Databehandleravtale

i henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (personvernforordningen) med henblikk på databehandlerens behandling av personopplysninger

mellom

Kunde

heretter «den behandlingsansvarlige»

og

Wittario AS
Org.nr. 915979025
Værftsgata 1 C
1511 Moss
Norge

heretter «databehandleren» som hver for seg er en «part» og sammen utgjør «partene». HAR AVTALT følgende standardavtalevilkår (Vilkårene) med henblikk på å overholde personvernforordningen og sikre beskyttelse av fysiske personers grunnleggende rettigheter og friheter.

Innhold

1. Innledning

1. Disse Vilkårene fastsetter den behandlingsansvarlige og databehandlerens rettigheter og plikter når databehandleren utfører behandling av personopplysninger på vegne av den behandlingsansvarlige.

2. Disse Vilkårene er utformet med for å sikre partenes etterlevelse av artikkel 28 nummer 3 i Europaparlamentets og Rådets forordning (EU) 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 (personvernforordningen).

3. I forbindelse med leveringen av «*Wittario med app/dashboard/nettløsning*» behandler databehandleren personopplysninger på vegne av den behandlingsansvarlige i overensstemmelse med disse Vilkårene.

4. Vilkårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.

5. Det er fire vedlegg til disse Vilkårene, og vedleggene utgjør en integrert del av Vilkårene.

6. Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder om behandlingens formål og art, typen av personopplysninger, kategoriene av registrerte og behandlingens varighet.

7. Vedlegg B inneholder den behandlingsansvarliges betingelser for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som den behandlingsansvarlige har godkjent.

8. Vedlegg C inneholder den behandlingsansvarliges instruks når det gjelder databehandlerens behandling av personopplysninger, en beskrivelse av de sikkerhetstiltakene som databehandleren som minimum skal gjennomføre, og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal utføres.

9. Vedlegg D inneholder bestemmelser om andre aktiviteter som ikke er omfattet av Vilkårene.

10. Vilkårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.

11. Disse Vilkårene fritar ikke databehandleren fra plikter som databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

2. Den behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernforordningen (se personvernfor-

ordningen artikkel 24), gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes[1] nasjonale rett og disse Vilkårene.

2. Den behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

3. Den behandlingsansvarlige er ansvarlig for, blant annet, å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om å gjøre.

3. Databehandleren handler etter instrukser

1. Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige, med mindre noe annet kreves av unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Disse instruksene skal være spesifisert i vedlegg A og C. Etterfølgende instrukser kan også gis av den behandlingsansvarlige mens det skjer behandling av personopplysninger, men instruksene skal alltid være dokumenterte og oppbevares skriftlig, herunder elektronisk, sammen med disse Vilkårene.

2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige, etter databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes nasjonale rett.

4. Konfidensialitet

1. Databehandleren kan bare gi tilgang til personopplysninger som behandles på den behandlingsansvarliges vegne til personer underlagt databehandlerens instruksjonsmyndighet som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i det nødvendige omfang. Listen av personer som har fått tilgang skal gjennomgås fortløpende. På bakgrunn av en slik gjennomgang kan tilgangen til personopplysninger stenges, dersom den ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelig for disse personene.

2. Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de aktuelle personene underlagt databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

5. Sikkerhet ved behandlingen

1. Personvernforordningen artikkel 32 fastslår 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.

[1] Henvisninger til «medlemsstater» i disse Vilkårene skal forstås som en henvisning til stater som er del av det europeiske økonomiske samarbeidsområdet (EØS-stater).

Den behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av relevans kan tiltakene omfatte:

a. pseudonymisering og kryptering av personopplysninger

b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene

c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse

d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. Ifølge personvernforordningen artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå risikoene. Med henblikk på denne vurderingen skal den behandlingsansvarlige stille den nødvendige informasjonen til rådighet for databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.

3. Databehandleren skal også bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges plikter etter personvernforordningen artikkel 32, ved blant annet å stille til den behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sine plikter etter personvernforordningen artikkel 32.

