GSGroup Privacy Terms – Databehandleravtale

I henhold til EU forordning 2016/679 artikkel 28 (3) (personvernforordningen/GDPR)

mellom

kunden, som angitt i Avtalen mellom partene

(behandlingsansvarlig)

og

GSGroup AS
963 299 850
Tassebekkveien 354
3160 Stokke
Norge[1]

(databehandleren)

enkeltvis referert til som en «part»; samlet «partene»

har blitt enige om følgende databehandleravtale for å oppfylle kravene i personvernforordningen og for å sikre beskyttelse av den registrertes rettigheter.

[1] og de tilknyttede selskapene: GSGroup Danmark AS (27047599), GSGroup AB (556445-6704), GSGroup Deutschland GmbH (DE258074748), GSGroup Finland Oy (0973454-5), GSGroup Innovation Centre Zrt (25416866-2-43), GSGroup MyFleet Zrt (01-10-048455), Guard Systems Estonia OU (11165968), Guard Systems Latvia SIA (40003797354), UAB Guard Systems (300574578), Flextrack ApS (19670546), GSGroup DK ApS (41551526).

1. Innholdsfortegnelse

2. Innledende bestemmelser

1. Denne databehandleravtalen (DBA) fastsetter rettighetene og forpliktelsene til den behandlingsansvarlige og databehandleren ved behandling av personopplysninger på vegne av den behandlingsansvarlige, som en del av GSGroup Tjenester.

2. Denne DBA er utformet for å sikre partenes overholdelse av artikkel 28 (3) i europaparlaments- og rådsforordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning). Denne DBA er basert på en standard som er godkjent av tilsynsmyndighetene i Norge og Danmark.

3. I forbindelse med leveringen av GSGroup Tjenester, som skal leveres til Kunden fra tid til annen i henhold til avtalen mellom partene (Avtalen), vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i samsvar med denne DBA. Denne DBA er en integrert del av Avtalen.

4. Denne DBA skal prioriteres fremfor eventuelle lignende bestemmelser i andre avtaler mellom partene.

5. Det er to vedlegg til DBA, og disse utgjør en integrert del av DBA.

6. Vedlegg A inneholder følgende angående GSGroups sensorløsninger:

    a. Informasjon om behandlingen av personopplysninger, herunder formålet med og arten av behandlingen, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.

    b. Adresserer databehandlerens bruk av underbehandlere.

    c. Inneholder de avtalte minimum sikkerhetstiltakene som skal gjennomføres av databehandleren, samt stedet der behandlingen skal utføres.

7. Vedlegg B inneholder følgende angående GSGroup Field service-løsninger:

    a. Informasjon om behandlingen av personopplysninger, herunder formålet med og arten av behandlingen, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.

    b. Adresserer databehandlerens bruk av underbehandlere.

    c. Inneholder de avtalte minimum sikkerhetstiltakene som skal gjennomføres av databehandleren, samt hvor behandlingen skal utføres.

8. Denne DBA med vedlegg skal oppbevares skriftlig, inkludert elektronisk, av begge parter.

9. Denne DBA skal ikke frita databehandleren fra forpliktelser som databehandleren er underlagt i henhold til personvernforordningen (GDPR) eller annen lovgivning.

3. Rettighetene og forpliktelsene til den behandlingsansvarlige

1. Behandlingsansvarlig er behandlingsansvarlig og databehandler er databehandler i forbindelse med GDPR og relevant lovgivning i EU- og EØS-land.

2. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i samsvar med personvernforordningen (jf. personvernforordningen artikkel 24), gjeldende personvernbestemmelser i EU- eller EØS-medlemsstatene og denne DBA.

3. Den behandlingsansvarlige har rett og plikt til å treffe beslutninger om formålene med og midlene til behandling av personopplysninger.

4. Den behandlingsansvarlige skal blant annet være ansvarlig for å sikre at behandlingen av personopplysninger, som databehandleren er bedt om å utføre, har et rettslig grunnlag. I den grad gjeldende lovverk krever det, eller der samtykke brukes som juridisk basis for behandling av personopplysninger, har databehandleren ansvaret for å sikre at den registrerte har gitt et informert, fritt, uttrykt og utvetydig samtykke før behandlingen samt for å kunne dokumentere at samtykke er gitt.

