Vedlegg til Alminnelige vilkår

Databehandleravtale

INNHOLDSFORTEGNELSE

1. BAKGRUNN OG AVTALENS FORMÅL 1
2. DEFINISJONER 1
3. BEHANDLING AV PERSONOPPLYSNINGER 1
4. INSTRUKSER 2
5. UNDERDATABEHANDLERE 2
6. OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND 2
7. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK 3
8. SIKKERHET OG KONFIDENSIALITET 3
9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN 3
10. BISTAND TIL KUNDEN 4
11. REVISJON 4
12. AVTALEPERIODE OG OPPHØR 4
13. ØVRIG 5
UNDERVEDLEGG 1 – SPESIFIKASJON AV BEHANDLINGEN 6
UNDERVEDLEGG 2 – TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK 8
UNDERVEDLEGG 3 – FORHÅNDSGODKJENTE UNDERDATABEHANDLERE 9

1. BAKGRUNN OG AVTALENS FORMÅL

Denne databehandleravtalen (**”Avtalen”**) utgjør et vedlegg til de alminnelige vilkårene (**”Alminnelige Vilkår”**) som regulerer leveringen av tjenester (**”Tjenestene”**) mellom Leverandøren og Kunden. Begrepene ”Leverandøren”, ”Kunden” og ”Partene” har den betydningen som er angitt i Alminnelige Vilkår. Avtalen regulerer Leverandørens behandling av personopplysninger på vegne av Kunden i forbindelse med Tjenestene, og er utarbeidet for å oppfylle kravene i artikkel 28 i Europaparlaments- og rådsforordning (EU) 2016/679 (**”GDPR”**).

Ved motstrid mellom Avtalen og Alminnelige Vilkår skal Avtalen ha forrang i spørsmål som gjelder behandling av personopplysninger. Øvrige spørsmål reguleres av Alminnelige Vilkår, som også gjelder for Avtalen.

Nærmere detaljer om Behandlingen er angitt i Undervedlegg 1 (Spesifikasjon av Behandlingen). Ved motstrid mellom Avtalen og Undervedlegg 1 har Undervedlegg 1 forrang i spørsmål som gjelder den spesifikke Behandlingens art og omfang.

2. DEFINISJONER

I Avtalen har følgende begreper den betydningen som er angitt nedenfor. Øvrige begreper som brukes i Avtalen med stor forbokstav, har den betydningen som er angitt i Alminnelige Vilkår eller i GDPR.

- ”Behandling”, ”Personopplysning”, ”Behandlingsansvarlig”, ”Databehandler”, ”Brudd på personopplysningssikkerheten”, ”Registrert” og ”Tredjeland” har den betydningen som er angitt i artikkel 4 i personvernforordningen.
- **”**Personvernlovgivning**”** betyr GDPR, lov (2018:218) med utfyllende bestemmelser til EUs personvernforordning samt øvrige til enhver tid gjeldende lover og forskrifter og bindende avgjørelser fra kompetent tilsynsmyndighet om behandling av personopplysninger.
- ”Kundedata” har den betydningen som er angitt i Alminnelige Vilkår.
- **”**Underdatabehandler**”** betyr databehandler som Leverandøren benytter for å utføre Behandlingen, helt eller delvis, på vegne av Kunden.

3. BEHANDLING AV PERSONOPPLYSNINGER

Leverandøren er Databehandler og Kunden er Behandlingsansvarlig for den Behandlingen som utføres innenfor rammen av Tjenestene. Leverandøren behandler Personopplysninger utelukkende for å levere Tjenestene og utelukkende i samsvar med Kundens dokumenterte instrukser etter denne Avtalen og Undervedlegg 1.

Behandlingens gjenstand, art, varighet, formål, kategorier av Registrerte og kategorier av Personopplysninger fremgår av Undervedlegg 1.

