Denne fil er kun til informationsformål. Den bindende juridiske version er den originale tyske version.

Aftale om ordrebehandling

(i henhold til EU's GDPR artikel 28)

mellem

lejeren af videoovervågningsløsningen fra hovedkontrakten

- - herefter benævnt: Klient –

og

the VIDEO GUARD ApS , Tagholm 2, 9400 Nørresundby

- herefter: Databehandler (i henhold til artikel 28 i GDPR) –

1. Almindelige bestemmelser og kontraktens genstand

1.1 Genstanden for denne kontrakt er behandling af personoplysninger på vegne af databehandleren (artikel 28 i EU GDPR). Kontraktens indhold, kategorier af registrerede og datatyper samt aftalens formål findes i bilag 1.

1.2 Databehandlerens behandling af data finder udelukkende sted på Forbundsrepublikken Tysklands, en EU-medlemsstats eller en EØS-aftalens område. Behandling uden for disse lande vil kun finde sted i henhold til kapitel 5 i EU's GDPR (artikel 44-50) og med klientens forudgående samtykke.

1.3 Honoraret vil blive aftalt uden for denne kontrakt.

2. Kontraktperiode og opsigelse

Kontraktens løbetid er baseret på hovedkontraktens løbetid. Retten til ekstraordinær opsigelse af gyldig grund forbliver uændret.

3. Instruktioner fra klienten

3.1 Klienten har en udtømmende ret til at give instruktioner vedrørende typen, omfanget og de nærmere bestemmelser for databehandling . til processoren. I denne rolle kan han navnlig kræve øjeblikkelig sletning, berigtigelse, blokering eller videregivelse af de data, der er omfattet af kontrakten. Databehandleren er forpligtet til at følge klientens instruktioner, medmindre der foreligger legitime kontraktlige eller juridiske interesser, der er i konflikt hermed.

3.2 Databehandleren skal straks underrette klienten, hvis databehandleren mener, at en instruktion fra klienten overtræder lovbestemmelser. Hvis der gives en instruktion, hvis lovlighed databehandleren væsentligt betvivler, er databehandleren berettiget til midlertidigt at suspendere udførelsen af instruktionen, indtil klienten udtrykkeligt bekræfter eller ændrer den igen.

3.3 Instruktioner skal generelt gives skriftligt eller i elektronisk format (f.eks. via e-mail). Mundtlige instruktioner skal bekræftes af klienten skriftligt eller i elektronisk format på databehandlerens anmodning. Behandleren skal registrere personen, datoen og tidspunktet for den mundtlige instruktion i en passende form.

3.4 På databehandlerens anmodning skal klienten udpege en eller flere personer, der er bemyndiget til at give instruktioner. Ændringer skal meddeles databehandleren med det samme.

3.5 Personer, der er bemyndiget til at give instruktioner, er navngivet i kontraktens bilag 4.

4. **Klientens kontrolbeføjelser**

4.1 Klienten har ret til at kontrollere overholdelsen af lovmæssige og kontraktlige bestemmelser om databeskyttelse og datasikkerhed inden databehandlingens start og regelmæssigt i kontraktens løbetid i det nødvendige omfang eller til at få dette kontrolleret af tredjeparter. Databehandleren vil tolerere disse kontroller og understøtte dem i det nødvendige omfang. Leverandøren skal især give klienten alle oplysninger, der er relevante for inspektionerne, på en fuldstændig og sandfærdig måde, give klienten adgang til de lagrede data og databehandlingsprogrammer/-systemer og muliggøre inspektioner på stedet. Hvis klienten har givet samtykke til behandling af data uden for forretningslokalerne (f.eks. privatbolig), skal databehandleren sikre, at klienten også har tilladelse til at få adgang til disse lokaler med henblik på inspektion.

4.2 Klienten skal sikre, at kontrolforanstaltningerne er forholdsmæssige og ikke forringer databehandlerens drift mere end nødvendigt. Især bør inspektioner på stedet generelt udføres i den normale åbningstid og efter aftale med rimeligt varsel, forudsat at formålet med inspektionen ikke er i konflikt med forudgående varsel.

4.3 Resultaterne af kontrollerne og instruktionerne skal registreres på passende måde af begge kontraherende parter.

5. **Databehandlerens generelle forpligtelser**

5.1 Databehandlerens behandling af kontraktoplysningerne udføres udelukkende på grundlag af kontraktaftalerne i forbindelse med eventuelle instruktioner fra klienten. Enhver behandling, der afviger fra dette, er kun tilladt på grundlag af ufravigelig europæisk ret eller medlemsstatsret (f.eks. i tilfælde af efterforskninger foretaget af retshåndhævende myndigheder eller statslige sikkerhedsmyndigheder). Hvis behandling er påkrævet i henhold til ufravigelig lov, skal databehandleren underrette den dataansvarlige herom inden behandlingen, medmindre den pågældende lov forbyder en sådan underretning af hensyn til vigtige samfundsinteresser.

