Databehandleraftale

Databehandleraftale efter artikel 28, stk. 3, i forordning (EU) 2016/679 (databeskyttelsesforordningen). Bygger på Datatilsynets skabelon.

Version 1.5, gældende fra 12. november 2026 · contact@justparity.com

Version 1.5 gælder for aftaler, der indgås fra 12. november 2026. For aftaler, der er indgået før, gælder den først, når den dataansvarlige har accepteret den skriftligt, jf. afsnit 14. Indtil da gælder den aftalte version. Version 1.3 og senere kan hentes som PDF på /data-processing-agreement/versioner.

1. Parterne

Databehandler

Just Parity ApS
CVR: 46363906, Vesterbrogade 208, 1800 Frederiksberg C

Kontakt: contact@justparity.com

Dataansvarlig

Kunden
Som defineret i serviceaftalen med Justparity

Der hver især er en "part" og sammen udgør "parterne". Nærværende bestemmelser ("Bestemmelserne") udgør en integreret del af serviceaftalen mellem parterne. Bestemmelserne bygger på Datatilsynets skabelon til databehandleraftaler, men er tilpasset Justparity-platformen og er derfor ikke standardkontraktbestemmelser efter databeskyttelsesforordningens artikel 28, stk. 8.

2. Præambel

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

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).

I forbindelse med leveringen af Justparity compliance-platformen behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

- Bilag A: Oplysninger om behandlingen (formål, datakategorier, registrerede, varighed)
- Bilag B: Underdatabehandlere (godkendte underdatabehandlere og betingelser)
- Bilag C: Instruks vedrørende behandling (sikkerhedsforanstaltninger, lokalitet, overførsler, revisioner)
- Bilag D: Parternes regulering af andre forhold

> **Vedrørende køn og særlige kategorier af personoplysninger**
>
> Justparity behandler lønoplysninger fordelt på køn til lønforskelsanalyse med ligelønsloven og løntransparensdirektivet 2023/970 som retlig forpligtelse. Køn indgår ikke i den udtømmende opregning i artikel 9, stk. 1, og er derfor en almindelig personoplysning med behandlingsgrundlag i artikel 6, stk. 1, litra c. Behandlingen kan derudover omfatte oplysninger om fagforeningsmedlemskab via lønindberetninger, som er en særlig kategori efter artikel 9. Den dataansvarlige hæfter for, at behandlingsgrundlaget for fagforeningsmedlemskab foreligger, typisk artikel 9, stk. 2, litra b, jf. databeskyttelsesloven § 7, stk. 2, og § 12.

3. Den dataansvarliges rettigheder og forpligtelser

Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller dansk ret samt disse Bestemmelser.

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

Den dataansvarlige er ansvarlig for at sikre, at der er et behandlingsgrundlag for den behandling 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 dansk 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. Instruksen er specificeret i bilag A og C. Efterfølgende instruks kan gives, mens der sker behandling, men instruksen skal altid være dokumenteret og opbevares skriftligt.

4.2 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens vurdering er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller dansk ret. Databehandleren er ikke forpligtet til at efterkomme en instruks, der vil medføre overtrædelse af gældende ret.

4.3 Den dataansvarliges aktivering af en lønsystemintegration eller upload af en fil via Justparity-platformen udgør en dokumenteret instruks til databehandleren om at modtage og behandle de personoplysninger af de typer, der står i bilag A.3, som lønsystemet overfører, eller som filen indeholder. Den dataansvarlige er ansvarlig for at sikre, at overførslen har et lovligt grundlag.

5. Fortrolighed

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 med adgang gennemgås løbende. Adgangen lukkes, hvis den ikke længere er nødvendig. Fortrolighedsforpligtelsen gælder også efter Bestemmelsernes ophør.

6. Behandlingssikkerhed (artikel 32)

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 databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Behandlingen omfatter lønoplysninger og kønsdata. Fagforeningsmedlemskab, som er en særlig kategori efter artikel 9, kan desuden forekomme. Der skal derfor etableres et højt sikkerhedsniveau.

