikationskampagne for at sikre, at Capgemini medarbejdere er opmærksomme på deres forpligtelser i henhold til disse BCR.

I tilfælde af en væsentlig opdatering af disse BCR, skal Capgemini informere Medarbejderne via kommunikation på Intranettet.



Databehandler-aktiviteter

I rollen som Databehandler, skal Capgemini sikre, at der er en reference til disse BCR i Serviceaftaler, sammen med et link til den offentlige version af disse BCR.

I tillæg hertil, skal Capgemini efter anmodning sende den offentlige version af disse BCR til den Dataansvarlige og/eller vedhæfte den til Serviceaftalen som aftalt mellem parterne.

17. Opdateringer af BCR

Capgemini skal kommunikere en opdateret liste over Capgeminiselskaber til sin ledende Tilsynsmyndighed, CNIL, en gang om året.

Når Capgemini vælger at lave væsentlige ændringer til disse BCR, at afspejle nye regulatoriske krav eller ændringer til sin interne organisation, for eksempel, skal man informere CNIL såvel som alle Capgeminiselskaber.

Hvis sådanne ændringer væsentlig påvirker vilkårene for Behandlingen af Persondata, skal Capgemini, i rollen som Databehandler, på behørig vis informere de Dataansvarlige.



Appendiks 1 – Capgeminis Behandlingsaktiviteter



Når Capgemini er i rollen som Dataansvarlig

▪ Medarbejderpersondata

Disse BCR omfatter Persondata for Capgeminimedarbejdere, vikaransatte og andre tredjeparter der arbejder på vegne af Capgemini såvel som jobansøgere. Capgeminis Medarbejderpersondata kan inkludere men er ikke begrænset til:

- **Kontaktdetaljer**, så som navn, fødselsdato, køn, alder, adresse, telefonnumre, e-mailadresse, antal børn, statsborgerskab, detaljer om ID, visa, arbejdstilladelse, nødkontakter, familiemedlemmer, ægteskabsstatus, livsforsikringsbegunstigede, billeder;
- **Finansiell information** relateret til compensation, goder og pensionsarrangementer, så som detaljer om løn, bankkonto, skat, rejseudgifter, aktieoptioner, aktiekøbsplaner;
- **Rekrutteringsinformation**, så som CV, ansøgningsblanket, interviewnoter, referencer (hvis noteret), kvalifikationer, testresultater (hvis relevant);
- **Medarbejderadministrationsinformation**, såsom ansættelse og karrierehistorik, karakterer, managere, ansættelseskontraktdetaljer, fraværfortegnelser, sikkerhedsfortegnelser, sundheds- og sygdomsfortegnelser, skadesfortegnelser, MUS-fortegnelser, kørekortsinformationer og relaterede dokumenter, færdighedsfortegnelser, statsudstedte ID-numre;
- **Erhvervsmæssig erfaringsinformation**, såsom erhvervs-CV, kvalifikationer, oversigt over projekter Medarbejderen har arbejdet på, uddannelsesoversigter, mobilitetsoversigter;
- **Detaljer om Medarbejderes opholdssted** i Capgemini lokationer i det omfang dette er registreret i Capgeminis elektroniske adgangskortsystem;
- **Detaljer om IT og forbindelsesdata** til Capgeminis IT-systemer;
- **Billeder.**

Capgemini behandler alene Medarbejderpersondata for arbejdsrelaterede formål. Sådanne formål inkluderer men er ikke begrænset til følgende aktiviteter:

- Rekruttering, inklusiv baggrundstjek i henhold til relevant lovgivning;
- Vurdering af arbejdsindsats og uddannelse;
- Aflønning og administration af andre medarbejderrelaterede goder (inklusive aktieoptioner, aktiekøbsplaner eller andre forretningsplaner eller goder);
- Dag-til-dag-ledelsesaktiviteter, såsom tilknytning til projekter, forfremmelser, disciplinære aktiviteter, håndtering af klager;
- Markedsføring af de forretningsmæssige services fra konsulenter til potentielle Capgemini kunder (f.eks. ved at give detaljer om erfaring fra tidligere projekter);
- Administration af nuværende goder, inklusiv Capgeminis personlige pensionsplaner,