4. Databehandleren opptrer i henhold til instrukser

1. Databehandleren skal kun behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige, med mindre det kreves av lovgivning i EU- eller EØS-medlemsstatene som databehandleren er underlagt. Slike instrukser skal spesifiseres i vedlegg A og B. Etterfølgende instrukser kan også gis av den behandlingsansvarlige i løpet av den tiden personopplysningene behandles, men slike instrukser skal alltid dokumenteres og lagres skriftlig, inkludert elektronisk, sammen med denne DBA.

2. I den grad en tredjeparts leverandør av integrasjonstjenester får i oppdrag å sikre at behandlingsansvarlig kan bruke GSGroup Tjenester, instruerer behandlingsansvarlig herved databehandleren om å behandle personopplysninger i forbindelse med tjenestene fra slik tredjeparts leverandør av integrasjonstjenester for å levere GSGroup Tjenester. Databehandleren kan ikke holdes ansvarlig for konsekvenser som følge av atferd, utelatelser eller feil fra tredjeparts leverandør av integrasjonstjenester. For å eliminere enhver tvil engasjeres slik tredjeparts leverandør av integrasjonstjenester som den behandlingsansvarliges databehandler, ikke som databehandlerens underbehandler, med mindre partene har avtalt noe annet skriftlig.

3. Databehandleren skal umiddelbart informere den behandlingsansvarlige dersom instrukser gitt av den behandlingsansvarlige etter databehandlerens mening strider mot personvernforordningen eller gjeldende personvernbestemmelser i EU- eller EØS-medlemsstatene, i den grad databehandleren er klar over eller med rimelighet kan forventes å være klar over slike brudd. Under slike omstendigheter skal ikke databehandleren være pålagt å følge den behandlingsansvarliges instrukser, med mindre den behandlingsansvarlige skaffer en rettslig uttalelse fra et anerkjent advokatfirma med god anseelse som bekrefter at slike instrukser er i samsvar med personvernforordningen og alle andre gjeldende personvernbestemmelser.

4. Ved endringer i gjeldende personvernlovgivning har behandlingsansvarlig rett til å endre instruksjonene i denne DBA ved å gi 30 dagers skriftlig varsel før databehandleren får nye skriftlige instruksjoner.

5. Databehandleren kan behandle anonymiserte data i forbindelse med statistikk, analyser og andre formål. Slike andre formål kan inkludere å forbedre, støtte og drifte GSGroup Tjenester. Slike data skal ikke kunne brukes til identifikasjon.

5. Konfidensialitet

1. Databehandleren skal kun gi tilgang til personopplysningene som behandles på vegne av den behandlingsansvarlige til personer under databehandlerens myndighet som har forpliktet seg til konfidensialitet eller er underlagt en egnet lovfestet taushetsplikt, og kun ved behov for kunnskap. Listen over personer som har fått tilgang fra databehandleren, skal gjennomgås regelmessig. På bakgrunn av denne gjennomgangen kan slik tilgang til personopplysninger opphøre dersom tilgang ikke lenger er nødvendig, og personopplysninger vil dermed ikke lenger være tilgjengelig for disse personene.

2. Databehandleren skal på anmodning fra den behandlingsansvarlige legge frem dokumentasjon som viser at de berørte personene under databehandlerens myndighet er underlagt ovennevnte konfidensialitet.

3. Databehandleren kan ikke holdes ansvarlig for at den behandlingsansvarlige gir andre tilgang til konfidensiell informasjon.

6. Sikkerhet ved behandlingen

1. Personvernforordningen artikkel 32 fastsetter at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

2. Den behandlingsansvarlige skal vurdere risikoen for fysiske personers rettigheter og friheter forbundet med behandlingen og gjennomføre tiltak for å begrense disse risikoene.

3. I henhold til personvernforordningen artikkel 32 skal databehandleren også – uavhengig av den behandlingsansvarlige – vurdere risikoen for fysiske personers rettigheter og friheter forbundet med behandlingen og gjennomføre tiltak for å begrense disse risikoene. For å sikre dette skal den behandlingsansvarlige gi databehandleren all informasjon som er nødvendig for å identifisere og vurdere slike risikoer.

