Databehandleravtale etter EUs forordning for personvern (General Data Protection Regulation)

Databehandleravtale

(versjon 200319)

I henhold til EUs forordning for personvern Artikkel 28

mellom

Kunde

(Behandlingsansvarlig)

og

Stanley Security AS

(Databehandler)

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter EUs forordning for personvern om behandling av personopplysninger. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

Begge parter har et selvstendig ansvar for behandlingen av personopplysninger, avtalen regulerer arbeidsdelingen mellom partene.

Avtalen inngås elektronisk via https://www.stanleysecurity.no/databehandleravtale.

2. Formål

Behandling av personopplysninger skal kun gjøres innenfor rammen av denne avtale og videre være tilknyttet formålet med den enkelte tjeneste / sikkerhetsleveranse.

I leveranseavtalen mellom partene fremkommer hvilke nedenfor stående tjeneste som omfattes, og derav hvilke personopplysninger som behandles.

Nr.:	Tjeneste:	Beskrivelse:	Type personopplysning:
eAlarm			
3101	Alarmmottak Standard	Mottak og aksjonering på innkommende alarmer for innbrudd og sabotasje samt tekniske anlegg. Behandling av alarmer iht. avtalt aksjonsplan. Brukerstøtte for betjening av alarmpanel	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3110	Tillegg Ran/Trussel-alarm	Mottak og aksjonering på innkommende alarmer for Ran, Trussel/Gissel og Assistanse. Behandling av alarmer iht. avtalt aksjonsplan. Brukerstøtte for betjening av alarmpanel	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3120	Tillegg Røykvarsling	Mottak og aksjonering på innkommende alarmer for røyk. Behandling av alarmer iht. avtalt aksjonsplan. Brukerstøtte for betjening av alarmpanel	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3190	Til-/frakoblingskontroll	Kontroll av at alarmanlegget er aktivert i aktuell tidsperiode. Aksjonering ved avvik iht aksjonsplan	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3197	Auto SMS varsling	Varsling via SMS for Til/frakoblingkontroll	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3198	Auto e-post varsling	Varsling av alarmer via e-post	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.

3220	Fjernadministrasjon Alarm	Betjene alarmanlegget fra vårt kundesenter. Brukerstøtte. Programmere og følge opp helligdager. Endre automatisk til- og frakobling. Skrive ut logg fra alarmsystemet. Stille klokke og dato. Sikkerhetskopi av anleggsdata på sentralapparat. Alle endringer utføres i Kundesenterets åpningstid.	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, PIN-kode.
3222	Fjernadministrasjon Alarm og Dørkontroll	Betjene alarmanlegget fra vårt kundesenter. Brukerstøtte. Programmere og følge opp helligdager. Programmere automatisk til- og frakobling av alarmen og åpning/lukking av dører. Fjernstyre dører og alarmanlegg ved behov utenom ordinær tidsprogrammering. Legge inn og administrere brukere, kort og koder. Endre automatisk til- og frakobling. Skrive ut logg fra alarmsystemet. Stille klokke og dato. Sikkerhetskopi av anleggsdata på sentralapparat. Alle endringer utføres i Kundesenterets åpningstid.	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, PIN-kode.
3225	Stanley Safe	Sikker kundetilgang via app eller web mot SPC alarmsentral	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, PIN-kode.
3240	Elektronisk Driftskontroll Alarm	Kvartalsvis kontroll av SPC alarmanlegg via Internett: Tilknytning, driftsstatus og oppsett. Rapport med forslag til endringer.	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, PIN-kode.
3904	Alarmmottak Heis	Mottak og aksjonering på innkommende alarmer for heis Verifikasjon av innkommende alarmer Behandling av alarmer iht. avtalt aksjonsplan Brukerstøtte for betjening av alarmpanel Samtale med personer i heisen	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3801	Alarmmottak Mobile Enheter	GPS overvåkning av mobile enheter som konteinere og biler Mottak og aksjonering på innkommende alarmer Verifikasjon av innkommende alarmer Behandling av alarmer iht. avtalt aksjonsplan	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, GPS-koordinater
3802	Alarmmottak Mobil Personalarm	Mobil personalarm basert på egen alarmsender eller via smarttelefon	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger, GPS-koordinater
eLink			
3211	Alarmoverføring Høysikkerhet	Kryptert og overvåket overføring av alarmsignaler via Internett med polling hvert 3. min. Alternativ trådløs føringsvei via GPRS Benytter eksisterende internettforbindelse hos kunde Gir mulighet for fjernservice	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3213	Alarmoverføring Standard	Kryptert og overvåket overføring av alarmsignaler via Internett med polling hvert 30. min Alternativ trådløs føringsvei via GPRS Benytter eksisterende internettforbindelse hos kunde Gir mulighet for fjernservice	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.