5.2 Databehandleren skal overholde alle lovbestemmelser ved udførelsen af ordren. Han skal især implementere de tekniske og organisatoriske foranstaltninger, der kræves i henhold til artikel 12. 32 i EU-GDPR og gør det i overensstemmelse med art.
30 (2) i GDPR, i det omfang dette er påkrævet ved lov.

5.3 Hvis databehandleren er forpligtet til at udpege en databeskyttelsesrådgiver i henhold til EU's GDPR eller andre lovbestemmelser, bekræfter databehandleren, at denne har udvalgt en sådan person i overensstemmelse med lovbestemmelserne, og forsikrer klienten om, at databehandleren vil underrettes om denne person med angivelse af dennes kontaktoplysninger (f.eks. via e-mail). Enhver ændring af person- og/eller kontaktoplysningerne for databeskyttelsesrådgiveren skal straks meddeles klienten.

5.4 Databehandling uden for databehandlerens eller dens lokaler
Underleverandører og/eller i private hjem (f.eks. fjernadgang eller databehandlerens hjemmekontor) er kun tilladt med klientens udtrykkelige samtykke.

5.5 Databehandleren skal sikre, at de personer, der er bemyndiget til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovpligtig fortrolighedsforpligtelse (artikel 28 (3) (b) i EU's GDPR). Før de berørte personer har påtaget sig tavshedspligten, må de ikke gives adgang til de personoplysninger, som klienten har oplyst.

5.6 Databehandleren vil regelmæssigt og uafhængigt overvåge opfyldelsen af sine forpligtelser og dokumentere dette på passende måde.

6. Tekniske og organisatoriske foranstaltninger

6.1 Databehandleren har etableret passende tekniske og organisatoriske foranstaltninger for at sikre et tilstrækkeligt beskyttelsesniveau og har registreret disse i bilag 2 til denne aftale. De der beskrevne foranstaltninger blev udvalgt i overensstemmelse med kravene i art. 32 EU GDPR og aftalt med klienten.

6.2 Databehandleren vil løbende og/eller efter behov gennemgå og tilpasse de tekniske og organisatoriske foranstaltninger. Eventuelle nødvendige justeringer vil blive dokumenteret af databehandleren og stillet til rådighed for klienten efter anmodning. Væsentlige ændringer, der kan reducere beskyttelsesniveauet, skal aftales med klienten på forhånd.

6.3 Databehandleren skal, når det er relevant, men mindst én gang årligt, foretage en gennemgang, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger, der skal sikre behandlingssikkerheden (artikel 32 (1) (d) i EU's GDPR). Resultaterne, herunder den komplette revisionsrapport, skal meddeles klienten.

7. Databehandlerens supportforpligtelser

7.1 Databehandleren vil informere klienten i overensstemmelse med art. 28 stk. 3 tændte. e EUDSGVO i sine forpligtelser til at beskytte registreredes rettigheder i henhold til kapitel III, artikel 12-22 i EUDSGVO. Dette gælder især for videregivelse af oplysninger og sletning, berigtigelse eller begrænsning af personoplysninger. Omfanget af forpligtelsen til at yde støtte fastsættes i hvert enkelt tilfælde under hensyntagen til behandlingstypen.

7.2 Databehandleren vil også informere klienten i overensstemmelse med art. 28 stk. 3 tændte. ff EUDSGVO i sine forpligtelser i henhold til art. 32 – 36 EU-DSGVO (især rapporteringsforpligtelser). Omfanget af denne forpligtelse til at yde bistand fastsættes i hvert enkelt tilfælde under hensyntagen til typen af behandling og de oplysninger, der er tilgængelige for databehandleren.

8. **Brug af underleverandører**

8.1 Databehandleren er kun bemyndiget til at anvende underleverandører med klientens samtykke. Hvis Databehandleren har til hensigt at anvende yderligere underleverandører (se bilag 1), vil Databehandleren underrette Kunden skriftligt eller elektronisk, så Kunden kan gennemgå deres anvendelse. Hvis klienten ikke giver sit samtykke, må de pågældende underleverandører ikke anvendes.

8.2 Underleverandører udvælges af databehandleren i overensstemmelse med juridiske og kontraktlige krav. Supplerende tjenester, der anvendes af databehandleren til at udføre sine forretningsaktiviteter, udgør ikke underleverandørforhold. Tillægstjenester i denne forstand omfatter især telekommunikationstjenester uden en specifik forbindelse til hovedtjenesten, post- og transporttjenester, vedligeholdelses- og brugerservice samt andre foranstaltninger, der har til formål at sikre hardwarens og softwarens fortrolighed og integritet, og som ikke har nogen specifik forbindelse til hovedtjenesten. Databehandleren vil dog også sikre overholdelse af lovpligtige databeskyttelsesstandarder for disse tredjepartstjenester.

