Databehandleraftale – skabelon

SMTP.dk og mySMTP

Databehandleraftale efter GDPR artikel 28, stk. 3

Aftalen regulerer SMTP.dk ApS' behandling af personoplysninger ved levering af SMTP e-mail relay til kunden. Bilag A til D angiver behandling, underdatabehandlere, instruks, sikkerhed og øvrige forhold.

Version 22. november 2026. Kundespecifikke felter udfyldes ved indgåelsen.

Parterne

Den dataansvarlige

	Kundens juridiske navn
	CVR eller registreringsnummer
	Adresse og land

Databehandleren

SMTP.dk ApS
CVR 29849439
Refshalevej 163A
1432 København K
Danmark

Hver for sig en part og tilsammen parterne.

HAR AFTALT følgende databehandlerbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Henvisninger til medlemsstater i bestemmelserne omfatter EØS-medlemsstater.

1 Indhold

2 til 15 Databehandlerbestemmelser

2 Præambel

2.1 Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2.2 Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

2.3 I forbindelse med leveringen af SMTP e-mail relay under navnene SMTP.dk og mySMTP behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

2.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

2.5 Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

2.6 Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

2.7 Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt

brugen af.

2.8 Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

2.9 Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

2.10 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

2.11 Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3 Den dataansvarliges rettigheder og forpligtelser

3.1 Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

3.2 Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3.3 Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4 Databehandleren handler efter instruks

4.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

4.2 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 Fortrolighed

5.1 Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

5.2 Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6 Behandlingssikkerhed

6.1 Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, 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, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a) Pseudonymisering og kryptering af personoplysninger

b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2 Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

6.3 Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7 Anvendelse af underdatabehandlere

7.1 Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

7.2 Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

7.3 Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

7.4 Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil

gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

7.5 Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

7.6 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8 Overførsel til tredjelande eller internationale organisationer

8.1 Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

8.2 Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

8.3 Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

a) overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

b) overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

c) behandle personoplysningerne i et tredjeland

8.4 Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

8.5 Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9 Bistand til den dataansvarlige

9.1 Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a) oplysningspligten ved indsamling af personoplysninger hos den registrerede

b) oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

c) indsigtsretten

d) retten til berigtigelse

e) retten til sletning (”retten til at blive glemt”)

f) retten til begrænsning af behandling

g) underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h) retten til dataportabilitet

i) retten til indsigelse

j) retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

9.2 I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

a) den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b) den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c) den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d) den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

9.3 Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10 Underretning om brud på persondatasikkerheden

10.1 Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

10.2 Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

10.3 I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

a) karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

b) de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c) de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

10.4 Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11 Sletning og returnering af oplysninger

11.1 Når behandlingsydelserne ophører, sletter eller tilbageleverer databehandleren efter den dataansvarliges valg alle personoplysninger, som er behandlet på dennes vegne, og sletter eksisterende kopier. Databehandleren bekræfter sletningen. Dette gælder medmindre EU-retten eller en medlemsstats nationale ret kræver fortsat opbevaring. Proceduren følger bilag C.4.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12 Revision herunder inspektion

12.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, 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.

12.2 Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Parternes aftale om andre forhold

13.1 Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14 Ikrafttræden og ophør

14.1 Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

14.2 Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

14.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

14.5 Underskrift

Den dataansvarlige		**Databehandleren**	
Navn		Navn	
Stilling		Stilling	
Dato		Dato	
Underskrift		Underskrift	

15 Kontaktpersoner hos den dataansvarlige og databehandleren

15.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

15.2 Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontakt	Den dataansvarlige	Databehandleren
Navn og funktion		
E-mail til drift og databrud		
Telefon til hastesager		

Bilag A Oplysninger om behandlingen

A1 Formål

Formålet er at sende den dataansvarliges e-mails til de modtagere, som den dataansvarlige angiver, samt at understøtte levering, fejlsøgning og dokumentation af e-mailtransaktionerne. Tjenesten omfatter SMTP e-mail relay under navnene SMTP.dk og mySMTP.

