Databehandleraftale

Changelog

Version	Ændring
1.0 (18/12-2025)	Oprettelse af første udgave
1.1 (19/12-2025)	Mindre justeringer til opstilling
1.2 (05/08 -2026)	- Tilføjelse til Bilag: A.1, A.2 og C.1, ang. indledende discovery / scoping forløb. - Generel formattering

Standardkontraktbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Navn	_____	**Navn**	ankon ApS
CVR	_____	**CVR**	46116550
Adresse	_____	**Adresse**	Spidstoftvej 4
Postnummer	_____	**Postnummer**	8800
By	_____	**By**	Viborg
Land	_____	**Land**	Denmark
"Dataansvarlige"		**"Databehandleren"**	

herefter "databehandleren" der hver især er en "part" og sammen udgør "parterne"

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

Indhold

1. Præambel

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

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).

3. I forbindelse med leveringen af Shopify udviklings- og konsulentydelser 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.

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.

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

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.

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

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

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

2. Den dataansvarliges rettigheder og forpligtelser

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[1] nationale ret 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.

3. 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. 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.

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.

4. 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.

[1] Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

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

5. 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 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.

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.

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.

6. 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 (en underdatabehandler).

2. Databehandleren må således 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 underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 7 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.

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.

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.

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.

7. Overførsel til tredjelande eller internationale organisationer

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 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

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.

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.

8. 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 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

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.

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.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig 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 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.

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.

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.

10. Sletning og returnering af oplysninger

1. Ved ophør af samarbejdet mellem parterne 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. Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som eventuelle opbevaringsregler foreskriver.

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

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.

12. 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.

13. Ikrafttræden og ophør

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

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

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.

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.

5. Underskrift

På vegne af den dataansvarlige		**På vegne af databehandleren**	
Navn		**Navn**	Carsten Andersen
Stilling		**Stilling**	Co-founder
Telefon		**Telefon**	31762324
Email		**Email**	carsten@ankon.dk
			
Underskrift		**Underskrift**	

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

På vegne af den dataansvarlige		**På vegne af databehandleren**	
Navn	_____	**Navn**	Carsten Andersen
Stilling	_____	**Stilling**	Co-founder
Telefon	_____	**Telefon**	31762324
Email	_____	**Email**	carsten@ankon.dk

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Levering af Shopify-relaterede ydelser til den dataansvarlige. Dette omfatter, afhængigt af det konkret aftalte omfang, alt fra indledende gennemgang, rådgivning, discovery og analyse (f.eks. forud for en business case / scope af større projekt) til udvikling, tilpasning, vedligeholdelse og løbende teknisk support af Shopify themes, apps og UI extensions.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Adgang til og arbejde i kundens Shopify Admin samt eventuelle relaterede platforme nødvendigt for udførelse af udviklingsopgaver eller indledende discovery og scoping. Behandling sker primært gennem webbaserede interfaces.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Navn, e-mailadresse, leveringsadresse, faktureringsadresse, telefonnummer, ordredata, IP-adresser og andre oplysninger som normalt behandles i en e-handelsplatform.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kundens slutbrugere/kunder samt eventuelt kundens medarbejdere.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Fra opstart af det første aftalte forløb mellem parterne - uanset om dette er et indledende gennemgangsforløb eller et udviklingssamarbejde, og så længe samarbejdet varer i en eller anden form, og indtil 30 dage efter kundeforholdets ophør.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

Navn	CVR	Adresse	Beskrivelse af behandling
Shopify Inc.	N/A	151 O'Connor Street, Ottawa, ON Canada	E-handelsplatform
GitHub, Inc.	N/A	88 Colin P Kelly Jr St, San Francisco, USA	Versionskontrol af kildekode
n8n GmbH	N/A	Bülowstraße 66, 10783 Berlin, Tyskland	Workflow automation platform

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

7 dages varsel som angivet i hovedaftalen.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører den opgave, der er nærmere beskrevet i Bilag A.1 og A.2.

Databehandleren må alene tilgå og behandle personoplysninger i det omfang, det er nødvendigt for at udføre den konkret aftalte opgave, jf. Bilag A - uanset om opgaven på det pågældende tidspunkt angår indledende gennemgang og rådgivning eller udvikling, tilpasning og drift af kundens Shopify-løsning.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter almindelige personoplysninger som typisk behandles i forbindelse med e-handelsplatforme, herunder navne, kontaktoplysninger, adresser og ordredata. Behandlingen omfatter ikke særlige kategorier af personoplysninger som defineret i databeskyttelsesforordningens artikel 9. Der skal etableres et sikkerhedsniveau svarende til almindelig god praksis for webudvikling og teknisk konsulentvirksomhed.

Databehandleren er herefter 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 skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Pseudonymisering og kryptering af personoplysninger:

Alle passwords og adgangskoder opbevares i password manager med stærk kryptering. Testdata pseudonymiseres hvor muligt, således at produktionsdata ikke anvendes i udviklingsmiljøer.

Evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester:

To-faktor-autentificering (2FA) aktiveres på alle logins til Shopify Admin og andre platforme med adgang til personoplysninger. Adgang tildeles kun til medarbejdere med konkret arbejdsmæssigt behov. Adgangstilladelser gennemgås løbende og fjernes ved projektafslutning eller når de ikke længere er nødvendige.

Evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse: Databehandleren anvender Shopifys standardbackup-procedurer for al data i Shopify-platformen. Kildekode versioneres i GitHub med automatisk backup. Ved tab af adgang kan logins genskabes gennem kundens administrator-adgang.

Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden:
Sikkerhedsforanstaltninger gennemgås kvartalsvis af databehandlerens ledelse. Medarbejdere instrueres i korrekt håndtering af adgangskoder og fortrolige data ved onboarding og løbende efter behov.

Adgang til oplysningerne via internettet:
Al adgang til personoplysninger sker via krypterede HTTPS/TLS-forbindelser. Databehandleren anvender kun officielle webinterfaces fra Shopify og andre godkendte platforme.

Beskyttelse af oplysninger under transmission:
Al datatransmission mellem databehandlerens systemer og Shopify samt andre platforme sker via krypterede forbindelser (HTTPS/TLS 1.2 eller nyere). E-mails med følsomme oplysninger sendes ikke uden kryptering eller password-beskyttelse.

Beskyttelse af oplysninger under opbevaring:
Alle arbejdsstationer anvendt til behandling af personoplysninger er sikret med adgangskode og disk encryption (FileVault, BitLocker eller tilsvarende). Lokale kopier af data med personoplysninger opbevares kun så længe det er nødvendigt for opgaveløsningen og slettes derefter.

Fysisk sikring af lokaliteter, hvor der behandles oplysninger:
Databehandlerens kontorfaciliteter er sikret med adgangskontrol. Arbejdsstationer låses når de forlades. Skærme placeres således at uvedkommende ikke kan aflæse personoplysninger.

Anvendelse af hjemme-/fjernarbejdspladser: Medarbejdere må arbejde fra hjemmearbejdspladser under samme sikkerhedskrav som på kontoret. Dette indebærer brug af sikrede internetforbindelser, låsning af arbejdsstationer ved fravær, og at uvedkommende ikke får adgang til personoplysninger.

Logning: Databehandleren fører register over hvilke medarbejdere der har adgang til hvilke systemer indeholdende personoplysninger. Shopify og andre platforme logger automatisk adgang og aktiviteter, hvilke logs er tilgængelige for den dataansvarlige gennem platformenes standard-logningsfunktioner.

C.3 Bistand til den dataansvarlige

Databehandleren bistår den dataansvarlige med at besvare henvendelser fra registrerede ved at videregive relevante henvendelser og tilvejebringe nødvendig teknisk information inden for 5 arbejdsdage.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger slettes senest 30 dage efter projektafslutning eller ophør af samarbejde. Dette omfatter:

- Sletning af logins til kundens systemer
- Sletning af lokale kopier af data
- Sletning af testdata indeholdende personoplysninger

C.5 Lokalitet for behandling

Behandling finder sted fra databehandlerens arbejdsstationer i Danmark samt via cloud-baserede udviklingsværktøjer (Shopify Admin, GitHub etc.). Behandling sker ikke fra tredjelande uden forudgående godkendelse.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren må ikke overføre personoplysninger til tredjelande uden den dataansvarliges forudgående skriftlige godkendelse. Brug af Shopify-platformen (som er hostet globalt) er godkendt, idet Shopify overholder GDPR gennem standardkontraktbestemmelser.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige kan med 14 dages varsel gennemføre revision af databehandlerens behandling af personoplysninger. Revision kan ske ved:

- Besvarelse af skriftlige spørgsmål om sikkerhedsprocedurer
- Udlevering af dokumentation for sikkerhedsforanstaltninger
- Fysisk inspektion af arbejdspladser efter aftale

Omkostninger til revision afholdes af den dataansvarlige.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren anvender udelukkende anerkendte, etablerede platforme som Shopify og GitHub, der er industristandard inden for henholdsvis e-handel og softwareudvikling.

Disse platforme har offentligt dokumenteret GDPR-compliance, herunder:

- Data Processing Agreements (DPA)
- Certificeringer (ISO 27001, SOC 2 Type II eller tilsvarende)

- Standardkontraktbestemmelser for dataoverførsler

Databehandleren kan på anmodning udlevere links til underdatabehandleres compliance-dokumentation.
Databehandleren gennemfører ikke fysiske inspektioner hos underdatabehandlere, da dette ikke er praktisk muligt hos globale cloud-platforme. Valget af disse platforme er baseret på deres status som industristandard og dokumenterede sikkerhedsniveau.
Hvis den dataansvarlige ikke accepterer brug af disse specifikke platforme, skal dette meddeles inden projektstart.

Bilag D Parternes regulering af andre forhold

Ingen yderligere bestemmelser.