

Avtal om orderhantering

(i enlighet med EU:s dataskyddsförordning art. 28)

mellan

hyresgästen för videoövervakningslösningen från huvudavtalet

- - i följande: Klient

och

of International Security GmbH, Wehrden Ost 5, 26835 Hesel, Germany

- i följande fall: Personuppgiftsbiträde (enligt art. 28 EU GDPR) -

1. Allmänna bestämmelser och föremålet för beslutet

- 1.1 Föremålet för detta avtal är behandling av personuppgifter för personuppgiftsbitrådets räkning (artikel 28 i EU:s dataskyddsförordning). Innehållet i beställningen, kategorier av registrerade och typer av uppgifter samt syftet med avtalet finns i bilaga 1.
- 1.2 Personuppgiftsbitrådets behandling av uppgifterna sker uteslutande inom Förbundsrepubliken Tysklands territorium, en medlemsstat i Europeiska unionen eller en avtalsslutande stat i EES-avtalet. Behandling utanför dessa länder sker endast under de förutsättningar som anges i kapitel 5 i EU:s dataskyddsförordning (art. 44-50) och med kundens förhandsgodkännande.
- 1.3 Ersättningen ska överenskommas utanför detta avtal.

2. Avtalstid och uppsägning

Detta avtals giltighetstid baseras på huvudavtalets giltighetstid. Rätten till extraordinär uppsägning av goda skäl förblir oförändrad.

3. Instruktioner från uppdragsgivaren

- 3.1 Kunden har en omfattande rätt att ge instruktioner till personuppgiftsbiträdet om typ, omfattning och villkor för databehandlingen. I denna roll kan den i synnerhet kräva omedelbar radering, korrigering, blockering eller överlämnande av avtalsuppgifterna. Personuppgiftsbiträdet är skyldigt att följa kundens instruktioner, förutsatt att det inte finns några legitima avtalsmässiga eller rättsliga intressen som talar emot detta.
- 3.2 Personuppgiftsbiträdet ska omedelbart informera Kunden om det anser att en instruktion från Kunden strider mot lagbestämmelser. Om en instruktion utfärdas vars laglighet styrks av Personuppgiftsbiträdet, ska Personuppgiftsbiträdet ha rätt att tillfälligt avbryta dess utförande till dess att Uppdragsgivaren uttryckligen bekräftar eller ändrar den igen.

- 3.3 Instruktioner ska alltid lämnas skriftligen eller i elektroniskt format (t.ex. via e-post). Muntliga instruktioner måste bekräftas skriftligen eller i elektroniskt format av Kunden på begäran av Personuppgiftsbiträdet. Personuppgiftsbiträdet ska registrera personen, datumet och tiden för den muntliga instruktionen i ett lämpligt formulär.
- 3.4 Kunden ska på begäran av Personuppgiftsbiträdet utse en eller flera personer med rätt att utfärda instruktioner. Personuppgiftsbiträdet ska utan dröjsmål informeras om eventuella ändringar.
- 3.5 Behöriga instruktörer anges i bilaga 4 till avtalet.

4. Kontroll av klientens behörigheter

- 4.1 Kunden har rätt att i nödvändig utsträckning regelbundet kontrollera efterlevnaden av lagstadgade och avtalsenliga bestämmelser om dataskydd och datasäkerhet innan databehandlingen påbörjas och under avtalets löptid, eller att låta tredje part kontrollera detta. Personuppgiftsbiträdet ska tolerera dessa kontroller och stödja dem i den utsträckning som krävs. I synnerhet ska denne lämna fullständig och sanningsenlig information till Kunden som är relevant för kontrollerna, ge Kunden tillgång till lagrade uppgifter och databehandlingsprogram/-system samt möjliggöra kontroller på plats. Om Kunden har samtyckt till behandling av uppgifter utanför verksamhetslokalerna (t.ex. privatbostad) ska Personuppgiftsbiträdet se till att Kunden även får tillträde till dessa lokaler för kontrolländamål.
- 4.2 Kunden måste se till att kontrollåtgärderna är proportionerliga och inte försämrar personuppgiftsbitrådets verksamhet mer än nödvändigt. I synnerhet ska inspektioner på plats i allmänhet utföras under normal arbetstid och efter överenskommelse med rimlig framförhållning, förutsatt att syftet med inspektionen inte strider mot förhandsanmälan.
- 4.3 Resultatet av kontrollerna och instruktionerna ska registreras av båda avtalsparterna på lämpligt sätt.