Databehandleren gennemfører som minimum følgende foranstaltninger, jf. bilag C:

- **Kryptering:** TLS 1.2 eller nyere for data under transport, AES-256 for data i hvile, krypterede databaseforbindelser og backup
- **Adgangskontrol:** Rollebaseret adgang (RBAC) med least-privilege-princippet, unikke brugerkonti, login med personlig adgangskode og en bremse på gentagne mislykkede loginforsøg, automatisk sessionstimeout. Er den dataansvarliges virksomhed i onboardingen, skal ejere, administratorer og andre med en rolle i onboardingen også bekræfte deres login med en kode fra en autentificeringsapp (totrinslogin). For øvrige brugere er totrinslogin ikke slået til på platformen i dag
- **Dataisolering:** Multi-tenant Row Level Security (RLS). Kundedata er logisk adskilt via Row-Level Security, så en kundes data er beskyttet mod adgang fra andre kunder
- **Logning og overvågning:** Visning af den enkelte medarbejders løn og følsomme felter, eksport og download logges i platformens revisionsspor med bruger og tidspunkt. Handlinger fra databehandlerens administratorer i platformen logges separat. Databehandlerens direkte adgang til databasen sker kun til drift og fejlretning og er begrænset til navngivne personer
- **Sårbarhedshåndtering:** Løbende sårbarhedsscanning, kritiske sikkerhedspatches implementeres hurtigst muligt og inden for risikobaserede frister i incident response-proceduren. Ekstern penetrationstest er under forberedelse og gennemføres derefter mindst hvert andet år
- **Backup og genopretning:** Daglig automatisk backup, krypteret og opbevaret i samme EU-region som databasen. Gendannelse er mulig mindst 7 dage tilbage. Point-in-time recovery, der tillader gendannelse til et vilkårligt tidspunkt i perioden, er aktiveret på den produktionsdatabase, der indeholder den dataansvarliges personoplysninger, fra det tidspunkt hvor data indlæses. Formelle RTO- og RPO-mål er ikke fastsat
- **Incident response:** Dokumenteret procedure for håndtering af sikkerhedshændelser, klassificering efter alvor, eskalering og underretning jf. afsnit 10
- **Personale:** Alle medarbejdere med adgang til personoplysninger har underskrevet fortrolighedserklæring og modtager periodisk sikkerhedstræning

Databehandleren kan opdatere foranstaltningerne i dette afsnit, når teknikken udvikler sig, forudsat at det samlede sikkerhedsniveau ikke forringes, og giver den dataansvarlige skriftlig besked om opdateringen. Databehandleren reducerer ikke sikkerhedsniveauet uden den dataansvarliges forudgående skriftlige accept.

7. Anvendelse af underdatabehandlere

7.1 Databehandleren har den dataansvarliges generelle godkendelse til brug af de underdatabehandlere, der fremgår af bilag B. Databehandleren sikrer, at der indgås skriftlig aftale med enhver underdatabehandler, som pålægger denne de samme databeskyttelsesforpligtelser som fastsat i disse Bestemmelser.

7.2 Databehandleren underretter skriftligt den dataansvarlige om planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og giver derved den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

7.3 Den dataansvarlige kan gøre begrundet indsigelse mod en ny underdatabehandler inden for 14 dage efter modtagelse af underretningen. Databehandleren vil i rimelig udstrækning forsøge at finde en alternativ løsning. Kan parterne ikke nå til enighed, kan den dataansvarlige opsige serviceaftalen helt eller delvist med virkning fra den dato, hvor den nye underdatabehandler skulle have været taget i brug. Forudbetalt vederlag for den resterende periode refunderes.

7.4 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 efter databeskyttelsesforordningen, herunder artikel 79 og 82.

8. Overførsel til tredjelande eller internationale organisationer

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

Databasen med den dataansvarliges personoplysninger og alle sikkerhedskopier ligger i EU (AWS eu-central-1, Frankfurt, Tyskland), jf. afsnit 6 og bilag B. Oplysninger kan behandles i USA i disse tilfælde: mails fra platformen sendes via Google, Netlifys CDN kan levere sider fra en kant uden for EU, og de amerikanske underdatabehandlere i bilag B kan have adgang fra USA som led i drift og support. For hver underdatabehandler står lokaliteten og overførselsgrundlaget i bilag B: EU-US Data Privacy Framework (artikel 45), hvor udbyderens certificering omfatter HR-data, og ellers EU-standardkontraktbestemmelser (SCC) efter artikel 46, stk. 2, litra c.

Kræver EU-ret eller dansk ret, som databehandleren er underlagt, en overførsel, som databehandleren ikke er instrueret i, underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Den dataansvarliges instruks vedrørende overførsel af personoplysninger til tredjelande, herunder overførselsgrundlaget, er angivet i bilag C. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i kapitel V.

