



DATABASEHANDLERAFTALE (DPA)

Standard-DPA

gramflows 2026

Generel databehandleraftale mellem gramflows (databehandler) og kunden (dataansvarlig). Gælder automatisk for alle aftaler og abonnementer der involverer behandling af personoplysninger.

VERSION

v2026.1.2

GYLDIG FRA

1. august 2026

ERSTATTER

v2026.1.1

UDSTEDER

gramflows

Indholdsfortegnelse

Anvendelse og accept	3
1 / Parterne og kontaktoplysninger	3
2 / Præambel	4
3 / Den dataansvarliges rettigheder og forpligtelser	5
4 / Databehandleren handler efter instruks	5
5 / Fortrolighed	6
6 / Behandlingssikkerhed	6
7 / Anvendelse af underdatabehandlere	7
8 / Overførsel til tredjelande	8
9 / Bistand til den dataansvarlige	9
10 / Underretning om brud på persondatasikkerheden	10
11 / Sletning og returnering af oplysninger	11
12 / Revision og inspektion	11
13 / Parternes aftale om andre forhold	12
14 / Ikrafttræden og ophør	12
Bilag A — Oplysninger om behandlingen	14
Bilag B — Underdatabehandlere	18
Bilag C — Instruks og sikkerhedsforanstaltninger	22
Bilag D — Øvrige forhold	28
Versionshistorik	30

Anvendelse og accept

Denne databehandlersaftale (herefter "DPA" eller "Bestemmelserne") er gramflows' standard-aftale om behandling af personoplysninger på vegne af kunder. DPA'en accepteres automatisk som en integreret del af ethvert tilbud, abonnement, ordre eller løbende aftale mellem gramflows og kunden, der involverer behandling af personoplysninger på kundens vegne.

Den til enhver tid gældende version af DPA'en er tilgængelig på gramflows.com/dpa. DPA'en kræver ikke separat underskrift, men gramflows udleverer på anmodning en underskriftsklar version til kunder, hvis interne politikker kræver fysisk eller elektronisk signering.

I denne DPA betegnes parterne som følger:

- **"Den dataansvarlige" eller "kunden"**: den juridiske person, som modtager gramflows' ydelser, og som bestemmer formålet med og hjælpemidlerne til behandling af personoplysninger.
- **"Databehandleren"**: gramflows (VAT: CZ7309231259), som behandler personoplysninger på vegne af kunden i forbindelse med levering af aftalte ydelser.

DPA'en bygger på Datatilsynets standardkontraktbestemmelser (senest opdateret marts 2024) og er tilpasset gramflows' ydelser. DPA'en gælder uanset hvilken konkret ydelse, kunden modtager — herunder Webmanager, hosting, udvikling, automation (Make/n8n), SEO/content og konsulent/sparring. Bilag A specificerer behandlingens karakter for de enkelte ydelser.

Forrang ved konflikt

I tilfælde af uoverensstemmelse mellem denne DPA og kommercielle aftaler mellem parterne (tilbud, ordrer, abonnementsbetingelser, SOW'er m.v.) har DPA'en forrang for så vidt angår spørgsmål om databeskyttelse. Kommercielle vilkår (pris, leveringstider, opsigelsesvarsel m.v.) reguleres af den underliggende aftale samt gramflows' handelsbetingelser.

1 / Parterne og kontaktoplysninger

1.1 Den dataansvarlige

Den dataansvarlige er den kunde, som har indgået aftale med gramflows om levering af ydelser, der involverer behandling af personoplysninger. Kundens identifikation

(firmanavn, CVR-nummer, adresse og kontaktperson) fremgår af den underliggende kommercielle aftale (tilbud, ordrebekræftelse, faktura eller abonnementsbevis).

Kunden er ansvarlig for at sikre, at de kontaktoplysninger, gramflows har registreret, til enhver tid er korrekte og opdaterede, herunder kontaktoplysninger til kundens DPO eller anden ansvarlig for databeskyttelse, hvis kunden har udpeget en sådan.

1.2 Databehandleren

Firma	gramflows
VAT	CZ7309231259
Adresse	Belehradská 858/23, 120 00 Prag, Tjekkiet
Telefon	+45 88 70 70 57
E-mail (generel)	support@gramflows.com
E-mail (DPA-spørgsmål)	dg@gramflows.com
Kontaktperson	Dennis Erik Gam Nielsen, Indehaver
Tilsynsmyndighed	Úřad pro ochranu osobních údajů (ÚOOÚ), Tjekkiet

Tilsynsmyndighed: Da gramflows er etableret i Tjekkiet, er den primære tilsynsmyndighed ÚOOÚ. For kunder i Danmark fungerer Datatilsynet (datatilsynet.dk) som lokal tilsynsmyndighed for den dataansvarlige selv.