8.3 Alle kontrakter mellem databehandleren og underdatabehandleren (underleverandørkontrakter) skal overholde kravene i denne kontrakt og de lovmæssige bestemmelser om behandling af personoplysninger på databehandlerens vegne; Dette vedrører især implementeringen af passende tekniske og organisatoriske foranstaltninger i overensstemmelse med art. 32 EU GDPR i forbindelse med driften af underleverandør. Underleverandøraftalerne skal også sikre, at de kontrol- og instruktionsbeføjelser, der er aftalt i denne kontrakt, kan udøves af klienten på samme måde og i fuldt omfang over for underleverandøren. Hvis Kunden anmoder om det, er Databehandleren forpligtet til at give oplysninger om underleverandørens forpligtelser i henhold til databeskyttelseslovgivningen og om nødvendigt at inspicere de relevante kontraktdokumenter eller kontrol- og tilsynsresultater samt Databehandlerens relevante dokumentation, optegnelser og registre eller at anmode om en kopi af disse dokumenter.

8.4 Kontrakten med underleverandøren skal specificere underleverandørens ansvarsområder, så klienten kan gennemgå dem i overensstemmelse hermed. Desuden skal kontrakten med underleverandøren sikre, at klienten ... underleverandøren udøver de samme kontrolrettigheder som over for . databehandleren har ret til. Databehandleren skal sikre, at de instruktioner, som klienten giver, også følges og registreres af underleverandørerne. Overholdelsen af disse forpligtelser vil blive overvåget og dokumenteret af databehandleren inden indgåelse af kontrakten med underleverandøren og derefter regelmæssigt.

8.5 har opfyldt sine forpligtelser i henhold til art. 32 (4) og artikel 32 (4) 29 EUDSGVO . personerne under hans kommando.

8.6 Databehandleren er ansvarlig for at sikre, at de underdatabehandlere, som denne anvender, overholder databeskyttelsesreglerne. Han er ansvarlig for . klienten for overholdelse af juridiske og kontraktlige databeskyttelsesforpligtelser.

8.7 Databehandleren skal indhente bekræftelse fra sine underdatabehandlere på, at de har udpeget en databeskyttelsesrådgiver, hvor det er påkrævet ved lov.

8.8 Brug af underleverandører i tredjelande er kun tilladt, hvis de juridiske krav i artikel 44-50 i EU's GDPR er opfyldt, og klienten har givet samtykke.

9. Databehandlerens underretningsforpligtelser

9.1 Overtrædelser af denne kontrakt, af klientens instruktioner eller af andre databeskyttelsesbestemmelser skal straks rapporteres til klienten; Det samme gælder, hvis der er en tilsvarende velbegrundet mistanke. Denne forpligtelse gælder uanset om bruddet blev begået af databehandleren selv, en person ansat af denne, en underdatabehandler eller enhver anden person, som denne har engageret til at opfylde sine kontraktlige forpligtelser.

9.2 Databehandleren er forpligtet til at bistå klienten med at opfylde dennes lovpligtige informationsforpligtelser i henhold til artikel 33 og 34 i EU's GDPR. Databehandleren må kun foretage uafhængige underretninger til myndigheder eller registrerede i henhold til artikel 33 og 34 i EU's GDPR efter forudgående instruktioner fra klienten.

9.3 Hvis en registreret, en myndighed eller en anden tredjepart anmoder databehandleren om oplysninger, rettelse, blokering eller sletning, vil databehandleren straks videresende anmodningen til klienten; Databehandleren vil under ingen omstændigheder efterkomme den registreredes anmodning uden den dataansvarliges samtykke.

9.4 Databehandleren vil straks underrette klienten, hvis tilsynsforanstaltninger eller andre foranstaltninger fra en myndighed er forestående, som også kan påvirke behandlingen, brugen eller indsamlingen af de personoplysninger, som klienten har leveret. Derudover skal databehandleren straks underrette klienten om enhver begivenhed eller handling fra tredjeparter, der kan bringe de data, der er omfattet af kontrakten, i fare eller forringe dem.

10. Opsigelse af kontrakt, sletning og returnering af data

10.1 Der vil ikke blive lavet kopier eller dubletter af dataene uden klientens viden. Undtaget herfra er sikkerhedskopier, i det omfang de er nødvendige for at sikre korrekt databehandling, samt data, der er nødvendige for at overholde lovpligtige opbevaringsfrister.

10.2 Ved afslutningen af det kontraktligt aftalte arbejde eller tidligere efter anmodning fra klienten – senest ved ophør af serviceaftalen – skal leverandøren overdrage alle dokumenter, oprettede behandlings- og brugsresultater og datasæt relateret til kontraktforholdet, som er kommet i klientens besiddelse, eller med forudgående samtykke destruere dem i overensstemmelse med databeskyttelsesbestemmelserne. Det samme gælder for test- og kasseringsmateriale. Sletningsprotokollen skal fremvises på anmodning.

10.3 Dokumentation, der tjener som bevis for den ordnede og korrekte databehandling, skal opbevares af Leverandøren efter kontraktens udløb i overensstemmelse med de respektive opbevaringsperioder. Han kan overdrage dem til klienten ved kontraktens udløb for at fritage sig selv for ansvar.