9. Bistand til den dataansvarlige

9.1 Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III. Dette indebærer bistand vedrørende:

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

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

9.2 Databehandleren bistår endvidere den dataansvarlige med:

a. anmeldelse af brud på persondatasikkerheden til Datatilsynet, jf. artikel 33

b. underretning af registrerede om brud, jf. artikel 34

c. konsekvensanalyser vedrørende databeskyttelse (DPIA), jf. artikel 35, ved at stille al nødvendig teknisk information til rådighed om platformens behandlingsaktiviteter, sikkerhedsforanstaltninger og dataflows

d. forudgående høring af Datatilsynet, jf. artikel 36

e. den dataansvarliges forpligtelse efter artikel 32, ved at stille oplysninger om de tekniske og organisatoriske foranstaltninger i afsnit 6 og bilag C og anden information, der er nødvendig for den dataansvarliges overholdelse af artikel 32, til rådighed

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. Underretningen sker senest 24 timer efter, at databehandleren er blevet bekendt med bruddet, så den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet til Datatilsynet inden for 72 timer, jf. artikel 33.

10.2 Underretningen skal indeholde følgende oplysninger (jf. artikel 33, stk. 3):

- karakteren af bruddet, herunder kategorierne og det omtrentlige antal berørte registrerede
- kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- de sandsynlige konsekvenser af bruddet
- de foranstaltninger der er truffet eller foreslås for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger
- kontaktoplysninger til databehandlerens kontaktperson

11. Sletning og returnering af oplysninger

11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger sletter eller tilbageleverer databehandleren efter den dataansvarliges valg alle personoplysninger. Ved tilbagelevering sker det i et struktureret, almindeligt anvendt og maskinlæsbart format (CSV eller JSON). Tilbageleveringen omfatter alle personoplysninger og det indhold, den dataansvarlige har oprettet på platformen: medarbejdere, løndele, jobarkitektur, lønbånd, kriterier, begrundelser, lønspørgsmål og svar, rapporter og aktivitetslog. Filer, som den dataansvarlige selv har lagt op som dokumentation, udleveres på anmodning. Sletning af eksisterende kopier i driftsmiljøet sker senest 30 dage efter ophør, medmindre EU-retten eller dansk ret, som databehandleren er underlagt, foreskriver opbevaring af personoplysningerne. Har den dataansvarlige bedt om tilbagelevering efter handelsbetingelsernes punkt 7.3, løber fristen fra udleveringen. Har den dataansvarlige bedt om at skifte udbyder efter handelsbetingelsernes punkt 7.4, løber fristen fra udløbet af den periode, hvor data kan hentes.

11.1 a Personoplysninger i systembackups slettes ikke enkeltvis, men udgår af backupsættene efter den fastsatte backupperiode, jf. afsnit 6. Indtil da er data isoleret fra driftsmiljøet og genskabes ikke, medmindre det er nødvendigt af hensyn til genopretning efter et driftsnedbrud.

11.2 Databehandleren bekræfter skriftligt over for den dataansvarlige, at sletning er gennemført, herunder hos alle underdatabehandlere.

11.3 Databehandleren opbevarer ikke personoplysninger om den dataansvarliges medarbejdere, der behandles efter disse Bestemmelser, ud over fristen i 11.1 og backupperioden i 11.1 a. Bogføringsloven gælder kun databehandlerens eget regnskabsmateriale om den dataansvarlige som kunde, fx fakturaer, og det er ikke omfattet af disse Bestemmelser. Opbevaring efter skatte- og arbejdsretlig lovgivning er den dataansvarliges egen forpligtelse. Bliver databehandleren underlagt et krav om at opbevare personoplysninger, der behandles efter disse Bestemmelser, underretter databehandleren straks den dataansvarlige og behandler alene oplysningerne til det formål og i den periode, kravet 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 Den dataansvarlige kan foretage en ordinær revision en gang om året med mindst 30 dages forudgående varsel. Revisionen kan udføres af en uafhængig tredjepart efter gensidig aftale. Databehandleren kan supplere med en uafhængig revisionsrapport som dokumentation for overholdelse. Dette begrænser ikke den dataansvarliges ret til at foretage inspektion. Hver part bærer egne omkostninger ved en ordinær revision.