3214	Alarmoverføring Intro	Kryptert og overvåket overføring av alarmsignaler via Internett med polling hver 7. time Benytter eksisterende internettforbindelse hos kunde eller SIM-kort	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3215	Alarmoverføring GPRS	Kryptert og overvåket overføring av alarmsignaler via Internett med polling 1 gang pr. døgn Benytter integrert SIM-kort	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
3251	eLink Sikkerhetsnett	Design av kommunikasjonsløsning mellom kunde og Stanley Etablering og drift av VPN forbindelse Dokumentasjon	IP-adresse
Utrykning			
1903	Utrykningsavtale Basic	Utrykning i henhold til aksjonsplan, basert på mottatt alarm. Dekker utrykninger med kriminell årsak samt vakthold på stedet inntil kunde ankommer. Nøkkelhåndtering og beredskap	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
1905	Utrykningsavtale Premium	Utrykning i henhold til aksjonsplan, basert på mottatt alarm. Dekker alle utrykninger uansett årsak, dog ikke assistanseoppdrag. Nøkkelhåndtering og beredskap	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
1949	Utrykning etter regning	Utrykning i henhold til aksjonsplan, basert på mottatt alarm. Faktureres pr utrykning. Nøkkelhåndtering og beredskap	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
1997	Manuelt Oppdrag	Flaggheis, flagghal eller andre manuelle oppdrag hos kunde	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
19102	Manuelt Vakthold 07-21	Bemannet vakthold hos kunde	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
19103	Manuelt Vakthold 21-07	Bemannet vakthold hos kunde	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
19104	Manuelt Vakthold Helg/Helligdag	Bemannet vakthold hos kunde	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
eVakt			
3740	Fjernadministrasjon Video	Uttak av video knyttet til hendelser. Endre oppsett for skjermbilde og brukere. Justere parametere på kamera som oppløsning og antall bilder pr. sek. Endre oppsettet for bevegelsesdeteksjon.	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.
3242	Elektronisk Driftskontroll Video	Kvartalsvis kontroll av videoanlegg via Internett: Tilknytning, driftsstatus og oppsett. Rapport med forslag til endringer.	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.

3742	Alarmverifisering	Verifisering av hendelse ved Innbrudd, Ran eller Trussel/Gissel. Tilleggsinformasjon til alarmhendelse pr. tlf. iht. aksjonsplan. Melding om ev. feil på kamera. Loggføring av hendelser.	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.
3743	Videorunder	3 inspeksjoner pr. døgn basert på avtalt kartskisse med innlagte kamerapunkter Melding til kontaktperson ved avvik Hver kamerarunde loggføres som en hendelse. Preventiv skilting om skjult inspeksjon 2 alternative tidsperioder: - Ferievakt (15 uker):Uke 8, Påskeuka, 24-32, 40,51,52, - Hele året	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.
3744	Videoalarm	Alarmmelding basert på videodeteksjon fra utvalgte kamera på Milestone server. Meldinger via høyttaler fra operatør til stedet ved hendelser Aksjon basert på video fra aktuelle kamera med melding til aktuell kontaktperson iht. aksjonsplan Aktuell hendelse og aksjon loggføres	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.
3745	Fjernlagring Video	Sentralisert lagring av video basert på Stanley Hosted Video Solution - eVideo Cloud. 3 nivåer basert på lagringstid og oppløsning: Basic, Deluxe og Platinum	Navn, telefonnummer, e-postadresse, bilder, adresse, tale.
eAccess			
3611	eAccess Kortleveranse	Produksjon og levering av adgangskort Bestilling og administrasjon via egen portal - WebID	Navn, telefonnummer, e-postadresse, Pinkode, adresse, kort nummer.
3651	eAccess Administrasjon	Administrasjon av brukere og tilganger Tidsstyring av dører. Online håndtering av endringer via WebID. 4 logger pr år på forespørsel. Backup av oppsett og brukerdata ved sentral serverløsning	Navn, telefonnummer, e-postadresse, Pinkode, adresse, kort nummer.
Brann			
3131	Alarmmottak Brann	Mottak og aksjonering på innkommende alarmer fra brannsentral til Stanley. Fritt valg av varslingstyper (Tlf, SMS, epost)	Navn, telefonnummer, e-postadresse, adresse, kodeord.
3130	Fire Online Basic	Statuskontroll seksjoner. Månedlige statusrapporter pr e-post til kunde.	Navn, telefonnummer, e-postadresse, adresse.
Service (1=Alarm, 2=Brann, 3=Video, 4=Adgangskontroll, 5= Annet)			
6x15	Serviceavtale m/deler Alarm, Brann, Video, Adgangskontroll, Varesikring.	Teknisk service inkludert deler, arbeid og reise inntil 60 km t/r og 1 time reisetid Påbegynt fjernservice innen avtalt responstid Service på stedet ved behov Service tilgjengelig virkedager 08-16	Navn, telefonnummer, e-postadresse, adresse.