2 / Præambel

1. Disse Bestemmelser fastsætter den dataansvarliges og databehandlerens rettigheder og forpligtelser, når der foretages behandling af personoplysninger på vegne af den dataansvarlige.
2. Bestemmelserne 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 (Databeskyttelsesforordningen, "GDPR").
3. I forbindelse med leveringen af gramflows' ydelser behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne:
 - Bilag A — oplysninger om behandlingens formål, karakter, typer af personoplysninger, kategorier af registrerede og varighed
 - Bilag B — godkendte underdatabehandlere og varsel for ændringer
 - Bilag C — instruks og minimumskrav til tekniske og organisatoriske sikkerhedsforanstaltninger samt revisionsprocedurer
 - Bilag D — øvrige forhold (lovvalg, værneting, ansvar m.v.)
6. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
7. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter Databeskyttelsesforordningen eller enhver anden lovgivning.

3 / Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med Databeskyttelsesforordningen (jf. forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret (herunder den danske databeskyttelseslov) og disse Bestemmelser.
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. 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. Den dataansvarlige er ansvarlig for at orientere de registrerede om behandlingen i overensstemmelse med GDPR artikel 13 og 14.

4 / Databehandleren handler efter instruks

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; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art. 28, stk. 3, litra a.

2. Den dataansvarliges dokumenterede instruks til databehandleren udgøres af denne DPA's Bilag C samt af den underliggende kommercielle aftale (herunder tilbud, ordrebekræftelse, abonnementsbeskrivelse eller SOW). Yderligere instrukser kan gives skriftligt til dg@gramflows.com.
3. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 / Fortrolighed

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.
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

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 sikkerhedsniveau, der passer til disse risici.
2. 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:
 - Pseudonymisering og kryptering af personoplysninger
 - Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

- En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed
- 3.** 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, således at vedkommende kan identificere og vurdere sådanne risici.
- 4.** 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.
- 5.** Databehandlerens minimumssikkerhedsforanstaltninger fremgår af Bilag C.2. 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, skriftligt til databehandleren.

7 / Anvendelse af underdatabehandlere

- 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 (underdatabehandler).
- 2.** Databehandleren må ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
- 3.** Databehandleren har den dataansvarliges generelle godkendelse til brug af de underdatabehandlere, der fremgår af Bilag B. 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).
- 4.** Underretning om ændringer i underdatabehandlere sker ved e-mail til kundens primære kontaktperson registreret hos gramflows samt via opdatering af listen på gramflows.com/dpa. Det er kundens ansvar at sikre, at den registrerede kontaktperson modtager og videreformidler sådanne underretninger internt.

5. 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.
6. Databehandleren er ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og Databeskyttelsesforordningen.
7. Underdatabehandlersaftale(n) og eventuelle senere ændringer hertil sendes — efter den dataansvarliges anmodning herom — i kopi til den dataansvarlige. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandlersaftalen, skal ikke sendes til den dataansvarlige.
8. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere.
9. 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.

8 / Overførsel af personoplysninger til tredjelande

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.
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.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren ikke inden for rammerne af disse Bestemmelser:
 - Overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - Overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - Behandle personoplysningerne i et tredjeland
4. Databehandlerens standardpolitik er, at alle personoplysninger behandles inden for EU/EØS. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland — hvis sådan instruks gives — samt det eventuelle overførselsgrundlag i Databeskyttelsesforordningens kapitel V (f.eks. EU-Kommissionens Standard Contractual Clauses), som overførslen er baseret på, skal angives skriftligt i Bilag C.6 eller i et særskilt addendum.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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

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, jf. Databeskyttelsesforordningens kapitel III. Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
 - Oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - Indsigtsretten
 - Retten til berigtigelse
 - Retten til sletning ("retten til at blive glemt")
 - Retten til begrænsning af behandling
 - Underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - Retten til dataportabilitet
 - Retten til indsigelse

- Retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
- 2.** I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 9.1, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
- Den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - Den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - Den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse / DPIA)
 - Den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, 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
- 3.** De fornødne tekniske og organisatoriske foranstaltninger samt omfang og udstrækning for databehandlerens bistand fremgår af Bilag C.3.

10 / Underretning om brud på persondatasikkerheden

- 1.** Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
- 2.** Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 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.
- 3.** I overensstemmelse med Bestemmelse 9.2 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:

- 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
 - De sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - 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
- 4.** Underretning om brud sker ved e-mail til kundens registrerede primære kontaktperson samt via telefonisk opfølgning, hvis bruddets karakter tilsiger det. I akutte tilfælde anvendes telefon som første kontakt.