Kundens konkrete anvendelse:

A2 Behandlingens karakter

SMTP.dk/mySMTP leverer almindelig SMTP-relay. Kundens færdige e-mails modtages og videresendes til de angivne modtageres mailservere. Der foretages ikke redaktionel bearbejdning af meddelelsernes indhold eller særskilt tilpasning af kundens headere. Den nødvendige mailtransport og autentificering kan tilføje tekniske headere, herunder transportoplysninger og DKIM-signatur. SPF, DKIM og DMARC indgår i den driftsmæssige opsætning for afsenderautentificering og korrekt e-mailafsendelse. Den konkrete opsætning følger den aftalte tjeneste og kundens afsenderdomæner. Forbindelser håndteres efter tjenestens almindelige TLS-politik. E-mails opbevares ikke i en afsendelseskø. Kan en e-mail ikke sendes, gives afsenderen et fejlsvar eller en bouncemeddelelse. Transaktions- og leveringslogs kan stilles til rådighed i højst 30 dage fra den oprindelige transaktion og slettes derefter. Autoriseret support kan tilgå nødvendige oplysninger inden for instruksen.

A3 Typer af personoplysninger

Behandlingen omfatter afsender- og modtageradresser samt de personoplysninger, som kunden medtager i e-mailens headere, emne, meddelelsesindhold og eventuelle vedhæftede filer. Desuden behandles relevante transaktionsoplysninger, eksempelvis tidsstempler, IP-adresser, meddelelsesidentifikatorer, leveringsstatus og SMTP-fejl, i det omfang de indgår i tjenesten.

Kundens konkrete oplysningstyper:

Der er ikke aftalt nogen specifik behandling af særlige kategorier af personoplysninger efter artikel 9, oplysninger om strafbare forhold efter artikel 10 eller CPR-numre. Sådan behandling kræver en særskilt skriftlig aftale om kategorier og nødvendige supplerende sikkerhedsforanstaltninger inden behandlingen.

A4 Kategorier af registrerede

Afsendere, modtagere og andre personer, der omtales i kundens e-mails. Afhængigt af kundens anvendelse kan det eksempelvis være kunder, brugere, deltagere, ansatte og kontaktpersoner hos samarbejdspartnere.

Kundens konkrete kategorier:

A5 Varighed

Behandlingen kan begynde, når aftalen er trådt i kraft, og fortsætter under levering af tjenesten. Den enkelte e-mails indhold behandles i den periode, der er nødvendig for den aftalte transmission. Der opbevares ikke e-mails i en afsendelseskø. Logoplysninger er tilgængelige i højst 30 dage fra den oprindelige e-mailtransaktion og slettes derefter, herunder eventuelle kopier og backupkopier af disse logs. Øvrige sletterutiner følger bilag C.4. Aftalen gælder, indtil de omfattede oplysninger er slettet eller tilbageleveret efter bestemmelserne.

Bilag B Underdatabehandlere

B1 Godkendte underdatabehandlere

Navn og registrering	Adresse	Behandling
AdeoDC CVR 37593184	Herstedvang 8 2620 Albertslund Danmark	Hosting af SMTP-platformen i Danmark.
Expertlance v/Radu Milcoveanu RO51704680	Bulevardul Iuliu Maniu 7 Corp T061072 Bucharest Rumænien	Udvikling og support af SMTP-platformen i Rumænien.

Ved aftalens ikrafttræden har den dataansvarlige godkendt de ovennævnte underdatabehandlere til de beskrevne aktiviteter. Godkendelsen omfatter alene behandling inden for den aftalte instruks og de godkendte lokaliteter.

B2 Ændringer og varsel

Der anvendes generel skriftlig godkendelse efter bestemmelse 7.2 og 7.3. Tilføjelse eller udskiftning af underdatabehandlere varsles skriftligt mindst 30 dage før ibrugtagning. Varslet angiver leverandør, aktivitet, behandlingslande, relevante adgangsforhold og eventuelle ændringer i overførselsgrundlag.

Den dataansvarlige kan gøre indsigelse inden ibrugtagning. En rettidig indsigelse afklares, før den berørte behandling overdrages til den nye eller udskiftede underdatabehandler. Udvidelse af behandlingsaktiviteter eller lokaliteter kræver skriftlig godkendelse efter bilag C.5.