6x21	Serviceavtale u/deler Alarm, Brann, Video, Adgangskontroll.	Teknisk service inkludert arbeid og reise inntil 60 km t/r og 1 time reisetid Påbegynt fjernservice innen avtalt responstid Service på stedet ved behov Service tilgjengelig virkedager 08-16	Navn, telefonnummer, e-postadresse, adresse.
6x99	Service etter regning Alarm, Brann, Video, Adgangskontroll, Varesikring.	Teknisk service etter regning Deler, arbeid og reise faktureres pr. hendelse	Navn, telefonnummer, e-postadresse, adresse.
6x56	Software Versjonsoppgradering Brann, Video, Adgangskontroll	Rett til oppgradering av programvare basert på produsentens vilkår	Navn, telefonnummer, e-postadresse, adresse.
6x46	Responstid Alarm, Brann, Video, Adgangskontroll (Gull).	Enhetlig kontaktpunkt for service IP tilknytning for effektive servicetjenester Brukerveiledning på utstyr og programvare Portaltilgang Årlig evalueringsmøte Personkontakt salg Responstid: Hendelse 4 timer, Endring 1 dag	Navn, telefonnummer, e-postadresse, adresse.
6x46	Responstid Alarm, Brann, Video, Adgangskontroll (Sølv).	Enhetlig kontaktpunkt for service IP tilknytning for effektive servicetjenester Brukerveiledning på utstyr og programvare Portaltilgang Responstid: Hendelse 1 dag, Endring 3 dager	Navn, telefonnummer, e-postadresse, adresse.
6x46	Responstid Alarm, Brann, Video, Adgangskontroll (Bronse).	Enhetlig kontaktpunkt for service IP tilknytning for effektive servicetjenester Brukerveiledning på utstyr og programvare Portaltilgang Responstid: Hendelse 3 dager, Endring 5 dager	Navn, telefonnummer, e-postadresse, adresse.
6x25	Serviceavtale beredskap Alarm, Video, Adgangskontroll.	Utvidelse av servicetid fra virkedager 8-16 til alle dager 00 - 24	Navn, telefonnummer, e-postadresse, adresse.
6x01	Periodisk kontroll Alarm, Brann, Video, Adgangskontroll, Varesikring.	Funksjonstesting av sikkerhetsanlegg Tilstandsrapport med forslag til tiltak og endringer	Navn, telefonnummer, e-postadresse, adresse.
Andre tjenester			
3230	Kundeportal	Portal for oversikt over alarmer, utrykninger, årsakskoder etc. Endringer av kontaktpersoner via web	Navn, telefonnummer, e-postadresse, kodeord, adresse, tale, til-frakoplinger.
7880	Forsikring Assure	Forsikring av installert utstyr hos kunde	Navn, telefonnummer, e-postadresse, adresse.
6501	Rutineservice iht. avtale	Tjeneste som utføres regelmessig av partner	Navn, telefonnummer, e-postadresse, adresse.
3600	Stanley Premium service	Formidlingstjenste	Navn, telefonnummer, e-postadresse, adresse.
3601	Endring av varslingslister	Endring av varslingslister for 3360 Formidlingstjeneste	Navn, telefonnummer, e-postadresse, adresse.

- Hvordan personopplysningene skal behandles

Databehandler skal bare behandle personopplysninger iht. formålet med den enkelte tjeneste.

Databehandler har ikke råderett over personopplysningene, og kan dermed heller ikke behandle disse til egne formål.

Behandling av personopplysninger skjer innenfor EU/EØS-området, ved avvik fra dette følges definerte rutiner beskrevet i denne avtale.

