Databehandleravtale – Kooi

Kooi-enheten som har inngått hovedavtalen (heretter kalt «**Databehandleren**»), behandler personopplysninger for _____, heretter kalt «**Behandlingsansvarlig**», i henhold til artikkel 4 nr. 2 og artikkel 28 i personvernforordningen (GDPR), på grunnlag av hovedavtalen. For forpliktelsene knyttet til personvern gjelder følgende bestemmelser, heretter kalt «Databehandleravtalen».

På bakgrunn av at:

A. Partene har inngått en avtale om tjenestene som skal leveres av Kooi-enheten som opptrer som databehandler etter denne databehandleravtalen (heretter kalt «**Hovedavtalen**»);
B. Databehandleren har tilgang til personopplysninger, som definert i GDPR, som tilhører den behandlingsansvarlige og/eller dennes kunder, uavhengig av om personopplysningene behandles på vegne av den behandlingsansvarlige;
C. Partene er enige om å overholde bestemmelsene i denne databehandleravtalen ved behandling av personopplysninger;
D. Databehandleren skal overholde nasjonale og internasjonale lover og forskrifter samt bestemmelsene i denne databehandleravtalen ved tilgang til personopplysninger.

1. Definisjoner

1.1. Registrert: personen som personopplysningene gjelder.
1.2. Databehandler: Kooi-enheten som har inngått hovedavtalen med den behandlingsansvarlige, og som behandler personopplysninger på vegne av denne.
1.3. Personopplysningsbrudd: et brudd på sikkerheten til personopplysninger som har negative konsekvenser for personvernet.
1.4. Personell: personene partene benytter til å gjennomføre denne databehandleravtalen, og som arbeider under deres ansvar.
1.5. Personopplysninger: enhver opplysning om en identifisert eller identifiserbar fysisk person. En person anses som identifiserbar når vedkommende kan identifiseres direkte eller indirekte, for eksempel ved henvisning til navn, identifikasjonsnummer, lokaliseringsopplysninger, nettidentifikator eller andre faktorer som er særegne for vedkommendes fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.
1.6. Underdatabehandler: en tredjepart som databehandleren engasjerer til å behandle personopplysninger på databehandlerens vegne, uten å være underlagt databehandlerens direkte myndighet. For tjenestene etter hovedavtalen benytter databehandleren Kooi Service & Security Centre B.V., med registrert kontor og hovedforretningssted i Zonnedauw 10, 9202 PA Drachten, Nederland, som underdatabehandler for overvåking og behandling av alarmmeldinger og tilhørende videobilder.

1.7. Behandlingsansvarlig: den behandlingsansvarlige for behandling av personopplysninger i henhold til GDPR. Dersom den behandlingsansvarlige behandler personopplysninger på vegne av en kunde, fungerer kunden som behandlingsansvarlig etter denne databehandleravtalen.

1.8. Behandling: enhver operasjon eller rekke av operasjoner som utføres på personopplysninger, herunder innsamling, registrering, organisering, lagring, oppdatering, endring, gjenfinning, søking, bruk, utlevering ved overføring, spredning eller enhver annen form for tilgjengeliggjøring, sammenstilling, samkjøring, samt sperring, utveksling eller sletting av opplysninger.

1.9. Hovedavtale: avtalen mellom den behandlingsansvarlige og databehandleren som beskriver tjenestene databehandleren skal levere, herunder tjenestenes art og varighet.

2. Gjenstand, formål og lagringstid

2.1. Dersom databehandleren i hovedavtalen har forpliktet seg til å behandle personopplysninger, skal dette gjøres med stor aktsomhet og i samsvar med formålene med behandlingen og nasjonale og internasjonale lover og forskrifter om personopplysninger, særlig GDPR, og bestemmelsene i denne databehandleravtalen, dersom og i den grad den behandlingsansvarlige i god tid på forhånd har informert databehandleren om tilgjengeligheten av personopplysningene og hvor de lagres.