12.3 Ved begrundet mistanke om overtrædelse eller efter et sikkerhedsbrud kan den dataansvarlige foretage ekstraordinær revision med rimeligt varsel.

12.4 Databehandleren er forpligtet til at give Datatilsynet, som efter gældende lovgivning har adgang til den dataansvarliges eller databehandlerens faciliteter, adgang til databehandlerens faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

13.1 Databehandlerens samlede erstatningsansvar under disse Bestemmelser er begrænset til det beløb, den dataansvarlige har betalt i abonnement i de 12 måneder forud for den hændelse, der giver anledning til kravet. Begrænsningen gælder ikke for a) tab, der skyldes forsæt eller grov uagtsomhed hos databehandleren eller hos nogen, databehandleren bruger til at opfylde Bestemmelserne, herunder dennes ansatte og underdatabehandlere, b) skade på liv, legeme eller helbred, og c) ansvar, som ikke kan begrænses ved aftale efter ufravigelige regler i den lov, der gælder for Bestemmelserne, eller efter regler, der gælder uanset lovvalget. Begrænsningen gælder kun mellem parterne og begrænser ikke de registreredes rettigheder efter databeskyttelsesforordningen, herunder retten til erstatning efter artikel 82.

13.2 Disse Bestemmelser er underlagt dansk ret. Tvister afgøres ved de danske domstole med Retten på Frederiksberg som værneting i første instans.

14. Ikrafttræden og ophør

Bestemmelserne træder i kraft ved indgåelse af serviceaftalen. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder giver anledning hertil.

En ny version af Bestemmelserne gælder først for den dataansvarlige, når den er aftalt skriftligt. Indtil da gælder den version, der står i serviceaftalen. Står der ingen, eller en version, der ikke står på versionssiden, gælder den version, der var gældende på datoen for serviceaftalens indgåelse. Ændringer i bilag B følger afsnit 7.2-7.3, og opdateringer af foranstaltningerne i afsnit 6, der ikke forringer sikkerhedsniveauet, følger afsnit 6, sidste afsnit. Den dataansvarlige, der har indgået aftale på en tidligere version, får en skriftlig oversigt over ændringerne. Den tidligere version gælder, til den nye er aftalt.

Bestemmelserne er gældende, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige. Ved ophør finder bestemmelserne om fortrolighed (afsnit 5) og sletning (afsnit 11) fortsat anvendelse.

15. Kontaktpersoner

Parternes kontaktpersoner for spørgsmål vedrørende disse Bestemmelser og for underretning om brud på persondatasikkerheden er:

Databehandler (Just Parity ApS)
Generelle henvendelser:
contact@justparity.com
Brud på persondatasikkerheden:
security@justparity.com

Dataansvarlig (kunden)
Udfyldes ved indgåelse af aftalen:
Kontaktperson: _____
Databeskyttelsesrådgiver (DPO), hvis relevant: _____
E-mail: _____

Bilag

Bilag A: Oplysninger om behandlingen

A.1 Formål	Levering af Justparity compliance-platform til EU's løntransparensdirektiv (direktiv (EU) 2023/970), herunder jobarkitektur, lønrammer, lønforskelsanalyse, rapportering til myndigheder, håndtering af medarbejderforespørgsler og revisionsspor
A.2 Behandlingens karakter	Indsamling via integration med lønsystemer og via filer (CSV og Excel), som den dataansvarlige selv lægger op, modtagelse af filer, som den dataansvarlige lægger op som dokumentation, strukturering og kategorisering, statistisk analyse og beregning, rapportgenerering, visning i webapplikation, opbevaring i krypteret database, sletning ved ophør eller instruks
A.3 Personoplysninger	**Almindelige:** Navn, medarbejder-ID, fødselsdato, stilling, jobniveau, jobkategori, afdeling, ansættelsesdato, fratrædelsesdato, ansættelsesform, arbejdstid, overenskomst, løngruppe og løntrin, basisløn, tillæg, bonus, pension, benefits, lønhistorik, nærmeste leder, DISCO-kode, ferieret, orlovsperioder, målopfyldelse, lønspørgsmål og svar, e-mail, telefonnummer, adresse (hvis lønsystemet eller filen leverer den), aktivitetslog og, ved login og ved handlinger, der skal kunne dokumenteres bagefter (fx underskrift, godkendelse, svar via link og import af filer), IP-adresse og browser. Desuden andre oplysninger om ansættelses- og lønforhold af samme art, som lønsystemet overfører, eller som den dataansvarlige selv lægger ind på platformen, herunder i fritekstfelter og filer. CPR- og kontonumre er ikke omfattet af denne sætning, men af punkterne nedenfor. Andre særlige kategorier af personoplysninger end fagforeningsmedlemskab og oplysninger om strafbare forhold er ikke omfattet, og den dataansvarlige må ikke lægge dem ind på platformen **Køn:** Behandles til beregning af lønforskel. Køn indgår ikke i den udtømmende opregning i art. 9, stk. 1, og er derfor en almindelig personoplysning med behandlingsgrundlag i art. 6, stk. 1, litra c, jf. ligelønsloven og direktiv 2023/970; den dataansvarlige hæfter for grundlaget. Oplysningen behandles med de samme