   Hvis imøtegåelse av de identifiserte risikoene – etter den behandlingsansvarliges vurdering – krever at det gjennomføres ytterligere tiltak enn det databehandleren allerede har gjennomført, skal den behandlingsansvarlige angi disse tiltakene i vedlegg C.

6. Bruk av underdatabehandlere

1. Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 nummer 2 og nummer 4 for å gjøre bruk av en annen databehandler (en underdatabehandler).

2. Databehandleren må således ikke bruke en underdatabehandler for å oppfylle Vilkårene uten på forhånd å ha innhentet *en generell skriftlig godkjennelse* fra den behandlingsansvarlige.

3. Databehandleren har den behandlingsansvarliges generelle godkjennelse til å benytte underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planlagte endringer som gjelder tilføyelse eller utskiftning av underdatabehandlere med minst *30 dagers* varsel og dermed gi den behandlingsansvarlige mulighet til å motsette seg slike endringer før den eller de beskrevne underdatabehandler(e) engasjeres. Lengre varslingsfrister for spesifikke underdatabehandlertjenester kan angis i vedlegg B. Listen over underdatabehandlere som den behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.

4. Når databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal underleverandøren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilkårene, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning.

   Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som minimum overholder databehandlerens forpliktelser etter disse Vilkårene og personvernforordningen.

5. En kopi av slik underdatabehandleravtale og eventuelle etterfølgende endringer skal – ved den behandlingsansvarliges anmodning – sendes til den behandlingsansvarlige, som på denne måten har mulighet for å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilkårene. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den behandlingsansvarlige.

6. Databehandleren skal i underdatabehandleravtalen inkludere den behandlingsansvarlige som begunstiget tredjepart i tilfelle databehandleren går konkurs, slik at den behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakeføre personopplysningene.

7. Hvis underdatabehandleren ikke oppfyller sine personopplysningsvernforpliktelser blir databehandleren fullt ut ansvarlig overfor den behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen – særlig de nedfestet i personvernforordningen artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

7. Overføring til tredjeland eller internasjonale organisasjoner

1. Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den behandlingsansvarlige, og slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.

2. Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumentert instruks fra den behandlingsansvarlige kan databehandleren innenfor rammene av disse Vilkårene således ikke:

a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon
b. overlate behandling av personopplysninger til en underdatabehandler i et tredjeland
c. behandle personopplysningene i et tredjeland

4. Den behandlingsansvarliges instruks når det gjelder overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningen kapittel V som overføringen er basert på, skal angis i vedlegg C.6.

5. Disse Vilkårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 nummer 2 bokstav c og d, og disse Vilkårene kan ikke utgjøre et grunnlag for overføring av personopplysninger under personvernforordningen kapittel V.

8. Bistand til den behandlingsansvarlige

1. Databehandleren bistår, idet det tas hensyn til behandlingens art og i den grad det er mulig, ved hjelp av egnede tekniske og organisatoriske tiltak, 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 så langt det er mulig skal bistå den behandlingsansvarlige i den behandlingsansvarlige oppfyllelse av:

   a. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
   b. opplysningsplikten dersom personopplysninger ikke er blitt samlet inn 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. underretningsplikten 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 automatisk behandling, herunder profilering

2. I tillegg til databehandlerens forpliktelse til å bistå den behandlingsansvarlige i henhold til Vilkårene 6.3., bistår databehandleren også, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, den behandlingsansvarlige med:

   a. den behandlingsansvarliges forpliktelse ved brudd på personopplysningssikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningssikkerheten til den kompetente tilsynsmyndigheten, *Datatilsynet*, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter

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

c. den behandlingsansvarliges forpliktelse til før behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (vurdering av personvernkonsekvenser)

d. den behandlingsansvarliges forpliktelse til å rådføre seg med den kompetente tilsynsmyndigheten, *Datatilsynet*, 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.