5. Personuppgiftsbitrådets allmänna skyldigheter

- 5.1 Personuppgiftsbitrådets behandling av avtalsuppgifterna sker uteslutande på grundval av avtalsöverenskommelserna i samband med eventuella instruktioner från kunden. All behandling som avviker från detta är endast tillåten på grundval av tvingande europeisk lagstiftning eller medlemsstaternas lagstiftning (t.ex. vid utredningar av brottsbekämpande myndigheter eller statliga säkerhetsmyndigheter). Om behandling är nödvändig på grund av tvingande lagstiftning ska personuppgiftsbiträdet informera kunden om detta före behandlingen, såvida inte den aktuella lagstiftningen förbjuder ett sådant meddelande på grund av ett viktigt allmänintresse.
- 5.2 Personuppgiftsbiträdet måste följa alla lagstadgade bestämmelser vid fullgörandet av avtalet. I synnerhet måste det genomföra nödvändiga tekniska och organisatoriska åtgärder i enlighet med artikel 32 i GDPR och uppfylla de rättsliga krav som anges i artikel. 30 (2) EU GDPR, i den mån detta krävs enligt lag.
- 5.3 Om personuppgiftsbiträdet är skyldigt att utse ett dataskyddsombud i enlighet med EU:s dataskyddsförordning eller andra lagstadgade bestämmelser, bekräftar personuppgiftsbiträdet att det har valt ett sådant ombud i enlighet med de lagstadgade bestämmelserna och försäkrar kunden att det kommer att namnge dataskyddsombudet

och ange dess kontaktuppgifter (t.ex. via e-post). Kunden måste omedelbart informeras om eventuella ändringar av person och/eller kontaktuppgifter för dataskyddsombudet.

- 5.4 Databehandling utanför personuppgiftsbiträdets eller den personuppgiftsansvariges lokaler underleverantörer och/eller i privata bostäder (t.ex. fjärråtkomst eller hemmakontor för processorn) är endast tillåtet med kundens uttryckliga medgivande.
- 5.5 Personuppgiftsbiträdet måste se till att de personer som är behöriga att behandla personuppgifterna har förbundit sig till sekretess eller omfattas av en lämplig lagstadgad tystnadsplikt (artikel 28.3 b i GDPR). De berörda personerna får inte ges tillgång till de personuppgifter som tillhandahålls av kunden innan de omfattas av tystnadsplikten.
- 5.6 Personuppgiftsbiträdet ska regelbundet och oberoende övervaka fullgörandet av sina skyldigheter och dokumentera dem på lämpligt sätt.

6. Tekniska och organisatoriska åtgärder

- 6.1 Personuppgiftsbiträdet har definierat lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig skyddsnivå och har registrerat dessa i bilaga 2 till detta avtal. De åtgärder som beskrivs däri har valts i enlighet med kraven i artikel 32 i GDPR och överenskommit med kunden.
- 6.2 Personuppgiftsbiträdet ska se över och anpassa de tekniska och organisatoriska åtgärderna fortlöpande och/eller på ad hoc-basis. Eventuella nödvändiga justeringar ska dokumenteras av Personuppgiftsbiträdet och på begäran göras tillgängliga för Kunden. Väsentliga förändringar som kan minska skyddsnivån måste överenskommas med Kunden i förväg.
- 6.3 Personuppgiftsbiträdet måste genomföra en granskning, bedömning och utvärdering av effektiviteten hos de tekniska och organisatoriska åtgärderna för att säkerställa säkerheten vid behandlingen (artikel 32.1 d i EU:s dataskyddsförordning). Resultatet, inklusive en fullständig revisionsrapport, måste meddelas till kunden.