B3 WHMCS som selvhostet kundeplatform

WHMCS drives selvhostet af SMTP.dk og anvendes til kundeadministration, produkter, abonnementer og fakturering under SMTP.dk’s eget dataansvar, jf. bilag D.2. WHMCS.com medtages derfor ikke som ekstern underdatabehandler alene på grund af softwarelicensen. En eventuel særskilt adgang for softwareleverandørens support skal vurderes og reguleres, inden adgang til oplysninger på kundens vegne gives.

Bilag C Instruks og sikkerhedsforanstaltninger

C1 Behandlingens genstand og instruks

Kunden fremsender e-mails til SMTP.dk’s servere, hvorfra de videresendes til kundens angivne slutmodtagere som en digital transaktion. E-mails opbevares ikke i en afsendelseskø. Kan en e-mail ikke sendes, gives afsenderen et fejlsvar eller en bouncemeddelelse. Transaktionsdetaljer og logoplysninger behandles til driftskontrol og fejlsøgning og slettes efter bilag C.4.

Instruksen omfatter alene den aftalte e-mailtjeneste og den nødvendige drift, sikkerhed og support. Kundedata må ikke anvendes til andre formål uden særskilt behandlingsgrundlag og klar regulering af rollerne.

Roller ved direkte kundeforhold

Kunden er dataansvarlig, SMTP.dk er databehandler, og leverandørerne i bilag B er underdatabehandlere. Kundens system afleverer e-mailen til SMTP.dk, som leverer den til slutmodtagerens mailserver.

Roller når kunden selv er databehandler

Hvis kunden sender på vegne af en anden dataansvarlig, er kæden den oprindelige dataansvarlige, kunden som databehandler og SMTP.dk som underdatabehandler. Kunden skal have den nødvendige bemyndigelse og sikre, at instruksen og denne aftale svarer til forpligtelserne over for den oprindelige dataansvarlige. Leverandørerne i bilag B indgår da som yderligere underdatabehandlere. Rollebetegnelserne i aftalen tilpasses dette forhold ved indgåelsen.

C2 Behandlingssikkerhed

Sikkerhedsniveauet fastlægges ud fra behandlingens karakter, omfang, sammenhæng og formål samt risikoen for de registrerede. Databehandleren vælger og vedligeholder de tekniske og organisatoriske foranstaltninger, der er nødvendige for det aftalte niveau. Alle omfattede oplysninger håndteres med høj fortrolighed; det ændrer ikke deres juridiske kategori.

Risikostyring og politikker

Risikostyringen baseres på en dokumenteret og regelmæssigt opdateret risikovurdering med fokus på de registreredes rettigheder og behandlingsaktiviteterne. Informationssikkerhedspolitikker og procedurer gennemgås mindst årligt og godkendes af ledelsen. Relevante politikker og procedurer stilles til rådighed for kunden på anmodning.

Udvikling og ændringer

Udvikling og ændringer styres efter dokumenterede procedurer med databeskyttelse gennem design og standardindstillinger. Kritiske netværksadgangspunkter beskyttes, og systemerne testes løbende for svagheder.

Identitet og adgang

Hver medarbejder og anden person, der arbejder for databehandleren og har adgang, tildeles en unik personlig konto, som ikke må deles. Adgange begrænses til det nødvendige, godkendes af en autoriseret person og gennemgås løbende. En opdateret oversigt viser, hvem der har adgang til hvilke oplysninger og systemer. Adgang tilbagekaldes, når behovet ophører.

Adgangskoder og fjernadgang

Passwordpolitikken gælder alle medarbejdere og gennemgås mindst årligt. Adgangskoder har som minimum 12 tegn med store og små bogstaver, tal og specialtegn. Kunder tildeles en automatisk genereret kode ved første login. Fjernadgang sker via en krypteret forbindelse og tofaktorautentifikation.

Fortrolighed og uddannelse

Medarbejdere er skriftligt forpligtet til tavshed under og efter ansættelsen. Relevante medarbejdere gennemgår mindst årligt GDPR, interne databeskyttelses- og sikkerhedspolitikker samt bevidstgørelse om social engineering.

