

Databehandleraftale

mellem

Peoplez ApS
Nupark 45, 3
7500 Holstebro
CVR nr. 37402370
(herefter "Databehandleren")

og Peoplez' hjemmesidekunder, herefter "Den dataansvarlige".

Når Databehandler indgår en kommerciel aftale med Dataansvarlige, gælder denne databehandleraftale mellem Databehandleren og den Dataansvarlige.

Aftalen vedrører parternes persondataretlige forpligtelser og rettigheder i forhold til den Dataansvarliges køb af Databehandlerens ydelser.

Indholdsfortegnelse

1	Bilagsfortegnelse:	3
2	Baggrund og formål	3
3	Behandling af personoplysninger	3
4	Fortrolighed	4
5	De registreredes rettigheder.....	4
6	Behandlingssikkerhed	4
7	Dokumentationskravet	5
8	Ikrafttræden, ændring og ophør af aftalen	5
9	Lovvalg og værneting.....	5

1 Bilagsfortegnelse:

- 1.1 Følgende bilag er en del af nærværende aftale:
 - 1.1.1 Bilag 1 – Instruks til Databehandleren
 - 1.1.2 Bilag 2 – Minimumskrav til Databehandlerens sikkerhed

2 Baggrund og formål

- 2.1 Den Dataansvarlige har købt Databehandlerens ydelse i medfør af den kommercielle hovedaftale mellem parterne, der indebærer behandling af personoplysninger. Parterne har derfor dags dato indgået denne databehandleraftale.
- 2.2 Aftalen skal regulere de to parters persondataretlige pligter og rettigheder, som deres forhold giver anledning til.
- 2.3 Samarbejdet omhandler den Dataansvarliges køb af Databehandlerens ydelser inden for marketing. Dette kan omfatte hosting og vedligeholdelse af hjemmeside og udsendelse af nyhedsbreve.
 - 2.3.1 Databehandleren anses kun som databehandler i disse to forhold. Databehandleren anses ikke som en databehandler ved køb af andre ydelser, eksempelvis ved annoncering på vegne af den Dataansvarlige. Denne vurdering bygger delvist på Artikel 29-gruppens udtalelse om spørgsmålet i WP 171 (Opinion 2/2010).
 - 2.3.2 Ved annoncering på den Dataansvarliges vegne, anses Databehandleren som en selvstændig konsulent, der rådgiver om og udfører de praktiske forhold vedr. den Dataansvarliges annoncering. Den Dataansvarlige har det persondataretlige ansvar for denne behandling.

3 Behandling af personoplysninger

- 3.1 Denne aftale omfatter al behandling af personoplysninger, Databehandleren foretager på vegne af den Dataansvarlige i medfør af den kommercielle hovedaftale mellem parterne om den Dataansvarliges køb af Databehandlerens ydelser.
 - 3.1.1 Personoplysninger forstås i overensstemmelse med persondataforordningens art. 4, nr. 1. Behandling forstås i overensstemmelse med persondataforordningens art. 4, nr. 2.
- 3.2 Databehandleren må kun foretage de behandlinger af personoplysninger, der fremgår af instruksen i bilag 1 eller efterfølgende konkrete instrukser udstedt af den Dataansvarlige, medmindre andet er påkrævet af gældende ret.
- 3.3 Den Dataansvarlige har ansvaret for, at behandlingen lever op til lovgivningen på området, herunder persondataforordningens og databeskyttelseslovens regler.

4 Fortrolighed

- 4.1 De omfattede personoplysninger betragtes som fortrolige og vil kun blive videregivet, hvis det er nødvendigt for at løse de i denne aftale beskrevne opgaver, eller det er påkrævet af gældende ret.
- 4.2 Databehandlerens personale er forpligtet til fortrolighed med hensyn til de omfattede personoplysninger.