- livsforsikringsplaner, helbredsfor sikringsplaner;
- Medarbejderanalyse, for eksempel, sammenligning af forskellige rekrutterings og/eller Medarbejderfastholdelsesprogrammer;
- Overholdelse af helbreds- og sikkerhedsregler og andre lovkrav på Capgemini som arbejdsgiver;
- Hvor nødvendigt, behandling designet til at gøre det muligt for Capgemini at udøve sine juridiske rettigheder og/eller udføre dets juridiske forpligtelser som arbejdsgiver, så længe det er krævet af den Gældende Persondataret i det land hvor Capgeminiselskabet, der er ansvarligt for Persondataene, er etableret;
- IT, sikkerhed, cybersecurity og adgangskontrol;
- HR-management, karrierehåndtering og mobility;
- Intern og ekstern kommunikation;
- Disaster recovery planer og krisehåndtering;
- Virksomhedsressourcehåndtering;
- Revision og statistikker;

▪ **Forretningskontakter**

Forretningskontakt betyder en Capgeminileverandør, underleverandør, aktionær, kunde eller alliancepartner, hvad enten der er et vedvarende kommercielt forhold med Capgemini eller værende en tidligere eller potentiel Forretningskontakt. De Persondata Capgemini kan have om personale af dets Forretningskontakter inkluderer men er ikke begrænset til:

- **Kontaktdetaljer**, såsom navn, jobtitel, arbejdsgiver, adresse, telefonnumre, e-mailadresse, faxnumre;
- **Finansielle detaljer** relateret til fakturering og betaling, såsom bankkontoinformationer (når Forretningskontakten er en fysisk person);
- **Relevant erfaring og/eller kvalifikationer** (for eksempel for personale hos underleverandører);
- **Detaljer om forretningsinteresser og holdninger** (såsom hvor information er opbevaret i en CRM-markedsføringsdatabase).

Capgemini behandler alene Persondata om Forretningskontakter til forretningsrelaterede formål. Sådanne formål inkluderer men er ikke begrænset til følgende aktiviteter:

- Indgåelse af og opfyldelse af kontrakter med Capgemini kunder, leverandører, underleverandører eller alliancepartnere;
- Håndtering af Capgemini konti og fortegnelser;
- Reklamering, markedsføring og PR;
- Kommunikation med Forretningskontakter;
- Markedsundersøgelser;
- Helbred, sikkerheds, miljø og kvalitet;
- Overholdelse af juridiske og regulatoriske forpligtelser;
- Opretholdelse af certifikationer;
- Revisioner og statistikker.

Som en overordnet regel, indsamler eller behandler Capgemini ikke Særlige Kategorier af Persondata som nærmere defineret i EU-retten. Dog kan Capgemini behandle Særlige Kategorier af Persondata hvor det er nødvendigt for at gøre det muligt for Capgemini at udøve sine juridiske rettigheder og/eller udføre sine juridiske forpligtelser som en arbejdsgiver, så længe det er strengt krævet af Gældende Lov i det land, hvor Capgeminiselskab ansvarligt for Persondataene er etableret.



Som en overordnet regel foretager Cappgemini ikke individuelle afgørelser der betydeligt påvirker en Registreret, alene baseret på automatisk behandling i henhold til GDPR, artikel 22.



Når Cappgemini er i rollen som Databehandler

Cappgemini tilbyder sine kunder en fuld vifte af ydelser i konsulent-, applikations-, infrastruktur-, BPO-, og lokale professionelle services.

Et Cappgeminiselskab kan behandle en bred vifte af omfattet Persondata i relation til leveringen af services til sine kunder, uagtet om behandlingen af Persondata er hovedforpligtelsen i leverancen eller om det er en supplerende ydelse i relation til udførelsen af en anden service til kunden.