4. Videre skal databehandleren bistå den behandlingsansvarlige med å sikre overholdelse av den behandlingsansvarliges forpliktelser i henhold til personvernforordningen artikkel 32, ved blant annet å gi den behandlingsansvarlige informasjon om de tekniske og organisatoriske tiltakene som allerede er gjennomført av databehandleren i henhold til personvernforordningen artikkel 32, sammen med all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sin forpliktelse i henhold til personvernforordningen artikkel 32.

5. Dersom reduksjon av de identifiserte risikoene senere – etter den behandlingsansvarliges vurdering – krever at flere tiltak gjennomføres av databehandleren, enn de som allerede er gjennomført av databehandleren i henhold til personvernforordningen artikkel 32, skal den behandlingsansvarlige spesifisere disse ytterligere tiltakene skriftlig. Databehandleren er ikke pålagt å følge en eventuell anmodning fra den behandlingsansvarlige om slike ytterligere tiltak, med mindre de ytterligere tiltakene som den behandlingsansvarlige har anmodet om er rimelige og forholdsmessige under alle omstendigheter.

7. Bruk av underbehandlere

1. Databehandleren skal oppfylle kravene som er angitt i personvernforordningen artikkel 28 (2) og (4) for å engasjere en annen behandler (en underbehandler).

2. Databehandleren skal derfor ikke engasjere en annen databehandler (underbehandler) for oppfyllelse av denne DBA, uten at det på forhånd er innhentet generell skriftlig tillatelse til dette fra den behandlingsansvarlige.

3. Databehandleren har den behandlingsansvarliges generelle tillatelse til å engasjere underbehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere minst 14 dager i forkant, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer før den/de aktuelle underbehandleren(e) engasjeres. Listen over underbehandlere som allerede er godkjent av den behandlingsansvarlige, er tilgjengelig på databehandlerens nettsted.

4. Når databehandleren engasjerer en underbehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal de samme personvernforpliktelsene som er fastsatt i denne DBA pålegges underbehandleren ved kontrakt eller annen rettslig handling i henhold til lovgivning i EU- eller EØS-medlemsstatene, og det skal særlig gis tilstrekkelige garantier for gjennomføring av egnede tekniske og organisatoriske tiltak, på en slik måte at behandlingen vil oppfylle kravene i denne DBA og personvernforordningen. Databehandleren skal derfor være ansvarlig for å kreve at underbehandleren i det minste overholder forpliktelsene som databehandleren er underlagt i henhold til denne DBA og personvernforordningen.

5. En kopi av en slik underbehandleravtale og etterfølgende endringer skal – på anmodning fra den behandlingsansvarlige – sendes til den behandlingsansvarlige, slik at den behandlingsansvarlige gis mulighet til å sikre at de samme personvernforpliktelsene som fremgår av denne DBA pålegges underbehandleren. Bestemmelser om forretningsrelaterte spørsmål som ikke påvirker det rettslige innholdet om personvern i underbehandleravtalen trengs ikke sendes til den behandlingsansvarlige.

6. Dersom underbehandleren ikke oppfyller sine personvernforpliktelser, skal databehandleren være fullt ut ansvarlig overfor den behandlingsansvarlige med hensyn til oppfyllelsen av underbehandlerens forpliktelser. Dette påvirker ikke rettighetene til de registrerte etter personvernforordningen – spesielt de som fremgår av personvernforordningen artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, herunder underbehandleren.

7. Tjenester levert til databehandleren som er supplementære eller perifere sammenlignet med databehandlerens tjenester som leveres til den behandlingsansvarlige, skal ikke anes som underbehandling etter punkt 7. Disse inkluderer, for eksempel, telekommunikasjonstjenester, vedlikehold og brukerservice, renholdstjenester, revisorer, advokater, fjerning av datalagringsmedier, ERP-systemer (NetSuite og Visma Netvisor) og kontorstøttesystemer/administrasjonssystemer. Databehandleren er imidlertid forpliktet til å inngå egnede avtaler med slike tredjeparts tjenesteleverandører og til å sikre vern av og sikkerheten til opplysninger som eventuelt behandles på vegne av den behandlingsansvarlige.