3. Partene skal i vedlegg C oppgi de egnede tekniske og organisatoriske tiltakene gjennom hvilke databehandleren skal bistå den behandlingsansvarlige, samt omfanget og utstrekningen av den påkrevde bistanden. Dette gjelder for forpliktelsene som følger av Vilkårene 9.1. og 9.2.

9. Underretning om brudd på personopplysningssikkerheten

1. Ved brudd på personopplysningssikkerheten skal databehandleren underrette den behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.

2. Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje innen *12 timer* etter at databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, slik at den behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.

3. I overensstemmelse med Vilkår 9 nummer 2 bokstav a skal databehandleren bistå den behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Det innebærer at databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 nummer 3 skal fremgå av den behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndigheten:

a. arten av bruddet på personopplysningssikkerheten, 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 konsekvenser av bruddet på personopplysningssikkerheten

c. de tiltak 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.

4. Partene skal i vedlegg C oppgi all informasjon som databehandleren skal fremskaffe når vedkommende bistår den behandlingsansvarlige med å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

10. Sletting og returnering av opplysninger

1. Ved opphør av databehandlertjenestene skal databehandleren *slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet*, med mindre unionsretten eller medlemsstatenes nasjonale rett krever oppbevaring av personopplysningene.

11. Revisjon, herunder inspeksjon

1. Databehandleren skal stille til den behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og disse Vilkårene. Videre skal databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor som er bemyndiget av den behandlingsansvarlige.

2. Prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av databehandleren og underdatabehandlere er spesifisert i vedlegg C.7 og C.8.

3. Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens lokaler, eller representanter som opptrer på slike tilsynsmyndigheters vegne, adgang til databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

12. Partenes avtale om andre forhold

1. Partene kan avtale andre bestemmelser som gjelder databehandlertjenestene, f.eks. erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot disse Vilkårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

13. Ikrafttredelse og opphør

1. Vilkårene trer i kraft på datoen for begge partenes underskrift.

2. Begge partene kan kreve Vilkårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilkårene gir grunn til dette.

3. Vilkårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilkårene ikke sies opp, med mindre partene avtaler andre vilkår som regulerer levering av databehandlertjenestene.

4. Hvis leveringen av databehandlertjenestene opphører, og personopplysningene er slettet eller returnert til den behandlingsansvarlige i overensstemmelse med Vilkårene 11.1 og vedlegg C.4, kan Vilkårene sies opp med skriftlig varsel av begge partene.

5. Underskrift

På vegne av den behandlingsansvarlige

Navn
Stilling
Telefonnummer
E-postadresse
Dato
Underskrift

På vegne av databehandleren

Navn	Lars Gunnar Fledsberg
Stilling	CEO
Telefonnummer	4794019520
E-postadresse	lgf@wittario.com
Dato	xx.xx.20xx
Underskrift	

14. Kontaktpersoner hos den behandlingsansvarlige og databehandleren

1. Partene kan kontakte hverandre via nedenstående kontaktpersoner.

2. Partene forplikter seg til å orientere hverandre løpende om endringer som gjelder kontaktpersoner.

Navn
Stilling
Telefonnummer
E-postadresse

Navn	Lars Gunnar Fledsberg
Stilling	CEO
Telefonnummer	+4794019520
E-postadresse	lgf@wittario.com

Vedlegg A Opplysninger om behandlingen

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

Å gi ansatte hos Kunde opplæring og utvikling gjennom bruk av «Wittario med app/dashboard/nettløsning» som tilrettelegger for spillbasert læring med aktivitet og mål om økt læringsutbytte.

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal primært dreier seg om (behandlingens art):

Innsamling, lagring, organisering, analyse og rapportering av personopplysninger knyttet til de ansattes læringsaktiviteter og prestasjoner.

Ledelse legger til rette for en læringssti gjennom å utforme kreative og selvrettende oppgaver. Denne læringsstien tar form som et spill, der de ansatte leverer f.eks. praktiske besvarelser via kamerabilder, spiller inn lydopptak eller gjennom å svare på quizer og refleksjonsoppgaver. Spillet kan spilles inne og utendørs, med eller uten fysisk aktivitet. Utendørs spill kan legges til en forhåndsbestemt rute eller med et distansekrav, slik at deltakerne forflytter seg i fysiske omgivelser utendørs.