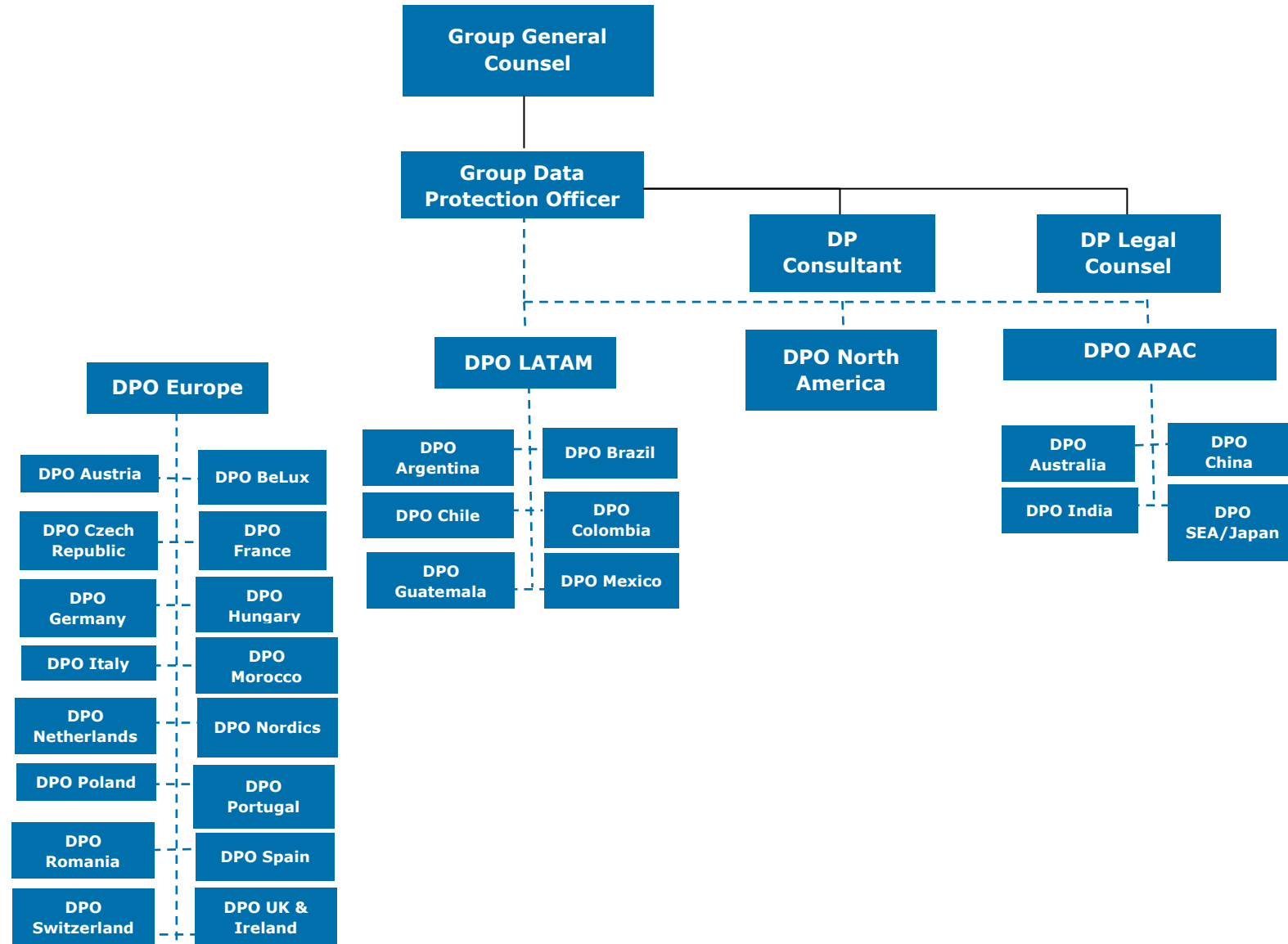
Omfattet Persondata i relation til Cappgeminis aktiviteter som en Databehandler, kan inkludere Persondata som beskrevet ovenfor i punkt 2.1 såvel som enhver anden type Persondata, som anmodet af den Dataansvarlige.

I henhold til kundens instruktioner, kan omfattet Persondata kan også inkludere Særlige Kategorier af Persondata.

Appendix 2 – Capgemini’s Databeskyttelsesorganisation



Data Protection Champions GBLs / Sales / Delivery / FS / Group Functions





Appendiks 3 – Procedure for håndtering af anmodninger fra Registrerede

Denne procedure skal offentliggøres på alle Capgeminis hjemmesider og tilpasses, så den omfatter eventuelle relevante lokale lovkrav.

Formålet med dette dokument er at forklare personer, hvis Persondata behandles af Capgemini ("Registrerede"), hvordan de kan udøve deres rettigheder.

Vi værner om dit privatliv, og det er derfor vigtigt for os, at du ved, hvordan og hvorfor vi indsamler og viderebehandler dine Persondata, og særligt hvad dine rettigheder er, og hvordan du kan udøve dem.