8. Overføring av opplysninger til land utenfor EØS eller internasjonale organisasjoner

1. Enhver overføring av personopplysninger til land utenfor EØS eller internasjonale organisasjoner gjort av databehandleren skal kun skje på grunnlag av dokumenterte instrukser fra den behandlingsansvarlige og alltid i samsvar med personvernforordningen kapittel V.

2. Ved overføringer til land utenfor EØS eller internasjonale organisasjoner, som databehandleren ikke har fått beskjed om å utføre av den behandlingsansvarlige, med mindre det kreves i henhold til EU-retten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumenterte instrukser fra den behandlingsansvarlige kan ikke databehandleren innenfor denne DBAs ramme:

    a. overføre personopplysninger til en behandlingsansvarlig eller en databehandler i et land utenfor EØS eller i en internasjonal organisasjon

    b. overføre behandlingen av personopplysninger til en underbehandler i et land utenfor EØS

    c. få personopplysningene behandlet av databehandleren i et land utenfor EØS

4. Den behandlingsansvarliges instrukser om overføring av personopplysninger til et land utenfor EØS, herunder, hvis aktuelt, overføringsverktøyet som de er basert på etter personvernforordningen kapittel V, skal angis skriftlig.

5. Denne DBA skal ikke forveksles med standard personvernbestemmelser i henhold til personvernforordningen artikkel 46 (2) (c) og (d), og denne DBA kan ikke anses som et overføringsverktøy av partene i henhold til personvernforordningen kapittel V.

9. Bistand til den behandlingsansvarlige

1. Idet det tas hensyn til behandlingens art og i den grad det er mulig, skal databehandleren ved hjelp av egnede tekniske og organisatoriske tiltak bistå den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

    Dette innebærer at databehandleren, i den grad det er mulig, skal bistå den behandlingsansvarlige i dennes overholdelse av:

    a. retten til å bli informert ved innhenting av personopplysninger fra den registrerte
    b. retten til å bli informert når personopplysninger ikke er innhentet fra den registrerte
    c. den registrertes rett til innsyn
    d. retten til retting
    e. retten til sletting («retten til å bli glemt»)
    f. retten til begrensning av behandling
    g. underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
    h. retten til dataportabilitet
    i. retten til å protestere
    j. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering

2. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt 6.3., skal databehandleren videre, idet det tas hensyn til behandlingens art og informasjonen som er tilgjengelig for databehandleren, bistå den behandlingsansvarlige med å sikre overholdelse av:

    a. Den behandlingsansvarliges forpliktelse til, uten unødig forsinkelse, og, der det er mulig, senest 72 timer etter å ha fått kjennskap til det, å varsle bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, med mindre bruddet på personopplysningssikkerheten sannsynligvis ikke vil innebære en risiko for fysiske personers rettigheter og friheter;

    b. den behandlingsansvarliges forpliktelse til, uten unødig forsinkelse, å underrette den registrerte om bruddet på personopplysningssikkerheten, når det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre høy risiko for fysiske personers rettigheter og friheter;

    c. den behandlingsansvarliges plikt til å foreta en vurdering av virkningen av de planlagte prosessene for behandling når det gjelder vern av personopplysninger (en vurdering av personvernkonsekvenser);

    d. den behandlingsansvarliges plikt til å rådføre seg med vedkommende tilsynsmyndighet før behandlingen, dersom en vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

10. Melding av brudd på personopplysningssikkerheten

1. Ved brudd på personopplysningssikkerheten skal databehandleren, uten unødig forsinkelse, etter å ha blitt oppmerksom på det, varsle den behandlingsansvarlige om bruddet på personopplysningssikkerheten.

2. Databehandlerens melding til den behandlingsansvarlige skal om mulig fremsettes innen 36 timer etter at databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, for at den behandlingsansvarlige skal kunne overholde sin plikt til å melde bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, jf. personvernforordningen art. 33.

3. I samsvar med punkt 9 (2) (a) skal databehandleren bistå den behandlingsansvarlige med å melde bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, hvilket betyr at databehandleren er pålagt å bistå med å innhente den informasjonen som er oppført nedenfor, som i henhold til personvernforordningen artikkel 33 (3) skal fremsettes i den behandlingsansvarliges melding til vedkommende tilsynsmyndighet:

    a. Personopplysningenes art, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt;

    b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;

    c. tiltakene som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

11. Sletting og tilbakelevering av opplysninger

1. Ved avsluttet Avtalen skal databehandleren være forpliktet til, på skriftlig anmodning, å tilbakelevere alle personopplysningene til den behandlingsansvarlige og slette eksisterende kopier, med mindre medlemsstatenes nasjonal lovgivning i EU- eller EØS-landet inneholder krav om lagring av personopplysningene.