7. Bearbetningsföretagets supportskyldigheter

- 7.1 Personuppgiftsbiträdet ska i enlighet med artikel 28.3 e i GDPR stödja kunden i dennes skyldigheter att skydda de registrerades rättigheter enligt kapitel III, artiklarna 12-22 i GDPR. Detta gäller i synnerhet tillhandahållande av information och radering, rättelse eller begränsning av personuppgifter. Omfattningen av skyldigheten att tillhandahålla stöd bestäms från fall till fall med hänsyn till typen av behandling.
- 7.2 Personuppgiftsbiträdet ska också stödja kunden i enlighet med artikel 28.3 lit. ff EU GDPR i dess skyldigheter enligt artikel 32 - 36 EU GDPR (särskilt rapporteringsskyldigheter). Omfattningen av denna stödskyldighet ska fastställas från fall till fall, med hänsyn till typen av behandling och den information som är tillgänglig för personuppgiftsbiträdet.

8. Användning av bearbetningsföretag som anlitas av underleverantörer (underleverantörer)

- 8.1 Personuppgiftsbiträdet får endast anlita underbiträden (underleverantörer) med Kundens samtycke. Om Personuppgiftsbiträdet avser att anlita ytterligare underleverantörer (se bilaga 1) ska detta meddelas Kunden skriftligen eller elektroniskt så att Kunden kan kontrollera anlitandet. Om Kunden inte lämnar sitt samtycke får de aktuella underleverantörerna inte anlitas.
- 8.2 Underleverantörer väljs av personuppgiftsbiträdet i enlighet med rättsliga och avtalsenliga krav. Stödtjänster som personuppgiftsbiträdet använder för att utföra sin affärsverksamhet utgör inte underleverantörsrelationer. Stödtjänster i denna mening omfattar i synnerhet telekommunikationstjänster utan någon specifik koppling till huvudtjänsten, post- och transporttjänster, underhålls- och användartjänster samt andra åtgärder som syftar till att säkerställa konfidentialitet och integritet för hårdvara och programvara som inte har någon specifik koppling till huvudtjänsten. Personuppgiftsbiträdet ska emellertid också se till att de lagstadgade dataskyddsstandarderna för dessa tredjepartstjänster följs.
- 8.3 Alla avtal mellan personuppgiftsbiträden och underbiträden (underleverantörsavtal) måste uppfylla kraven i detta avtal och de lagstadgade bestämmelserna om behandling av personuppgifter för personuppgiftsbitrådets räkning; detta gäller särskilt genomförandet av lämpliga tekniska och organisatoriska åtgärder i enlighet med artikel 32 i EU:s allmänna dataskyddsförordning i underbitrådets verksamhet.
underleverantör. Underleverantörsavtalen ska även säkerställa att de kontroll- och instruktionsbefogenheter som avtalas i detta avtal även kan utövas av Uppdragsgivaren på samma sätt och i full utsträckning gentemot underbiträdet. Vid en motsvarande begäran från uppdragsgivaren ska personuppgiftsbiträdet vara skyldigt att tillhandahålla information om underleverantörens skyldigheter som är relevanta enligt dataskyddslagstiftningen och vid behov inspektera motsvarande avtalshandlingar eller kontroll- och övervakningsresultat samt motsvarande dokumentation, loggar och kataloger hos personuppgiftsbiträdet eller begära att kopior av dessa handlingar översänds.
- 8.4 I avtalet med underleverantören ska underleverantörens ansvar specificeras så att uppdragsgivaren kan kontrollera detta. Vidare ska det i avtalet med underleverantören säkerställas att uppdragsgivaren har rätt att utöva samma kontrollrättigheter gentemot underleverantören som gentemot personuppgiftsbiträdet. Personuppgiftsbiträdet måste se till att de instruktioner som utfärdas av kunden också följs och registreras av underleverantörerna. Efterlevnaden av dessa skyldigheter ska kontrolleras och dokumenteras av Personuppgiftsbiträdet innan avtalet med underleverantören ingås och därefter regelbundet.
- 8.5 Vidarebefordran av uppgifter till underleverantören är endast tillåten om underleverantören har uppfyllt sina skyldigheter enligt artikel 32.4 och artikel 29 i GDPR gentemot de personer som står under dess kontroll.
- 8.6 Personuppgiftsbiträdet ansvarar för att de underbiträden som det anlitar följer dataskyddsbestämmelserna. Personuppgiftsbiträdet är ansvarigt gentemot kunden för efterlevnaden av de lagstadgade och avtalsenliga dataskyddsskyldigheterna.
- 8.7 Personuppgiftsbiträdet måste få bekräftelse från sina underbiträden att de har utsett ett dataskyddsombud, om så krävs enligt lag.
- 8.8 Anlitande av underleverantörer i tredje land är endast tillåtet om de rättsliga kraven i artikel 44-50 i EU:s dataskyddsförordning är uppfyllda och kunden har gett sitt samtycke.