2.2. Formålet med databehandlerens behandling er å oppfylle hovedavtalen og levere tjenestene som er avtalt der, på vegne av den behandlingsansvarlige.
Behandlingen omfatter særlig registrering og overføring av signaler om unormale eller uønskede situasjoner på den behandlingsansvarliges lokasjoner, for eksempel (mistanke om) uvedkommende tilstedeværelse eller andre potensielt farlige hendelser. Signalene genereres innenfor de tekniske mulighetene til det installerte overvåkingssystemet og overføres til kontrollrommet. Kontrollrommet behandler signalene utelukkende for å overvåke, analysere og identifisere slike hendelser.

2.3. Behandlingen av personopplysninger etter denne databehandleravtalen gjelder:

- Registrerte personer (herunder uvedkommende) som kan gjenkjennes på videobilder;
- Kontakt- og virksomhetsopplysninger om den behandlingsansvarlige (herunder blant annet navn, adresse, telefonnummer, e-postadresse, organisasjonsnummer og bankkontoopplysninger).

2.4. Lagringstiden for personopplysninger fastsettes i samsvar med gjeldende lover og forskrifter og tilpasses formålene med behandlingen. For kameraopptak gjelder følgende lagringstider:

- **Ordinære opptak:** opptak som rutinemessig gjøres av databehandlerens kamerasystemer, lagres i maksimalt 7 dager;
- **Alarmopptak:** opptak som gjøres som følge av en alarmutløsning eller hendelsesmelding, lagres i maksimalt 28 dager.

Lengre lagringstid er bare tillatt dersom det kreves ved lov eller er nødvendig for å ivareta den behandlingsansvarliges berettigede interesser, for eksempel ved undersøkelse av en hendelse.
De fastsatte lagringstidene dokumenteres internt, gjennomgås jevnlig og justeres ved behov, og kan gjøres tilgjengelige for den behandlingsansvarlige etter skriftlig anmodning.

3. Den behandlingsansvarliges forpliktelser

3.1. Den behandlingsansvarlige garanterer at alle krav i GDPR overholdes. Den behandlingsansvarlige har truffet nødvendige sikkerhetstiltak.

3.2. Den behandlingsansvarlige skal i rett tid, som hovedregel innen 10 virkedager, varsle databehandleren om endringer i behandlingen (dersom relevant) og eventuelle konsekvenser av disse.

3.3. Den behandlingsansvarlige garanterer at eget personell overholder GDPR og bestemmelsene i denne databehandleravtalen, i den grad de på noen måte deltar i behandling av personopplysninger.

3.4. Den behandlingsansvarlige garanterer at oppdraget om å behandle personopplysninger (dersom relevant) ikke er ulovlig eller krenker tredjeparts rettigheter.

3.5. Den behandlingsansvarlige gir databehandleren tillatelse til å benytte tredjeparter til behandlingen som ledd i gjennomføringen av hovedavtalen og denne databehandleravtalen.

4. Databehandlerens forpliktelser

4.1. Databehandleren skal bare se og/eller behandle personopplysninger i den grad det er nødvendig for å oppfylle hovedavtalen, og skal følge alle rimelige instrukser fra den behandlingsansvarlige.

4.2. Databehandleren skal ikke lagre personopplysninger utenfor Det europeiske økonomiske samarbeidsområdet (EØS) eller overføre dem til land utenfor EØS uten den behandlingsansvarliges skriftlige forhåndssamtykke. Den behandlingsansvarlige kan stille vilkår for samtykket.

4.3. Databehandleren garanterer at personellet kjenner kravene i GDPR og overholder GDPR og denne databehandleravtalen, i den grad de på noen måte deltar i behandling av personopplysninger. Databehandlerens ansatte har taushetsplikt.

4.4. På den behandlingsansvarliges første anmodning skal databehandleren straks overlevere til den behandlingsansvarlige eller slette alle kopier av personopplysninger som stammer fra og/eller behandles på oppdrag og under instruks fra den behandlingsansvarlige.