11 / Sletning og returnering af oplysninger

- 1.** Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige, og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
- 2.** Sletning af personoplysninger gennemføres senest 30 dage efter ophør af den underliggende aftale, medmindre andet aftales skriftligt mellem parterne, eller den dataansvarlige inden udløb af 30-dagesfristen anmoder om returnering af data i et struktureret, almindeligt anvendt og maskinlæsbart format.
- 3.** Backup-data, der indeholder personoplysninger, slettes i takt med den almindelige backup-rotation som beskrevet i Bilag C, dog senest 90 dage efter ophør.
- 4.** Databehandleren udsteder skriftlig bekræftelse på sletning til den dataansvarlige senest 30 dage efter sletningens gennemførelse.

12 / Revision, herunder inspektion

- 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.
- 2.** Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning 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

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.
2. Sådanne andre forhold er reguleret i Bilag D samt i parternes underliggende kommercielle aftale og gramflows' handelsbetingelser (gramflows.com/ handelsbetingelser).

14 / Ikrafttræden og ophør

1. Bestemmelserne træder i kraft samtidig med ikrafttrædelsen af den underliggende kommercielle aftale mellem parterne og accepteres automatisk som en integreret del af denne. Ingen separat underskrift er påkrævet.
2. Den til enhver tid gældende version af Bestemmelserne er tilgængelig på gramflows.com/dpa. Databehandleren forbeholder sig ret til at opdatere Bestemmelserne med mindst 30 dages skriftligt varsel til den dataansvarlige. Væsentlige ændringer kommunikerer pr. e-mail til kundens registrerede primære kontaktperson.
3. Hvis den dataansvarlige gør indsigelse mod en planlagt opdatering, kan den dataansvarlige opsiges den underliggende kommercielle aftale med det varsel, der er angivet i denne aftale eller i gramflows' handelsbetingelser. Indtil opsigelsen træder i kraft, gælder den foregående version af Bestemmelserne.
4. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
5. 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.
6. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i

overensstemmelse med Bestemmelse 11 og Bilag C, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.



Oplysninger om behandlingen

Behandlingens formål, karakter, typer af personoplysninger, kategorier af registrerede og varighed — pr. ydelseskategori.

Bilag A — Oplysninger om behandlingen

A.1 Formål med behandlingen

Databehandleren leverer en eller flere af nedenstående ydelser til den dataansvarlige. Hvilke konkrete ydelser, der er omfattet i det enkelte kundeforhold, fremgår af den underliggende kommercielle aftale (tilbud, ordrebekræftelse, abonnementsbevis eller SOW).

Databehandleren behandler kun personoplysninger i det omfang, det er nødvendigt for at levere de aftalte ydelser, og udelukkende efter dokumenteret instruks fra den dataansvarlige, jf. Bestemmelse 4.

A.2 Ydelseskategorier (behandlings karakter)

Nedenstående tabel beskriver karakteren af behandlingen for hver ydelseskategori. Kun de kategorier, der indgår i det enkelte kundeforhold, er relevante.

Ydelseskategori	Behandlings karakter
Webmanager (drift og vedligehold af eksisterende WordPress-sites)	Adgang til kundens WordPress-installation (filer, database, admin-konti) med henblik på opdateringer, backup, fejlsøgning, sikkerhedstiltag og support. Databehandleren har som udgangspunkt læse- og redigeringsadgang til alle data, der er lagret i kundens installation, men behandler kun personoplysninger i det omfang, det er nødvendigt for at udføre opgaven.
Hosting (managed WordPress hosting)	Drift af serverinfrastruktur, hvor kundens WordPress-installation og tilhørende database er hostet. Lagring, backup, monitorering, sikkerhedsfiltrering (WAF/DDoS) og levering af content over internettet.
Udvikling (custom builds, nye sites, plugins, integrationer)	Udvikling og implementering af kode, integrationer og funktionalitet på kundens sites. Adgang til test-, staging- og produktionsmiljøer kan være nødvendig. Test med kundens reelle data sker kun efter eksplicit aftale; ellers anvendes anonymiserede eller syntetiske testdata.

Automation

(Make/n8n-flows der behandler kundedata)

Design, opsætning og drift af automatiserede arbejdsgange, der overfører, transformerer eller beriger data mellem kundens systemer og tredjepartstjenester. Personoplysninger kan passere gennem flows i transit; persistent lagring i automation-plattformen begrænses til det strengt nødvendige.