Arbejdspladser og mobile medier

Arbejdsstationer låses, når de forlades. Fysiske dokumenter med personoplysninger opbevares aflåst. Personoplysninger må ikke opbevares lokalt på bærbare computere, telefoner, USB-medier eller eksterne diske uden en specifik aftale med kunden. Mobile enheders adgang til data kræver tofaktorautentifikation.

Netværk og endpoints

Der anvendes firewalls og antivirusbeskyttelse. Netværksadgang begrænses, og relevante systemer vedligeholdes og opdateres efter dokumenterede procedurer. Konstaterede sikkerhedssvagheder vurderes og håndteres efter risiko.

Logning

Adgangshændelser og væsentlige system- og nøglehændelser logges og er tilgængelige for autoriserede personer til kontrol, fejlsøgning og hændelseshåndtering. Logdata beskyttes mod uvedkommendes adgang og slettes efter bilag C.4.

Sikker udveksling og e-mailtransport

Administrativ dataudveksling sker primært via SSH. Hvis dette ikke er muligt, må data efter kundens accept udveksles via e-mail med tvungen ende-til-ende-kryptering. Dette krav vedrører administrativ udveksling og beskriver ikke i sig selv sikkerheden i alle e-mails, som kunden sender gennem relaytjenesten.

Fysisk sikkerhed

Servere og andet udstyr, der behandler oplysningerne, opbevares i aflåste lokaler. Serverrum beskyttes mod brand og tyveri. Databehandlerens egne lokaler og relevante fysiske medier sikres mod uvedkommendes adgang.

Backup og gendannelse

Eventuelle backupkopier af logdata er omfattet af den samme maksimale opbevaringsperiode på 30 dage regnet fra den oprindelige e-mailtransaktion. Backup forlænger ikke denne periode. Der skal være dokumenterede procedurer til at genoprette tilgængelighed efter fysiske og tekniske hændelser og til at kontrollere, at gendannelse fungerer.

Hændelser og kontrol

Der vedligeholdes procedurer til at forebygge, opdage, klassificere og håndtere databrud samt underrette kunden. Proceduren for databrud testes mindst årligt. Processer og politikker til forebyggelse af tab af personoplysninger evalueres mindst årligt. Konstaterede afvigelser afhjælpes efter en dokumenteret plan med opfølgning.

SMTP-tjenesten anvender en almindelig TLS-politik for transportkryptering på forbindelser, hvor TLS understøttes og etableres. Der er ikke aftalt et særskilt krav om tvungen TLS på alle eksterne forbindelser eller ende-til-ende-kryptering af kundens e-mails. Kundespecifikke krav om et højere beskyttelsesniveau aftales skriftligt inden den pågældende behandling.

C3 Bistand til den dataansvarlige

Databehandleren bistår inden for behandlingens karakter og de oplysninger, der er tilgængelige, med at identificere, udtrække, begrænse, slette eller tilbagelevere relevante oplysninger ved anmodninger fra registrerede. Anmodninger, som databehandleren modtager direkte fra en registreret om kundens behandling, videresendes til kunden uden unødig forsinkelse og besvares ikke selvstændigt, medmindre kunden har instrueret herom eller loven kræver det.

Bistanden omfatter oplysninger om behandlingsaktiviteter, dataflow og sikkerhedsforanstaltninger til brug for kundens risikovurdering, konsekvensanalyse og eventuelle forudgående høring. Databehandleren vejleder også om fremsendelse og modtagelse via de aftalte sikrede kanaler.

Ved databrud gives uden unødig forsinkelse og om muligt senest 24 timer efter kendskab en første underretning med de foreliggende oplysninger. Underretningen angiver hændelsens karakter, tidsforløb, berørte systemer og oplysningstyper, omtrentligt antal registrerede og registreringer, sandsynlige konsekvenser, trufne og planlagte foranstaltninger samt kontaktperson. Manglende oplysninger eftersendes løbende, så kunden kan opfylde sine frister. Kunden træffer beslutning om anmeldelse og underretning af registrerede.