Centrale databeskyttelsesbegreber



"**Persondata**" refererer ikke kun til oplysninger, som relaterer sig til dit privatliv, men omfatter enhver form for oplysninger, som giver mulighed for at identificere dig – enten direkte eller indirekte.

"**Behandling**" betyder enhver operation, som Persondata gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse, samkøring, begrænsning, sletning eller tilintetgørelse.

"**Dataansvarlig**" betyder den fysiske eller juridiske person, som afgør, til hvilket formål og med hvilke hjælpemidler der foretages behandling af Persondata.

"**Databehandler**" betyder den fysiske eller juridiske person, der behandler Persondata på den Dataansvarliges vegne.

"**Formål**" betyder årsagen eller årsagerne til, at den Dataansvarlige har behov for at indsamle og viderebehandle Persondata.

Capgemini Service SAS og/eller selskaber, der er koncernforbundne med Capgemini SE (samlet refereret til som "**Capgemini**") indsamler og viderebehandler dine Persondata som Dataansvarlig eller som Databehandler på vegne af en Dataansvarlig. Under alle omstændigheder kan du kontakte Capgemini – ved at følge proceduren beskrevet nedenfor – for at udøve dine databeskyttelsesrettigheder.



Hvad er dine rettigheder?

Som Registreret kan du anmode om at udøve følgende rettigheder i forhold til de Persondata, som vedrører dig, og som Capgemini indsamler og viderebehandler:



Indsigt i dine Persondata	Du kan bede Capgemini om at bekræfte, om der behandles Persondata om dig, og hvis det er tilfældet, kan du anmode om indsigt i dine Persondata.
Anmode om sletning af dine Persondata	I nogle tilfælde kan du anmode om, at Capgemini sletter dine Persondata.
Anmode om berigtigelse af dine Persondata	Du kan bede Capgemini om at berigtige unøjagtige Persondata om dig. Det betyder, at du også kan anmode om, at Capgemini opdaterer eller fuldstændiggør dine Persondata.
Gøre indsigelse mod behandlingen af dine Persondata	I nogle tilfælde er du berettiget til at bede Capgemini om ikke at behandle dine Persondata.
Anmode om begrænsning af behandlingen af dine Persondata	I nogle tilfælde kan du bede Capgemini om at begrænse behandlingen af dine Persondata til nogle formål og under visse betingelser.
Tilbagekalde dit samtykke til behandlingen af dine Persondata	Du kan tilbagekalde dit samtykke til behandlingen af dine Persondata, selv hvis du oprindeligt havde givet Capgemini et sådant samtykke til at behandle dine Persondata.
Ret til dataportabilitet	I nogle tilfælde kan du bede Capgemini om at give dig dine Persondata i et struktureret, almindeligt anvendt og maskinlæsbart format og/eller om at dine data overføres til en anden Dataansvarlig.
Indgive en klage	Du kan også indgive en klage, hvis du mener, at Capgemini overtræder gældende databeskyttelseslovgivning eller BCR.



Bemærk venligt, at disse rettigheder kan være begrænsede i visse tilfælde i henhold til gældende lovgivning. F.eks. hvis du ville få adgang til Persondata om en anden person, hvis du fik indsigt i dine Persondata, eller hvis du beder Capgemini om at slette dine Persondata, mens Capgemini er forpligtet til at bevare dem.

Hvordan udøver du dine rettigheder?

Hvis du vil udøve dine rettigheder, eller hvis du har nogen spørgsmål til vores databeskyttelsespolitikker, kontakt os venligst:

- Ved at sende en e-mail til os på følgende adresse: d pocapgemini.global@capgemini.com
Bemærk venligt, at den Globale DPO, når det er relevant, skal videregive din anmodning til den lokale DPO;
- Ved at skrive til os på et af vores kontorers adresser, som du kan finde på følgende link: <https://www.capgemini.com/fr-fr/nous-contacter/#undefined>
- Ved at kontakte et af Capgeminis kontorer i dit land pr. telefon.

Giv os venligst følgende oplysninger, så vi har mulighed for at håndtere din anmodning:



- **Dit fulde navn***
- Din status (medarbejder, ansøger, osv.)
- **Din e-mailadresse eller et andet foretrukket kommunikationsmiddel***
- Identitetskontrol: Du kan blive bedt om at fremlægge passende identitetsdokumentation
- Land / Region
- **Din anmodnings art***

* Uden disse oplysninger vil Capgemini ikke kunne håndtere din anmodning.