SEO / content

(analyse, ranking, evt. CMS-adgang)

Analyse af søgeordsdata, ranking-data, performance-data og indholdsoptimering. Kan inkludere redaktionel adgang til kundens CMS (typisk WordPress) til implementering af on-page-optimering. Personoplysninger behandles kun i det omfang, det er knyttet til content (f.eks. forfatternavne) eller analytics-data.

Konsulent / sparring

(ad hoc, kortvarig adgang)

Tidsbegrænset rådgivning, gennemgang eller løsning af konkrete problemstillinger. Adgang til kundens systemer er som udgangspunkt minimal og tidsbegrænset; adgangsrettigheder fjernes umiddelbart efter opgavens afslutning.

A.3 Typer af personoplysninger

Behandlingen kan omfatte følgende typer af personoplysninger, afhængigt af ydelse og kundens konkrete systemer:

Almindelige personoplysninger (GDPR art. 6):

- Identifikationsoplysninger: navn, brugernavn, kundeID, medlemsnummer
- Kontaktoplysninger: e-mail, telefonnummer, postadresse
- Demografiske oplysninger: fødselsdato, køn, sprog
- Tekniske oplysninger: IP-adresse, brugeragent, sessionsdata, cookie-ID
- Kontooplysninger: krypterede passwords, login-historik, brugerroller
- Indholdsdata: kommentarer, formularindsendelser, uploads, korrespondance
- Transaktionsdata: ordrer, fakturaer, betalingsstatus (ikke kortdata)
- Analytics- og performance-data: side-views, klikadfærd, konverteringer

Følsomme personoplysninger (GDPR art. 9) og personnummer (CPR, databeskyttelseslovens § 11):

Databehandleren behandler som udgangspunkt ikke følsomme personoplysninger eller CPR-numre. Hvis kundens systemer indeholder sådanne oplysninger, eller hvis en specifik ydelse forudsætter behandling af dem, skal dette aftales skriftligt forud for behandling, og særlige tekniske og organisatoriske foranstaltninger kan være påkrævet (f.eks. ende-til-ende-kryptering, adgangsadskillelse, særlig logning). Se Bilag C.2 for

forhøjede sikkerhedsforanstaltninger ved behandling af særlige kategorier af oplysninger.

A.4 Kategorier af registrerede

Behandlingen kan omfatte følgende kategorier af registrerede personer:

- Kundens egne kunder og medlemmer (slutbrugere)
- Kundens medarbejdere, freelancere og partnere
- Besøgende på kundens website
- Nyhedsbrevs- og marketing-modtagere
- Formularudfyldere, kontaktformularhenvendelser, supportsager
- Administratorer og brugere af kundens backend-systemer

A.5 Behandlingens varighed

Behandlingen er ikke tidsbegrænset og varer, indtil den underliggende kommercielle aftale opsiges eller ophører.

Opbevaringsperioder for forskellige datatyper hos databehandleren:

- Produktionsdata (data i kundens aktive systemer): så længe aftalen er i kraft, eller indtil kunden selv sletter data
- Backups: 50 dage rolling retention (se Bilag C.2)
- Audit- og adgangslogs: op til 24 måneder
- Fejllogs og support-tickets: op til 12 måneder efter sagens lukning
- Sikkerhedslogs (login-forsøg, WAF-events): op til 6 måneder

Ved aftalens ophør slettes alle personoplysninger jf. Bestemmelse 11 og Bilag C.4.



Underdatabehandlere

Liste over godkendte underdatabehandlere samt varsel
for ændringer.

Bilag B — Underdatabehandlere

B.1 Generelt

Databehandleren har den dataansvarliges generelle godkendelse til brug af de underdatabehandlere, der er anført i tabellerne nedenfor. Underdatabehandlerne er opdelt i:

- **Aktive underdatabehandlere** — anvendes som standard for alle eller størstedelen af ydelser
- **Betingede underdatabehandlere** — anvendes kun ved konkrete ydelser, hvor de er relevante, og kun efter forudgående aftale med kunden

Databehandleren har sikret, at der er indgået databehandlersaftale med samtlige nedenstående underdatabehandlere i overensstemmelse med kravene i Bestemmelse 7, herunder at underdatabehandlerne er pålagt tilsvarende databeskyttelsesforpligtelser. Dokumentation kan udleveres til den dataansvarlige på anmodning.