A.3. Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

- Kontaktinformasjon bruker: Navn og e-post
- Organisasjonstilhørighet /enhets-ID
- Passord
    i. Lagres **ikke** i klartekst.
- Kontaktinformasjon for eier av organisasjonskonto; navn og kontaktinformasjon
- Organisasjon (som selskap, skole, forening mv.)
- Resultater for spill som er spilt, inkludert svar på spillene

A.4. Behandlingen omfatter følgende kategorier av registrerte:

Alle ansatte hos Kunde.

A.5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan begynne etter at Vilkårene har trådt i kraft. Behandlingen har følgende varighet:

Behandlingen skal vare å lenge Databehandleren leverer «Wittario med app/dashboard/nettløsning» til Behandlingsansvarlig. Nærmere beskrivelse for «Sletting og returnering av opplysninger» finnes i punkt 10.

Vedlegg B Underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
Google Norway AS	988 588 261	C. J. Hambros plass 2 D 0164 OSLO	Wittario lagrer data i Google FireStore Database og Firebase Storage. Fysisk beliggenhet for datasenteret er Frankfurt (Europa-vest 3).
Microsoft Norway AS	957 485 030	Lysaker torg 45 NO-1366 Lysaker	Wittario lagrer data i CosmosDb og Azure Storage. Fysisk beliggenhet for databasesenteret er Oslo (Norway East). Wittarios AI tjenester behandler data i det svenske datasentere Sweden Central. Databehandlingen foregår i Sweden Central for å utnytte spesialiserte AI-ressurser som ikke er tilgjengelige i Norway East. Ingen data lagres i Sweden Central.
MixPanel			Wittario bruker MixPanel til å analysere generelle bruksmønstre i produktet for å ha et datagrunnlag for å forbedre brukeropplevelsen. Data lagres i EU datasentre (Europe-West4): https://docs.mixpanel.com/docs/privacy/eu-residency Ingen direkte personopplysninger lagres i MixPanel, men systemet bruker en pseudonymisert identifikator (GUID) for å

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
			skille unike brukeres handlinger innad i MixPanel. Eksempler på slike handlinger er: *Starte spill* *Lage spill* *Lage oppgave* Det er kun metadata relatert til den utførste handlingen som overføres til MixPanel, ingen av brukerenes data (eksempelvis læringsinnhold, spillbesvarelser eller lignende) overføres. Mer informasjon om MixPanel som databehandler finnes her: https://mixpanel.com/legal/cdpa/
HubSpot CRM			Kundedata lagres i HubSpot sitt CRM system med det formål å håndtere Wittarios kundeforhold, support og kommunikasjon. HubSpot prosesserer data under sin DPA og er GDPR-compliant: https://legal.hubspot.com/legal-stuff Wittarios data i HubSpot lagres i deres europeiske datasenter i Tyskland.

Ved Vilkårenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. Databehandleren kan ikke – uten den behandlingsansvarliges eksplisitte skriftlige godkjennelse – benytte en underdatabehandler til en annen behandlingsaktivitet enn den som er avtalt for vedkommende eller bruke en annen underdatabehandler til den beskrevne behandlingsaktiviteten.

B.2. Varsel for godkjennelse av underdatabehandlere

Se punkt 6 «Bruk av underdatabehandlere».

Vedlegg C Instruks for behandling av personopplysninger

C.1. Behandlingens gjenstand/instruks for behandlingen

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

Databehandleren instrueres om å samle inn, lagre, organisere, analysere og rapportere data for å tilrettelegge for spillbasert læring i appen/dashboard/nettløsningen. Behandlingen skal utføres i henhold til avtalen og gjeldende personvernregler.