5 De registreredes rettigheder

- 5.1 Databehandleren skal under hensyntagen til behandlingens karakter så vidt muligt bistå den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i persondataforordningens kapitel III.
- 5.2 Databehandleren er dog aldrig forpligtet til at opfylde oplysningspligten efter persondataforordningens art. 13-14.
- 5.3 Det er desuden den Dataansvarliges ansvar, at der er et retligt grundlag for behandlingen. Såfremt et samtykke er påkrævet, er det den Dataansvarliges ansvar, at der indhentes samtykke til behandlingen.

6 Behandlingssikkerhed

- 6.1 Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal Databehandleren gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:
- 6.1.1 pseudonymisering og kryptering af personoplysninger
- 6.1.2 evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- 6.1.3 evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
- 6.1.4 en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
- 6.2 Databehandleren skal overholde de konkrete krav til Databehandlerens sikkerhedsforanstaltninger, der fremgår af bilag 2 – Minimumskrav til Databehandlerens sikkerhed.
- 6.3 Databehandleren skal bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af persondataforordningens art. 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren.

7 Dokumentationskravet

7.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i persondataforordningens art. 28, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige.

8 Ikrafttræden, ændring og ophør af aftalen

8.1 Aftalen træder i kraft på datoen hvor Dataansvarlige har bekræftet modtagelsen af databehandleraftalen pr. mail.

8.2 Parterne kan til enhver tid ændre aftalen ved enighed. Ændringerne skal være skriftlige.

8.3 Den Dataansvarlige kan derudover inden for rammerne af den kommercielle hovedaftale og databehandleraftalen give Databehandleren konkrete instrukser vedr. behandling af personoplysninger mod et rimeligt vederlag til Databehandleren. Databehandlerens til enhver tid almindelige timetakst anses for at være et rimeligt vederlag.

8.3.1 Databehandleren skal straks underrette den Dataansvarlige, hvis en instruks opfattes af databehandleren som værende i strid med gældende ret.

8.4 Databehandleraftalen ophører ved ophør af alle aftaler mellem parterne, der involverer behandling af personoplysninger.

8.4.1 Ved databehandleraftalens ophør kan den Dataansvarlige kræve alle de omfattede personoplysninger slettet eller tilbageleveret, medmindre gældende ret kræver, de fortsat holdes opbevaret. Databehandleren har dog ret til at anonymisere oplysningerne inden sletning eller tilbagelevering. Databehandleren har den fulde ejendomsret til de anonymiserede oplysninger og kan videregive dem til andre.

9 Lovvalg og værneting

9.1 Denne aftale reguleres og fortolkes efter gældende dansk ret.

9.2 Tvister vedrørende aftalen skal afgøres efter dansk ret ved den ret, hvor sagsøgte har hjemting. Parterne kan aftale et andet værneting i forbindelse med en retlig tvist.

Med venlig hilsen
Peoplez ApS

Per Tornvig, administrerende direktør

Bilag 1- Instruks til Databehandleren

Indholdsfortegnelse

1	Baggrund og rækkevidde	7
2	Hvilke behandlinger skal Databehandleren foretage	7
4	Hvilke personoplysninger skal Databehandleren behandle	8
5	Hvor skal behandlingerne foregå	8
6	Varigheden af behandlingerne	8
7	Underdatabehandlere	8

1 Baggrund og rækkevidde

1.1 Dette bilag udgør den Dataansvarliges instruks til Databehandleren og er en fast del af databehandleraftalen.

1.1.1 Denne instruks gælder for alle behandlinger, der er omfattet af databehandleraftalen.

2 Hvilke behandlinger skal Databehandleren foretage

2.1 Begrebet behandlinger skal forstås i overensstemmelse med definitionen i persondataforordningens art. 4, nr. 2.

2.2 De af aftalen omfattede personoplysninger kan udsættes for en lang række forskellige behandlinger, herunder: indsamling, registrering, systematisering, opbevaring, ændring, søgning, brug, videregivelse, overdragelse, profilering, sammenstilling eller samkøring, sletning, anonymisering samt blokering.