B.2 Aktive underdatabehandlere

Navn	Lokation	Behandlingens karakter
Hetzner Online GmbH HRB 3204 (Reg. Fürth)	Tyskland (EU)	Hosting af dedikeret cloud-server / VPS-infrastruktur. Lagring af WordPress-installationer, databaser og krypterede personoplysninger.
Cloudflare Ireland Ltd. Reg. 554251	Irland (EU)	CDN, Web Application Firewall (WAF), DDoS-beskyttelse, SSL/TLS-terminering. Behandling af IP-adresser og request-metadata. EU-kontrakt anvendes; data routes via EU-noder.
LIVEN STUDIO SAS SIRET 901 423 434	Frankrig (EU)	Daglig inkrementel backup af WordPress-installationer (filer og database, AES-256-krypteret). Backup-retention: 50 dage.
Google Ireland Limited (Google Workspace) Reg. 368047	Irland (EU)	Google Workspace til intern e-mail, dokumenthåndtering og support-korrespondance. Ugentlig fuld backup-lagring (krypterede backup-arkiver) via Google Drive (EU-region).

Make s.r.o. / Celonis SE Make.com	Tjekkiet / Tyskland (EU)	Automation-plattform til opsætning og drift af workflows mellem kundens systemer. Personoplysninger kan passere gennem flows i transit. EU-dataresidens anvendes hvor tilgængelig.
---	-----------------------------	--

Siber Systems Inc. (RoboForm)	USA EU SCCs	Sikker opbevaring af adgangskoder og credentials til kundens systemer (kun til drifts- og supportformål). AES-256-krypteret med zero-knowledge-arkitektur. Overførselsgrundlag: EU-Kommissionens Standard Contractual Clauses (SCCs) + supplerende foranstaltninger.
---	----------------	--

B.3 Betingede underdatabehandlere

Anvendes kun, hvis den konkrete ydelse forudsætter det. Den dataansvarlige underrettes specifikt, før en betinget underdatabehandler aktiveres for kundens aftale.

Navn	Lokation	Anvendelse
Idura ApS (tidl. Criipto ApS) CVR 35142207	Danmark (EU)	Leverandør af MitID-integration (certificeret MitID-broker). Aktiveres kun ved løsninger med MitID-flow. Behandler navn og fødselsdato i verifikations-flowet. CPR behandles ikke af Idura.

B.4 Værktøjer der ikke er underdatabehandlere

Følgende værktøjer anvendes af databehandleren i forbindelse med eget arbejde, men behandler ikke kundens personoplysninger og udgør derfor ikke underdatabehandlere i henhold til denne DPA:

AI-værktøjer (Anthropic Claude, Claude Code m.fl.)

Databehandleren anvender AI-værktøjer (herunder Anthropic Claude og Claude Code) til generelt udviklings- og produktivitetsarbejde, der ikke involverer behandling af kundens personoplysninger. AI-værktøjer fodres ikke med kundens persondata, kunde-databasedumps, kundens slutbrugerdata, eller andet materiale, der kan identificere kundens registrerede. Hvis behandling af kundens personoplysninger med AI-værktøjer fremover måtte blive aktuel, vil dette først ske efter forudgående skriftlig aftale med kunden, opdatering af denne DPA's Bilag B og fastlæggelse af passende overførselsgrundlag og sikkerhedsforanstaltninger.

B.5 Varsel for ændringer i underdatabehandlere

Databehandleren skal underrette den dataansvarlige om planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel, jf. Bestemmelse 7.3. Underretningen sker pr. e-mail til kundens registrerede primære kontaktperson samt via opdatering af den til enhver tid gældende liste på gramflows.com/dpa.

Såfremt den dataansvarlige gør indsigelse mod ændringen, kan den dataansvarlige vælge at opsige Bestemmelserne (og dermed den underliggende kommercielle aftale) med det varsel, der er angivet i den underliggende aftale eller gramflows' handelsbetingelser.



Instruks og sikkerhed

Den dataansvarliges instruks samt minimumskrav til tekniske og organisatoriske sikkerhedsforanstaltninger.

Bilag C — Instruks og sikkerhedsforanstaltninger

C.1 Behandlingens genstand / instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører de ydelser, der er beskrevet i Bilag A.2 og i den underliggende kommercielle aftale. Dette omfatter typisk en eller flere af følgende aktiviteter:

- Drift, hosting og vedligehold af kundens WordPress-installationer eller andre web-løsninger
- Udvikling og implementering af kode, plugins, integrationer og custom funktionalitet
- Opsætning og drift af automatiserede workflows (Make/n8n)
- SEO- og content-analyse samt redaktionel implementering
- Backup og genoprettelse af data
- Support, fejlsøgning og rådgivning
- Logning af driftshandlinger med henblik på audit-trail og sikkerhed

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle karakteren af de personoplysninger, der behandles. Databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige og aftalte sikkerhedsniveau.