12. Revisjon og inspeksjon

1. Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 og denne DBA er oppfylt, samt muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

2. Databehandleren skal være pålagt å gi tilsynsmyndighetene, som i henhold til gjeldende lovgivning har tilgang til den behandlingsansvarliges og databehandlerens anlegg, eller representanter som handler på vegne av slike tilsynsmyndigheter, tilgang til databehandlerens fysiske anlegg ved presentasjon av riktig identifikasjon.

13. Skadesløshet og ansvarsbegrensning

1. Behandlingsansvarlig skal holde databehandleren skadesløs og for egen regning forsvare databehandleren mot kostnader, krav, skader eller utgifter som påløper databehandleren eller som databehandleren er ansvarlig for som følge av feil fra behandlingsansvarlig eller dennes ansatte/agenter eller som følge av at behandlingsansvarlig eller dennes ansatte/agenter ikke har oppfylt sine forpliktelser som angitt i gjeldende lovgivning eller denne DBA.

2. Databehandleren skal holde behandlingsansvarlig skadesløs og for egen regning forsvare behandlingsansvarlig mot kostnader, krav, skader eller utgifter som påløper behandlingsansvarlig eller som databehandleren er ansvarlig for som følge av feil fra databehandleren eller dennes ansatte/agenter eller som følge av at databehandleren eller dennes ansatte/agenter ikke har oppfylt sine forpliktelser som angitt i gjeldende lovgivning eller denne DBA.

3. Ansvarsbegrensningene som er fastsatt i GSGroups Generelle vilkår påvirkes ikke av vilkårene i denne DBA og gjelder i sin helhet. Databehandlerens ansvar skal under ingen omstendigheter overskride enten beløpet som behandlingsansvarlig har betalt for GSGroup Tjenester til databehandleren i løpet av de 12 månedene umiddelbart før eventuelle brudd på Avtalen eller denne DBA eller 100 000 euro, avhengig av hvilket beløp som er lavest.

14. Ikrafttredelse og oppsigelse

1. Denne DBA trer i kraft den datoen den behandlingsansvarlige godtar Avtalen eller denne DBA, avhengig av hva som kommer først. Denne DBA trenger ikke å signeres for at den skal være gyldig.

2. Databehandleren har rett til å endre denne DBA hvis det oppstår endringer i lovverket, hvis det er hensiktsmessig for denne DBA eller hvis andre krav til samsvar fører til behov for slike endringer.

3. Denne DBA gjelder så lenge Avtalen løper. Så lenge Avtalen løper kan ikke denne DBA avsluttes med mindre partene har avtalt en annen databehandleravtale i forbindelse med Avtalen.

4. Dersom Avtalen sies opp og personopplysningene slettes i samsvar med punkt 11.1., kan begge parter si opp denne DBA skriftlig.

15. Kontakter/kontaktpunkter for behandlingsansvarlig og databehandler

1. Partene kan kontakte hverandre ved hjelp av deres kontakter/kontaktpunkter. Den behandlingsansvarlige skal gi databehandleren minst to kontakter/kontaktpunkter på tidspunktet for inngåelse av en avtale knyttet til levering av GSGroup Tjenester. Databehandlerens kontaktpunkt for saker vedrørende DBA er: privacy@onegsgroup.com. Partene skal ha plikt til kontinuerlig å informere hverandre om endringer i kontakter/kontaktpunkter, og de har rett til å kontakte hverandre med rimelige intervaller for å forsikre seg om at de har riktige kontakter/kontaktpunkter.

Vedlegg A: GSGroup Sensorløsninger – Informasjon om behandlingen

Dette vedlegget er en del av den behandlingsansvarliges instruks til databehandleren i forbindelse med databehandlerens databehandling på vegne av den behandlingsansvarlige.

1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

Å levere tjenestene i henhold til Avtalen.