Forpliktelser vedrørende behandling

Artiklene 4.5 til 4.7 gjelder bare dersom databehandleren har forpliktet seg til å utføre behandling.

4.5 Databehandleren skal treffe egnede tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger mot tap og ulovlig behandling. Med hensyn til teknologien som brukes, og kostnadene ved gjennomføringen, skal tiltakene sikre et passende sikkerhetsnivå ut fra risikoene ved behandlingen og arten av opplysningene som skal beskyttes.

4.6 Databehandleren skal samarbeide fullt ut og i rett tid med den behandlingsansvarlige slik at registrerte kan få innsyn i, slettet eller rettet sine personopplysninger, og/eller få dokumentert at opplysningene er slettet eller rettet, eller, dersom den behandlingsansvarlige er uenig med den registrerte, få registrert at den registrerte mener personopplysningene er uriktige.

4.7 Databehandleren skal innføre tilstrekkelige interne kontrolltiltak for å oppfylle forpliktelsene etter denne databehandleravtalen og dokumentere dem slik at etterlevelsen enkelt kan kontrolleres. Ved behandling av personopplysninger skal aktiviteter og hendelser knyttet til opplysningene registreres i loggfiler.

4.8 På anmodning fra den behandlingsansvarlige skal databehandleren samarbeide om kryptering ved overføring av fortrolig informasjon over nettverk. Dersom dette medfører økte kostnader for databehandleren, skal den behandlingsansvarlige dekke disse.

4.9 Den behandlingsansvarlige kan én gang i året få kontrollert om behandlingen av personopplysninger skjer i samsvar med databehandleravtalen, ved en undersøkelse utført av en uavhengig registrert EDP-revisor (Electronic Data Processing). Revisoren har taushetsplikt. Databehandleren skal gi alle opplysninger revisoren ber om. Den behandlingsansvarlige dekker alle kostnader ved undersøkelsen.

4.10 Oppdragets innhold og omfang vedrørende behandlingen og kostnadene knyttet til dette følger hovedavtalen. Databehandleren skal følge den behandlingsansvarliges instrukser om behandling og/eller lagring av personopplysninger.

5. Underdatabehandler

5.1. Databehandleren kan sette bort hele eller deler av gjennomføringen av databehandleravtalen til en underdatabehandler etter skriftlig forhåndssamtykke fra den behandlingsansvarlige. Den behandlingsansvarlige skal ikke nekte samtykke uten saklig grunn. Databehandleren forblir kontaktpunkt for den behandlingsansvarlige og er ansvarlig for at bestemmelsene i denne databehandleravtalen overholdes.

5.2. Databehandleren skal pålegge underdatabehandleren de samme forpliktelsene som følger av denne databehandleravtalen, og kontrollere at underdatabehandleren overholder dem.

5.3. Databehandleren er fullt ansvarlig overfor den behandlingsansvarlige for konsekvensene av å sette bort arbeid til en underdatabehandler.

5.4. Artikkel 4.2 gjelder også fullt ut for underdatabehandleren.

5.5. Databehandleren oppfyller for tiden hovedavtalen i samarbeid med underdatabehandlerne oppført i **vedlegg 1**, noe den behandlingsansvarlige samtykker til.

6. Utlevering av personopplysninger

6.1. Databehandleren kan ikke utlevere personopplysninger til andre enn den behandlingsansvarlige, med mindre dette følger av en rettslig forpliktelse eller den behandlingsansvarlige har gitt skriftlig tillatelse. Databehandleren skal bekrefte enhver utlevering til tredjepart skriftlig, med angivelse av alle involverte parter og/eller personer.

6.2. Dersom databehandleren utleverer personopplysninger til den behandlingsansvarlige, enten på anmodning eller på eget initiativ, skal den behandlingsansvarlige aldri offentliggjøre eller spre de utleverte opplysningene uten rettskjennelse og aldri skade databehandlerens ære eller omdømme. Databehandleren eller den behandlingsansvarlige kan etter gjeldende nasjonal lovgivning være forpliktet til å utlevere personopplysninger til kompetente myndigheter uten rettskjennelse, avhengig av jurisdiksjon.
Ved brudd på denne artikkelen skal den behandlingsansvarlige betale databehandleren en konvensjonalbot på 10 000 euro per hendelse per dag.

