

Afsnit A - Databehandleraftale**Artikel 1 Definitioner**

- 1.1 "Aftalen" henviser til aftalen mellem Siemens og Virksomheden, som denne Databehandleraftale er tilknyttet.
- 1.2 "Gældende Databeskyttelseslovgivning" henviser til den lovgivning, som vedrører behandling af personoplysninger, herunder GDPR.
- 1.3 "Virksomhedens Kontaktperson" henviser til den i artikel 8 anførte kontaktperson
- 1.4 "Dataansvarlig" henviser til Virksomheden og Andre Tjenestemodtagere, der alene eller sammen med andre bestemmer, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af Personoplysninger.
- 1.5 "DBA" henviser til denne Databehandleraftale.
- 1.6 "Andre Tjenestemodtagere" henviser til enhver tredjepart (såsom en af Virksomhedens tilknyttede selskaber), der har ret til at modtage Tjenesteydelser i henhold til Aftalen.
- 1.7 "GDPR" henviser til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 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 (General Forordning om Databeskyttelse).
- 1.8 "Personoplysninger" har den betydning som defineret i artikel 4, stk. 1, i GDPR, og omfatter i forbindelse med denne DBA kun Personoplysninger, der behandles af Siemens som Virksomhedens Databehandler.
- 1.9 "Brud på Persondatasikkerhed" henviser til brud på sikkerheden, som fører til hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til Personoplysninger, der er behandlet i henhold til denne DBA.
- 1.10 "Databehandler" henviser til en fysisk eller juridisk person, som behandler Personoplysninger på vegne af en Dataansvarlig.
- 1.11 "Databehandling" har den betydning som defineret i Artikel 4, stk. 2, i GDPR.
- 1.12 "Tjenesteydelse" henviser til tjenesteydelser, der leveres i henhold til Aftalen og indebærer behandlingen af Personoplysninger, som Siemens udfører i sin rolle som Databehandler for Virksomheden, Virksomheden er Dataansvarlig. Tjenesteydelserne er nærmere specificeret i **Afsnit A.1**.
- 1.13 "Underdatabehandler" henviser til enhver anden Databehandler, som på vegne af Siemens udfører de Tjenesteydelser, der leveres i henhold til denne DBA. Underdatabehandler henviser udelukkende til en underleverandør med adgang til Personoplysninger.

Artikel 2 Databehandleraftalens formål og anvendelsesområde

- 2.1 Denne DBA fungerer som en skriftlig Databehandleraftale mellem Virksomheden og Siemens og finder anvendelse på Tjenesteydelser, der involverer behandling af Personoplysninger og som Siemens udfører i rollen som Databehandler for Virksomheden og/eller Andre Tjenestemodtagere.
- 2.2 Databehandleraftalen regulerer Virksomhedens og Siemens' rettigheder og forpligtelser i forbindelse med behandling af Personoplysninger. Alle andre rettigheder og forpligtelser reguleres udelukkende af Aftalens øvrige dele.
- 2.3 Siemens behandler Personoplysninger i overensstemmelse med Aftalen og denne DBA.
- 2.4 Ved udførelsen af Tjenesteydelserne skal Siemens overholde alle love og forskrifter om databeskyttelse gældende for databehandlere. Virksomheden er ansvarlig for at overholde love og forskrifter, der gælder for Virksomheden og eventuelt Andre Tjenestemodtagere (navnlig love og forskrifter gældende for Dataansvarlige), samt ligeledes at sikre over for Andre Tjenestemodtagere, at Siemens og Siemens'

- 2.5 I tilfælde af uoverensstemmelse mellem bestemmelser i denne DBA og Aftalen – som angår parternes forpligtelser i forbindelse med behandling af Persondata - skal bestemmelserne i denne DBA have forrang. Enhver begrænsning af Databehandlerens ansvar i Aftalen eller andre tilknyttede aftaler skal ligeledes være gældende for denne DBA og have forrang for bestemmelser i denne DBA.