Kunden er ansvarlig for at det foreligger et rettslig grunnlag etter Personvernlovgivningen for Behandlingen, og for at de instruksene Kunden gir Leverandøren er forenlige med Personvernlovgivningen. Kunden er videre ansvarlig for å ivareta de Registrertes rettigheter, for å melde Brudd på personopplysningssikkerheten til tilsynsmyndigheten i den grad det påhviler Kunden, samt for å sikre at personer som behandler Personopplysninger under Kundens instruksjonsmyndighet bare gjør det i samsvar med gitte instrukser.

Leverandøren påtar seg, i samsvar med artikkel 30 nr. 2 i personvernforordningen, å føre en protokoll over de kategoriene av Behandling som utføres på vegne av Kunden.

4. INSTRUKSER

Leverandøren kan bare behandle Personopplysninger i samsvar med Kundens

dokumenterte instrukser. Avtalen, herunder Undervedleggene, samt Alminnelige Vilkår utgjør Kundens fullstendige instrukser ved Avtalens inngåelse. Kunden kan i avtaleperioden gi ytterligere skriftlige instrukser i den grad det er nødvendig for å oppfylle Personvernlovgivningen.

Dersom Leverandøren vurderer at en instruks er i strid med Personvernlovgivningen, skal Leverandøren uten ugrunnet opphold skriftlig underrette Kunden. Leverandøren har rett til å avvente utførelsen av en slik instruks inntil Kunden har bekreftet eller endret instruksen.

For håndtering av instrukser eller endringer som ikke er foranlediget av lovkrav som samtlige eller størstedelen av Leverandørens kunder er underlagt, har Leverandøren rett til rimelig vederlag i henhold til den til enhver tid gjeldende prislisten. Leverandøren skal underrette Kunden på forhånd om slikt vederlag, og Kunden skal godkjenne faktureringen før arbeidet påbegynnes. Dersom Kunden ikke godkjenner faktureringen, kan Leverandøren si opp den aktuelle Tjenesten med iakttakelse av rimelig oppsigelsestid.

5. UNDERDATABEHANDLERE

Kunden gir med dette Leverandøren en generell forhåndstillatelse til å benytte Underdatabehandlere for utførelsen av Tjenestene. Forhåndsgodkjente Underdatabehandlere er angitt i Undervedlegg 3. En til enhver tid oppdatert oversikt over benyttede Underdatabehandlere, herunder opplysning om sted for Behandlingen, er publisert på https://caspeco.com/gdpr/.

Leverandøren skal skriftlig underrette Kunden minst tretti (30) dager før en ny Underdatabehandler benyttes eller en eksisterende Underdatabehandler erstattes. Underretning skjer ved oppdatering av oversikten på det ovenfor angitte nettstedet, samt, dersom Kunden ber om det, ved direkte skriftlig melding eller tilsvarende abonnementstjeneste.

Kunden har rett til innen tretti (30) dager fra underretningen skriftlig å protestere mot endringen på legitime grunner knyttet til vernet av Personopplysninger. Dersom Leverandøren ikke kan imøtekomme Kundens legitime innsigelse, har Kunden rett til skriftlig å si opp den eller de berørte Tjenestene med iakttakelse av den oppsigelsestiden som følger av Alminnelige Vilkår. Dersom Kunden verken godkjenner eller protesterer innen angitt frist, anses Underdatabehandleren som godkjent.

Leverandøren skal inngå skriftlig avtale med hver Underdatabehandler som pålegger Underdatabehandleren i det alt vesentlige de samme forpliktelsene med hensyn til personvern som følger av denne Avtalen, særlig kravene etter artikkel 28 nr. 3 i personvernforordningen. Leverandøren er overfor Kunden ansvarlig for Underdatabehandlerens oppfyllelse av sine forpliktelser på samme måte som for sine egne forpliktelser.

6. OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND

Personopplysninger skal som utgangspunkt behandles innenfor EU/EØS. Leverandøren kan overføre Personopplysninger til, eller gi tilgang fra, et land utenfor EU/EØS bare dersom (i) landet omfattes av en beslutning om tilstrekkelig beskyttelsesnivå fra Europakommisjonen, (ii) overføringen skjer med grunnlag i Europakommisjonens standard personvernbestemmelser eller bindende virksomhetsregler, eller (iii) det foreligger et annet gyldig overføringsgrunnlag etter kapittel V i personvernforordningen.

Leverandøren skal, når det kreves, gjennomføre en vurdering av beskyttelsesnivået i mottakerlandet (transfer impact assessment) og iverksette slike supplerende tekniske, organisatoriske og avtalemessige beskyttelsestiltak som er nødvendige for å sikre et beskyttelsesnivå som i det vesentlige tilsvarer nivået innenfor EU/EØS. Leverandøren har rett til å inngå

standard personvernbestemmelser med Underdatabehandlere på vegne av Kunden.

Dersom det rettslige grunnlaget for en pågående overføring opphører å gjelde, skal Partene uten ugrunnet opphold samarbeide for å identifisere en alternativ overføringsmekanisme eller supplerende beskyttelsestiltak. Dersom slike tiltak ikke kan iverksettes innen rimelig tid, skal overføringen avbrytes.

Dersom Leverandøren mottar en bindende anmodning fra en myndighet i et Tredjeland om utlevering av Personopplysninger, skal Leverandøren, med mindre det er forbudt etter gjeldende lov, uten ugrunnet opphold underrette Kunden samt iverksette rimelige rettslige tiltak for å begrense utleveringen.

7. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Leverandøren skal iverksette egnede tekniske og organisatoriske sikkerhetstiltak etter artikkel 32 i personvernforordningen for å sikre et sikkerhetsnivå som er egnet i forhold til risikoen ved Behandlingen. En overordnet beskrivelse av Leverandørens sikkerhetstiltak fremgår av Undervedlegg 2. Leverandøren har rett til fra tid til annen å oppdatere sikkerhetstiltakene, forutsatt at beskyttelsesnivået ikke svekkes vesentlig.

For Tjenester som omfatter kortbehandling, anvendes Payment Card Industry Data Security Standard (PCI DSS) i den grad det er relevant. Kunden er ansvarlig for å holde seg informert om og følge de reglene og rutinene som banker og andre aktører som Leverandøren samarbeider med, til enhver tid anvender for leveringen av Tjenestene.

Kunden er innenfor sitt system og sin kontrollsfære ansvarlig for behandling av innloggingsopplysninger, transaksjonsinformasjon og øvrig datasikkerhet. Kunden skal umiddelbart underrette Leverandøren ved mistanke om brudd på datasikkerheten på Kundens side.

Dokumentasjon over Leverandørens tekniske og organisatoriske sikkerhetstiltak skal på Kundens skriftlige anmodning gjøres tilgjengelig uten ugrunnet opphold.

8. SIKKERHET OG KONFIDENSIALITET

Leverandøren skal sikre at personer som har tilgang til å behandle Personopplysninger under Avtalen, har påtatt seg å iaktta konfidensialitet eller er underlagt en egnet lovbestemt taushetsplikt. Leverandøren skal videre sikre at tilgangen til Personopplysninger begrenses til de personene som trenger tilgangen for å utføre sine arbeidsoppgaver.

Leverandøren kan ikke, uten Kundens samtykke eller grunnlag i lov eller bindende myndighetsvedtak, utlevere Personopplysninger til tredjepart. Dersom Leverandøren må utlevere Personopplysninger som følge av lov eller myndighetsvedtak, skal Kunden, med mindre det er forbudt, underrettes før utleveringen skjer.