	skærpede foranstaltninger som særlige kategorier, jf. afsnit 6. **Særlige kategorier (art. 9):** Fagforeningsmedlemskab kan forekomme indirekte i importerede løndatasæt (behandlingsgrundlag: art. 9, stk. 2, litra b, jf. databeskyttelsesloven § 7, stk. 2, og § 12). **CPR-numre:** Kan modtages transient fra tilknyttede lønsystemer og anvendes udelukkende til teknisk udledning af køn (sidste ciffer). CPR-nummeret lagres ikke. En fil, som den dataansvarlige selv lægger op, kan indeholde CPR- eller kontonumre. En kolonne, der er navngivet som CPR- eller kontonummer, kortlægges og læses ikke, og for danske virksomheder gemmes et medarbejdernummer med form som et dansk CPR-nummer ikke. Den dataansvarlige skal fjerne CPR- og kontonumre fra filen, før den lægges op. Den dataansvarlige er ansvarlig for, at behandlingen af personnumre, herunder udledning af køn, har hjemmel i databeskyttelseslovens § 11, stk. 2. **Kontonumre:** Kan følge med fra lønsystemet eller i en fil. En kolonne, der er navngivet som kontonummer eller IBAN, kortlægges og læses ikke. Kontonumre bruges ikke til noget formål. Den dataansvarlige skal fjerne dem fra filen, før den lægges op. **Dokumentation:** Filer, som den dataansvarlige selv lægger op som dokumentation, fx bilag til en lønbeslutning, kan indeholde personoplysninger af de typer, der står ovenfor.
A.4 Registrerede	Nuværende og tidligere medarbejdere hos den dataansvarlige samt platformbrugere (HR-medarbejdere, ledere)
A.5 Varighed	Behandlingen pågår, så længe serviceaftalen er gældende. Sletning i driftsmiljøet efter afsnit 11.1. Kopier i systembackups udgår efter backupperioden, jf. afsnit 11.1 a.

Bilag B: Underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere. Ændringer varsles mindst 30 dage før ikrafttrædelse, jf. afsnit 7.2.

Juridisk enhed	Land	Data-lokation	Behandlingsaktivitet	Overførselsgrundlag
Supabase Inc.	USA	EU (AWS eu-central-1, Frankfurt)	Cloud hosting, database, autentificering. Kerne: alle persondata inkl. køn og evt. art. 9 samt transient CPR	SCC (art. 46, stk. 2, litra c). Ikke DPF-certificeret
Netlify, Inc.	USA	Serverfunktioner og Blobs i EU (AWS eu-central-1, Frankfurt). CDN'et leverer siderne fra den kant, der er tættest på den besøgende, også uden for EU	Hosting, CDN, serverless functions; gemmer Gmail-service-secret i Netlify Blobs	SCC (art. 46, stk. 2, litra c) for oplysninger om den dataansvarliges medarbejdere. Netlifys DPF-certificering omfatter ikke HR-data
Google Ireland Limited (drift: Google LLC, USA)	Irland / USA	EU/US	Transaktionelle e-mails (Gmail DWD)	EU-US DPF (Google LLC) samt SCC
Slack Technologies LLC (Salesforce, Inc.)	USA	EU/US	Interne beskeder til os om henvendelser fra kontakt- og bookingformularen på hjemmesiden. Modtager ikke personoplysninger fra platformen	EU-US DPF (Salesforce) samt SCC
Functional Software, Inc. (Sentry)	USA	Ikke i brug. Kan kun slås til med EU-regionen (de.sentry.io)	Fejlmonitorering. Ikke i brug i dag. Tages den i brug, varsles det efter afsnit 7.2	Ingen overførsel (EU-region)

Rate-limiting sker i platformens egen hukommelse og involverer ingen ekstern udbyder.