Databehandleren gennemfører som minimum følgende foranstaltninger:

Tekniske foranstaltninger

- Al datatransmission sker over HTTPS med TLS 1.2 eller nyere. HTTP Strict Transport Security (HSTS) er aktiveret hvor relevant.
- Følsomme datafelter (hvor relevant, f.eks. CPR ved særlig aftale) lagres udelukkende AES-256-krypteret. Krypteringsnøgler opbevares adskilt fra den krypterede data.
- Backup-filer er AES-256-krypteret såvel under transit som at-rest.
- Web Application Firewall (WAF) og DDoS-beskyttelse via Cloudflare.
- Dedikeret server med fast IP. Administrativ adgang er kun mulig via SSH med nøglebaseret autentifikation.
- To-faktor-autentifikation (2FA) er obligatorisk for alle administratorconti hos databehandleren samt alle administratoradgange til WordPress-backend.
- Adgangskoder opbevares i krypteret passwordmanager (RoboForm) med zero-knowledge-arkitektur og 2FA.

- Automatiske og manuelle sikkerhedsopdateringer af WordPress-kerne, plugins og server-OS i ugentlig opdateringscyklus.
- Daglige inkrementelle backups samt ugentlig fuld backup. Backup-retention: 50 dage. Backups gemmes på minimum to geografisk adskilte lokationer inden for EU.
- Aktivitetslog (audit-trail) registrerer administratorhandlinger, login-forsøg og kritiske systemhændelser.
- Monitorering af uptime, sikkerhedshændelser og fil-integritet.

Organisatoriske foranstaltninger

- Adgang til personoplysninger er begrænset til personer med et arbejdsbetinget behov (need-to-know-princippet).
- Alle personer med adgang er underlagt skriftlig tavshedspligt.
- Liste over personer med adgang gennemgås minimum halvårligt og opdateres løbende ved personaleændringer.
- Dokumenterede procedurer for håndtering af persondatasikkerhedsbrud (incident response).
- Dokumenterede procedurer for backup, genoprettelse og test heraf.
- Databehandleren holder sig løbende opdateret om relevante trusler og sikkerhedsforanstaltninger.
- AI-værktøjer (Claude, ChatGPT, Copilot m.fl.) anvendes ikke til behandling af kundens personoplysninger uden forudgående skriftlig aftale, jf. Bilag B.4.

Forhøjet sikkerhed ved særlige kategorier af oplysninger

Ved aftalt behandling af følsomme oplysninger (GDPR art. 9), personnummer (databeskyttelseslovens § 11) eller andre oplysninger med forhøjet risikoprofil, gennemfører databehandleren — efter forudgående aftale — supplerende foranstaltninger såsom:

- Feltniveau-kryptering med adskilt nøgleopbevaring
- Forstærket adgangslogging og periodisk gennemgang heraf
- Stramme adgangsregler (separation of duties)
- Indsnævret retention

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt — inden for det nedenstående omfang og udstrækning — bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Besvare henvendelser fra registrerede (indsigt, berigtigelse, sletning, begrænsning, dataportabilitet, indsigelse) inden for rimelig tid, dog maksimalt 10 arbejdsdage fra anmodningen videresendes af den dataansvarlige

- Leverer teknisk udtræk af registreredes data i et struktureret format ved anmodning
- Bistå med sletning på anmodning, herunder bekræfte at sletning er gennemført
- Bistå den dataansvarlige med anmeldelse af brud på persondatasikkerheden, jf. Bestemmelse 10
- Bistå i forbindelse med udarbejdelse af konsekvensanalyse (DPIA), hvis den dataansvarlige vurderer dette relevant

Bistand ud over almindelig drift kan være tidskrævende. Databehandleren forbeholder sig ret til at fakturere bistand i henhold til den til enhver tid gældende timepris, hvis bstanden går væsentligt ud over, hvad der med rimelighed kan forventes inden for den almindelige drift.