9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

Leverandøren skal uten ugrunnet opphold, og senest innen syttito (72) timer fra Leverandøren ble kjent med et Brudd på personopplysningssikkerheten, skriftlig underrette Kunden. Underretningen skal, i den grad informasjonen er tilgjengelig, inneholde:

(a) en beskrivelse av bruddets art, herunder, om mulig, kategoriene og det omtrentlige antallet Registrerte samt Personopplysninger som berøres;

(b) navn og kontaktopplysninger til Leverandørens personvernombud eller annet kontaktpunkt der ytterligere informasjon kan innhentes;

(c) en beskrivelse av de sannsynlige konsekvensene av bruddet; og

(d) en beskrivelse av de tiltakene Leverandøren har iverksatt eller foreslår å iverksette for å håndtere bruddet og, der det er

hensiktsmessig, begrense dets negative virkninger.

Dersom all informasjon som nevnt ovenfor ikke kan gis samtidig, kan informasjonen gis trinnvis uten ugrunnet opphold. Leverandøren skal dokumentere samtlige Brudd på personopplysningssikkerheten og på Kundens skriftlige anmodning gjøre dokumentasjonen tilgjengelig.

Leverandøren skal omgående iverksette egnede utbedrende tiltak for å forhindre eller begrense de potensielle negative virkningene av bruddet, samt, ved behov, samarbeide med Kunden og kompetent tilsynsmyndighet.

10. BISTAND TIL KUNDEN

Leverandøren skal, ut fra Behandlingens art og den informasjonen Leverandøren har tilgjengelig, i rimelig utstrekning bistå Kunden med å oppfylle sine forpliktelser etter artikkel 32–36 i personvernforordningen om sikkerhet ved Behandlingen, melding av Brudd på personopplysningssikkerheten, vurderinger av personvernkonsekvenser samt forhåndsdrøfting med tilsynsmyndigheten.

Leverandøren skal videre, ut fra Behandlingens art, bistå Kunden gjennom egnede tekniske og organisatoriske tiltak for å oppfylle Kundens plikt til å besvare anmodninger fra Registrerte om utøvelse av deres rettigheter etter kapittel III i personvernforordningen (innsyn, retting, sletting, begrensning, dataportabilitet og innsigelse). Dersom en Registrert henvender seg direkte til Leverandøren, skal Leverandøren uten ugrunnet opphold videresende anmodningen til Kunden.

Bistand etter dette punktet skal ytes uten ugrunnet opphold. Leverandøren har rett til rimelig vederlag i henhold til den til enhver tid gjeldende prislisten for bistand som går ut over det som følger direkte av Leverandørens egne forpliktelser etter Personvernlovgivningen. Kontaktpunkt hos Leverandøren for Kundens anmodning om bistand er Leverandørens personvernombud, eller en annen funksjon anvist av Leverandøren.

11. REVISJON

Leverandøren skal gi Kunden den informasjonen som med rimelighet kreves for å vise at forpliktelsene etter artikkel 28 i personvernforordningen er oppfylt, samt muliggjøre og bidra til gjennomganger og inspeksjoner som gjennomføres av Kunden eller en uavhengig revisor som ikke er konkurrent til Leverandøren. Leverandøren kan oppfylle denne forpliktelsen ved å fremlegge en oppdatert uavhengig revisjonsrapport (slik som SOC2 Type II eller ISO/IEC 270001) én gang per kalenderår på Kundens skriftlige anmodning og under egnet konfidensialitet. Inspeksjon på stedet kan skje med minst tretti (30) dagers varsel dersom revisjonsrapporten ikke er tilstrekkelig eller dersom det foreligger velbegrunnet mistanke om vesentlig mangel; Kunden bærer kostnaden med mindre vesentlig mangel konstateres.

12. AVTALEPERIODE OG OPPHØR

Avtalen gjelder så lenge Leverandøren behandler Personopplysninger på vegne av Kunden innenfor rammen av Tjenestene. Avtalen opphører automatisk når Leverandørens behandling av Personopplysninger på vegne av Kunden har opphørt og eventuell sletting eller tilbakelevering etter nedenstående er gjennomført.