11. Datahemmelighed og fortrolighed

11.1 Databehandleren er forpligtet til på ubestemt tid og ud over udløbet af denne kontrakt at behandle de personoplysninger, der indhentes inden for rammerne af dette kontraktforhold, fortroligt og til at overholde de relevante regler om tavshedspligt, som klienten er underlagt (f.eks. § 203 i den tyske straffelov). Klienten er forpligtet til at informere databehandleren om enhver evt.
at påpege eksisterende særlige regler om beskyttelse af tavshedspligt.

11.2 Databehandleren forpligter sig til at gøre sine medarbejdere bekendt med de relevante databeskyttelsesbestemmelser og fortrolighedsregler og forpligte dem til at opretholde fortrolighed, inden de påbegynder deres arbejde for databehandleren.

11.3 Databehandleren skal dokumentere overholdelsen af de i dette afsnit omhandlede foranstaltninger på passende måde. Dokumentationen skal forevises klienten efter anmodning.

Endelige bestemmelser

11.4 Ændringer til denne kontrakt og tilhørende aftaler skal foretages skriftligt eller elektronisk og skal tydeligt angive, at de har til formål at ændre eller supplere disse vilkår og betingelser, og hvilke ændringer eller tilføjelser de indeholder.

11.5 Hvis EU's GDPR eller andre nævnte lovbestemmelser ændres i løbet af kontraktperioden, gælder henvisningerne her også for de respektive efterfølgende bestemmelser.

11.6 Hvis enkelte dele af denne aftale er eller bliver ugyldige, forbliver gyldigheden af de resterende bestemmelser uændret.

11.7 Alle bilag til denne kontrakt er en del af kontrakten.

Bilag 1 – Ordreoplysninger

Denne kontrakt omfatter (hvis relevant i forbindelse med hovedkontrakten) følgende ydelser:

Databehandleren leverer og driver mobile overvågningsløsninger (VIDEO GUARD) til klienten. Disse mobile overvågningssystemer overvåger adgang til klientens private lokaler. Hvis der opstår en alarm inden for den overvågningstid, der er aftalt med Kunden, dvs. generelt uden for arbejdstiden, skal Databehandleren verificere alarmen og træffe de foranstaltninger, der på forhånd er aftalt med Kunden. Afhængigt af den involverede fare kan et videoklip af alarmen stilles til rådighed for klienten før eller efter hændelsen. Videobillederne slettes eller overskrives automatisk efter en lagringsperiode på maksimalt 7 dage.

Følgende typer data behandles regelmæssigt inden for rammerne af kontraktlig levering af tjenester:

1. Identifikationsoplysninger: Navn, adresse, telefonnummer, e-mailadresse, erhverv/virksomhed,
   Kontraktdata, kundenummer
2. Faktureringsdata: bankoplysninger, tilbudsdata, kontakthistorik
3. Sikkerhedsdata: Videoovervågning

Den persongruppe, der er berørt af databehandling, er:

1. Især kundens medarbejdere og eksterne
   Kontaktperson.
2. Især kundens virksomhedsdata.
3. Alle besøgende i det overvågede område (videodata)

Adgang til de pågældende data sker på følgende måde:

De berørte data tilgås via et sikkert mobilnetværk af det interne kontrolcenter. Klienten vil blive informeret telefonisk.

Følgende underleverandører vil blive brugt til at evaluere videodataene og igangsætte de interventioner, der er aftalt med klienten:

Virksomhedens underleverandør	Adresse/Land	Præstation
International Security GmbH	Wehrden Ost 5, 26835 Hesel	Levering af VIDEO Guard-infrastrukturen, herunder kontrolcentertjenester
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen	Serverhosting
Bosch Security Systems GmbH	Großhandelsring 3 49084 Osnabrück	Serverhosting / cloud

Bilag 2 – Liste over eksisterende tekniske og organisatoriske foranstaltninger (TOM) for underdatabehandleren (International Security GmbH) i henhold til art. 32 EU GDPR

Databehandleren implementerer følgende tekniske og organisatoriske foranstaltninger for at beskytte de personoplysninger, der er omfattet af kontrakten. Foranstaltningerne blev defineret i overensstemmelse med art. 32 EU GDPR og aftalt med klienten.

I. Formålsbegrænsning og adskillelse

Følgende foranstaltninger sikrer, at data indsamlet til forskellige formål behandles separat:

☑ fysisk separat lagring på separate systemer eller databærere
☑ Logisk klientseparation (softwareside)
☑ Autorisationskoncept
☑ Kryptering af dataposter behandlet til samme formål
☑ Forsyning af dataposterne med formålsattributter / datafelter / signaturer
☑ For pseudonymiserede data: adskillelse af tildelingsfilen og lagring på et separat og sikkert IT-system
☑ Adskillelse af produktions- og testsystemer

II. Fortrolighed og integritet

Følgende foranstaltninger sikrer fortroligheden og integriteten af databehandlerens systemer:

1. Kryptering

De data eller databærere, der behandles på kundens vegne, krypteres som følger:

☑ End -to -end-kryptering ved overførsel af videofiler til klienten

2. Pseudonymisering

"Pseudonymisering" betyder, at personoplysninger behandles på en måde, der udelukker identifikation af den registrerede uden brug af yderligere oplysninger (f.eks. brug af fiktive navne, der ikke kan henføres til en bestemt person uden yderligere oplysninger).