C.4 Opbevaringsperiode / sletterutine

Personoplysninger opbevares hos databehandleren i følgende perioder:

- Produktionsdata: så længe den underliggende aftale er i kraft
- Backup-data: 50 dages rolling retention
- Log-data (audit-trail, administratorhandling): op til 24 måneder
- Sikkerhedslog (fejlede login-forsøg, WAF-events): op til 6 måneder
- Support-tickets og fejllogs: op til 12 måneder efter sagens lukning

Ved ophør af tjenesten skal databehandleren slette alle personoplysninger inden for 30 dage, jf. Bestemmelse 11. Backup-data slettes i takt med den almindelige backup-rotation, dog senest 90 dage efter ophør. Sletning bekræftes skriftligt over for den dataansvarlige.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- Primær produktionsserver: Hetzner, Tyskland (EU)
- CDN/WAF/edge: Cloudflare EU-noder
- Daglig backup-lagring: LIVEN STUDIO SAS, Frankrig (EU)
- Ugentlig backup-lagring og Workspace: Google Ireland Limited, Irland (EU)
- Automation-platform: Make s.r.o. / Celonis SE, Tjekkiet / Tyskland (EU)
- Password management: RoboForm (Siber Systems Inc., USA) — krypteret zero-knowledge-lagring
- Databehandlerens eget administrative miljø: Tjekkiet (EU)

Samtlige lokaliteter — bortset fra RoboForm — er beliggende inden for EU/EØS. For RoboForm gælder, at lagring er zero-knowledge-krypteret, hvilket betyder, at leverandøren teknisk ikke har adgang til indholdet af lagrede credentials. Overførselsgrundlag for RoboForm er EU-Kommissionens Standard Contractual Clauses (SCCs).

C.6 Instruks vedrørende overførsel til tredjelande

Med undtagelse af RoboForm (jf. C.5) instruerer den dataansvarlige ikke databehandleren i at overføre personoplysninger til tredjelande eller internationale organisationer. Enhver eventuel fremtidig overførsel kræver en ny, dokumenteret og skriftlig instruks fra den dataansvarlige samt etablering af et gyldigt overførselsgrundlag efter Databeskyttelsesforordningens kapitel V (f.eks. EU-Kommissionens Standard Contractual Clauses) samt gennemførelse af en transfer impact assessment.

C.7 Procedurer for revision af databehandleren

Den dataansvarlige er berettiget til at gennemføre revision (herunder inspektion) af databehandlerens overholdelse af disse Bestemmelser én gang årligt eller oftere, såfremt særlige forhold giver anledning dertil (eksempelvis brud på persondatasikkerheden).

Revisionen kan gennemføres af den dataansvarlige selv eller af en uafhængig tredjepart udpeget af den dataansvarlige. Databehandleren stiller ved revision alle relevante oplysninger, dokumentation og systemer til rådighed i det omfang, det er nødvendigt for at påvise overholdelse.

Revisionen skal varsles skriftligt minimum 14 dage forud og må ikke unødigt forstyrre databehandlerens drift. Den dataansvarlige afholder egne omkostninger i forbindelse med revisionen; databehandleren afholder egne omkostninger til den nødvendige medvirken. Ved væsentlige konstaterede mangler kan den dataansvarlige dog kræve, at databehandleren afholder rimelige omkostninger til udbedring.

Den dataansvarlige har herudover løbende adgang til at anmode om dokumentation for gennemførte sikkerhedsforanstaltninger, herunder seneste audit-rapport, sletterapporter og backup-tests.

C.8 Procedurer for revision af underdatabehandlere

Databehandleren er forpligtet til årligt at indhente og gennemgå dokumentation for underdatabehandlernes overholdelse af Databeskyttelsesforordningens artikel 28, herunder:

- Senest offentliggjorte revisions-/audit-rapporter (f.eks. ISO 27001, SOC 2, ISAE 3402/3000) hvor tilgængelig
- Underdatabehandlerens gældende privatlivspolitik og sikkerhedspolitik

- Dokumentation for seneste penetrationstest og/eller sårbarhedsscanning hvor tilgængelig

Den dataansvarlige har — hvis det vurderes nødvendigt — ret til at modtage kopi af ovennævnte dokumentation. Den dataansvarlige har endvidere ret til — ved særlige forhold — at gennemføre selvstændig revision (eller lade en tredjepart gennemføre revision) af en underdatabehandler, dog under iagttagelse af eventuelle aftalebegrænsninger hos den pågældende underdatabehandler.



Øvrige forhold

Ansvar, lovvalg, værneting og forrang ved konflikt mellem aftaledokumenter.

Bilag D — Parternes regulering af andre forhold

D.1 Ansvar og erstatning

Parternes indbyrdes ansvar og eventuel erstatning i anledning af brud på denne DPA eller Databeskyttelsesforordningen reguleres af den til enhver tid gældende kommercielle aftale mellem parterne samt gramflows' handelsbetingelser. I det omfang intet andet er aftalt, gælder dansk rets almindelige regler om erstatning.

D.2 Lovvalg og værneting

Denne DPA er underlagt dansk ret for så vidt angår databeskyttelsesretlige forhold, da behandlingen i overvejende grad vedrører registrerede personer i Danmark.