2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal i hovedsak omfatte (behandlingens art):

Innhenting, lagring, registrering, strukturering, tilpasning, tilgjengeliggjøring av opplysninger for Kunden og dens brukere for å levere tjenester i henhold til Avtalen.

Gjøre opplysninger tilgjengelige for GSGroups tekniske personell og støttepersonell for å levere tjenester i henhold til Avtalen.

Innhenting og analyse av hvordan GSGroup Tjenester benyttes for å forbedre hvordan tjenester leveres i henhold til Avtalen.

Anonymisering, pseudonymisering og sletting.

3. Behandlingen omfatter følgende typer personopplysninger om registrerte:[2]

Navn og kontaktinformasjon, innloggingsinformasjon (påloggingstidspunkt, brukernavn og passord), objektrelatert informasjon, bruk av objekt, ID-informasjon, førerkort, ansattnummer, stilling, stedsdata, reiseformasjon (inkludert start- og stoppsteder), hastighet, retning, varighet, avstand, temperatur, digital signatur, føreraktiviteter (f.eks. kjøring og hvile), bompasseringer (inkludert timing), bomstasjoner og eierskap, bompenger som skal betales.

Logging av bruk/brukermønstre, statistikk og analysedata, herunder IP-adresse.

Behandlingen kan kun omfatte noen og ikke alle typer personopplysninger som er nevnt ovenfor, avhengig av det nøyaktige produktet/tjenesten som Kunden har kjøpt. Ved tvil skal den behandlingsansvarlige kontakte databehandleren.

4. Behandlingen omfatter følgende kategorier av registrerte:

Kunder

Kundens ansatte

Kundens kunder (og andre personers opplysninger som Kunden har valgt at skal behandles som en del av GSGroup Tjenester)

[2] Partene har avtalt at databehandleren kan behandle andre typer personopplysninger som gjøres tilgjengelig av behandlingsansvarlig for å levere GSGroup Tjenester. Behandlingsansvarlig gir herved databehandleren i oppdrag å behandle alle typer slike opplysninger i samsvar med denne DBA for det formålet.

5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan utføres når denne DBA trer i kraft. Behandlingen har følgende varighet:

Databehandleren kan behandle personopplysninger på vegne av behandlingsansvarlig til behandlingsansvarlig skriftlig ber databehandler om å returnere alle personopplysningene til den behandlingsansvarlige og slette eksisterende kopier (se punkt 11 om sletting ved terminering), med mindre lovverket i EU- eller EØS-landet krever at personopplysningene lagres.

6. Godkjente underbehandlere og behandlingssted

Behandlingsansvarlig godkjenner engasjeringen av underbehandlerne som er oppført på databehandlerens nettsted for behandling av personopplysninger som en del av GSGroup Sensorløsninger. Denne behandlingen utføres på stedene som er angitt på databehandlerens nettsted.

7. Minimumstiltak for sikker behandling

Idet det tas hensyn til mengden personopplysninger, hvorav de fleste, hvis ikke samtlige, ikke faller inn under de særlige kategoriene av personopplysninger i personvernforordningen artikkel 9, i sammenheng med og for det formål å levere GSGroup Sensorløsninger der behandling av personopplysninger er et tilfeldig aspekt / en følge av databehandlerens tjenester, samt en generell lav risiko for fysiske personers rettigheter og friheter ved behandlingen av slike opplysninger, er partene enige om at databehandleren skal utøve skjønn når det gjelder beslutninger om tekniske og organisatoriske sikkerhetstiltak som skal anvendes for å skape det nødvendige og avtalte nivået av datasikkerhet. Databehandleren skal imidlertid – under alle omstendigheter og som et minimum – gjennomføre følgende tiltak, som avtalt med den behandlingsansvarlige:

- GSGroups ansatte skal være underlagt taushetsplikt og få regelmessig opplæring i overholdelse av personvernforordningen.
- Opplysninger som overføres skal krypteres (HTTPS, TLS 1.2 eller nyere), med mindre Kunden ber om at opplysningene leveres via et ikke-kryptert medium.
- GSGroup vil gjennomføre tekniske tiltak for å kunne gjenopprette tilgjengeligheten og tilgangen til personopplysninger i tide ved en fysisk eller teknisk hendelse, herunder: daglig og automatisert sikkerhetskopiering, sikre avbruddsfri strømforsyning, enheter for overvåking av temperatur og fuktighet i serverrom, brann- og røykvarslersystemer i serverrom, klimaanlegg og alarmer for uautorisert tilgang til serverrom.
- Der det er relevant skal GSGroup gjennomføre tekniske tiltak for å sikre nøyaktigheten til opplysninger som behandles på vegne av Kunden.
- Tilgang til Kundens opplysninger skal begrenses og kontrolleres, både fysisk (inkludert alarm- og låsesystem) og digitalt (autentisering ved hjelp av brukernavn- og passordbegrensninger).
- GSGroup skal benytte loggføring i driftsmiljøene der Kundens opplysninger behandles.
- GSGroup skal bruke VPN-teknologi for tilgang til driftsmiljøer.
- Lagrede opplysninger skal beskyttes av brannmurer.
- Lagrede opplysninger skal sikkerhetskopieres på minst ett annet separat og sikkert sted enn der de vanligvis lagres.

- GSGroup driftsmiljøer er atskilt fra GSGroup administrasjonsmiljøer.
- Kun autorisert personell med driftsbehov og kunder med begrensede tilgangsrettigheter har tilgang til driftsmiljøer. Passord til autorisert personell er kryptert og lagres også kryptert.
- GSGroup skal gjennomføre tekniske tiltak for antivirus, antimalware og antispam.
- GSGroup skal sørge for at det opprettholdes tilstrekkelig intern kompetanse for overholdelse av personvernforordningen.
- GSGroup Sensorløsninger har innebygd personvern ved at Kunden gis systemadministratorrettigheter.
- GSGroup skal sørge for at det finnes retningslinjer for makulering, rent skrivebord og ren skjerm.

Vedlegg B: GSGroup Field service-løsninger – Informasjon om behandlingen

Dette vedlegget er en del av den behandlingsansvarliges instruks til databehandleren i forbindelse med databehandlerens databehandling på vegne av den behandlingsansvarlige.

1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

Å levere tjenestene i henhold til Avtalen.

2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal i hovedsak omfatte (behandlingens art):

Innhenting, lagring, registrering, strukturering, tilpasning, tilgjengeliggjøring av opplysninger for Kunden og dens brukere for å levere tjenester i henhold til Avtalen.

Gjøre opplysninger tilgjengelige for GSGroups tekniske personell og støttepersonell for å levere tjenester i henhold til Avtalen.

Innhenting og analyse av hvordan GSGroup Tjenester benyttes for å forbedre hvordan tjenester leveres i henhold til Avtalen.

Anonymisering, pseudonymisering og sletting.

3. Behandlingen omfatter følgende typer personopplysninger om registrerte:[3]

Navn og kontaktinformasjon, påloggingsinformasjon (påloggingstidspunkt, brukernavn og passord), språk, kvalifikasjoner (lisenser, sertifikater og lignende), dato og klokkeslett for dataregistrering, ID-informasjon, førerkort, fødselsdato, ansattnummer, stilling, timelister, ansattlister, sjekklister, bruk av materialer, fotografier, informasjon om sikkerhet og miljø, informasjon om nærmeste pårørende, stedsdata, planlagte og personlige oppgaver, tidspunkt for synkroniseringer, IP-adresser til mobile enheter, type og modell mobil enhet, ferie og sykefravær.

Hvis Kunden kjøper en GSGroup Sensorløsning som en del av GSGroup Field service-løsninger (for eksempel sensormodul), inkluderer typene av personopplysninger som blir registrert, de typene som er inkludert i vedlegg A til denne DBA (se også vedlegg A for kategorier av registrerte samt annen relevant informasjon om behandling av personopplysninger).

Logging av brukermønstre, statistikk og analysedata, herunder IP-adresse.

Behandlingen kan kun omfatte noen og ikke alle typer personopplysninger som er nevnt ovenfor, avhengig av det nøyaktige produktet/tjenesten som Kunden har kjøpt. Ved tvil skal den behandlingsansvarlige kontakte databehandleren.

