

## **Vilkår for databehandling (Databehandlersaftale for Erhverv) ved anvendelse af tyverialarm- og adgangskontrolanlægget SPC Connect**

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Kunden; "den dataansvarlige"

og

G4S Security Services A/S  
Roskildevej 157  
2620 Albertslund  
Danmark  
CVR nr. 26891280

herefter; "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

<b>1. Indhold</b>	
2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige	6
10. Underretning om brud på persondatasikkerheden	7
11. Sletning og returnering af oplysninger	8
12. Revision, herunder inspektion	8
13. Parternes aftale om andre forhold	8
14. Ikrafttræden og ophør	8
Bilag A Oplysninger om behandlingen	10
Bilag B Underdatabehandlere	11
Bilag C Instruks vedrørende behandling af personoplysninger	12
Bilag D Parternes regulering af andre forhold	14

## 2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i 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 (databeskyttelsesforordningen).
3. I forbindelse med leveringen af den aftalte ydelse behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

## 3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes<sup>1</sup> nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

---

<sup>1</sup> Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

#### **4. Databehandleren handler efter instruks**

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

#### **5. Fortrolighed**

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

#### **6. Behandlingssikkerhed**

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger
- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

- d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
  3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

## 7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren har den dataansvarliges generelle godkendelse til anvendelse af underdatabehandlere. Databehandleren benytter de underdatabehandlere, der er anført i Bilag B. Den dataansvarlige accepterer, at databehandleren er berettiget til at udskifte eller tilføje underdatabehandlere uden forudgående underretning til eller godkendelse fra den dataansvarlige, forudsat at databehandleren sikrer, at underdatabehandleren overholder de samme databeskyttelsesforpligtelser, som påhviler databehandleren i henhold til disse Bestemmelser.
3. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

4. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

5. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

## **8. Overførsel til tredjelande eller internationale organisationer**

1. Den dataansvarlige giver ved indgåelse af denne aftale databehandleren fuldmagt og instruks til at foretage overførsel af personoplysninger til tredjelande (lande uden for EU/EØS) via de underdatabehandlere, som databehandleren anvender til drift af tjenesten jf. Bilag B og punkt 7.2, herunder overførsel til interne selskaber i Allied Universal®-koncernen til administrative formål.
2. Ved anvendelse af de underdatabehandlere, der er nævnt i Bilag B, anses den fornødne instruks for overførsel til tredjeland for givet. Såfremt databehandleren udskifter eller tilføjer underdatabehandlere i overensstemmelse med den generelle godkendelse i punkt 7.2, omfatter instruksen ligeledes overførsel til disse nye underdatabehandlere, forudsat at kravene i punkt 8.3 er opfyldt.
3. Databehandleren indestår for, at overførsel til tredjelande alene sker under iagttagelse af et lovligt overførselsgrundlag i medfør af databeskyttelsesforordningens kapitel V. For underdatabehandlere etableret uden for EU/EØS sikrer databehandleren, at overførslen er dækket af nødvendige tilstrækkelighedsafgørelser jf. Databeskyttelsesforordningens artikel 45 eller fornødne garantier jf. Databeskyttelsesforordningens artikel 46 suppleret med eventuelle nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, herunder Transfere Impact Assessments.
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Ved indgåelse af denne aftale bekræfter parterne, at instruksen i punkt 8.1-8.3 samt de i Bilag B anførte underdatabehandlere udgør den dataansvarliges dokumenterede instruks for så vidt angår overførsel af personoplysninger til tredjelande. Databehandleren er berettiget til at foretage overførsler inden for rammerne af denne instruks uden yderligere godkendelse, såfremt betingelserne i kapitel V i databeskyttelsesforordningen er opfyldt.

## **9. Bistand til den dataansvarlige**

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

- c. indsigtsretten
  - d. retten til berigtigelse
  - e. retten til sletning ("retten til at blive glemt")
  - f. retten til begrænsning af behandling
  - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  - h. retten til dataportabilitet
  - i. retten til indsigelse
  - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
- a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
  - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  - c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
  - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

## 10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

- a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
  - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
  - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

## **11. Sletning af oplysninger**

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

## **12. Revision, herunder inspektion**

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

## **13. Parternes aftale om andre forhold**

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

## **14. Ikrafttræden og ophør**

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Databehandler kontaktoplysninger:



Frederik Boesgaard  
Chief Legal Counsel  
+45 4386 5000  
[gdpr@dk.g4s.com](mailto:gdpr@dk.g4s.com)

## **Bilag A      Oplysninger om behandlingen**

### **A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige**

Formålet med behandlingen er levering af ydelsen:

- Alarmhåndtering og -notifikationer.
- Brugerstyring og adgangskontrol.
- Mulighed for visning af live videobilleder fra eventuelle tilkoblede kameraer.
- Systemkonfiguration og -vedligeholdelse.

### **A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)**

- Transmission af alarmdata og brugeroplysninger til SPC Connects cloud-platform og G4S Kontrolcentral.
- Lagring af alarmdata, brugeroplysninger og systemkonfigurationsdata i sikrede datacentre.
- Bearbejdning af alarmdata til alarmhåndtering og -notifikationer.
- Levering af fjernadgang til autoriserede brugere via webportal eller mobilapp.
- Visning af live billeder fra eventuelt tilkoblede kameraer.

### **A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede**

Behandlingen omfatter personoplysninger, som den Dataansvarlige selv vælger at inddatere eller få inddateret i systemet som fx navn, medarbejdersnummer, adgangskortnummer og øvrige brugeroplysninger samt logning af brug af eventuelle adgangskort og videobilleder fra tilkoblede kameraer.

