

Databehandleraftale mellem

Heyloyalty ApS
Jens Baggesens Vej 47
8200 Aarhus N
Cvr: 29394458
(i det følgende HL eller databehandleren)

og

Kunden
(i det følgende kunden eller dataansvarlig)

1. Baggrund

Databehandleren skal fra 25. maj 2018 overholde Persondataforordningen (Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) med tilhørende retsakter samt heraf afledt national lovgivning.

Det er et krav i Persondataforordningen, at der mellem den dataansvarlige og databehandleren indgås skriftlig aftale om den behandling, som skal foretages, en såkaldt 'databehandleraftale'. Denne aftale er bilag til Heyloyalty (efterfølgende kaldet HL) Forretningsbetingelser som udgør samhandelsaftale grundlaget mellem HL og kunden. Databehandleraftalen er gældende for de i samhandelsaftalen beskrevne produkter og ydelser og er gældende såfremt kunden har en gyldig licens.

Databehandleraftalen definerer databehandlerens behandling af alle typer personoplysninger på vegne af den dataansvarlige.

Der indgås hermed følgende databehandleraftale ("Aftalen") mellem Kunden (den juridiske enhed der benævnes Kunden i Forretningsbetingelserne for Heyloyalty systemet og som er dataansvarlig) og Heyloyalty ApS ("Leverandøren" og som er databehandleren).

2. Genstanden for behandlingen og typen af personoplysninger

HL behandler persondata vedrørende medlemmer af kundens nyhedsbrevs-/medlemslister i HL. Disse data vil normalt være af betegnelsen "almindelige personoplysninger", som medlemmet afgiver ved tilmelding til listerne eller ved senere opdatering af egne data. Kunden kan bede medlemmet om yderligere data, herunder følsomme personoplysninger. Dette har HL ingen kontrol over, og det er kundens ansvar, at indsamlingen af personoplysninger lever op til gældende lovgivning og kunden indestår for, at have fornøden hjemmel til behandling af personoplysningerne omfattet af nærværende aftale.

HL opsamler data om medlemmers adfærd på kundens hjemmeside/webshop. Adfærden indbefatter dels "tabt kurv", dvs. når kunden lægger ting i kurven med henblik på at købe, men ikke gennemfører købet, dels hvilke produkter og produktkategorier kunden søger og/eller klikker på.

3. Varigheden af behandlingen

Behandlingen af personoplysninger varer, indtil et medlem anmoder kunden om at stoppe databehandlingen. Afmeldelse af nyhedsbrev betragtes ikke i sig selv som en anmodning om at stoppe databehandlingen. Data vil altså stadig opbevares og kan i anonymiseret form bruges til statistiske formål.

4. Geografisk krav

Den behandling af persondata, som databehandleren foretager efter aftale med den dataansvarlige, må alene foretages af databehandleren eller underdatabehandlere, indenfor det Europæiske Økonomiske Samarbejde (EØS). Databehandleren er ingenlunde berettiget til at lade databehandling foregå udenfor EØS uden den dataansvarliges skriftlige samtykke.

5. Den dataansvarliges rettigheder og forpligtelser

Den dataansvarlige har pligt til at overholde gældende lovgivning og informere HL om ændringer i lovgivningen, der påvirker HL's databehandling. Kunden har ret til at bede om indsigt i, hvorvidt HL behandler personoplysninger forsvarligt, og på kundens anmodning skal HL uden omkostning for kunden udlevere følgende:

- Navn og kontaktoplysninger på kundens repræsentant hos databehandleren, navn på eventuelle underleverandører, samt navn og kontaktoplysninger på HL's databeskyttelsesrådgiver (Data Protection Officer).
- Kategorierne af de behandlinger, databehandleren eller eventuelle underleverandører foretager for den dataansvarlige
- En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som HL har udført for at sikre personoplysninger

6. Om instruktion i databehandling

Databehandleren må kun behandle personoplysningerne på baggrund af dokumenterede instruktioner fra den dataansvarlige og må ikke behandle personoplysninger til andre formål, herunder opbevare eller videregive data.

Alle de for afviklingen af samhandlens nødvendige og beskrevne databehandlinger betragtes som dokumenterede af den dataansvarlige.

7. Formål med databehandling

HL modtager medlemmets personoplysninger ved tilmelding til nyhedsbrevs-/medlemslisterne samt ved senere opdatering af medlemmets oplysninger. Disse personoplysninger bruges til at personliggøre SMS beskeder og nyhedsbreve, fx med medlemmets navn. Data bruges også til at tilpasse indholdet af nyhedsbrev, fx jf. interesse- og/eller produktområder, som medlemmet har angivet særlig interesse for.

Hvis kunden har tilkøbt en Heycommerce licens, indsamles der personoplysninger om medlemmers adfærd på hjemmesiden med henblik på at skræddersy nyhedsbreve endnu mere og lave individuelt tilpassede kampagner. Herunder også kampagner på bl.a. Facebook og Instagram m.m.

8. Medarbejderfortrolighed

Alle medarbejdere hos databehandleren, der er autoriseret til at behandle oplysningerne, er underlagt en fortrolighedsforpligtelse og har modtaget relevant uddannelse i persondatasikkerhed og er alene berettiget til at anvende personoplysningerne som led i opfyldelsen af HL's forpligtelser og rettigheder i henhold til samhandelsaftalen med kunden.