C.2. Informasjonssikkerhet

Sikkerhetsnivået for behandlingen av personopplysninger skal gjenspeile risikoen forbundet med behandlingen og personopplysningenes art. Det innebærer at sikkerhetstiltakene må være proporsjonale og tilpasset både type opplysninger og konsekvensene for de registrerte dersom noe går galt (f.eks. datainnbrudd, tap av data eller uautorisert tilgang).

Databehandleren har heretter rett og plikt til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige (og avtalte) sikkerhetsnivået.

Databehandleren skal likevel – under enhver omstendighet og som minimum – gjennomføre følgende tiltak, som er avtalt med den behandlingsansvarlige:

KIT står for Konfidensialitet, Integritet og Tilgjengelighet, og er et sentralt prinsipp innen informasjonssikkerhet og GDPR (jf. artikkel 32 i GDPR om sikkerhet ved behandling av personopplysninger). Sikkerhetsnivået skal reflektere disse prinsippene for å sikre en helhetlig tilnærming til databeskyttelse.

- Risikovurdering:
    - Regelmessige vurderinger av sikkerhetsrisiko knyttet til databehandlingen
    - Testing av systemet (penetrasjonstester) for å avdekke sårbarheter
- Tilgangskontroll:
    - Kun autoriserte brukere skal ha tilgang til dataene. Dette inkluderer:
        - Krypterte påloginger
        - Streng rolle- og tilgangsstyring for administrasjon
        - Loggføring av tilgang og forsøk på uautorisert tilgang
- Databeskyttelse:
    - Kryptering av data både under lagring og overføring
    - Kontrollmekanismer for å sikre korrekt lagring og overføring av data
    - Regelmessige sikkerhetskopier for å forhindre tap eller korrupsjon av data
    - Autentisering av brukere som legger inn, endrer eller sletter data
    - Systemvarslinger ved mistenkelige endringer eller forsøk på endring av data
    - Redundante servere og løsninger for å minimere nedetid
    - Regelmessige sikkerhetskopier som kan gjenopprettes raskt ved feil
    - Overvåkning av systemets ytelse for å sikre stabilitet
- Overholdelse av personvernregler:
    - Implementering av dataminimering
    - Sikring av data under behandlingsprosessen og ved sletting
- Håndtering av sikkerhetsbrudd:
    - Varslingsprosedyrer dersom brudd på sikkerheten oppstår
    - Beredskapsplan for håndtering av hendelser som datatap, tekniske feil eller tjenestenektangrep

- Skalering av sikkerhetsnivå:
    - Dersom appen eller plattformen begynner å behandle opplysninger som definert som særlige kategorier av opplysninger må sikkerhetsnivået justeres tilsvarende.

C.3 Bistand til den behandlingsansvarlige

Databehandleren skal i den grad det er mulig – i det nedenfor beskrevne omfang og utstrekning – bistå den behandlingsansvarlige i samsvar med Vilkårene 9.1 og 9.2 ved å gjennomføre følgende organisatoriske tiltak:

- Gi ansatte hos databehandler nødvendig opplæring i informasjonssikkerhet og GDPR-forpliktelser for å sikre at de håndterer personopplysninger på en trygg måte
- Utvikle og implementere interne prosedyrer for behandling av personopplysninger, inkludert håndtering av forespørsler fra registrerte og rapportering av sikkerhetsbrudd
- Bistå den behandlingsansvarlige med å svare på forespørsler fra registrerte i henhold til GDPR, inkludert innsyn, retting, sletting og dataportabilitet
- Varsle den behandlingsansvarlige om eventuelle sikkerhetsbrudd uten ugrunnet opphold, samt bistå med nødvendige undersøkelser og tiltak
- Bistå med gjennomføring av risikovurderinger og konsekvensanalyser (DPIA) der det er nødvendig
- Sikre at underleverandører har tilsvarende tekniske og organisatoriske tiltak som beskytter personopplysninger
- Gi den behandlingsansvarlige tilgang til nødvendig dokumentasjon for å verifisere at personopplysninger behandles i samsvar med gjeldende regelverk.
- Bistå i forbindelse med revisjoner eller inspeksjoner som den behandlingsansvarlig, eller tilsynsmyndigheter, ønsker å gjennomføre

C.4 Oppbevaringsperiode/sletteprosedyrer

Se punkt 10 om «Sletting og returnering av opplysninger», samt vedlegg A, punkt A5.