9. Personuppgiftsbiträdets anmälningsskyldighet

- 9.1 Överträdelser av detta avtal, av Kundens instruktioner eller av andra bestämmelser i dataskyddslagstiftningen ska utan dröjsmål rapporteras till Kunden; detsamma gäller om det finns skäl原因 grund för misstanke. Denna skyldighet gäller oavsett om överträdelsen begåtts av Personuppgiftsbiträdet självt, en person anställd av Personuppgiftsbiträdet, ett underbiträde eller någon annan person anställd av Personuppgiftsbiträdet för att fullgöra sina avtalsförpliktelser.
- 9.2 Personuppgiftsbiträdet är skyldigt att stödja den Personuppgiftsansvarige i fullgörandet av dennes lagstadgade informationsskyldighet enligt art. 33 och 34 GDPR. Personuppgiftsbiträdet får endast utföra självständiga underrättelser till myndigheter eller registrerade i enlighet med art. 33 och 34 GDPR efter föregående instruktion från Uppdragsgivaren.
- 9.3 Om en registrerad, en myndighet eller någon annan tredje part begär information, rättelse, blockering eller radering från Personuppgiftsbiträdet ska Personuppgiftsbiträdet utan onödigt dröjsmål vidarebefordra begäran till Huvudmannen; Personuppgiftsbiträdet ska under inga omständigheter tillmötesgå den registrerades begäran utan Huvudmannens samtycke.
- 9.4 Personuppgiftsbiträdet ska utan onödigt dröjsmål informera Uppdragsgivaren om tillsynsåtgärder eller andra åtgärder från myndighet är nära förestående som även skulle kunna påverka behandlingen, användningen eller insamlingen av de personuppgifter som Uppdragsgivaren lämnat. Vidare ska Personuppgiftsbiträdet omedelbart informera Uppdragsgivaren om händelser eller åtgärder från tredje part som kan äventyra eller försämra de uppgifter som omfattas av avtalet.

10. Uppsägning av avtal, radering och återlämnande av uppgifter

- 10.1 Kopior eller duplikat av uppgifterna får inte skapas utan kundens vetskap. Undantagna från detta är säkerhetskopior, i den mån de är nödvändiga för att säkerställa en korrekt databehandling, samt data som krävs för att uppfylla lagstadgade lagringsskyldigheter.
- 10.2 När det avtalade arbetet har slutförts eller tidigare på uppdragsgivarens begäran - senast när serviceavtalet upphör - ska uppdragstagaren överlämna alla dokument, bearbetnings- och användningsresultat samt data som rör avtalsförhållandet och som har kommit i uppdragstagarens besittning till uppdragsgivaren eller, efter föregående samtycke, förstöra dem i enlighet med dataskyddsbestämmelserna. Detsamma gäller för test- och skrotmaterial. Raderingsprotokollet måste lämnas in på begäran.
- 10.3 Dokumentation som tjänar som bevis för korrekt databehandling i enlighet med beställningen ska behållas av uppdragstagaren efter avtalets slut i enlighet med respektive lagringstid. Uppdragstagaren kan överlämna dem till uppdragsgivaren vid avtalets slut för att befria uppdragsgivaren