9. Sikkerhedsforanstaltninger

HL har gennemført en kortlægning af sin behandling af personoplysninger, herunder en vurdering af følsomheden. Derudover har HL lavet en sikkerhedsvurdering af alle data-lokationer, herunder alle data-overførselssteder og øget sikkerheden efter behov, så personoplysninger altid behandles forsvarligt.

HL's tekniske og organisatoriske sikkerhedsforanstaltning sikrer derved mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.

10. Sikkerhedsbrud

Såfremt databehandleren måtte blive bekendt med et persondatasikkerhedsbrud, hvorved forstås et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, er databehandleren forpligtet til, uden unødigt forsinkelse, at søge at lokalisere sådan brud og søge at begrænse opstået skade i videst muligt omfang, samt i det omfang det er muligt reetablere eventuelt mistede data.

Databehandleren er endvidere forpligtet til uden unødigt forsinkelse at underrette den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden. Databehandleren skal herefter uden unødigt forsinkelse, i det omfang det er muligt, give skriftlig meddelelse til den dataansvarlige, med beskrivelse af bruddets karakter, sandsynlige konsekvenser af bruddet samt truffne foranstaltninger for at begrænse dets mulige skadevirkninger.

11. Brug af underdatabehandlere

De personoplysninger HL modtager fra kundens medlemmer opbevares hos 3.-part. Data lagres på servere i Danmark, der ejes af firmaet Inventio.IT A/S, med hvem der er indgået databehandleraftale, således datasikkerheden er garanteret.

HL har desuden en backup på Amazon Web Services' servere i Tyskland. Firmaet er certificeret i henhold til ISO/IEC 27018 og er forpligtet til at overholde den europæiske Databeskyttelsesforordning (GDPR).

Databehandleren må skifte til anden underdatabehandler, såfremt det garanteres, at den nye underdatabehandler lever op til gældende lovgivning, samt til denne databehandleraftale. HL er forpligtet til, at informere kunden herom forud for et sådant skifte, og kunden må gøre indsigelse, hvis der er berettiget grund til at modsætte sig et sådant skifte.

12. Forpligtelser over for de registrerede

HL bistår som databehandler den dataansvarlige med at opfylde dennes forpligtelser over for de registrerede. På den dataansvarliges anmodning slettes eller udleveres behandlede personoplysninger uden omkostninger for kunden og inden for rimelig tid.

13. Databehandlerens ansvar

HL lover at udlevere alle nødvendige informationer med henblik på, at den dataansvarlige kan dokumentere, at behandlingen hos databehandleren lever op til forpligtelserne, samt tillader og medvirker til kontrol og audits heraf i et rimeligt omfang. Herunder skal databehandleren være forpligtet til at informere den dataansvarlige, såfremt det er databehandlerens opfattelse, at en instruks er ulovlig.

HL informerer hermed kunden som dataansvarlig om, at indsamling af personoplysninger skal ske efter gældende lovgivning, specifikt orienteres kunden om, at medlemmer skal give informeret samtykke til den intenderede databrug, såfremt samtykke er nødvendigt efter gældende lovgivning. HL informerer også kunden om, at udsendelse af e-mails og sms'er via Heyloyalty sker i klartekst, dvs. et medium, der ikke er adækvat til at indeholde følsomme personoplysninger, og at medlemmets adgang til egne personoplysninger bør være password-beskyttet. Ukrypterede e-mails og sms'er må betragtes som et adækvat medium til almindelige personoplysninger, så som navn og adresse.

HL skal ydermere bistå den dataansvarlige med at sikre dennes overholdelse af forpligtelserne i forordningens artikel 32-36 om blandt andet sikkerhedsforanstaltninger, anmeldelse ved sikkerhedsbrud, udarbejdelse af risikoanalyser, herunder eventuelt en Data Protection Impact Assessment (DPIA) og eventuel konsultation med databeskyttelsesmyndighederne.

14. Databehandleraftalens ikrafttrædelse og varighed

Denne aftale træder i kraft, på samme tidspunkt, som samhandelsaftalen om HL og er gældende indtil samhandelsaftalen om HL ophører, dog for så vidt angår punkt 5, 10, 11 samt punkt 13, sidste træder disse i kraft fra og med 25. maj 2018, når den europæiske Databeskyttelsesforordning (GDPR) træder i kraft.

En forudsætning for databehandleraftalen er til enhver tid, at der eksisterer en samhandelsaftale mellem parterne på HL's ydelser, og at kunden overholder sine forpligtelser. Så længe disse betingelser gælder, har databehandleraftalen gyldighed.

I tilfælde af at samhandelsaftalen ophører, uanset årsag, ophører databehandleraftalen også. Databehandleren er dog forpligtet af denne aftale, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige, idet den dataansvarlige snarest muligt og senest 30 dage før ophør af samhandelsaftalen, skal oplyse databehandleren skriftligt, hvorledes databehandleren skal forholde sig til de behandlede personoplysninger. Ved kontraktens endelige udløb er databehandleren berettiget til at slette alle personoplysninger, som er blevet behandlet under den ophørte samhandelsaftale på vegne af den dataansvarlige, med mindre andet særskilt aftales.