Artikel 3 Oplysninger om Databehandlingen udført af Siemens

Detaljerne vedrørende behandlingen af Personoplysninger der udføres af Siemens - navnlig de forskellige typer af behandlede Personoplysninger samt kategorierne af registrerede personer - er nærmere angivet i **Afsnit A.1** til denne DBA.

Artikel 4 Rettigheder i forbindelse med instrukser

- 4.1 Som Databehandler vil Siemens udelukkende behandle Personoplysninger i henhold til skriftlig instruks fra Virksomheden. Parterne er enige om, at Aftalen og denne DBA udgør Virksomhedens endelige instruks vedrørende Siemens' behandling af Personoplysninger.
- 4.2 Yderligere eller alternative instrukser skal aftales skriftligt mellem Siemens og Virksomheden og kan medføre yderligere omkostninger, som pålægges Virksomheden.
- 4.3 Hvis de yderligere instrukser er et direkte krav i Gældende Databeskyttelseslovgivning, og Siemens og Virksomheden ikke når til enighed i overensstemmelse med Artikel 4.2, har Virksomheden ret til at opsiges Aftalen med rimeligt varsel.

Artikel 5 Tekniske og organisatoriske foranstaltninger

- 5.1 Siemens implementerer de tekniske og organisatoriske foranstaltninger, der er nærmere anført i **Afsnit A.2**. Virksomheden bekræfter hermed, at det angivne sikkerhedsniveau er passende for den risiko, der er forbundet med Siemens' behandling af Personoplysninger på vegne af Virksomheden.
- 5.2 Virksomheden anerkender og accepterer, at de tekniske og organisatoriske foranstaltninger er underlagt den tekniske udvikling. Siemens har i den forbindelse ret til at gennemføre passende alternative foranstaltninger, forudsat sikkerhedsniveauet for foranstaltningerne opretholdes.

Artikel 6 Forpligtelse til datasikkerhed

Siemens instruerer alle medarbejdere, der indgår direkte i leveringen af Tjenesteydelserne, til at holde Personoplysninger fortrolige.

Artikel 7 Underdatabehandlere

- 7.1 Virksomheden godkender herved Siemens' anvendelse af Underdatabehandlere. Underdatabehandlerne er nærmere angivet i **Afsnit A.3**.
- 7.2 På ethvert tidspunkt kan Siemens fjerne eller tilføje nye Underdatabehandlere, men skal underrette Virksomheden forinden. Virksomhedens kan inden for 10 dage efter modtagelse af underretningen gøre indvending, hvorefter parterne skal forsøge at opnå enighed (evt. ved udskiftning af Underdatabehandleren eller ophævelse af denne DBA). Underdatabehandleren anses for godkendt, hvis der ikke er rejst indvending indenfor den angivne frist.
- 7.3 Siemens har ret til at udskifte Underdatabehandlere, i en kortere periode, såfremt dette anses nødvendigt for at levere Tjenesteydelser til Virksomheden uden afbrydelse. I et sådant tilfælde skal Siemens uden unødigt ophold underrette Virksomheden herom, Artikel 7.2 i denne DBA regulerer Virksomhedens adgang til at gøre indvendinger.

Artikel 8 Virksomhedens Kontaktperson for databeskyttelse

- 8.1 Virksomheden skal underrette Siemens om kontaktdetaljer på den persondataansvarlige i Virksomheden, såfremt Virksomheden har udpeget en DPO skal dennes kontaktdetaljer fremsendes til Siemens. Eventuelle ændringer skal straks underrettes skriftligt til Siemens.
- 8.2 Alle oplysninger og underretninger, der kræves i henhold til denne DBA, fremsendes skriftligt (e-mail er tilstrækkeligt) til Virksomhedens Kontaktperson, medmindre andet udtrykkeligt er aftalt.

Artikel 9 Berigtigelse, sletning og begrænsning af Databehandlingen

Siemens berigtiger, sletter eller begrænser behandlingen af Personoplysninger efter instruks fra Virksomheden.

