

DATABEHANDLERAFTALE

Mellem

Foreningen Faldsled Havn
Fiskerstræde 1
5642 Millinge
CVR. nr.: 71914011
(herefter "Den Dataansvarlige")

og

BEAS A/S
Brørupvænget 10
7650 Bøvlingbjerg
CVR. nr.: 1994 3178
(herefter "Leverandør")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens
behandling af personoplysninger på vegne af Den Dataansvarlige:

1. Generelt

- 1.1** Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:
- (i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).
 - (ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).
- 1.2** Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.
- 1.3** I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandlereftaler.
- 1.4** Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

- 2.1** Leverandøren behandler i medfør af aftale med Den Dataansvarlige, BEASportalen (herefter "Hovedaftalen") personoplysninger for Den Dataansvarlige, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Den Dataansvarliges rettigheder og forpligtelser

- 3.1** Den Dataansvarlige er dataansvarlig for de personoplysninger, som Den Dataansvarlige instruerer Leverandøren om at behandle. Den Dataansvarlige har ansvaret for, at de personoplysninger, som Den Dataansvarlige instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Den Dataansvarliges opgavevaretagelse.
- 3.2** Den Dataansvarlige har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4. Leverandørens forpligtelser

- 4.1** Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Den Dataansvarlige, jf. pkt. 6 og bilag 3. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.
- 4.2** Leverandøren behandler alene de overladte personoplysninger efter instruks fra Den Dataansvarlige, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3** Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.
- 4.4** Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.
- 4.5** Leverandøren skal på opfordring fra Den Dataansvarlige hjælpe med at opfylde Den Dataansvarliges forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Den Dataansvarliges forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
- 4.6** Leverandøren skal fra 25. maj 2018 hjælpe Den Dataansvarlige med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.
- 4.7** Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Den Dataansvarliges personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.8** Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Den Dataansvarliges personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Den Dataansvarlige ved enhver ændring.
- 4.9** Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

- 5.1** Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Den Dataansvarlige.
- 5.2** Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Den Dataansvarlige anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Den Dataansvarlige har overladt til Leverandøren i medfør af Hovedaftalen. Den Dataansvarlige kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor.
- 5.3** Hvis Leverandøren overlader behandlingen af personoplysninger, som Den Dataansvarlige er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.4** Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 5.5** Når Leverandøren overlader behandlingen af personoplysninger, som Den Dataansvarlige er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Den Dataansvarlige ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.
- 5.6** Den Dataansvarlige kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Den Dataansvarlige.
- 5.7** Al kommunikation mellem Den Dataansvarlige og underdatabehandleren sker via Leverandøren.

6. Instrukser

- 6.1** Leverandørens behandling af personoplysninger på vegne af Den Dataansvarlige sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt. 5.3, får tilsendt Den Dataansvarliges instruks, jf. bilag 3.

- 6.2** Leverandøren giver fra 25. maj 2018 omgående besked til Den Dataansvarlige, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 7.1** Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:
- (i) tilintetgøres, mistes, ændres eller forringes,
 - (ii) kommer til uvedkommendes kendskab eller misbruges, eller
 - (iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.
- 7.2** Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
- 7.3** Leverandøren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 og 7.2, samt bilag 1.
- 7.4** Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 7.5** Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Den Dataansvarliges personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.
- 7.6** Leverandøren er forpligtet til straks at underrette Den Dataansvarlige om ethvert sikkerhedsbrud samt ved
- (i) enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Den Dataansvarlige er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,
 - (ii) anden manglende overholdelse af Leverandørens, samt eventuelle underdatabehandlers forpligtelser
- uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.
- 7.7** Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.6, uden forudgående skriftlig aftale med Den Dataansvarlige

om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

- 8.1** Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Den Dataansvaliges instruks herfor, jf. bilag 3.
- 8.2** Ved overførsel til tredjelande er Leverandøren og Den Dataansvarlige i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.
- 8.3** Hvis Den Dataansvaliges personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

9. Tavshedspligt og fortrolighed

- 9.1** Leverandøren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 9.2** Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

- 10.1** Leverandøren er forpligtet til at give Den Dataansvarlige nødvendige oplysninger til, at Den Dataansvarlige kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2** Den Dataansvarlige, en repræsentant for Den Dataansvarlige eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.3** Leverandøren skal én gang årligt fremsende en erklæring til Den Dataansvarlige om overholdelse af denne Aftale. Den Dataansvarlige og Leverandøren skal aftale Leverandørens pris herfor. Erklæringen skal udarbejdes i overensstemmelse med

gældende anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandlers databehandling. Den første erklæring skal foreligge 12 måneder efter Hovedaftalens indgåelse.

11. Ændringer i Aftalen

- 11.1** Den Dataansvarlige kan til enhver tid, med et forudgående varsel på mindst 90 dage, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne aftales skriftligt mellem Den Dataansvarlige og Leverandøren i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.
- 11.2** I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Den Dataansvarlige med et varsel på 30 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

- 12.1** Den Dataansvarlige træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.
- 12.2** Den Dataansvarlige skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Den Dataansvarlige. I det tilfælde, hvor personoplysningerne tilbageleveres til Den Dataansvarlige, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Den Dataansvarliges meddelelse.
- 12.3** Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

13. Misligholdelse og tvistigheder

- 13.1** Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

14. Erstatning og forsikring

- 14.1** Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen.