6.3. Dersom databehandleren er rettslig forpliktet til å utlevere personopplysninger, skal databehandleren:

- Kontrollere grunnlaget for anmodningen og identiteten til personen som har fremsatt den, og informere den behandlingsansvarlige før utleveringen;
- Begrense utleveringen til det som er rettslig påkrevd;
- Gi den behandlingsansvarlige mulighet til å utøve rettighetene:
    - Til den behandlingsansvarlige og de registrerte, og;
    - Til å ivareta interessene til den behandlingsansvarlige og de registrerte.

7. Informasjonssikkerhet

7.1. Den behandlingsansvarlige og databehandleren skal sikre personopplysningene og eventuell behandling av dem i samsvar med GDPR og annen relevant særlovgivning samt europeiske regler og retningslinjer. Sikkerhetsnivået bør være i samsvar med anerkjente standarder som ISO 27001.

7.2. Den behandlingsansvarlige og databehandleren skal gjøre sitt ytterste for å beskytte personopplysningene mot inntrengere, eksterne katastrofer og uforsiktig, ukyndig eller uautorisert bruk. Begge parter skal treffe sikkerhetstiltak, herunder blant annet tilgangskontroll, fysisk sikring, kryptografi og kontinuitetsstyring.

7.3. Dersom den behandlingsansvarlige ber skriftlig om det, skal databehandleren treffe særskilte tiltak for sikkerhet og/eller fortrolighet for de angitte personopplysningene. Dersom dette medfører økte kostnader for databehandleren, skal den behandlingsansvarlige dekke disse.

8. Brudd på personopplysningssikkerheten

8.1. Dersom den behandlingsansvarlige eller databehandleren blir kjent med et (mistenkt) brudd på personopplysningssikkerheten som også kan være relevant for den andre parten, skal vedkommende part varsle den andre uten ugrunnet opphold og senest innen 24 timer etter at bruddet ble oppdaget, ved skriftlig melding. Meldingen skal minst inneholde:

- en beskrivelse av arten av bruddet på personopplysningssikkerheten, herunder kategorier av registrerte og berørte personopplysninger;
- de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;
- tiltakene som er truffet eller foreslått for å håndtere bruddet og begrense skadevirkningene;
- kontaktopplysninger til et utpekt kontaktpunkt for ytterligere informasjon.

8.2. I samsvar med GDPR gjelder en plikt til å melde brudd på personopplysningssikkerheten. Det innebærer at virksomheter må melde alvorlige brudd til kompetent tilsynsmyndighet innen 72 timer. Databehandleren og den behandlingsansvarlige skal overholde denne meldeplikten og om nødvendig inngå tilleggsavtaler om hvordan den skal oppfylles, samt om oppdagelse, identifisering og undersøkelse av sikkerhetshendelser og årsakene til dem. Melding skal sendes til tilsynsmyndigheten som er kompetent i den behandlingsansvarliges jurisdiksjon.

9. Taushetsplikt

9.1. Alle opplysninger som tilhører den behandlingsansvarlige og dennes kunder, er fortrolige og skal behandles fortrolig av databehandleren. Databehandleren plikter å bevare taushet om alle personopplysninger og all informasjon som behandles eller blir kjent i forbindelse med hovedavtalen eller denne databehandleravtalen.

9.2. Taushetsplikten gjelder ikke følgende opplysninger:

- Opplysninger som er offentlig kjent uten at offentliggjøringen skyldes en uautorisert handling;
- Opplysninger som må utleveres etter lovbestemmelse eller rettskjennelse, forutsatt at den utleverende parten på forhånd varsler skriftlig parten opplysningene gjelder;
- Opplysninger som en part har utviklet selvstendig;
- Opplysninger som en part allerede besitter uten taushetsplikt.