2.3 Den Dataansvarlige har bestemt, at Databehandleren skal foretage følgende behandlinger:

2.3.1 Databehandleren skal tilbyde de ydelser, der er aftalt mellem parterne i overensstemmelse med den kommercielle hovedaftale mellem parterne. Dette kan omfatte hosting af hjemmeside og udsendelse af nyhedsbreve.

2.3.2 Databehandleren har ret til løbende at vedligeholde, teste og drive sine systemer. Dette kan betyde, at personoplysninger behandles, herunder søgning, ændring og sletning af personoplysninger.

2.3.3 Databehandleren kan foretage andre behandlinger end de nævnte, såfremt behandlingerne er tæt knyttet til løsningen af den af den Dataansvarlige pålagte opgave.

2.4 Databehandleren kan altid foretage enhver form for behandling af en hvilken som helst personoplysning, herunder følsomme personoplysninger efter persondataforordningens art. 9, stk. 1, såfremt dette er påkrævet af gældende ret, herunder hvis det er endeligt og bindende påbudt af en offentlig myndighed.

2.4.1 Den Dataansvarlige skal underrettes om en retligt påkrævet behandling, inden behandlingen foretages, medmindre en sådan underretning er i strid med gældende ret.

3 Retten til at blive glemt (sletning)

3.1.1 Den Dataansvarlige styrer selv, hvornår personoplysninger bliver slettet, når Databehandleren hoster den Dataansvarliges hjemmeside, ved at anmode om sletning af bestemte oplysninger eller ved selv at sørge for sletning.

3.2 Når Databehandleren udsender nyhedsbreve på vegne af den Dataansvarlige, bliver personer på mailinglisten automatisk slettet, såfremt de elektronisk anmoder om at blive slettet.

4 Hvilke personoplysninger skal Databehandleren behandle

4.1 Begrebet personoplysninger skal forstås i overensstemmelse med definitionen i persondataforordningens art. 4, nr. 1.

4.2 Ved hosting af hjemmesider, omhandler personoplysningerne de kategorier af registrerede, som den Dataansvarlige ønsker skal fremgå af hjemmesiden. Dette vil primært dreje sig om ansatte.

4.2.1 Databehandleren skal endvidere behandle yderligere personoplysninger, såfremt det er påkrævet for at løse den af den Dataansvarlige pålagte opgave.

5 Hvor skal behandlingerne foregå

5.1 Behandlingerne styres fra Databehandlerens adresse Nupark 45, 3, 7500 Holstebro.

5.2 Databehandleren kan valgfrit hoste data inden for EU eller i et tredjeland, såfremt de relevante krav i lovgivningen er opfyldt. Den Dataansvarlige kan altid anmode om at få oplyst, hvor den Dataansvarliges data befinder sig.

6 Varigheden af behandlingerne

6.1 Databehandleren skal fortsætte behandlingerne, så længe databehandleraftalen er i kraft.

7 Underdatabehandlere

7.1 Databehandleren må antage underdatabehandlere, såfremt der indgås en databehandleraftale mellem Databehandleren og underdatabehandleren, der har de samme eller skærpede databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale.

7.2 Såfremt en underdatabehandler antages, skal Databehandleren underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

7.3 Overholder underdatabehandleren ikke sine forpligtelser, er Databehandleren fuldt ud ansvarlig herfor over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

- 7.4 Databehandleren har ret til at benytte følgende virksomheder som underdatabehandlere:
 - 7.4.1 VSI Group Asia Co., Ltd. VSI har hjemsted ved no. 9/9 - soi Srimongkol 3 , T. Patan Subdistric, M. Chiang Mai, Chiang Mai – 50000 (Thailand). Data bliver hosted i datacentre i EU.
 - 7.4.2 Metalab. CVR 33186282. Data hostes i EU.
 - 7.4.3 Digital Ocean, Inc. 101 Avenue of the Americas 10th Floor, New York, NY 10013. Data hostes i EU.
 - 7.4.4 The Rocket Science Group, LLC (Mailchimp): 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308. Data hostes i USA.
 - 7.4.5 Google Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043 USA.
 - 7.4.6 Facebook, Inc., 1 Hacker Way, Menlo Park, California 94025.
 - 7.4.7 Bing, 555 110th Ave NE; Bellevue, Washington 98004, USA.
 - 7.4.8 Instagram, 1 Hacker Way, Building 14, First floor, Menlo Park, California 94025.