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parter underskrift og løber indtil ophør af Hovedaftalen.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Den Dataansvarlige og Leverandøren.



KOMBIT

Kommunernes it-fællesskab

For Den Dataansvarlige

Dato

For Leverandøren

Dato

21/6 - 2018

Bente Madsen

Karl Kristian Mikkelsen

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører
(underdatabehandlere)

Bilag 3 – Instruks

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

Generelle sikkerhedsforanstaltninger

BEAS kærer om høj datasikkerhed og personlivets fred og har derfor også en officiel politik på området. Derfor er det udelukkende de betroede medarbejdere hos BEAS, der har behov for adgang til systemer, der får det. Al kommunikation mellem terminaler, portal og browser krypteres med anerkendte og gennemprøvede krypteringsalgoritmer. Følsomme data, der kun må kunne lukkes op og læses af helt specifikke brugere, krypteres. Der installeres løbende sikkerhedsopdateringer, når disse er tilgængelige. Vi holder os orienterede med, hvad der sker i IT branchen vedr. nye sikkerhedstiltag. Data opbevares i velrenommeret datacenter inden for EU i Vesteuropa. Der foretages live backup til BEAS A/S for at sikre data ikke går tabt. Det testes jævnligt, at backup kan reetableres. Derudover opbevarer vi ikke data, der ikke er nødvendige. Backupbånd og harddiske bliver fysisk destrueret, når de ikke længere skal bruges eller fungerer.

Autorisation og adgangskontrol

Al adgang til BEASportal sker via brugernavn/password verifikation både for såvel Den Dataansvarliges brugere som BEAS medarbejdere. Den Dataansvarlige kan specificere, hvem der har adgang til kundekartoteket samt om vedkommende samtidig har adgang til at se CPR-nr. BEAS medarbejdere har ikke adgang til at se CPR-numre med mindre en medarbejder hos Den Dataansvarlige gør dette synligt for BEAS medarbejderen. CPR-numre ligger i krypteret form i databasen, og det er ikke umiddelbart muligt for en udvikler/administrator at dekryptere informationen på egen hånd. Hovednøglen til at

dekryptere data opbevares offline (papir og USB-drive) i et sikret pengeskab, hvortil kun direktøren for BEAS A/S har adgang. Hovednøglen eksisterer udelukkende af hensyn til, hvis alle medarbejdere med adgang til CPR data hos Den Dataansvarlige skulle miste adgangen til BEASportal. Ellers ville CPR data være endegyldigt tabt.

Alle succesfulde og afviste adgangsforsøg til portalen og det bagvedliggende operativsystem logges til separate logfiler.

Alle medarbejdere i BEAS med adgang til BEASportal følger BEAS's politik for datasikkerhed, der bl.a. angår gode stærke passwords. Det er Den Dataansvarliges ansvar at sikre at Den Dataansvarliges brugere på BEASportal anvender tilstrækkeligt sikre adgangskoder jf. Den Dataansvarliges politik på området.

Alle passwords opbevares i saltede og hash'et form og kan ikke genskabes, hvis det skulle blive glemt.

Yderligere er det kun muligt for en bruger at være logget ind fra et sted ad gangen. Logges ind fra et andet sted med ens brugernavn/password, logges man automatisk ud på det første sted.

Inddatamateriale som indeholder personoplysninger

BEAS A/S behandler som udgangspunkt ikke inddatamateriale med personfølsom karakter. Dog har der, til opstart, været foretaget en konvertering af eksisterende kunder på gammelt medlemssystem. Data herfra har været opbevaret hos BEAS i form af excel ark, inden de er blevet hentet ind i BEASportal. Excel arkene har været gemt i en dedikeret AES krypterede container, hvortil kun 2 medarbejdere har haft adgang. Efter data er blevet importeret i BEASportal er de krypterede containere blevet slettet og eksisterer ikke længere hos BEAS A/S. Lignende fremgangsmåde vil blive anvendt igen, hvis personfølsomt materiale igen skulle behandles af BEAS A/S.

Uddatamateriale som indeholder personoplysninger

Medarbejdere hos BEAS A/S har som udgangspunkt ikke adgang til uddatamateriale med personfølsom karakter.

Fra BEASportal genereres fakturadata, der sendes til KMD Opus. Dette sker uden BEAS medarbejders medvirken. Fakturadata indeholder CPR numre, men ellers ikke yderligere personhenførbare data. Fakturadata genereres på foranledning af Den Dataansvarliges bruger og sendes direkte via krypteret forbindelse til KMD Opus. Fakturadata bliver således ikke gemt på en server hos BEAS. En enkelt udvikler hos BEAS har mulighed for at hente de sendte fakturadata igen fra det øjeblik, hvor det er sendt til KMD og til KMD har taget filen, til evt. debug brug. Så vidt BEAS er oplyst, kigger KMDs system, om der er data en gang per døgn, om aftenen. Efterfølgende har BEAS ikke adgang til data.