Hvordan vil Capgemini håndtere din anmodning?

Din anmodning vil blive sendt til den kompetente DPO, afhængigt af hvilken Capgemini-enhed du har adresseret din anmodning til. Du vil så modtage en e-mail der anerkender modtagelse af din anmodning. Capgemini skal stræbe efter at adressere din anmodning uden unødigt forsinkelse, og ikke senere end 1 måned efter, at have anerkendt modtagelse af din anmodning. Hvis din anmodning er særligt kompleks, eller hvis du har sendt adskillige anmodninger, kan tiden for svar forlænges med yderligere 2 måneder. Vi vil informere dig om sådan forlængelse inden for en måned efter at have modtaget din anmodning.


Hvis du vælger at sende din anmodning elektronisk, og medmindre du ikke anmoder om andet, vil Capgemini levere information til dig i et almindeligt anvendt elektronisk format.

Selvom vi klart opfordrer dig til at følge denne proces for at indgive din anmodning, så vær venligst opmærksom på, at du også kan klage til en Tilsynsmyndighed og/eller søge juridiske retsmidler ved domstolene.



Hvordan vil Capgemini adressere din anmodning?

Når Capgemini har behandlet din anmodning internt, vil du blive informeret – via den foretrukne kommunikationsmetode du har indikeret – og modtage de relevante informationer i forhold til din anmodning. Se venligst i tabellen nedenfor, hvordan Capgemini adresserer de Registreredes mest almindelige anmodninger:

 Adgang til dine Persondata	Capgemini skal først bekræfte til dig hvorvidt man behandler dine Persondata; hvis det er tilfældet, vil du få en kopi af dine Persondata og alle andre relevante informationer om behandlingen.
Anmodning om sletning af dine Persondata	Hvis anmodningen er berettiget, vil den behandlede DPO anmode de(n) relevante funktioner(er) om at slette dine Persondata.
Anmodning om berigtigelse af dine Persondata	Den behandlende DPO skal instruere de(n) relevante funktion(er) om at berigtige dine Persondata; og du skal modtage bekræftelse på at dine Persondata er blevet berigtigede eller opdaterede.

Vær venligst opmærksom på, at når denne har modtaget din anmodning, skal den kompetente DPO gennemføre en indledende vurdering for at fastslå hvorvidt:

- Capgemini har brug for yderligere informationer for at håndtere din anmodning:

eller

- Din anmodning ikke kan blive behandlet. I sådant tilfælde vil vi forklare årsagen til vores konklusion.



Når Capgemini er i rollen som Databehandler

Når Capgemini behandler Persondata på vegne af en Dataansvarlig, opfordrer vi dig stærkt til at sende din anmodning direkte til den Dataansvarlige.

I ethvert tilfælde, hvis Capgemini modtager en anmodning direkte, så skal man orientere den Dataansvarlige uden unødigt forsinkelse i henhold til de aftalte betingelserne mellem Capgemini og den Dataansvarlige.

Skulle Capgemini blive instrueret af den Dataansvarlige til at håndtere din anmodning direkte, så skal Capgemini følge den ovenfor beskrevne procedure i tæt koordinatation med den Dataansvarlige.



Om Capgemini

Capgemini er en førende global leverandør af rådgivning, teknologiservices og digital transformation. Virksomheden er i front, når det kommer til innovation for at kunne realisere sine kunders potentiale inden for cloud, digital og platforme. Baseret på 50 års erfaring og dyb industrispecifik ekspertise, gør Capgemini organisationer i stand til at realisere deres forretningsmæssige ambitioner via en række ydelser fra strategi til drift. Capgemini er drevet af den overbevisning at forretningsværdien af teknologi kommer fra og af folk. Det er en multikulturel virksomhed med 200.000 holdmedlemmer i over 40 lande. Gruppen rapporterede i 2017 global omsætning på EUR 12,8 milliarder.

Lær mere om os på www.capgemini.com

Dette dokument indeholder information, der kan være beskyttet eller fortroligt og tilhører Capgemini-gruppen.
Copyright © 2018 Capgemini. Alle rettigheder forbeholdes.