Når Behandlingen avsluttes, ved oppsigelse av Tjenesten eller Alminnelige Vilkår eller på Kundens skriftlige anmodning, skal Leverandøren etter Kundens valg enten slette eller tilbakelevere samtlige Personopplysninger til Kunden. Dersom Kunden ikke angir annet, skal Leverandøren slette Personopplysningene.

Leverandøren har rett til å lagre Kundedata som inneholder Personopplysninger i en periode på inntil tre (3) måneder etter Tjenestens opphør for å muliggjøre Kundens uttak av data, med mindre Kunden skriftlig ber om umiddelbar sletting. Leverandøren har videre rett til fortsatt å lagre Personopplysninger i den grad det kreves etter unionsretten eller medlemsstatenes nasjonale rett, men bare så lenge og i det omfanget

lagringen er nødvendig for det aktuelle formålet.

På Kundens skriftlige anmodning skal Leverandøren bekrefte at sletting eller tilbakelevering er gjennomført. I tillegg gjelder det som er fastsatt om Kundedata i Alminnelige Vilkår.

13. ØVRIG

Endringer og tillegg til Avtalen skal være skriftlige for å være gyldige. For spørsmål om ansvarsbegrensning, lovvalg og tvisteløsning gjelder det som er angitt i Alminnelige Vilkår.

Avtalen er utarbeidet på svensk. Ved en eventuell oversettelse til et annet språk skal den svenske versjonen ha forrang ved tolkningstvist.

UNDERVEDLEGG 1 – SPESIFIKASJON AV BEHANDLINGEN

Dette undervedlegget spesifiserer den Behandlingen av Personopplysninger som Leverandøren utfører på vegne av Kunden etter Avtalen, i samsvar med artikkel 28 nr. 3 i personvernforordningen.

1.1 GJENSTAND OG FORMÅL

Gjenstanden for Behandlingen er Leverandørens levering av Tjenestene til Kunden etter Alminnelige Vilkår og de spesifikke tjenesteavtalene som Partene har inngått. Formålet med Behandlingen er å muliggjøre levering, drift, support, vedlikehold og utvikling av Tjenestene samt å oppfylle Leverandørens forpliktelser etter avtale og lov.

1.2 BEHANDLINGENS ART OG VARIGHET

Behandlingens art omfatter innsamling, registrering, organisering, strukturering, lagring, bearbeiding, lesing, bruk, utlevering ved overføring, sammenstilling, begrensning, sletting og tilintetgjøring av Personopplysninger i den grad det kreves for å levere Tjenestene.

Behandlingen pågår i den tiden Tjenestene leveres til Kunden samt i den eventuelle perioden etter Tjenestenes opphør som er angitt i punkt 12 i Avtalen.

1.3 KATEGORIER AV REGISTRERTE

Følgende kategorier av Registrerte kan komme til å omfattes av Behandlingen:

- **Kundens ansatte og oppdragstakere** (f.eks. serveringspersonale, kjøkken- og barpersonale, ledere og eiere);
- **Personer hos Kundens leverandører og samarbeidspartnere** (f.eks. bemanningskonsulenter, innleid ekstrapersonale, artister, leverandørkontakter);
- **Kontaktpersoner og tekniske brukere hos systemintegrasjonspartnere** (f.eks. regnskaps- og lønnskonsulenter, hotellsystem/PMS, betalingsleverandører og forhandlere); og
- **Kundens gjester** (f.eks. bordbestillere, takeaway-bestillere, hotellgjester og deltakere i lojalitetsprogram).
- **Mottakere av digital kvittering** (privatpersoner som angis av Kundens gjest eller kunde på kjøpstidspunktet for at kvitteringen skal kunne formidles digitalt via en tredjepartstjeneste, f.eks. Kivra-brukere).