☑ Ja, på følgende måde:

Kunder pseudonymiseres med kundenumre, byggepladser med projektnumre og videodata med kameranumre. Tydelig adskillelse af videodata og personlige data.

3. Adgangskontrol

Følgende foranstaltninger er truffet for at forhindre uautoriserede personer i at få adgang til de databehandlingssystemer, der anvendes til at behandle eller bruge personoplysninger:

☑ alarmsystem
☑ Sikring af bygningsskakte
☑ Automatisk adgangskontrolsystem
☑ Chipkort/transponder-låsesystem
☑ Manuelt låsesystem
☑ Videoovervågning af indgangene
☑ Lysbarrierer / bevægelsesdetektorer
☑ Sikkerhedslåse
☑ Nøgleregulering (nøglefordeling osv.)
☑ Omhyggelig udvælgelse af rengøringspersonale
☑ Omhyggelig udvælgelse af sikkerhedspersonale
☑ Adgangskoncept / besøgsregler

4. Adgangskontrol

Følgende foranstaltninger er truffet for at forhindre uautoriserede tredjeparters brug af datasystemerne:

☑ Tildeling af brugerrettigheder
☑ Oprettelse af brugerprofiler
☑ Tildeling af adgangskode
☑ Adgangskodepolitikker (regelmæssige ændringer, minimumslængde, kompleksitet osv.)
☑ Godkendelse med brugernavn/adgangskode
☑ Tildeling af brugerprofiler til IT-systemer
☑ Huslåse
☑ Brug af VPN-teknologi til dataoverførsel
☑ Kryptering af mobile IT-systemer
☑ Brug af antivirussoftware
☑ Kryptering af datalagringsenheder i bærbare computere/notebooks
☑ Brug af en hardwarefirewall
☑ Brug af en softwarefirewall

5. Adgangskontrol

Følgende foranstaltninger er truffet for at sikre, at personer, der er autoriseret til at bruge et databehandlingssystem, kun kan tilgå de data, der er omfattet af deres adgangstilladelse, og at personoplysninger ikke kan læses, kopieres, ændres eller fjernes uden tilladelse under behandling, brug og efter opbevaring:
☑ Autorisationskoncept
☑ Administration af rettigheder af systemadministrator
☑ Regelmæssig gennemgang og opdatering af adgangsrettigheder (især når medarbejdere fratræder osv.)
☑ Antallet af administratorer er reduceret til et "absolut minimum"
☑ Adgangskodepolitik inklusive adgangskodelængde, ændring af adgangskode
☑ Logføring af adgang til applikationer, især ved indtastning, ændring og sletning af data
☑ Sikker opbevaring af datamedier
☑ fysisk sletning af databærere før genbrug
☑ Korrekt destruktion af datamedier (DIN 66399)
☑ Brug af dokumentmakulatorer eller tjenesteudbydere (hvis muligt med et databeskyttelsesstempel)
☑ Logføring af ødelæggelse
☑ Kryptering af databærere

6. Indgangskontrol

Følgende foranstaltninger kan anvendes til efterfølgende at kontrollere og fastslå, om og af hvem personoplysninger er blevet indtastet, ændret eller fjernet fra databehandlingssystemer:

☑ Logføring af dataindtastning, ændring og sletning
☑ Lav en oversigt over, hvilke applikationer der kan bruges til at indtaste, ændre og slette hvilke data.
☑ Sporbarhed af indtastning, ændring og sletning af data af enkeltpersoner
Brugernavne (ikke brugergrupper)
☑ Opbevaring af formularer, hvorfra data er overført til automatisk behandling
☑ Tildeling af rettigheder til at indtaste, ændre og slette data baseret på et autorisationskoncept

7. Ordrekontrol

Følgende foranstaltninger sikrer, at personoplysninger, der behandles på klientens vegne, kun kan behandles i overensstemmelse med klientens instruktioner:

☑ Udvælgelse af databehandler under hensyntagen til due diligence (især med hensyn til datasikkerhed)
☑ forudgående gennemgang og dokumentation af de sikkerhedsforanstaltninger, som databehandleren har truffet
☑ skriftlige instruktioner til databehandleren (f.eks. gennem en databehandleraftale)
☑ Forpligtelse for databehandlerens medarbejdere til at opretholde datahemmelighed
☑ Databehandleren har udpeget en databeskyttelsesrådgiver
☑ Sikring af destruktion af data efter kontraktens afslutning
☑ Effektive kontrolrettigheder aftalt med databehandleren
☑ løbende gennemgang af databehandleren og dens aktiviteter
☑ Kontraktlige sanktioner for overtrædelser