10. Immaterielle rettigheter

10.1. Alle immaterielle rettigheter, herunder opphavsrett, databaserettigheter og andre immaterielle rettigheter samt tilsvarende rettigheter til å beskytte informasjon om innsamling av data og personopplysninger, og kopier eller bearbeidelser av disse, tilhører den behandlingsansvarlige (eller en kunde av denne).

10.2. Alle immaterielle rettigheter – herunder opphavsrett, databaserettigheter og andre immaterielle rettigheter samt tilsvarende rettigheter til å beskytte informasjon – til databehandlerens produkter og tjenester tilhører databehandleren.

11. Ansvar og forsikring

11.1. I den grad databehandleren er erstatningsansvarlig etter denne databehandleravtalen, er databehandlerens samlede ansvar begrenset til erstatning for direkte tap, oppad begrenset til beløpet som er betalt for bruk av tjenesten eller produktet de siste 6 månedene før skaden oppstod.

11.2. Databehandleren er ikke ansvarlig for indirekte tap. Indirekte tap omfatter følgetap, tapt fortjeneste, tapte besparelser, redusert goodwill, tap som følge av driftsavbrudd og tap som følge av krav fra tredjeparter.

12. Varighet og opphør

12.1. Databehandleravtalen trer i kraft samme dag som partene undertegner hovedavtalen.

12.2. Bestemmelsene om varighet og opphør i hovedavtalen gjelder også for databehandleravtalen. Når hovedavtalen sies opp eller opphører, uansett årsak, sies også databehandleravtalen opp eller opphører.

12.3. Ved opphør av databehandleravtalen skal databehandleren, etter den behandlingsansvarliges valg, slette alle personopplysninger som tilhører den behandlingsansvarlige.

12.4. Forpliktelser som etter sin art er ment å gjelde etter at databehandleravtalen er opphørt, skal fortsatt gjelde. Dette omfatter bestemmelser om taushetsplikt, overføring og sletting, ansvar og lovvalg.

13. Heving

13.1. Hver part kan heve hovedavtalen helt eller delvis dersom den andre parten på klanderverdig måte unnlater å oppfylle databehandleravtalen og misligholdet ikke er rettet etter varsel, uten at dette berører retten til erstatning.

13.2. Hver part kan heve hovedavtalen helt eller delvis med umiddelbar virkning uten varsel dersom den andre parten får betalingsutsettelse, det begjæres konkurs hos den andre parten, eller den andre partens virksomhet avvikles eller opphører av andre grunner enn omstrukturering eller sammenslåing av selskaper.

14. Tilleggsbestemmelser

14.1. Endringer i eller tillegg til denne databehandleravtalen skal avtales skriftlig mellom databehandleren og den behandlingsansvarlige. Endringer eller tillegg skal dokumenteres i et tillegg til avtalen og er bare bindende dersom tillegget undertegnes av begge parter.

14.2. Denne databehandleravtalen er underlagt samme lovgivning som hovedavtalen. Tvister som oppstår som følge av eller i forbindelse med denne databehandleravtalen, er underlagt samme verneting eller tvisteløsningsmekanisme som avtalt i hovedavtalen.

På vegne av databehandleren	På vegne av den behandlingsansvarlige:
Navn:	Navn:
Stilling:	Stilling:
Dato:	Dato:
Signatur:	Signatur:

Vedlegg 1 Liste over underdatabehandlere

Databehandleren samarbeider for tiden med følgende underdatabehandlere ved gjennomføringen av hovedavtalen, noe den behandlingsansvarlige samtykker til.

- **Kooi Service & Security Centre B.V. (Nederland):**
  Overvåkings- og alarmsentral, herunder mottak, vurdering og behandling av alarmmeldinger, videobilder og tilhørende personopplysninger i forbindelse med tjenestene etter hovedavtalen.
  Zonnedauw 10, 9202 PA Drachten.