4. Behandlingen omfatter følgende kategorier av registrerte:

Kunder

[3] Partene har avtalt at databehandleren kan behandle andre typer personopplysninger som gjøres tilgjengelig av behandlingsansvarlig for å levere GSGroup Tjenester. Behandlingsansvarlig gir herved databehandleren i oppdrag å behandle alle typer slike opplysninger i samsvar med denne DBA for det formålet.

Kundens ansatte

Kundens kunder (og andre personers opplysninger som Kunden har valgt at skal behandles som en del av GSGroup Tjenester)

5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan utføres når denne DBA trer i kraft. Behandlingen har følgende varighet:

Databehandleren kan behandle personopplysninger på vegne av behandlingsansvarlig til behandlingsansvarlig skriftlig ber databehandler om å returnere alle personopplysningene til den behandlingsansvarlige og slette eksisterende kopier (se punkt 11 om sletting ved terminering), med mindre lovverket i EU- eller EØS-landet krever at personopplysningene lagres.

6. Godkjente underbehandlere og behandlingssted

Behandlingsansvarlig godkjenner engasjeringen av underbehandlerne som er oppført på databehandlerens nettsted for behandling av personopplysninger som en del av GSGroup Field service-løsninger. Denne behandlingen utføres på stedene som er angitt på databehandlerens nettsted. Behandlingen kan også utføres der den behandlingsansvarlige har IT-miljø/database.

7. Minimumstiltak for sikker behandling

Idet det tas hensyn til mengden personopplysninger, hvorav de fleste, hvis ikke samtlige, ikke faller inn under de særlige kategoriene av personopplysninger i personvernforordningen artikkel 9, i sammenheng med og for det formål å levere GSGroup Field service-løsninger der behandling av personopplysninger er et tilfeldig aspekt / en følge av databehandlerens aktiviteter, samt en generell lav risiko for fysiske personers rettigheter og friheter ved behandlingen av slike opplysninger, er partene enige om at databehandleren skal utøve skjønn når det gjelder beslutninger om tekniske og organisatoriske sikkerhetstiltak som skal anvendes for å skape det nødvendige og avtalte nivået av datasikkerhet. Databehandleren skal imidlertid – under alle omstendigheter og som et minimum – gjennomføre følgende tiltak, som avtalt med den behandlingsansvarlige:

- GSGroups ansatte skal være underlagt taushetsplikt og få regelmessig opplæring i overholdelse av personvernforordningen.
- GSGroup vil gjennomføre tekniske tiltak for å kunne gjenopprette tilgjengeligheten og tilgangen til personopplysninger i tide ved en fysisk eller teknisk hendelse, herunder: daglig og automatisert sikkerhetskopiering, sikre avbruddsfri strømforsyning, enheter for overvåking av temperatur og fuktighet i serverrom, brann- og røykvarslersystemer i serverrom, klimaanlegg og alarmer for uautorisert tilgang til serverrom.
- Der det er relevant skal GSGroup gjennomføre tekniske tiltak for å sikre nøyaktigheten til opplysninger som behandles på vegne av Kunden.
- Tilgang til Kundens opplysninger skal begrenses og kontrolleres, både fysisk (inkludert alarm- og låsesystem) og digitalt (autentisering ved hjelp av brukernavn- og passordbegrensninger).
- GSGroup skal benytte loggføring i driftsmiljøene der Kundens opplysninger behandles.
- GSGroup skal bruke VPN-teknologi for tilgang til driftsmiljøer.
- Lagrede opplysninger skal beskyttes av brannmurer.

- Lagrede opplysninger skal sikkerhetskopieres på minst ett annet separat og sikkert sted enn der de vanligvis lagres.
- GSGroup driftsmiljøer er atskilt fra GSGroup administrasjonsmiljøer.
- Kun autorisert personell med driftsbehov og kunder med begrensede tilgangsrettigheter har tilgang til driftsmiljøer. Passord til autorisert personell er kryptert og lagres også kryptert.
- GSGroup skal gjennomføre tekniske tiltak for antivirus, antimalware og antispam.
- GSGroup skal sørge for at det opprettholdes tilstrekkelig intern kompetanse for overholdelse av personvernforordningen.
- GSGroup Field service-løsninger har innebygd personvern ved at Kunden gis systemadministratorrettigheter.
- GSGroup skal sørge for at det finnes retningslinjer for makulering, rent skrivebord og ren skjerm.