8. Transport og overførselskontrol

Følgende foranstaltninger sikrer, at personoplysninger ikke kan tilgås eller ses af uautoriserede personer, når de videregives (fysisk og/eller digitalt):

☑ Brug af VPN-tunneler

Tredje. Systemers tilgængelighed, genoprettelsesevne og robusthed

Følgende foranstaltninger sikrer, at de anvendte databehandlingssystemer til enhver tid fungerer korrekt, og at personoplysninger er beskyttet mod utilsigtet ødelæggelse eller tab:

☑ Uafbrydelig strømforsyning (UPS)
☑ Aircondition i serverrummene
☑ Enheder til overvågning af temperatur og luftfugtighed i serverrum
☑ Beskyttende strømskinner i serverrum
☑ Brand- og røgdetekteringssystemer i serverrum
☑ Brandslukkere i serverrum
☑ Alarmmeddelelse i tilfælde af uautoriseret adgang til serverrum
☑ for backup og gendannelse
☑ Etableret beredskabsplan
☑ Opbevaring af databackups på et sikkert sted

IV. Særlige databeskyttelsesforanstaltninger

Følgende er tilgængelige skriftligt:

☑ interne adfærdsregler for medarbejdere
☑ Udnævnelse af en ekstern databeskyttelsesrådgiver

V. Gennemgang, evaluering og tilpasning af de nuværende foranstaltninger

Databehandleren vil, med inddragelse af databeskyttelsesrådgiveren, gennemgå, evaluere og om nødvendigt tilpasse de tekniske og organisatoriske foranstaltninger, der er fastsat i dette bilag, hver 12. måned og efter behov.

Bilag 3 - Databeskyttelsesmeddelelse for videoovervågning

1. Klienten skal informere berørte personer med et databeskyttelsesmæssigt skilt, inden vedkommende går ind i det område, der skal overvåges. (Banner til byggepladshegn / Information om artikel 13)

   Den maksimale opbevaringsperiode for videodata er, efter samråd med klienten: 7 dage

2. I henhold til art. I henhold til artikel 12 (7) i GDPR skal de nødvendige oplysninger på skiltet præsenteres i en letforståelig, letforståelig og klart forståelig form. De giver et databeskyttelsesmæssigt overblik over den påtænkte behandling dataene.

3. Klienten vil give oplysninger om videoovervågning på baggrund af EU's GDPR i et separat informationsark. Med denne forordning og kravene i artikel 12 ff. i EU's GDPR opfylder klienten sine gennemsigtighedsforpligtelser over for de registrerede.

4. Den registrerede har ret til at få fra den dataansvarlige bekræftelse af, om personoplysninger vedrørende dem data behandles; Hvis dette er tilfældet, har hun ret til at Oplysninger om disse personoplysninger og de rettigheder, der er nævnt i art. 15 Detaljeret information om EU's GDPR.

5. Den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. personoplysninger og, om nødvendigt, udfyldelsen at anmode om berigtigelse af ufuldstændige personoplysninger (artikel 16 i EU GDPR).

6. Den registrerede har ret til at få fra den dataansvarlige anmode om, at personoplysninger vedrørende dem slettes øjeblikkeligt slettes, hvis en af
   i art. 17 EU GDPR i detaljer de anførte grunde gælder, f.eks. B. hvis dataene for den sporede formål ikke længere er påkrævet (ret til sletning).

7. Den registrerede har ret til at indhente fra den dataansvarlige At anmode om begrænsning af behandling, hvis en af betingelserne i art. 18 EU GDPR er opfyldt, f.eks. B. hvis den registrerede har gjort indsigelse mod behandlingen, så længe den dataansvarlige gennemgår den.

8. Den registrerede har ret til, af grunde, der vedrører hans eller hendes i den specifikke situation, til enhver tid gøre indsigelse mod behandlingen at gøre indsigelse mod behandlingen af de pågældende personoplysninger. De Den dataansvarlige vil derefter ikke behandle personoplysningerne mere, medmindre han kan påvise tvingende legitime grunde til det behandling, der tilsidesætter den pågældendes interesser, rettigheder og friheder den registrerede vejer tungere end den registreredes legitime interesser, eller behandlingen tjener Påstand, udøvelse eller forsvar af retskrav (Artikel 21 i EU's persondataforordning).

9. Enhver registreret person skal, uden at det berører andre bestemmelser administrativ eller retslig klage, retten til Klage til en tilsynsmyndighed, hvis den registrerede gør indsigelse mod Det er opfattelsen, at behandlingen af personoplysninger vedrørende dem er i strid med EU's GDPR (artikel 77 i EU's GDPR). De Den registrerede kan udøve denne ret hos en tilsynsmyndighed i Medlemsstat, hvor de har bopæl, arbejdssted eller arbejdssted af den påståede overtrædelse.