Databehandleren har udarbejdet en overførselsvurdering (vurdering af følgerne af dataoverførsler) for Supabase Inc. efter Det Europæiske Databeskyttelsesråds anbefalinger

01/2020. Vurderingen udleveres til den dataansvarlige på anmodning og gennemgås mindst én gang årligt.

Bilag C: Instruks vedrørende behandling af personoplysninger

C.1 Behandlingens genstand

Databehandleren instrueres i at modtage løndata, ansættelsesdata og demografiske data fra den dataansvarliges lønsystem(er) via integration og fra filer (CSV og Excel), som den dataansvarlige lægger op, strukturere disse i jobarkitektur og lønrammer, foretage statistisk analyse af lønforskelle fordelt på køn, generere lovpligtige rapporter og stille data til rådighed for den dataansvarlige via en webbaseret platform.

C.2 Behandlingssikkerhed

Da behandlingen omfatter lønoplysninger, kønsdata og potentielt særlige kategorier af personoplysninger (fagforeningsmedlemskab), skal der etableres et højt sikkerhedsniveau. De konkrete foranstaltninger er beskrevet i afsnit 6.

C.3 Bistand til den dataansvarlige

Databehandleren bistår den dataansvarlige i det omfang og den udstrækning, der fremgår af afsnit 9. Databehandleren stiller teknisk information og dokumentation til rådighed til brug for konsekvensanalyser og forudgående høringer.

C.4 Opbevaringsperiode og sletterutine

Personoplysninger opbevares, så længe serviceaftalen er gældende. Ved ophør slettes eller tilbageleveres data efter afsnit 11.1. Kopier i systembackups udgår efter afsnit 11.1 a.

C.5 Lokalitet for behandling

Databasen med den dataansvarliges personoplysninger og alle sikkerhedskopier ligger i EU (AWS eu-central-1, Frankfurt, Tyskland), jf. afsnit 6 og bilag B. Oplysninger kan behandles i USA i disse tilfælde: mails fra platformen sendes via Google, Netlifys CDN kan levere sider fra en kant uden for EU, og de amerikanske underdatabehandlere i bilag B kan have adgang fra USA som led i drift og support. Behandling kan ikke uden den dataansvarliges forudgående skriftlige godkendelse finde sted på andre lokaliteter end dem, der står i bilag B.

C.6 Instruks vedrørende overførsel til tredjelande

Den dataansvarlige instruerer databehandleren i, at databasen med personoplysningerne og alle sikkerhedskopier ligger i EU (AWS eu-central-1, Frankfurt, Tyskland). Oplysninger må kun behandles i USA i de tilfælde, der står i afsnit 8 og C.5. Overførsel til tredjelande må kun ske til de underdatabehandlere og på det grundlag, der står i bilag B: EU-US Data Privacy Framework (artikel 45), hvor udbyderens certificering omfatter HR-data, og ellers EU-standardkontraktbestemmelser (SCC) efter artikel 46, stk. 2, litra c.

C.7 Procedurer for revision af databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige kan foretage en årlig revision med 30 dages varsel, jf. afsnit 12. Databehandleren kan stille en uafhængig revisionsrapport til rådighed som alternativ. Ekstraordinær revision kan foretages ved begrundet mistanke eller efter sikkerhedsbrud.

C.8 Procedurer for revision af underdatabehandlere

Databehandleren foretager løbende tilsyn med underdatabehandlerne og sikrer, at disse overholder databeskyttelsesforordningen og disse Bestemmelser. Den dataansvarlige kan anmode om dokumentation for underdatabehandlernes overholdelse.

Bilag D: Parternes regulering af andre forhold

D.1 Tredjepartsintegrationer

Justparity integrerer med eksterne lønsystemer via API (herunder Zenegy, Planday, Xena m.fl.). Aktivering af en integration udgør en dokumenteret instruks, jf. afsnit 4.3. Det samme gælder den dataansvarliges upload af en fil. Den dataansvarlige er ansvarlig for at sikre lovligt behandlingsgrundlag for overførslen fra lønsystemet til Justparity.