C4 Opbevaring og sletning

Oplysninger	Frist og sletterutine
E-mailindhold og vedhæftninger	Behandles i det omfang, det er nødvendigt for transmissionen. Der opbevares ikke e-mails i en afsendelseskø. Kan e-mailen ikke sendes, gives afsenderen et fejlsvar eller en bouncemeddelelse.
Transaktionsdetaljer og leveringslogs	Kan stilles til rådighed i højst 30 dage fra den oprindelige e-mailtransaktion. Derefter slettes oplysningerne og eventuelle kopier.
Eventuel backup af logdata	Samme maksimale alder på 30 dage fra den oprindelige e-mailtransaktion. Backup giver ingen yderligere opbevaringsperiode.
Andre logs med kundeoplysninger	Logs omfattet af denne aftale slettes efter højst 30 dage fra den registrerede hændelse.
Supportsager med kundens relaydata	Kopier af relaylogs er omfattet af samme 30-dagesfrist fra den oprindelige transaktion. Oplysninger omfattet af denne aftale må ikke deles med eksterne supportsystemer, medmindre leverandøren er godkendt efter bilag B.

Ved ophør er kundens udgangspunkt sletning med bekræftelse, jf. bestemmelse 11.1. Kunden kan inden sletning skriftligt ændre valget til tilbagelevering af de oplysninger, der fortsat findes, efterfulgt af sletning af eksisterende kopier. Allerede lovligt slettede oplysninger genskabes ikke med henblik på tilbagelevering.

Sletning ved ophør omfatter de oplysninger, der fortsat findes, og deres eksisterende kopier. Eventuelle backupkopier af logs må under ingen omstændigheder bevare de pågældende logs ud over 30 dage fra den oprindelige e-mailtransaktion. En gendannelse må ikke genindføre oplysninger, som efter sletteinstruksen skal være slettet. Afsluttet sletning bekræftes over for kunden.

Hvis EU-ret eller medlemsstaternes nationale ret kræver yderligere opbevaring af oplysninger omfattet af denne aftale, oplyser databehandleren kunden om hjemmel, omfang og periode, medmindre underretning er forbudt. Sådanne oplysninger anvendes alene til det lovpligtige formål.

C5 Lokalitet for behandling

Hosting af SMTP-platformen sker hos AdeoDC, Herstedvang 8, 2620 Albertslund, Danmark. Udvikling og support ved Expertlance foregår fra den i bilag B angivne lokalitet i Rumænien. Begge lande er i EU. SMTP.dk's egen behandling er knyttet til adressen angivet for databehandleren og de særskilt godkendte fjernarbejdspladser.

Oplysningerne må ikke behandles eller tilgås fra andre lokaliteter uden kundens forudgående skriftlige godkendelse. Godkendelse af en ny underdatabehandler erstatter ikke en nødvendig instruks om tredjelandsoverførsel efter C.6.

C6 Instruks vedrørende overførsel til tredjelande

Overførsel af personoplysninger til tredjelande og adgang til oplysninger fra tredjelande følger bestemmelse 8. Der gives ikke en generel tilladelse til nye tredjelandsoverførsler. De konkrete overførsler, der indgår i den godkendte leverandørbehandling, skal være omfattet af dokumenteret instruks og et gyldigt overførselsgrundlag, hvor databeskyttelsesforordningens kapitel V finder anvendelse.

Eventuel behandling i tredjelande kræver særskilt dokumenteret instruks og et gyldigt overførselsgrundlag, hvor kapitel V finder anvendelse.

C7 Kundens tilsyn med SMTP.dk

Det ordinære tilsyn sker ved, at den dataansvarlige sender et GDPR-spørgeskema til SMTP.dk. Mindst årligt besvarer SMTP.dk uden særskilt betaling kundens relevante spørgeskema og stiller den nødvendige dokumentation for svarene til rådighed. Besvarelsen fremsendes uden unødig forsinkelse eller inden for en rimelig aftalt frist. Kunden kan stille supplerende spørgsmål og kræve den dokumentation, der er nødvendig efter bestemmelse 12.