10. I Danmark er den kompetente tilsynsmyndighed:

Databeskyttelsesagenturet
Carl Jacobsens Vej 35
DK-2500 Valby

Telefon: +45 3319 3200

E-mail: dt@datatilsynet.dk

Bilag 4 - Kontaktperson

kontaktperson

Databeskyttelsesrådgiver/kontaktperson hos entreprenøren
Name: Secom It GmbH, Nienburger Straße 9a, 27232 Sulingen
Tel.: +49 4271 94 73 800
Email: datenschutz@videoguard24.de

Databeskyttelsesrådgiver/klientens kontaktperson
Navn, telefon, e-mail : se alarmplan

Klientens autoriserede personer
Navn, telefon, e-mail : se hovedkontrakt og alarmplan

Vereinbarung zur Auftragsverarbeitung

(gemäß EU-DSGVO Art. 28)

zwischen

dem Mieter der Videoüberwachungslösung aus dem Hauptvertrag

\- - im Folgenden: Auftraggeber –

und

der VIDEO GUARD ApS, Tagholm 2, 9400 Nørresundby

- im Folgenden: Auftragsverarbeiter (nach Art. 28 EU-DSGVO) –

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 EU-DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind der Anlage 1 zu entnehmen.

1.2 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der EU-DSGVO (Art. 44 - 50) und mit vorheriger Zustimmung des Auftraggebers.

1.3 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der Laufzeit des vorliegenden Vertrag richtet sich nach der Laufzeit des Hauptvertrages. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert

anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

3.5 Weisungsberechtigte werden in Anlage 4 des Vertrages benannt.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/-systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 EU-DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren und das nach Art.

30 Abs. 2 EU-DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3 Sofern der Auftragsverarbeiter nach der EU-DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b EU-DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 EU-DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen ständig und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

6.3 Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d EU-DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e EUDSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 EUDSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. ff EUDSGVO bei dessen Pflichten nach Art. 32 – 36 EU-DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer (Siehe Anlage 1), wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 EU-DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und Art. 29 EUDSGVO ggü. den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 - 50 EU-DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 EU-DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 EU-DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und die einschlägigen Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf die ggf.
bestehenden besonderen Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

Schlussbestimmungen

11.4 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

11.5 Sollte sich die EU-DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

11.6 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

11.7 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Der Auftragsverarbeiter stellt dem Auftraggeber mobile Überwachungslösungen (VIDEO GUARD) zur Verfügung und betreibt diese. Diese mobilen Überwachungssysteme überwachen den Zutritt auf die privaten Gelände des Auftraggebers. Sollte es während der mit dem Auftraggeber vereinbarten Überwachungszeit, d.h. generell außerhalb der Arbeitszeiten, zu einem Alarm kommen, so verifiziert der Auftragsverarbeiter den Alarm und ergreift die vorher mit dem Auftraggeber abgestimmten Maßnahmen. Dem Auftraggeber kann je nach vorliegender Gefahr zuvor oder danach ein Videoclip des Alarms zur Verfügung gestellt werden. Die Videobilder werden nach einer Speicherungsdauer von maximal 7 Tagen automatisiert gelöscht bzw. überschrieben.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

1. Identifikationsdaten: Name, Anschrift, Telefonnummer, Emailadresse, Beruf/Firma, Vertragsdaten, Kundennummer
2. Abrechnungsdaten: Bankverbindung, Angebotsdaten, Kontakthistorie
3. Sicherheitsdaten: Videoüberwachung

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

1. Insbesondere Mitarbeiter des Auftraggebers und von diesem mitgeteilte externe Ansprechpartner.
2. Insbesondere Firmendaten des Auftraggebers.
3. Alle Besucher des überwachten Bereichs (Videodaten)

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

Der Zugriff der betroffenen Daten erfolgt über ein gesichertes Mobilfunknetz durch die hauseigene Leitstelle. Die Information des Auftraggebers erfolgt per Telefon.

Folgende Subunternehmer werden zur Auswertung der Videodaten und Einleitung der mit dem Auftraggeber vereinbarten Interventionen eingesetzt:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
International Security GmbH	Wehrden Ost 5, 26835 Hesel	Bereitstellung der VIDEO Guard Infrastruktur inkl. Leitstellendienstleistung
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen	Serverhosting
Bosch Sicherheitssysteme GmbH	Großhandelsring 3 49084 Osnabrück	Serverhosting /Cloud

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen (TOM) des Unter-Auftragsverarbeiters (International Security GmbH) nach Art. 32 EU-DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 EU-DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- ☑ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☑ Logische Mandantentrennung (softwareseitig)
- ☑ Berechtigungskonzept
- ☑ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☑ Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- ☑ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
- ☑ Trennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

☑ End-to-End-Verschlüsselung bei der Weitergabe von Videodateien an den Auftraggeber

2. Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

☑ Ja, und zwar in folgender Art und Weise:

Kunden werden mit Kundennummern, Baustellen mit Projektnummern und Videodaten mit Kameranummern pseudonymisiert. Klare Trennung von Videodaten und personenbezogenen Daten.