11. Datasekretess och konfidentialitet

- 11.1 Personuppgiftsbiträdet är skyldigt att under obegränsad tid och efter detta avtals upphörande behandla de personuppgifter som erhållits inom ramen för detta avtalsförhållande konfidentiellt och att följa de relevanta sekretessregler som Kunden omfattas av (t.ex. avsnitt 203 i den tyska strafflagen). Kunden är skyldig att informera Personuppgiftsbiträdet om eventuella sekretessförpliktelser när beställningen görs.

befintliga särskilda regler om sekretesskydd.

11.2 Personuppgiftsbiträdet åtar sig att informera sina anställda om relevanta dataskyddsbestämmelser och sekretessregler samt att ålägga dem att iaktta sekretess innan de påbörjar sitt arbete för Personuppgiftsbiträdet.

11.3 Personuppgiftsbiträdet ska på lämpligt sätt dokumentera efterlevnaden av de åtgärder som anges i detta avsnitt. Dokumentationen ska på begäran uppvisas för Kunden.

Slutliga bestämmelser

11.4 Ändringar av detta avtal och tilläggsavtal ska göras skriftligen eller elektroniskt, varvid det tydligt ska framgå att och vilken ändring eller tillägg till dessa villkor som ska göras av dem.

11.5 Om EU:s dataskyddsförordning eller andra rättsliga bestämmelser som hänvisas till ändras under avtalets löptid, ska hänvisningarna här också gälla för respektive efterföljande bestämmelser.

11.6 Om enskilda delar av detta avtal skulle vara eller bli ogiltiga, ska detta inte påverka giltigheten av de återstående bestämmelserna.

11.7 Alla bilagor till detta avtal utgör en integrerad del av avtalet.

Bilaga 1 -

Detta avtal omfattar följande tjänster (i tillämpliga fall i samband med huvudavtalet):

Processorn förser kunden med mobila övervakningslösningar (VIDEO GUARD) och driver dem. Dessa mobila övervakningssystem övervakar åtkomst till kundens privata lokaler. Om ett larm utlöses under den övervakningsperiod som överenskommits med kunden, dvs. i allmänhet utanför arbetstid, ska personuppgiftsbiträdet verifiera larmet och vidta de åtgärder som tidigare överenskommits med kunden. Beroende på risken kan ett videoklipp av larmet göras tillgängligt för kunden före eller efter larmet. Videobilderna raderas eller skrivs över automatiskt efter en maximal lagringsperiod på 7 dagar.

Följande typer av uppgifter behandlas regelbundet som en del av det avtalsenliga tillhandahållandet av tjänster:

1. Identifikationsuppgifter: Namn, adress, telefonnummer, e-postadress, yrke/företag, Avtalsuppgifter, kundnummer
2. Faktureringsuppgifter: Bankuppgifter, offertdata, kontakthistorik
3. Säkerhetsdata:

De registrerade som berörs av databehandlingen är

1. I synnerhet anställda hos kunden och externa parter som meddelats av kunden
Kontaktpersoner.
2. I synnerhet kundens företagsuppgifter.
3. Alla besökare det övervakade området (videodata)

De berörda uppgifterna är tillgängliga på följande sätt:

Den interna kontrollcentralen får tillgång till de berörda uppgifterna via ett säkert mobiltelefonnät. Kunden informeras per telefon.