SMTP.dk har ingen ISAE-erklæring. Aftalen kræver ikke, at SMTP.dk indhenter en sådan erklæring. Den aftalte spørgeskemamodel begrænser ikke kundens ret til nødvendige revisioner og inspektioner efter bestemmelse 12 eller parternes øvrige ufravigelige forpligtelser.

Kunden eller en bemyndiget revisor kan gennemføre revisioner og inspektioner, herunder fysiske inspektioner, når det er nødvendigt. Planlægning aftales med rimeligt hensyn til drift, fortrolighed og andre kunders oplysninger. Der kan ikke kræves et varsel, som hindrer nødvendig kontrol ved hændelser, begrundet mistanke eller myndighedskrav.

SMTP.dk afsætter nødvendige ressourcer til kontrol og afhjælper dokumenterede afvigelser med opfølgning. Kunden kan kræve yderligere dokumentation og nødvendige foranstaltninger. Leverandørmateriale erstatter ikke dokumentation for SMTP.dk's egne processer.

C8 Tilsyn med underdatabehandlere

SMTP.dk fører dokumenteret tilsyn med de godkendte underdatabehandlere mindst årligt og ved væsentlige ændringer eller hændelser. Kontrollen tilpasses den enkelte leverandørs aktivitet og risiko og omfatter relevante aftaler, adgangsforhold, lokaliteter, sikkerhedsforanstaltninger, sletning og opfølgning på afvigelser.

Tilsynet baseres på skriftlige oplysninger, relevante spørgeskemaer og dokumentation for den enkelte underdatabehandlers faktiske kontroller. Hvor leverandøren anvender standardiseret kontrolmateriale, kan dette indgå i vurderingen. SMTP.dk følger op på utilstrækkelige svar og dokumentation og gennemfører yderligere nødvendig kontrol. Der indføres ikke et generelt krav om en bestemt ISAE-erklæring.

SMTP.dk stiller relevant kontroldokumentation til rådighed for kunden, følger op på mangler og sikrer de aftaleretlige rettigheder til nødvendig kontrol hos underdatabehandlere. Kunden kan kræve yderligere kontrol og om nødvendigt deltage i inspektion. SMTP.dk bevarer det fulde ansvar efter bestemmelse 7.

Bilag D Andre forhold

D1 Forholdet til tjenesteaftalen

Pris, abonnement, supportvilkår og andre kommercielle forhold følger parternes særskilte tjenesteaftale, i det omfang de ikke strider mod disse bestemmelser eller forringer de registreredes rettigheder. Dette bilag indfører ingen særskilt ansvarsbegrænsning.

D2 Oplysninger uden for denne databehandling

Oplysninger, som SMTP.dk eventuelt behandler som selvstændig dataansvarlig til egne formål, eksempelvis fakturering, bogføring og administration af kundeforholdet, omfattes ikke af instruksen om kundens e-mailindhold. Sådanne formål, behandlingsgrundlag og opbevaringsperioder beskrives i SMTP.dk's relevante privatlivsinformation. Klassifikationen afhænger af den konkrete behandling.

WHMCS drives selvhostet og anvendes som kundeplatform til produkter, abonnementer og fakturering. For disse formål er SMTP.dk dataansvarlig. Opbevaring til fakturering og kundeadministration følger egne formål og relevante lovkrav.

WHMCS.com er softwareleverandør til den selvhostede installation og er ikke alene af den grund databehandler for kundedatabasen. Hvis en ekstern leverandør får adgang til personoplysninger som led i support eller anden behandling, skal den konkrete rolle og det nødvendige aftalegrundlag være på plads inden adgangen.

D3 En instruks der kan være ulovlig

Hvis SMTP.dk efter bestemmelse 4.2 vurderer, at en instruks er ulovlig, underrettes kunden omgående med en begrundelse. Den berørte behandling sættes om nødvendigt i bero, mens parterne afklarer en lovlig instruks. Foranstaltningen begrænses til det nødvendige og ophæver ikke parternes øvrige forpligtelser.