### **A.4. Behandlingen omfatter følgende kategorier af registrerede**

Behandlingen omfatter kategorier som den Dataansvarlige vælger at inddatere eller få inddateret i systemet som fx brugere af SPC alarmsystemet.

Derudover kan omfattes personer, hvis adfærd registreres af alarmsystemets sensorer eller eventuelle tilkoblede kameraer og adgangskontrol.

Autoriserede brugere af SPC connect systemet.

### **A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser ikrafttræden. Behandlingen har følgende varighed**

Behandlingen pågår, indtil hovedaftalen vedrørende levering af ydelsen opsiges eller på anden vis ophører. Eventuelle fotos/video slettes automatisk inden for 30 dage.

## **Bilag B      Underdatabehandlere**

### **B.1. Godkendte underdatabehandlere**

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

Vanderbilt International AB  
Englundavägen, 171 41 Solna, Sweden  
VAT 556987-4661

Beskrivelse af behandlingen: Opbevaring og behandling af anlægsdata til brug for drift af alarmanlægget.

Lokalitet for behandling: Microsoft Azure, United Kingdom.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Se pkt. 7.2.

## **Bilag C Instruks vedrørende behandling af personoplysninger**

### **C.1. Behandlingens genstand/instruks**

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- i) Databehandleren behandler kun data i det omfang, at dette er nødvendigt for at Databehandleren kan levere ydelsen til den Dataansvarlige og udføre sine forpligtelser som fastsat i hovedaftalen mellem parterne; og
- ii) Databehandlerens behandling af persondata sker i overensstemmelse med den til enhver tid dokumenterede instruks fra den Dataansvarlige

### **C.2. Behandlingssikkerhed**

Sikkerhedsniveauet skal afspejle, at der er tale om almindelige persondata.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Databehandleren krypterer data, hvor det er relevant jf. Databehandlerens risikovurdering.

Databehandleren sikrer den vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og services.

Databehandleren skal rettidigt kunne genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

Databehandleren skal regelmæssigt afprøve, vurdere og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

Databehandleren skal bruge VPN når data tilgås online samt vedligeholde en høj grad af sikring når data tilgås via f.eks. hjemmearbejdsplads.

Under transmission af data skal databehandleren sikre dataene.

Databehandleren skal på tilstrækkelig vis sikre dataene under opbevaring.

Databehandleren skal sikre et højt niveau af fysisk sikkerhed på lokationer hvor data bliver behandlet eller gemt.

Databehandleren skal sikre, at tilgang, behandling, sletning af data og andre sådanne handlinger logges. Derudover skal databehandleren sikre at kun relevante medarbejdere vil have adgang til dataene, samt at det logges hvilke medarbejdere, som tilgår dataene.

### **C.3 Bistand til den dataansvarlige**

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren skal i tilfælde af databrud yde den fornødne bistand for at sikre, at bruddet anmeldes til den rette myndighed.

Databehandleren skal efter forespørgsel hjælpe den Dataansvarlige med besvarelse af forespørgsler vedr. de registreredes rettigheder, herunder udlevering af data, sletning af data, dataportabilitet, begrænsning af databehandling og sikre information ved indsamling af data fra registrerede.

#### **C.4 Opbevaringsperiode/sletterutine**

Behandlingen pågår, indtil hovedaftalen vedrørende levering af ydelsen opsiges eller på anden vis ophører. Eventuelle fotos/video slettes automatisk inden for 30 dage.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren slette personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal dokumenteres og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

#### **C.5 Lokaltet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ske på følgende lokaliteter:

Behandlingen finder sted på G4S Security Services A/S' lokationer i Danmark, herunder på:

- Hovedkontoret; Roskildevej 157, 2620 Albertslund
- Kontrolcentralen; Tangen 8, 8200 Århus

Lokalitet for underleverandørers behandling henvises til bilag B.

#### **C.6 Instruks vedrørende overførsel af personoplysninger til tredjelände**

Der henvises til de i punkt 8.1-8.3 og 8.5 indeholdt instrukser vedrørende overførsel til tredjelände i forbindelse med brug af godkendte underdatabehandlere.

Overførsel til tredjelände sker på baggrund af en tilstrækkelighedsafgørelse (artikel 45) / EU-US Data Privacy Framework eller på baggrund af EU's standardkontraktbestemmelser (artikel 46) og en dertilhørende Transfer Impact Assessment (TIA).

#### **C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren**

Den Dataansvarlige eller en repræsentant for den Dataansvarlige foretager skriftligt eller fysisk tilsyn hos Databehandleren.

Den Dataansvarliges eventuelle udgifter i forbindelse med tilsyn afholdes af den Dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den Dataansvarlige kan gennemføre sit tilsyn.

#### **C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

Databehandleren sikrer, at eventuelle underdatabehandlere overholder databeskyttelsesreglerne efter samme standard og under samme krav som der er fastsat efter denne aftale.

Den Dataansvarlige eller en repræsentant for den Dataansvarlige kan foretage skriftligt tilsyn af underdatabehandleren.

Den Dataansvarliges eventuelle udgifter i forbindelse med tilsyn afholdes af den Dataansvarlige selv. Databehandleren kan dog være nødsaget til at fakturere for afsatte ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den Dataansvarlige kan gennemføre sit tilsyn.

## **Bilag D      Parternes regulering af andre forhold**

Ingen andre forhold.