3. Zutrittskontrolle

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

☑ Alarmanlage
☑ Absicherung von Gebäudeschächten
☑ Automatisches Zugangskontrollsystem
☑ Chipkarten-/Transponder-Schließsystem
☑ Manuelles Schließsystem
☑ Videoüberwachung der Zugänge
☑ Lichtschranken / Bewegungsmelder
☑ Sicherheitsschlösser
☑ Schlüsselregelung (Schlüsselausgabe etc.)
☑ Sorgfältige Auswahl von Reinigungspersonal
☑ Sorgfältige Auswahl von Wachpersonal
☑ Zutrittskonzept / Besucherregelung

4. Zugangskontrolle

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

☑ Zuordnung von Benutzerrechten
☑ Erstellen von Benutzerprofilen
☑ Passwortvergabe
☑ Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
☑ Authentifikation mit Benutzername / Passwort
☑ Zuordnung von Benutzerprofilen zu IT-Systemen
☑ Gehäuseverriegelungen
☑ Einsatz von VPN-Technologie bei der Übertragung von Daten
☑ Verschlüsselung mobiler IT-Systeme
☑ Einsatz von Anti-Viren-Software
☑ Verschlüsselung von Datenträgern in Laptops / Notebooks
☑ Einsatz einer Hardware-Firewall
☑ Einsatz einer Software-Firewall

5. Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

☑ Berechtigungskonzept
☑ Verwaltung der Rechte durch Systemadministrator
☑ regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. Bei Ausscheiden von Mitarbeitern o.Ä.)
☑ Anzahl der Administratoren ist auf das „Notwendigste“ reduziert
☑ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

- ☑ Sichere Aufbewahrung von Datenträgern
- ☑ physische Löschung von Datenträgern vor Wiederverwendung
- ☑ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☑ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☑ Protokollierung der Vernichtung
- ☑ Verschlüsselung von Datenträgern

6. Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- ☑ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☑ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7. Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- ☑ Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☑ vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☑ schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- ☑ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- ☑ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- ☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☑ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☑ laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten
- ☑ Vertragsstrafen bei Verstößen

8. Transport- bzw. Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

- ☑ Einsatz von VPN-Tunneln

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- ☑ Unterbrechungsfreie Stromversorgung (USV)
- ☑ Klimatisierung der Serverräume
- ☑ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☑ Schutzsteckdosenleisten in Serverräumen
- ☑ Feuer- und Rauchmeldeanlagen in Serverräumen
- ☑ Feuerlöschgeräte in Serverräumen
- ☑ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☑ Backup- & Recoverykonzept
- ☑ Etablierter Notfallplans
- ☑ Aufbewahrung von Datensicherung an einem sicheren Ort

IV. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

- ☑ interne Verhaltensregeln für Mitarbeiter
- ☑ Benennung eines externen Datenschutzbeauftragten

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter unter Einbeziehung des Datenschutzbeauftragten wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 - Hinweis zum Datenschutz Videoüberwachung

1. Der Auftraggeber informiert betroffene Personen mit einem datenschutzkonformen Hinweisschild vor Betreten des zu überwachenden Bereichs. (Baustellenzaunbanner / Art. 13 Information)

   Die maximale Speicherdauer der Videodaten beträgt nach Absprache mit dem Auftraggeber: 7 Tage

2. Die notwendigen Informationen auf dem Hinweisschild sind nach Art. 12 Abs. 7 DSGVO in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form aufzuführen. Sie vermitteln einen datenschutzkonformen Überblick über die beabsichtigte Verarbeitung der Daten.

3. Mit einem gesonderten Hinweisblatt informieren der Auftraggeber über die Videoüberwachung auf der Grundlage der EU-DSGVO. Mit dieser Regelung sowie den sich aus Artikel 12 ff. EU-DSGVO ergebenden Anforderungen erfüllt der Auftraggeber seine Transparenzpflichten gegenüber betroffenen Personen.

4. Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 EU-DSGVO im einzelnen aufgeführten Informationen.

5. Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender, unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (Art. 16 EU-DSGVO).

6. Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 EU-DSGVO im Einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (Recht auf Löschung).

7. Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 EU-DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

8. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 EUDSGVO).

9. Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die EU-DSGVO verstößt (Art. 77 EU-

DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen.

10. In Dänemark ist die zuständige Aufsichtsbehörde:

Datatilsynet
Carl Jacobsens Vej 35
DK-2500 Valby

Telefon: +45 3319 3200

E-Mail: dt@datatilsynet.dk

Anlage 4- Ansprechpartner

Ansprechpartner

Datenschutzbeauftragter/-ansprechpartner des Auftragnehmers
Name: Secom It GmbH, Nienburger Straße 9a, 27232 Sulingen
Phone: +49 4271 94 73 800
Email: datenschutz@videoguard24.de

Datenschutzbeauftragter/-ansprechpartner des Auftraggebers
Name, Telefon, eMail : siehe Alarmplan

Weisungsbefugte des Auftraggebers
Name, Telefon, eMail : siehe Hauptvertrag und Alarmplan