Databehandler lagrer personopplysninger så lenge det er nødvendig for det formål personopplysningene ble samlet inn for, herunder ivaretakelsen av de gjensidige rettigheter og plikter som følger av kontraktsforholdet. Dette inkluderer ivaretakelse av dokumentasjonshensyn for eventuelt garanti, mangels og erstatningsansvar som kan oppstå i kontraktsforholdet.

Alle opptak med kameraovervåkning slettes når det ikke lenger er en saklig grunn for å oppbevare dem, og senest sju dager etter opptak. Dersom det er sannsynlig at et opptak vil bli utlevert til politiet, kan opptaket oppbevares i inntil 30 dager. Opptak fra bank eller postlokaler, inkludert opptak fra kasse med Bank i Butikk og Post i Butikk, kan oppbevares i inntil tre måneder.

Registrerte personopplysninger i adgangskontrollsystemer lagres maksimalt i 90 dager.

Databehandler gir ikke personopplysningene videre til andre med mindre det foreligger et lovlig grunnlag for slik utlevering. Eksempler på slikt grunnlag vil typisk være en avtale med behandlingsansvarlige eller et lovgrunnlag som pålegger databehandler å gi ut informasjonen.

Kategorier av registrerte vil variere iht. avtalt tjeneste, det kan eksempelvis være kontaktpersoner hos behandlingsansvarlige, brukere av sikkerhetssystemene eller registrerte av sikkerhetssystemet.

3. Behandlingsansvarliges rettigheter og plikter (Kunde)

Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24).

Den behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen (jf. artikkel 4 nr. 7).

Den behandlingsansvarlige skal gi *databehandler* dokumenterte instrukser for hvordan personopplysninger skal behandles (jf. artikkel 28 nr. 3 bokstav a). Instruksene skal være en del av avtalen eller lagt ved som et vedlegg til avtalen.

Den behandlingsansvarliges rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller lovens krav etter artikkel 28 nr. 1.

4. Databehandlers plikter (Stanley Security)

Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Videre skal databehandleren:

a) behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige, herunder med hensyn til overføring av personopplysninger til en tredjestat, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretning,
b) treffer alle tiltak som er nødvendig i henhold til artikkel 32,
c) idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommende sin plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter,
d) ved innsynskrav må databehandler bistå ved å samle opplysninger som er lagret om den registrerte. Databehandler må gjøre opplysningene tilgjengelig for den behandlingsansvarlige for at den behandlingsansvarlige kan vurdere innsynskravet.
e) bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32–36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren,

5. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med behandlingsansvarlige før behandlingen av personopplysninger starter.

Avtale med følgende underleverandører:
- Securitas - E2U Systems - Vanderbilt - Jablotron - Morphean *Databehandler har den behandlingsansvarliges generelle godkjennelse til å bruke andre databehandlere. Databehandler må likevel underrette den behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye databehandlere. Den behandlingsansvarlige må motta en slik underretning minimum 4 uker før endringen trer i kraft. Den behandlingsansvarlige skal ha mulighet til å motsette seg endringene, og skal melde databehandleren om dette senest 2 uker etter underretning er mottatt.*

Dersom det er innhentet en generell skriftlig tillatelse for bruk av underleverandører, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

Dersom en databehandler engasjerer en annen databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal nevnte andre databehandler pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne avtale, dette ved en egen avtale. Det skal gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende lovgivning. Dersom nevnte andre databehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal den opprinnelige databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at nevnte andre databehandler oppfyller sine forpliktelser.

6. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles til databehandler etter EUs forordning for personvern. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Følgende sikringstiltak skal databehandler ha på plass for å ivareta konfidensialitet, integritet og tilgjengelighet:

Konfidensialitet, integritet og tilgjengelighet.

Stanley Security AS skal beskytte personopplysninger mot uberettiget innsyn og endringer, samtidig skal opplysningene være tilgjengelige for dem som trenger opplysningene når de har behov for disse.

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet, rutiner og tekniske tiltak for informasjonssikkerhet.

7. Sikring av informasjonssystemer og nettverkskomponenter tilknyttet vår alarmstasjonstjeneste

Alarmstasjon er sikret iht. de krav som er satt i NEK EN50518 som inkluderer fysisk sikring, datasikring med brannmurer, sikring av alarmmottak og databehandling inklusiv redundans, mm.

Nettverkskomponenter:

Alle nettverkskomponenter plasseres under egen avlåsing, i eget rom eller skap, innenfor beskyttet eller sperret område. Kravet til plassering og egen avlåsing av nettverkskomponenter er minimumstiltak basert på en generell risikovurdering. Ekstra sikringstiltak kan være en kombinasjon av fysiske og logiske sperrer samt kontrolltiltak.