Skulle der være behov for at hente fakturadata til debug vil de blive opbevaret i en AES krypteret container indtil ikke længere relevant (højst få dage), og containeren vil herefter blive slettet.

Eksterne kommunikationsforbindelser

Almindelig adgang til BEASportal sker via krypterede http (dvs. https) forbindelser fra en standard webbrowser. Den krypterede forbindelse er signeret med certifikater fra udbydere, der er velkendte og anerkendte i it branchen, lige som anvendt krypteringsmetode også er den almindelige anerkendte metode som opdaterede browsere understøtter (pt. TLS 1.2).

Øvrige administrative adgange bag om systemet foregår ligeledes via krypterede forbindelser (SSH), hvortil kun enkelte BEAS medarbejdere har adgang.

Der opdateres løbende med sikkerhedsopdateringer fra leverandøren af operativsystemet (Debian).

Kontrol med afviste adgangsforsøg

Alle forsøg på adgang, succesfulde og afviste, såvel via BEASportal som administrative adgange logges. Hvis et forsøg afvises flere på hinanden følgende gange, vil forbindelse fra den pågældende IP adresse efterfølgende blive afvist i firewall'en. Afvisningen vil efter en rimelig tid igen blive fjernet og det er muligt for en legal bruger at logge ind. For adgang via web er grænsen pt. 30 min. og for administrative adgange er det pt. 2 dage. Afvisningen kan til hver en tid fjernes af en udvikler.

Logning

Det er BEAS's vurdering, at BEASportal ikke er omfattet af sikkerhedsbekendtgørelsens kapitel 3 jf. sikkerhedsbekendtgørelsens §15 og persondataloven §44 i det BEASportal ikke behandler anden personfølsom oplysning end CPR-nummer.

Det kan dog nævnes, at al adgang til BEASportal logges - både succesfulde og afviste. Ydermere logges det, hvem der tilføjer, retter og sletter data i kundekartoteket, og hvornår det er gjort. Når noget bliver rettet gemmes historik på, hvad der er blevet rettet.

Hjemmearbejdspladser

Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser:

☐ Ja

☒ Nej

Sikkerhedskrav fra 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a) tilintetgørelse af oplysningerne
 - b) tab af oplysningerne
 - c) ændring af oplysningerne
 - d) uautoriseret videregivelse af oplysningerne
 - e) uautoriseret adgang til oplysningerne

BEAS A/S er i gang med at gennemgå sikkerhedskrav for bestemmelser efter 25. maj 2018 og vil løbende foretage eventuelle tilretninger, hvis det viser sig, at det ikke allerede sker i vores system idag opfylder krav og bestemmelser

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen

BEAS A/S Brørupvænget 10, 7650 Bøvlingbjerg - CVR: 1994 3178

Hetzner Online GmbH Industriestr. 25, DE- 91710 Gunzenhausen, Tyskland,
Registergericht Ansbach, HRB6089 – Ust-Id Nr. DE812871812

2. Underdatabehandlere

Vetech Software Solutions Aps, Murervej 7a, 6710 Esbjerg V. – CVR: 28692811

Bilag 3 – Instruks

Instruks

Den Dataansvarlige instruerer hermed Leverandøren om at foretage behandling af Den Dataansvarliges oplysninger til brug for drift af BEAS produkter, jf. Hovedaftale om levering og support af BEAS produkter / BEASportalen, mellem Foreningen Faldsled Havn og BEAS A/S, underskrevet 21.06.2018.

1.1 Behandlingens formål

Behandling af Den Dataansvarliges oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Den Dataansvarlige.

1.2 Generel beskrivelse af behandlingen

Aftalen omfatter databehandling af standard personoplysninger for at varetage opgaven som leverandør af betalingsautomat med hertil hørende kort, der opdateres via en cloud baseret portal.

Databehandlingsopgaverne er oplysninger om bl.a. personers kundeforhold hos den dataansvarlige, der har stamdata som f.eks. navn, adresse, pladshaver/medlemsnummer, mailadresse, telefonnr. og bådoplysninger.

Det er muligt at tilføje nye databehandlingsopgaver til denne aftale, mod at der laves et tillæg, der underskrives af begge parter.

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):

☐ Racemæssig eller etnisk baggrund

- ☐ Politisk overbevisning
- ☐ Religiøs overbevisning
- ☐ Filosofisk overbevisning
- ☐ Fagforeningsmæssige tilhørsforhold
- ☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- ☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):

- ☐ Strafbare forhold
 - ☐ Væsentlige sociale problemer
 - ☐ Andre rent private forhold, som ikke er nævnt ovenfor:
-
-

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

- ☒ CPR-numre

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):

- A) [Borgere]
- B) [Virksomheder]
- C) [Offentlige virksomheder]

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren må overføre personoplysninger til følgende tredjelande: Ingen

Gyldigt overførselsgrundlag for overførslerne er: Ingen

Versionshistorik

Versionsnr.	Dato	Beskrivelse
1.0	03.04.2017	Skabelon KOMB:T aftale
1.1	01.05.2018	BEAS Databehandleraftale