Följande underleverantörer anlitas för att analysera videodata och initiera de åtgärder som överenskommits med kunden:

Företag Underleverantör	Adress/land	Prestanda
Hetzner Online GmbH	Industriestrasse 25 91710 Gunzenhausen	Serverhosting
Bosch Security Systems GmbH	Großhandelsring 3 49084 Osnabrück	Serverhosting /Cloud

Bilaga 2 - Förteckning över befintliga tekniska och organisatoriska åtgärder (TOM) hos personuppgiftsbiträdet i enlighet med artikel 32 i :s allmänna dataskyddsförordning

Personuppgiftsbiträdet vidtar följande tekniska och organisatoriska åtgärder för att skydda de personuppgifter som omfattas av avtalet. Åtgärderna har definierats i enlighet med artikel 32 i EU:s dataskyddsförordning och överenskommits med kunden.

I. Öronmärkning och avskiljbarhet

Följande åtgärder säkerställer att uppgifter som samlas in för olika ändamål behandlas separat:

- ☒ Fysiskt åtskild lagring på separata system eller databärare
- ☒ Logisk klientseparation (på mjukvarusidan)
- ☒ Begreppet auktorisation
- ☒ Kryptering av dataposter som behandlas för samma ändamål
- ☒ Förse dataposter med ändamålsattribut/datafält/signaturer
- ☒ För pseudonymiserade uppgifter: Separering av tilldelningsfilen och lagring på ett separat och säkert IT-system
- ☒ Separering av produktions- och testsystem

II Konfidentialitet och integritet

Följande åtgärder säkerställer konfidentialiteten och integriteten i personuppgiftsbiträdets system:

1. Kryptering

De uppgifter eller databärare som behandlas i ordern krypteras på följande sätt:

- ☒ End-to-end-kryptering när videofiler vidarebefordras till klienten

2. Pseudonymisering

"Pseudonymisering" innebär att personuppgifter behandlas på ett sådant sätt att den registrerade inte kan identifieras utan ytterligare information (t.ex. användning av fantasinamn som inte kan hänföras till en viss person utan ytterligare information).

- ☒ Ja, på följande sätt:

Kunder pseudonymiseras med kundnummer, byggarbetsplatser med projektnummer och videodata med kameranummer. Tydlig åtskillnad mellan videodata och personuppgifter.

3. Tillträdeskontroll

Följande åtgärder har vidtagits för att förhindra att obehöriga personer får tillgång till de databehandlingssystem med vilka personuppgifter behandlas eller används:

- ☒ Larmsystem
- ☒ Säkring av byggnadsschakt
- ☒ Automatiskt system för tillträdeskontroll
- ☒ Låssystem med chipkort/transponder
- ☒ Manuellt låssystem
- ☒ Videoövervakning av entréerna
- ☒ Ljusbarriärer / rörelsedetektorer
- ☒ Säkerhetslås
- ☒ Nyckelreglering (nyckelfråga etc.)
- ☒ Noggrant urval av städpersonal
- ☒ Noggrant urval av säkerhetspersonal
- ☒ Tillträdeskoncept / besöksregler

4. Tillträdeskontroll

Följande åtgärder har vidtagits för att förhindra att obehöriga tredje parter använder datasystemen:

- ☒ Tilldelning av användarrättigheter
- ☒ Skapa användarprofiler
- ☒ Tilldelning av lösenord
- ☒ Riktlinjer för lösenord (regelbunden ändring, minimilängd, komplexitet etc.)
- ☒ Autentisering med användarnamn/lösenord
- ☒ Tilldelning av användarprofiler till IT-system
- ☒ Förreglingslås för skåp
- ☒ Användning av VPN-teknik för överföring av data
- ☒ Kryptering av mobila IT-system
- ☒ Användning av antivirusprogram
- ☒ Kryptering av databärare i bärbara datorer / notebooks
- ☒ Användning av en hårdvarubrandvägg
- ☒ Användning av en mjukvarubrandvägg

5. Tillträdeskontroll

Följande åtgärder har vidtagits för att säkerställa att de som är behöriga att använda ett databehandlingssystem endast kan få tillgång till de uppgifter som omfattas av deras åtkomstbehörighet och att personuppgifter inte kan läsas, kopieras, ändras eller tas bort utan tillstånd under behandling, användning och efter lagring:

- ☒ Begreppet auktorisation
- ☒ Hantering av rättigheter av systemadministratör
- ☒ Regelbunden översyn och uppdatering av åtkomsträttigheter (särskilt när anställda slutar eller liknande)
- ☒ Antalet administratörer reduceras till ett "absolut minimum"
- ☒ Lösenordspolicy inkl. lösenordslängd, lösenordsbyte
- ☒ Loggning av åtkomst till applikationer, särskilt vid inmatning, ändring och radering av uppgifter
- ☒ Säker lagring av databärare
- ☒ Fysisk radering av databärare före återanvändning
- ☒ Korrekt förstöring av datalagringsmedia (DIN 66399)

- ☒ Användning av dokumentförstörare eller tjänsteleverantörer (om möjligt med ett dataskyddsgodkännande)
- ☒ Loggning av förstörelsen
- ☒ Kryptering av datamedier

6. Inmatningskontroll

Följande åtgärder kan användas för att i efterhand kontrollera och fastställa om och av vem personuppgifter har införts, ändrats eller tagits bort från databehandlingssystem:

- ☒ Loggning av inmatning, ändring och radering av uppgifter
- ☒ Skapa en översikt som visar vilka applikationer som kan användas för att mata in, ändra och radera vilka data.
- ☒ Spårbarhet för enskilda användares inmatning, ändring och radering av data
Användarnamn (inte användargrupper)
- ☒ Bevarande av formulär från vilka uppgifter har överförts till automatiserad behandling
- ☒ Tilldelning av rättigheter att registrera, ändra och radera uppgifter på grundval av ett behörighetskoncept

7. orderkontroll

Följande åtgärder säkerställer att personuppgifter som behandlas för kundens räkning endast kan behandlas i enlighet med kundens instruktioner:

- ☒ Val av personuppgiftsbiträde enligt due diligence-aspekter (särskilt med avseende på datasäkerhet)
- ☒ förhandsgranskning och dokumentation av de säkerhetsåtgärder som vidtas av personuppgiftsbiträdet
- ☒ Skriftliga instruktioner till personuppgiftsbiträdet (t.ex. genom ett avtal om orderhantering)
- ☒ Skyldighet för personuppgiftsbiträdets anställda att hålla uppgifterna hemliga
- ☒ Personuppgiftsbiträdet har utsett ett dataskyddsombud
- ☒ Säkerställa förstöring av data efter slutförd order
- ☒ Effektiva kontrollrättigheter som överenskommits med bearbetningsföretaget
- ☒ Löpande granskning av processorn och dess aktiviteter
- ☒ Avtalsenliga påföljder vid överträdelser

8. Transport och överföringskontroll

Följande åtgärder säkerställer att personuppgifter inte kan erhållas eller nås av obehöriga personer när de överförs (fysiskt och/eller digitalt):

- ☒ Användning av VPN-tunnlar

III Systemens tillgänglighet, återhämtningsförmåga och motståndskraft

Följande åtgärder säkerställer att de databehandlingssystem som används alltid fungerar korrekt och att personuppgifterna skyddas mot oavsiktlig förstörelse eller förlust:

- ☒ Avbrottsfri strömförsörjning (UPS)
- ☒ Luftkonditionering av serverrummen
- ☒ Enheter för övervakning av temperatur och luftfuktighet i serverrum
- ☒ Skyddande uttagslister i serverrum
- ☒ Brand- och rökdetekteringssystem i serverrum
- ☒ Brandsläckare i serverrum

- ☒ Larm vid obehörigt tillträde till serverrum
- ☒ Backup- och återställningskoncept
- ☒ Upprättad krisplan
- ☒ Förvara säkerhetskopior av data på en säker plats

IV. Särskilda åtgärder för dataskydd

Dessa har lämnats in skriftligen:

- ☒ Interna uppföranderegler för anställda
- ☒ Utnämning av ett externt dataskyddsombud

V. Översyn, utvärdering och anpassning av de befintliga åtgärderna

Personuppgiftsbiträdet ska, med medverkan av dataskyddsombudet, se över, utvärdera och vid behov anpassa de tekniska och organisatoriska åtgärder som anges i denna bilaga med 12 månaders intervall och vid behov.