Eventuelle tvister, som måtte udspringe af denne aftale, og som ikke kan løses i mindelighed, afgøres ved den dataansvarliges hjemting. For danske kunder vil dette typisk være Københavns Byret som første instans. Databehandleren kan dog vælge at anlægge sag ved databehandlerens eget hjemting i Prag, Tjekkiet.

D.3 Tilsynsmyndighed og Lead Supervisory Authority

I overensstemmelse med GDPR artikel 56 og betragtning 36 gælder følgende vedrørende kompetent tilsynsmyndighed:

- For tilsynssager der vedrører den dataansvarliges behandling af personoplysninger (herunder behandlingen gennem databehandleren) er den dataansvarliges primære tilsynsmyndighed kompetent som Lead Supervisory Authority. For danske kunder er dette typisk Datatilsynet (datatilsynet.dk). ÚOOÚ (Tjekkiet) deltager som concerned supervisory authority.
- For tilsynssager der udelukkende vedrører databehandlerens egne aktiviteter (uafhængigt af kundeforholdet) er ÚOOÚ (Úřad pro ochranu osobních údajů, uoou.cz) kompetent som primær tilsynsmyndighed.
- Databehandleren råder over sproglige og administrative ressourcer til at håndtere kommunikation med både Datatilsynet (dansk) og ÚOOÚ (tjekkisk/engelsk) og bistår den dataansvarlige med relevant kommunikation, jf. Bilag C.3.

D.4 Ændringer til aftalen

Ændringer eller tilføjelser til denne DPA udsendes som ny version af det centrale standarddokument på gramflows.com/dpa med mindst 30 dages skriftligt varsel til kundens registrerede primære kontaktperson. Hvis den dataansvarlige gør indsigelse mod en planlagt ændring, kan den dataansvarlige opsige den underliggende kommercielle aftale med det varsel, der er angivet i denne aftale eller i gramflows' handelsbetingelser.

D.5 Forrang

Ved uoverensstemmelse mellem denne DPA og de kommercielle aftaler mellem parterne har denne DPA forrang for så vidt angår spørgsmål om databeskyttelse. Kommercielle vilkår reguleres af den underliggende aftale samt gramflows' handelsbetingelser.

D.6 Ugyldighed (severability)

Hvis en eller flere bestemmelser i denne DPA erklæres ugyldige af en kompetent domstol eller tilsynsmyndighed, påvirker dette ikke gyldigheden af de øvrige bestemmelser. Parterne skal i så fald i fællesskab erstatte den ugyldige bestemmelse med en gyldig bestemmelse, der så vidt muligt afspejler den oprindelige hensigt.

Versionshistorik

Version	Dato	Ændringer
v2026.1.2	1. august 2026	Opdateret ikrafttrædelsesdato (gyldig fra 1. august 2026). Komprimeret sidefod, så versionsreference og sidetal står på én linje på alle sider. Redaktionel ensretning af virksomhedsnavnet "gramflows" (skrives gennemgående med småt). Ingen materielle ændringer i databeskyttelsesbestemmelserne.
v2026.1.1	14. maj 2026	Præciseret værneting (asymmetrisk: kundens hjemting / databehandlerens hjemting i Prag). Tilføjet selvstændigt afsnit D.3 om Lead Supervisory Authority jf. GDPR art. 56. Tilføjet erklæring om sprogkapacitet til kommunikation med både Datatilsynet og ÚOOÚ.
v2026.1	14. maj 2026	Første offentlige version af gramflows' generelle standard-DPA. Erstatte alle tidligere kundespecifikke DPA'er.

Bemærkning

Dette dokument er udarbejdet på baggrund af Datatilsynets standardkontraktbestemmelser (marts 2024) og tilpasset gramflows' ydelser samt cross-border-konfigurationen (tjekkisk databehandler, primært danske kunder). DPA'en bygger på Datatilsynets standardskabelon, der er EDPB-godkendt og anvendelig i hele EU. Dokumentet er klar til brug, men bør gennemgås regelmæssigt for at sikre overensstemmelse med eventuelle ændringer i Datatilsynets standardskabelon, EDPB-vejledninger eller tjekkisk databeskyttelseslovgivning.

DATABASEHANDLER

gramflows

VAT: CZ7309231259

Belehradská 858/23, 120 00 Prag, Tjekkiet

Kontakt: support@gramflows.com

DPA-spørgsmål: dg@gramflows.com

Tlf: +45 88 70 70 57

Web: gramflows.com · DPA: gramflows.com/dpa

Åbningstider: Mandag-torsdag 9-17 · Fredag 9-15