Artikel 10 Underretningspligt og støtte fra Siemens

- 10.1 I tilfælde af Brud på Persondatasikkerheden underretter Siemens uden ugrundet ophold Virksomheden, efter at Siemens er blevet bekendt med sådanne sikkerhedsbrud. Siemens (i) samarbejder i rimeligt omfang med Virksomheden i forbindelse med undersøgelsen af et sådant Brud på Persondatasikkerheden, (ii) yder i rimeligt omfang støtte til Virksomheden i forbindelse med dennes forpligtelse til underretning om sikkerhedsbrud i henhold til Gældende Databeskyttelseslovgivning og (iii) iværksætter passende foranstaltninger til afhjælpning af sikkerhedsbruddet.
- 10.2 Siemens underretter uden ugrundet ophold Virksomheden om (i) klager og anmodninger fra de registrerede personer, hvis Personoplysninger behandles i henhold til denne DBA (f.eks. i forbindelse med berigtigelse, sletning eller begrænsning af behandlingen af Personoplysninger) og (ii) påbud eller anmodninger fra domstolene eller de kompetente tilsynsmyndigheder.
- 10.3 Efter anmodning fra Virksomheden bistår Siemens i rimeligt omfang Virksomheden med
 - (i) håndtering af klager, anmodninger eller påbud som beskrevet i Artikel 10.2 i denne DBA
 - (ii) opfyldelse af Virksomhedens forpligtelser i henhold til Gældende Databeskyttelseslovgivning.

De ovennævnte ydelser leveret af Siemens, faktureres selvstændigt på baggrund af medgået tid og omkostninger.

Artikel 11 Revisioner

- 11.1 Virksomheden har ret til - ved hjælp af passende midler - i overensstemmelse med Artikel 11.2 og 11.3 nedenfor, at kontrollere Siemens' og Underdatabehandlernes overholdelse af databeskyttelsesforpligtelserne, herunder (navnlig i forbindelse med de tekniske og organisatoriske foranstaltninger) årlige kontroller og lejlighedsvis såfremt disse er nødvendige i henhold til Gældende Databeskyttelseslovgivning. Disse kontroller skal være begrænset til informations- og databehandlingssystemer, der er relevante for leveringen af Tjenesteydelserne.
- 11.2 Siemens og Underdatabehandlere har mulighed for at dokumentere overholdelse af databeskyttelsesforpligtelserne ved fremlæggelse af revisionserklæringer eller certificeringer. Virksomheden bekræfter at disse generelle erklæringer opfylder Virksomhedens revisionsbeføjelse i henhold til denne DBA. På Virksomhedens anmodning stiller Siemens (i) relevante uddrag af revisionsrapporter og/eller (ii) oplysninger samt dokumentation vedrørende gældende certificeringer for de pågældende Tjenesteydelser, til rådighed. Virksomheden forpligter sig til at behandle de fremlagte revisionsrapporter, oplysninger og dokumentation fortroligt.
- 11.3 Alene i tilfælde af, at certificeringerne og revisionsrapporterne ikke er tilstrækkelige til, at Virksomheden kan overholde gældende revisionskrav og forpligtelser i henhold til Gældende Databeskyttelseslovgivning, kan Virksomheden for egen regning (i) anmode om yderligere oplysninger og dokumentation eller (ii) - efter et rimeligt skriftligt varsel - foretage yderligere revisioner af Siemens' kontrolmiljø og sikkerhedspraksis, som er relevante for behandling af Personoplysninger omfattet af denne DBA. En revision skal foretages uden at afbryde Siemens' forretningsaktiviteter og i overensstemmelse med Siemens' sikkerhedspolitikker samt Gældende Databeskyttelseslovgivning.

Artikel 12 Gyldighedsperiode og opsigelse

Denne DBA har samme gyldighedsperiode som Aftalen. Ved opsigelse af denne DBA sletter Siemens alle Personoplysninger, der er stillet til rådighed for Siemens eller indhentet eller frembragt af Siemens på vegne af Virksomheden i forbindelse med Tjenesteydelserne, medmindre andet er aftalt mellem parterne. Sletningen bekræftes skriftligt af Siemens på anmodning.