8 Tredjelandsoverførsel

- 8.1 Den Dataansvarlige godkender, at Databehandleren kan foretage tredjelandsoverførsler, såfremt kravene hertil i lovgivningen er opfyldt. Databehandleren har eksempelvis ret til at overføre data til USA, såfremt modtageren er certificeret efter EU-US Privacy Shield.

Bilag 2 – Minimumskrav til databehandlerens sikkerhed

Indholdsfortegnelse

1	Baggrund og rækkevidde	11
1	Sikkerhedspolitik	11
2	Personale	11
3	Risikovurdering	11
4	Adgangskontrol	11
5	PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.	11
6	Bortskaffelse af hardware.....	11
7	Sikkerhedskopiering	12
8	Sikkerhedsbrud	12
9	Kontrol	12

9 Baggrund og rækkevidde

9.1 Dette bilag udgør den dataansvarliges minimumskrav til databehandlerens sikkerhed og er en fast del af databehandleraftalen.

1 Sikkerhedspolitik

1.1 Databehandleren skal udarbejde en sikkerhedspolitik.

1.2 Sikkerhedspolitikken skal sikre en tilstrækkelig sikkerhed under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

1.3 Sikkerhedspolitikken skal gennemføre de sikkerhedsforanstaltninger, der fremgår af dette bilag.

2 Personale

2.1 Databehandlerens personale skal være underkastet fortrolighed i overensstemmelse med databehandleraftalens punkt "Fortrolighed".

2.2 Personalet skal have en tilstrækkelig instruktion af, hvordan personoplysninger skal behandles i overensstemmelse med den vedtagne sikkerhedspolitik.

3 Risikovurdering

3.1 Databehandleren skal vurdere eventuelle risici i sin behandling af personoplysninger.

3.2 Vurderes en bestemt risiko til at være høj, skal databehandleren i vurderingen redegøre for, hvordan risikoen kan formindskes.

4 Adgangskontrol

4.1 Databehandleren skal sikre, at kun databehandlerens personale har adgang til personoplysninger. Tredjemænd kan dog i fornødent omfang få adgang til personoplysninger, hvis det er relevant for varetagelsen af databehandlerens opgaver og driften af databehandlerens systemer.

4.1.1 Tredjemand som omtalt i stk. 1, må ikke være en underdatabehandler, medmindre betingelserne i persondatalovgivningen og databehandleraftalen er opfyldt.

4.2 Adgangskontrollen skal sikres med brug af kodeord eller lignende.

5 PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

6 Bortskaffelse af hardware

6.1 Databehandleren skal sikre, at personoplysninger omfattet af denne databehandleraftale slettes, inden hardware bortskaffes eller overdrages til tredjemand.

7 Sikkerhedskopiering

7.1 Databehandleren skal i tilstrækkeligt omfang tage backups af personoplysninger omfattet af databehandleraftalen.

8 Sikkerhedsbrud

8.1 Databehandlerens sikkerhedspolitik skal indeholde en plan for håndtering af et sikkerhedsbrud.

8.2 Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på informationssikkerheden.

9 Kontrol

9.1 Databehandleren skal på den dataansvarliges anmodning give denne tiltrækkelige oplysninger om sikkerhedsforanstaltningerne til at afgøre, om sikkerhedsniveauet er tilstrækkeligt. Databehandleren kan tage et rimeligt vederlag herfor i overensstemmelse med databehandleraftalens pkt. 8.3.