1.4 KATEGORIER AV PERSONOPPLYSNINGER

Følgende kategorier av Personopplysninger kan komme til å omfattes av Behandlingen:

- Navn på Kundens ansatte og gjester;
- Kontaktopplysninger (slik som telefonnummer, adresse og e-postadresse) til Kundens ansatte og gjester;
- Innloggings- og brukeropplysninger for ansatte og administratorer (f.eks. brukernavn, krypterte autentiseringsopplysninger, øktdata, IP-adresse, enhetsinformasjon samt logger over innlogging og systemaktivitet);
- Rolle- og tilgangsdata i Tjenestene (rolletildeling, tilgangsnivå og tilgangsomfang);
- Fødselsnummer på ansatte*;
- Fødselsdato og juridisk kjønn for ansatte;
- Ansattes stilling og yrke hos Kunden;
- Ansattes lønns- og betalingsopplysninger, slik som ansettelsesavtaler, fraværsrapportering, kontonummer og lønnsbeløp;

- Ansettelsesrelaterte dokumenter som lastes opp i Tjenestene (ansettelsesavtaler, lønnsslipper, attester, sertifiseringer og andre HR-dokumenter; opplysninger i slike dokumenter kan i enkelttilfeller utgjøre helseopplysning etter artikkel 9 i personvernforordningen);
- Fritekstfelt som Kunden selv velger å registrere;
- Bilde av Kundens ansatte (for identifisering i vaktplan- og personalvisninger);
- Tids- og tilstedeværelsesdata for ansatte (inn-/utstemplinger, planlagt og faktisk arbeidet tid, pauser);
- Fraværsdata for ansatte (fraværsperioder og fraværstype; opplysning om fraværstype kan i enkelte tilfeller utgjøre en helseopplysning etter artikkel 9 i personvernforordningen);
- Personallistedata etter 39 kap. 11–12 §§ i den svenske skatteförfarandelagen (navn og tidspunkter for samtlige personer som arbeider på driftsstedet, uavhengig av ansettelsesforhold);
- Salgs-, tips- og prestasjonsdata knyttet til den enkelte ansatte (f.eks. salg per servitør, tipsfordeling og individuell omsetningsstatistikk);
- Bookingdata for Kundens gjester (kontaktopplysninger, antall personer i selskapet samt fritekstinformasjon som gjesten selv oppgir, f.eks. allergier eller andre kostpreferanser; allergiopplysning kan utgjøre helseopplysning etter artikkel 9 i personvernforordningen);
- Lojalitets- og gjesteprofildata (medlemskap, kjøpshistorikk, poengsaldo og preferanser) for gjester som deltar i lojalitetsprogram eller lignende;
- Samtykke- og kommunikasjonspreferanser (registrerte samtykker, opt-in/opt-out-status og valg av kommunikasjonskanaler);
- For hotellrelaterte Tjenester: gjestekoblingsdata mellom restaurant og hotell-PMS (romnummer, oppholdsperiode og kobling til hotellgjesteprofil for fakturering);
- Betalings- og transaksjonsdata samt, for Tjenester som omfatter kortbehandling, slike kortopplysninger som behandles i et PCI DSS-sertifisert miljø og som ikke er synlige for Leverandøren i klartekst;
- Kontakt- og identifikasjonsopplysninger for mottakere av digital kvittering (fødselsnummer*, mobilnummer eller e-postadresse) samt innhold og metadata i den digitale kvitteringen; og
- Øvrige kategorier av Personopplysninger som Kunden registrerer eller på annen måte tilfører Tjenestene.

* Fødselsnummer utgjør en særlig personvernsensitiv opplysning etter 3 kap. 10 § i den svenske loven (2018:218) med utfyllende bestemmelser til EUs personvernforordning.

Behandlingen er ikke ment å omfatte særlige kategorier av Personopplysninger etter artikkel 9 i personvernforordningen eller opplysninger om straffedommer og lovovertredelser etter artikkel 10. Visse opplysninger som Kunden eller Kundens gjester registrerer i Tjenestene (slik som fraværstype, informasjon om allergier i bookingens fritekstfelt eller innhold i opplastede HR-dokumenter som legeattester) kan likevel i enkelttilfeller utgjøre helseopplysninger etter artikkel 9 i personvernforordningen. Kunden er ansvarlig for at det foreligger et rettslig grunnlag etter artikkel 9 nr. 2 i personvernforordningen for slik registrering, og for å informere de Registrerte i samsvar med artikkel 13–14 i personvernforordningen.