Afsnit A.1: Beskrivelse af databehandlingsaktiviteter

Dette bilag indeholder en beskrivelse af de grundlæggende databehandlingsaktiviteter, der udføres af Siemens Building Technologies for at kunne opfylde de kontraktuelt aftalte ydelser i hovedaftalen.

Hvis en bestemt tjeneste indeholder behandling af yderligere eller forskellige kategorier af dataemner eller af personlig data, gives den respektive information i den relevante tjenestebeskrivelse.

Produkt	Tjeneste	Dermed forbunden behandling af personoplysninger
Sikringsløsninger: <ul style="list-style-type: none"> • TVO-anlæg • Automatisk indbrudsalarmanlæg • Adgangskontrolanlæg • Og tilhørende management platform (MM8000, DesigoCC) 	Vedligehold, eftersyn og reparation* (onsite eller via fjernadgang)	Personoplysninger gemt i systemet (f.eks. system logdata indeholdende brugernavn og brugeraktiviteter, videooptagelser) kan ses
	Driftsassistance	Ifm. assistance til standard betjeningsfunktioner af de købte sikringsløsninger kan personoplysninger i systemet på vegne af kunden tilgås og ændres af Siemens medarbejder (f.eks. oprettelser af nye brugere, redigering af kortholder, gennemgang af videooptagelser).
	Back-up tjenester	Back-up filer med systemernes konfigurationsdata, som bliver gemt hos Siemens indeholder personoplysninger som f.eks. brugernavn og kode. Filer som inkluderer yderligere person data som f.eks. brugernes aktiviteter, navne på ansatte og deres indtastninger på visse sikkerhedsområder eller optagelser lavet via videoovervågnings-systemer bliver gemt på kundens udstyr (f.eks. bærbar hard drive, lokal server) og kan gendannes.
Behandlingen omfatter følgende kategorier af registrerede: <ul style="list-style-type: none"> • Ansatte hos kunden og samarbejdspartner, som får adgang til kundens bygninger og/eller bliver oprettet som bruger/kortholder i kundens sikringsanlæg • Ansatte hos kunden, som er driftsansvarlig for kundens sikringsanlæg og-/eller tilhørende management platforme • Gæster / andre individer, der går ind på et overvåget område hos kunden • Personer, som er angivet som kontakt person på Siemens forholdsordre 		
Kategorier af personoplysninger: <ul style="list-style-type: none"> • Master data (navn, brugernavn, personnummer, kontoradresse, gyldighed for adgangsautorisation) • Forretningskontaktdata (e-mail adresse, telefonnummer) • Adgangsdata (lokation og adgangstidspunkt) • IP adresser på udstyr for at opnå adgang til relevante systemer • Logget aktivitet (f.eks. ændringer på systemkonfiguration) • Kun i tilfælde af videoovervågning: Videooptagelser 		

* I forbindelse med fejlretning og reparation kan det forekomme, at vores danske support organisation får assistance fra Siemens Building Technologies hovedkvarter i Schweiz. Denne supportydelse inkluderer ingen databehandlingsaktivitet, dog kan det ikke udelukkes at personoplysninger gemt i databasen af det enkelte system er synligt i fejlfindingsprocessen.