Dersom det er behov for øket fysisk kontroll med nettverkskomponentene kan rom eller oppbevaringsenheter forsynes med alarm eller annen overvåking. Som eget tiltak eller i kombinasjon med øket kontroll kan det være behov for å benytte forsterkede rom eller oppbevaringsenheter.

Servere:

Servere skal installeres i et serverrom som er sikret, beskyttet område brukes.

Kabler:

Kabelsystem og andre installasjoner skal installeres slik at de hindrer uvedkommende å få tilgang til systemet, sende uautorisert informasjon gjennom systemet, eller å skade systemet. Sikringen kan bestå av en kombinasjon av forseringshindringer, tilsyn og fysisk kontroll.

Kabelsystemet skal i sin helhet legges innenfor kontrollert område. I kabelsystemet skal omformere, tilkoblingsutstyr og tilkoblingspunkter plasseres innenfor beskyttet eller sperret område, og uvedkommende hindres adgang ved avlåsing.

Brukerterminaler/kontorer:

Avlåsing innenfor beskyttet område er pålagt minimumskrav.

Skrivere:

Plasseres på et eget rom med kode for utskrift.

Tilgangskontroll:

Stanley Security AS tildeler, endrer, sletter og føre kontroll med autorisasjon for tilgang til IT-ressursene, dette for å opprettholde konfidensialitet, integritet og tilgjengelighet til informasjon.

Medarbeiderne skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.

Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

Registrering av autorisert bruk av informasjonssystemet, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for

8. Avvik

Bruk av personopplysninger som er i strid med fastlagte rutiner og sikkerhetsbrudd skal behandles som avvik.

Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.

Databehandler skal uten ugrunnet opphold melde avvik til behandlingsansvarlig.
Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med forordning / nasjonale rett.

Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

9. Taushetsplikt

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

Databehandleren skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig, dette ved at de pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.

10. Protokoller over behandlingsaktiviteter

Databehandler og, dersom det er relevant, databehandlerens representant skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av en behandlingsansvarlig:

Protokoll over behandlingsaktiviteter

Kontaktopplysninger til behandlingsansvarlig fremkommer av signering av databehandleravtalen.

Kontaktopplysninger til databehandler.

Navn:	Ole Erik Strande
Telefonnummer:	+47 908 60 324
e-postadresse:	oleerik.strande@sbdinc.com

Kategorier av personopplysninger:
Ikke sensitive

Overføringer av personopplysninger til en tredjestat:
Ingen

Tekniske og organisatoriske sikkerhetstiltak:
Ref. punkt 7

Protokollene skal være skriftlige, herunder elektroniske.

Databehandleren og, dersom det er relevant, databehandlerens representant skal på anmodning gjøre protokollen tilgjengelig for tilsynsmyndigheten.

Forpliktelsene gjelder ikke for et foretak eller en organisasjon med færre enn 250 ansatte, med mindre behandlingen det/den utfører, trolig vil medføre en risiko for de registrertes rettigheter og friheter, behandlingen ikke skjer leilighetsvis eller omfatter særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1 eller personopplysninger om straffedommer og straffbare forhold nevnt i artikkel 10.

11. Sikkerhetsrevisjoner

Følgende sikkerhetsrevisjoner omfattes av denne avtalen:

Iht. nærmere avtale.

Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroll, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

Databehandler skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene til databehandler er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen inspektør på fullmakt fra den behandlingsansvarlige.

12. Dokumentasjon

Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.

Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.

13. Henvendelser fra de registrerte

Behandlingsansvarlige mottar henvendelse fra den registrerte å videreformidler denne til databehandler som oppfyller den registrertes forespørsel.

14. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig. Oppdatert databehandleravtale forefinnes på https://www.stanleysecurity.no/databehandleravtale.

Ved brudd på denne avtale eller EUs forordning for personvern kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

15. Ved opphør

Ved opphør av denne avtalen og når formålet med innhentingen av personopplysningene er ivaretatt, plikter databehandler å slette alle personopplysninger som er mottatt på vegne av Kunden og som omfattes av denne avtalen.

Databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Det skal avtales nærmere på hvilken måte sletting og/eller destruksjon skal skje etter avtalens opphør.

På forespørsel fra behandlingsansvarlige skal databehandler skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Det kan avtales at det skal gis en utskrift og kopi av alt innhold i databaser og lignende med data som er omfattet. Kostnader ved dette, eller opplysninger som skal leveres i særskilt format avtales.

16. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.