C.5 Lokasjon for behandling

Behandling av personopplysninger som omfattes av Vilkårene kan ikke, uten den behandlingsansvarliges skriftlige forhåndsgodkjennelse, finne sted på andre lokasjoner enn følgende:

Behandlingen finner sted innenfor EU/EØS, se lokasjon spesifisert i bilag B, punkt B.1.

C.6 Instruks for overføring av personopplysninger til tredjeland

Det skal ikke overføres personopplysninger til et tredjeland eller internasjonal organisasjon. Behandling skal kun skje innenfor EU/EØS.

C.7 Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

For å sikre etterlevelse av personvernregelverket (GDPR) og den inngåtte databehandleravtalen, skal den behandlingsansvarlige ha rett til å gjennomføre revisjoner, inkludert inspeksjoner, av databehandlerens behandling av personopplysninger. Revisjonene skal utføres i henhold til følgende prosedyrer:

- Varsling av revisjon
    - Den behandlingsansvarlige skal varsle databehandleren skriftlig i 30 dager før revisjonen
    - Varslet skal inneholde:
        - Formålet med revisjonen

        - Omfanget av revisjonen
        - Tidspunkt og varighet for revisjonen
        - Hvilke deler av behandlingen og systemene som vil bli inspisert
- Revisjonsfrekvens og omfang:
    - Revisjoner kan utføres årlig eller oftere ved behov, f.eks. ved mistanke om avvik, sikkerhetsbrudd eller endringer i databehandlerens systemer.
    - Revisjonen kan omfatte:
        - Fysiske lokaler der data behandles
        - Systemer og tekniske løsninger brukt til databehandling
        - Tilgangsstyring og loggføring
        - Dokumentasjon på implementerte tekniske og organisatoriske sikkerhetstiltak
        - Underleverandørers etterlevelse
- Gjennomføring av revisjon
    - Revisjonen skal utføres på en måte som ikke unødvendig forstyrrer databehandlerens daglige drift.
    - Revisjonen kan utføres:
        - Av den behandlingsansvarlige selv
        - Av en tredjepart (uavhengig revisor), utpekt av den behandlingsansvarlige
    - Databehandleren skal stille nødvendige ressurser til rådighet for å støtte revisjonen, herunder:
        - Gi tilgang til nødvendig dokumentasjon
        - Gi innsyn i systemer og prosesser der personopplysninger behandles
        - Besvare spørsmål fra revisor
- Revisjonsresultater og oppfølging
    - Etter revisjonen skal den behandlingsansvarlige utarbeide en revisjonsrapport med funn og anbefalinger.
    - Rapporten skal deles med databehandleren, som:
        - Skal gjennomgå funnene
        - Skal utarbeide en plan for nødvendige korrigerende tiltak dersom det oppdages avvik
        - Skal samarbeide med den behandlingsansvarlige for å løse identifiserte problemer innen en avtalt tidsfrist
- Kostnader
    - Revisjonskostnader bæres som hovedregel av den behandlingsansvarlige.
    - Hvis revisjonen avdekker vesentlige brudd på avtalen eller personvernregelverket, kan databehandleren være forpliktet til å dekke deler av kostnadene knyttet til revisjonen.
- Tredjepartsrevisjoner og sertifiseringer
    - Dersom databehandleren har tredjepartssertifiseringer (f.eks. ISO 27001), kan den behandlingsansvarlige be om kopi av gjeldende sertifiseringsrapporter som et alternativ til fysisk revisjon.
    - Slike tredjepartsrevisjoner kan bidra til å redusere behovet for omfattende inspeksjoner.
- Konfidensialitet
    - Revisjonsprosessen og funnene skal behandles som konfidensiell informasjon og ikke deles med uvedkommende med mindre det er pålagt i henhold til lov.

Vedlegg D Partenes regulering av andre forhold

Ingen.