Produkt	Tjeneste	Dermed forbunden behandling af personoplysninger
Bygningsautomatik	Back-up Services	Back-up filer med systemernes konfigurationsdata, som bliver gemt hos Siemens indeholder personoplysninger som f.eks. brugernavn og kode.
<p>Behandlingen omfatter følgende kategorier af registrerede:</p> <ul style="list-style-type: none"> • Ansatte hos kunden og samarbejdspartner, som bliver oprettet som bruger i kundens anlæg for bygningsautomatik 		
<p>Kategorier af personoplysninger:</p> <ul style="list-style-type: none"> • Brugernavn • IP adresser på udstyr for at opnå adgang til relevante systemer • Logget aktivitet (f.eks. ændringer på systemkonfiguration) 		

Afsnit A.2: Tekniske og organisatoriske foranstaltninger

Tekniske og organisatoriske foranstaltninger i henhold til Art. 32 Generel databeskyttelsesforskrift ("GDPR")

I. Introduktion

Dette dokument beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af persondata ("sikkerhedsforanstaltninger" og "tiltag"), hvilke databehandleren, som minimum, etablerer i forbindelse med den behandling, der udføres på vegne af den dataansvarlige, under hensyntagen til den teknologiske udvikling, omkostningerne for implementering, kontekst og formål for behandling samt risikoen for varierende sandsynlighed og alvor for personers rettigheder og frihed.

Hvis forskellige, særlige sikkerhedsforanstaltninger er aftalt i den til grundlæggende hovedaftale, gælder disse særlige tiltag i stedet for eller i tillæg til de sikkerhedsforanstaltninger, der beskrives i dette dokument.

II. Grundlæggende sikkerhedsforanstaltninger

De grundlæggende foranstaltninger sikrer beskyttelsen af fortrolighed og systemernes integritet, hvormed Siemens bearbejder persondata, især når det gælder fjernadgang. Disse sikkerhedsforanstaltninger gælder for al behandling, der udføres af Siemens, med mindre andet er aftalt i den til grundlæggende hovedaftale.

1. Virksomheders interne processer

Databehandleren har udnævnt en databeskyttelsesleder i firmaet. Alle ansatte og tjenesteudbydere, der har adgang til persondata, er forpligtede til at behandle disse data kun efter instruks fra den dataansvarlige og udelukkende til udførelsen af de kontraktuelt aftalte tjenester.

2. Beskyttelse mod uautoriseret adgang

Uautoriserede personer skal forhindres i at få adgang til computercentre eller forretningslokaliteter, hvor databehandling foregår.

Tiltag:

Databehandleren beskytter bygningerne eller forretningslokaliteter med passende kontrolsystemer, for fysisk adgang baseret på en sikkerhedsklassificering, af bygninger eller forretningslokaliteter og tilsvarende definerede adgangsautorisationskoncepter. Alle bygninger eller forretningslokaliteter skal være sikrede, med teknisk adgangskontroltiltag f.eks. ved brug af kortafslæsningsystemer. Afhængigt af sikkerhedsklassifikation, skal ejendom, bygninger eller individuelle områder sikres med yderligere tiltag. Dette kan inkludere særlige profiler for fysisk adgang, biometri, adgang ved pinkode, korbom systemer, der kun tillader individuel adgang, videoovervågning og sikkerhedspersonale. Rettigheder til at få adgang for autoriserede personer udstedes individuelt i henhold til fastsatte kriterier. Dette gælder også for eksterne personer.

3. Beskyttelse af computere

De computere, der benyttes til behandling, skal sikres og beskyttes mod uautoriseret brug.

Tiltag:

Kun autoriserede brugere får adgang til databehandlerens computer (både bærbare og stationære computer) og følgende sikkerhedsforanstaltninger beskytter yderligere mod uautoriseret adgang: datakryptering, individualiseret sikring af kodeord (mindst 8 tegn, normalt med automatisk udløbsdato), medarbejderidentitetskort med personlig identitetskryptering, automatisk nedlukning af inaktive systemer. Beskyttelsen af de benyttede computere mod angreb samt uheldig eller bevidst destruktion eller modifikation leveres blandt andre tiltag, ved systemer, der opdager indtrængen, firewalls og jævnlige opdaterede malware filtre.

4. Beskyttelse af data ved overførsel, transport og fjernadgang

Persondata må ikke kunne læses, kopieres, ændres eller fjernes under elektronisk transmission eller under transport af data eller lagring af den på datamedier. Det skal være muligt at undersøge og afgøre på hvilke steder en overførsel af persondata ved brug af udstyr til dataoverførsel er muligt.