Bilaga 3 - Information om dataskydd

1. Kunden ska informera berörda personer med en skylt som uppfyller kraven på dataskydd innan de går in i det område som ska övervakas. (Banderoll på byggarbetsplatsens staket / artikel 13 Information)

Den maximala lagringstiden för videodata är enligt överenskommelse med kunden: 7

2. Den nödvändiga informationen på anslagstavlan måste tillhandahållas i en lätt uppfattbar, begriplig och klart förståelig form i enlighet med artikel 12.7 i GDPR. De ger en översikt över den avsedda av uppgifterna som är förenlig med dataskyddet.
3. Kunden ska lämna information om videoövervakning på grundval av EU:s dataskyddsförordning i ett separat informationsblad. Med denna föreskrift och de krav som följer av artikel 12 ff. EU:s dataskyddsförordning uppfyller uppdragsgivaren sina transparenskyldigheter gentemot de registrerade.
4. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne behandlas eller inte och, om så är fallet, få tillgång till personuppgifterna och den information som anges i artikel 15 i GDPR.
5. Den registrerade har rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade och, i tillämpliga fall, få ofullständiga personuppgifter kompletterade (artikel 16 i EU:s dataskyddsförordning).
6. Den registrerade ska ha rätt att av den personuppgiftsansvarige sina personuppgifter raderade utan onödigt dröjsmål om någon av följande grunder är tillämplig de skäl som anges i detalj i artikel 17 i EU:s dataskyddsförordning gäller, t.ex. om uppgifterna inte längre behövs för de eftersträlvade syftena (rätt till radering).
7. Den registrerade har rätt att av den personuppgiftsansvarige få en begränsning av behandlingen om något av de villkor som anges i artikel 18 i GDPR är tillämpligt, t.ex. om den registrerade har invänt mot behandlingen, under den tid som den personuppgiftsansvariges granskning pågår.
8. Den registrerade har rätt att av skäl som hänför sig till hans eller hennes särskilda situation när som helst invända mot behandling av personuppgifter som rör honom eller henne. Den personuppgiftsansvarige kommer då inte längre att behandla personuppgifterna om inte den personuppgiftsansvarige kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller för att fastställa, göra gällande eller försvara rättsliga anspråk (artikel 21 i EU:s dataskyddsförordning).
9. Utan att det påverkar tillämpningen av andra administrativa eller rättsliga åtgärder har varje registrerad rätt att lämna in ett klagomål till en tillsynsmyndighet om den registrerade att behandlingen av personuppgifter som rör honom eller henne strider mot EU:s dataskyddsförordning (art. 77 EU GDPR). Den registrerade kan utöva denna rätt inför en tillsynsmyndighet i den medlemsstat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller platsen för den påstådda överträdelsen.
10. Den behöriga tillsynsmyndigheten i Niedersachsen är
Delstatlig kommissionär för dataskydd i Niedersachsen
Prinzenstrasse 5
30159 Hanover

Telefon: +49 (0511) 120 45 00

Fax: +49 (0511) 120 45 99

E-post: poststelle@lfd.niedersachsen.de

Kontaktpersoner

Dataskyddsbud/kontaktperson hos uppdragstagaren

Namn: secom IT GmbH

Tel.: 04271 9473 800

E-post: datenschutz@secom-it.de

Om annan, adress: Nienburger Straße 9a, 27232 Sulingen

Dataskyddsbud/kontaktperson hos kunden

Namn, telefon, e-post : se larmplan

Behörig företrädare för kunden

Namn, telefon, e-post : se huvudavtal och larmplan