1.5 STED FOR BEHANDLINGEN

Personopplysninger behandles som utgangspunkt innenfor EU/EØS. Leverandøren har virksomhet i Sverige, Norge, Belgia og Frankrike, og Personopplysninger kan komme til å behandles i ett av disse landene. Eventuell overføring av Personopplysninger til land utenfor EU/EØS skjer bare i samsvar med punkt 6 i Avtalen og i samsvar med Undervedlegg 3.

UNDERVEDLEGG 2 – TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Dette undervedlegget beskriver de tekniske og organisatoriske sikkerhetstiltakene som Leverandøren iverksetter etter artikkel 32 i personvernforordningen for å sikre et sikkerhetsnivå som er egnet i forhold til risikoen ved Behandlingen.

2.1 TILTAK FOR KONFIDENSIALITET, INTEGRITET OG TILGJENGELIGHET

- Kryptert overføring av Personopplysninger mellom Leverandøren og Kunden;
- Pseudonymisering eller kryptering av data ved statistikk- og markedsbearbeiding for eksternt formål;
- Tilgangskontroller som sikrer at bare personer med behov for tilgang for sine arbeidsoppgaver har tilgang til Personopplysninger;
- Flerfaktorautentisering ved innlogging til Leverandørens system fra eksternt nettverk;
- Inkrementell daglig sikkerhetskopiering og fullstendig ukentlig sikkerhetskopiering;
- Anvendelse av Payment Card Industry Data Security Standard (PCI DSS) i den grad det er relevant for Tjenester som omfatter kortbehandling.

2.2 ORGANISATORISKE TILTAK

- Avtalt taushetsplikt for samtlige ansatte hos Leverandøren;
- Etablerte rutiner for hendelseshåndtering, kontinuitetsplanlegging og regelmessig sikkerhetsevaluering;
- Opplæring av personale i personvern og informasjonssikkerhet.

2.3 OPPDATERING

Nærmere beskrivelse av Leverandørens sikkerhetstiltak er tilgjengelig på https://caspeco.com/gdpr/. Leverandøren har rett til fra tid til annen å oppdatere sikkerhetstiltakene, forutsatt at beskyttelsesnivået ikke svekkes vesentlig.

UNDERVEDLEGG 3 – FORHÅNDSGODKJENTE UNDERDATABEHANDLERE

Dette undervedlegget lister opp de Underdatabehandlerne som Kunden forhåndsgodkjenner etter punkt 5 i Avtalen.

3.1 GJELDENDE OVERSIKT

En til enhver tid oppdatert oversikt over benyttede Underdatabehandlere er publisert på https://caspeco.com/gdpr/. Oversikten inneholder for hver Underdatabehandler opplysning om (i) Underdatabehandlerens foretaksnavn og forretningssted, (ii) den tjenesten Underdatabehandleren leverer, (iii) det eller de landene der Behandlingen skjer, samt, for Underdatabehandlere i Tredjeland, (iv) det rettslige grunnlaget for overføringen.

Gjennom Avtalen godkjenner Kunden de Underdatabehandlerne som er angitt på det ovenfor angitte nettstedet ved Avtalens inngåelse. Tillegg eller bytte av Underdatabehandler skjer i samsvar med den fremgangsmåten som er angitt i punkt 5 i Avtalen.

3.2 UNDERDATABEHANDLERE I TREDJELAND

For Underdatabehandlere som behandler Personopplysninger i et Tredjeland, angis på nettstedet også det rettslige grunnlaget for overføringen (slik som beslutning om tilstrekkelig beskyttelsesnivå eller standard personvernbestemmelser) samt hvilke supplerende beskyttelsestiltak som anvendes i samsvar med punkt 6 i Avtalen.