Tiltag:

De elektroniske kommunikationskanaler skal sikres med installation af lukkede netværker og processer for datakryptering. I tilfælde af fysisk transport af datamedier skal data krypteres. Datamedier skal bortskaffes på en måde, der er passende for beskyttelse af data. Fjernforbindelser skal være beskyttet ved kryptering. Dato, type og omfang af fjern vedligeholdelsesaktiviteter skal noteres i protokoller.

III. Særlige sikkerhedsforanstaltninger for tjenester, hvori Siemens lagrer kundedata i IT systemer

Disse særlige tiltag sikrer beskyttelsen af fortrolighed, integritet, tilgængelighed og robusthed af IT systemer, hvori Siemens gemmer kundernes persondata. Disse tiltag gælder, når lagring af data repræsenterer en del af de kontraktuelle tjenester fra Siemens, og ikke kun er midlertidig.

1. Beskyttelse mod uautoriseret behandling

Kun medarbejdere, der er beskæftiget med de formål, hvortil personoplysningerne behandles, har adgang til IT systemer, som bruges til lagring af kundedata. Personoplysninger skal ikke kunne læses, kopieres, ændres eller fjernes uden tilladelse under behandling, brug og efter opbevaring.

Tiltag:

Adgang til persondata i IT systemer gives på basis af et autorisationskoncept, som begrænser medarbejdernes adgang til de personoplysninger, som er nødvendige for udførelsen af de kontraktuelt aftalte tjenester ("need to know"). Derudover stilles krav om, at uautoriseret adgang til persondata forhindres efter behov ved hjælp af datakryptering.

2. Sikring af sporbarhed

Det skal være muligt at undersøge og afgøre, om og af hvem persondata er indtastet, ændret eller fjernet i databehandlingsssystemer.

Tiltag:

Databehandleren tillader kun autoriserede brugere at have adgang til persondata på basis af et "need to know" autorisationskoncept. Adgang til persondata er angivet i logdatafiler, som i en protokol registrerer indtastning, modifikation og sletning af persondata.

3. Forsikring af integritet, tilgængelighed og stabilitet

De systemer, der benyttes til behandling, skal være sikrede mod fejl, og mod at persondata til enhver tid er fuldt tilgængelige og beskyttet mod tab.

Tiltag:

Databehandleren gemmer persondata ved brug af redundante systemer, afhængigt af sikkerhedsklassificering og samt benytter afbrydelsesfri strømforsyning (f.eks. UPS, batterier, generatorer) til sikring af strømforsyningen i egne computercentre. En omfattende, nedskrevet nødplan foreligger og nødprocedurer og -systemer testes regelmæssigt.

Afsnit A.3: Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr.	Adresse	Mulig involvering i databehandling
Securitas A/S	88663217	Sydvestvej 98 2600 Glostrup	<ul style="list-style-type: none">• Registrering af kundernes kontaktoplysninger i kontrolcentralens software og videregivelse af disse oplysninger til vægteren• Registrering af kundehenvendelser i kundeloggen• Modtagelse og behandling af signaler fra Siemens udstyr, bl.a. video "live stream" i alarmtilfældet• Fremsendelse af logudskrifter til kunden• Udfyldelsen af vagtpatroljerapporter med kundens kontaktoplysninger
Vanderbilt International (UK) Lim.	35435255	Engager 2-4 2605 Brøndby	<ul style="list-style-type: none">• Opbevaring af personoplysninger som registreres ifm. etablering og brugen af SPC Connect:<ul style="list-style-type: none">○ Brugernes personoplysninger som indtastes ifm. SPC Connect registreringsproces○ Personoplysninger som knyttes til brugernes konto ifm. driften af SPC Connect○ Back-up af centralens konfiguration, som indeholder brugernavne og adgangsrettigheder• Analyse af systemets konfiguration, logfiler og databasen til fejlfinding (3. niveau support)