

Databehandleraftale Coding Pirates Denmark Medlemssystem Standardkontraktbestemmelser

Denne aftale er lavet i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelses- forordningen) med henblik på databehandlerens behandling af personoplysninger.

Aftalen indgås mellem

Forening

Adresse

Postnummer og by

CVR

E-mail

herefter "den dataansvarlige"

og

Coding Pirates Denmark
c/o Coworking Plus
Kochsgade 31D
5000 Odense C
Danmark
CVR 35552316

herefter "databehandleren"

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

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

1. Indhold

2. Præambel.....	3
3. Den dataansvarliges rettigheder og forpligtelser.....	3
4. Databehandleren handler efter instruks.....	4
5. Fortrolighed.....	4
6. Behandlingssikkerhed.....	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer.....	6
9. Bistand til den dataansvarlige.....	6
10. Underretning om brud på persondatasikkerheden.....	7
11. Anonymisering og returnering af oplysninger.....	8
12. Revision, herunder inspektion.....	8
13. Parternes aftale om andre forhold.....	8
14. Ikrafttræden og ophør.....	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren.....	10
Bilag A Oplysninger om behandlingen.....	11
Bilag B Underdatabehandlere.....	13
Bilag C Instruks vedrørende behandling af personoplysninger.....	14

2. 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 Coding Pirates Medlemssystem behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Der gøres opmærksom på, at Coding Pirates Denmark gælder som dataansvarlig og databehandler, da Coding Pirates Denmark har adgang og brugsret til alle data i Coding Pirates Medlemssystem.
5. Der gøres opmærksom på, at alle lokalforeninger, som en person har en relation til, er dataansvarlig for den pågældende persons oplysninger. Det gælder for personer på venteliste, som er inviteret eller deltager i en aktivitet, samt medlemmer og frivillige i foreningen.
6. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
7. Der hører tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
8. 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.
9. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
10. 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.
11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
12. 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 (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

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. 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.

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 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.

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 (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 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
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.

8. 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 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 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 anonymisering ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller anonymisering 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 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, 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 unødigt 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 behandlingsaktivitetes 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.

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 72 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.

11. Anonymisering og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at anonymisere alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er anonymiseret, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

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 anonymiseret 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

Navn

Stilling

E-mail

På vegne af databehandleren

Navn

Stig Kristensen

Stilling

Medlem af Hovedbestyrelsen

E-mail

stig.kristensen@codingpirates.dk

15. 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.

Dataansvarlig:

Navn

Stilling

E-mail

Databehandler:

Navn

Stig Kristensen

Stilling

Medlem af Hovedbestyrelsen

E-mail

stig.kristensen@codingpirates.dk

Bilag A Oplysninger om behandlingen

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

Medlemmer, deltagere og venteliste (herefter beskrevet med termen medlem)

- At håndtere medlemmer herunder at opkræve kontingent og betale deltagelse i aktiviteter
- At drive den dataansvarliges aktiviteter, herunder planlægge, gennemføre og følge op på dem
- At opfylde lovgivning, herunder krav i serviceloven og bogføringsloven
- At administrere medlemmers relation til den dataansvarlige
- At administrere den dataansvarliges venteliste

Frivillige og bestyrelse

- At den dataansvarlige kan koordinere og håndtere frivilliges opgaver
- At kunne udbetale transport og rejsegodtgørelser, refusion og lignende
- At administrere frivilliges relation til den dataansvarlige

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

- Medlemmer afgiver deres personoplysninger til databehandleren via Coding Pirates Denmarks Medlemssystem
- Oplysningerne stilles til rådighed for den dataansvarlige via Coding Pirates Denmarks Medlemssystem
- Medlemmer tilmelder sig aktivitet og betaler online til databehandleren via Coding Pirates Denmarks Medlemssystem
- Medlemmernes oplysninger anvendes uden personhenførbare oplysninger til statistik for den videre udvikling af Coding Pirates' virke

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

Navn, e-mail, telefon, adresse, fødselsdato, køn, dato for indmeldelse, opskrivning, betalingsoplysninger, besked/note til aktivitet.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Medlemmer
- Frivillige
- Forældre og familiære relationer

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

Medlemmer

- Databehandler anonymiserer oplysninger efter personlig henvendelse inden for 30 dage med mindre, at der er registreret betaling, som skal opbevares ifølge bogføringsloven.
- Medlemssystemet sletter automatisk Besked/note 14 dage efter afslutningen af den aktivitet, som medlemmet deltog i.

Standardkontraktbestemmelser marts 2024

- Anonymisering af persondata sker automatisk 2 år efter sidste login, dog tidligst 5 år efter sidste køb i henhold til bogføringsloven.

Frivillige:

- Databehandler anonymiserer oplysninger efter personlig henvendelse inden for 30 dage. Men databehandler kan ikke anonymisere personens oplysninger, hvis personen fortsat er frivillig.
- Anonymisering af persondata sker automatisk 2 år efter sidste login, dog tidligst 5 år efter sidste køb i henhold til bogføringsloven.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	ADRESSE	PRODUKT	BESKRIVELSE AF BEHANDLING
SFDC Ireland Ltd.	Salesforce Tower Dublin North Dock, Dublin 1, D01 W2Y3 Ireland	Heroku	Heroku hoster application og database (EU)
Quickpay Aps	P. O. Pedersens Vej 2, 8200 Aarhus N Denmark	Quickpay	Quickpay håndterer onlinebetalinger (Tyskland)
Intuit Inc.	405 N Angier Ave. NE Atlanta, GA 30308 USA	Mailchimp	E-mails afsendes med Mailchimp (USA)

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.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker som beskrevet i bilag A.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at der behandles fortrolige personoplysninger, samt en større mængde personoplysninger, der omfatter børn.

Udbyderen af betalingsløsningen behandler og opbevarer de detaljerede betalingsoplysninger herunder kortnummer. Det er kun beløb og status for en betaling, som opbevares af Coding Pirates Denmarks Medlemssystem.

Der kan være beskyttede adresser, som personen selv har oplyst ved opskrivning.

Derudover behandles kun personoplysninger, hvor konsekvenser af brud på fortrolighed, integritet eller tilgængelighed er mindre risikable.

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:

Anonymisering og kryptering

Personoplysninger opbevares i en krypteret database, og der anvendes kryptering ved enhver overførsel af personoplysninger.

Brugernes adgangskode gemmes ikke i klartekst, men som en saltet hashværdi beregnet med PBKDF2 eller tilsvarende sikker algoritme.

Når personlige oplysninger er anonymiseret, kan de ikke gendannes.

Databehandleren skal sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.

Opbevaring og gendannelse af personoplysninger

Personoplysninger opbevares i en krypteret database i et datacenter i EU. Der tages kontinuerligt backup, som sikrer at databasen kan gendannes. Backuppen opbevares hos samme leverandør på datacenter i EU.

Mulighed for at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

Det er den dataansvarlige, der har ansvaret for sikker opbevaring af personlige oplysninger, hvis de eksporteres fra Coding Pirates Denmarks Medlemssystem. Databehandleren Coding Pirates Denmark anbefaler, at man i videst muligt omfang undgår eksport af oplysningerne. .

Sikkerhed og adgang til personoplysninger

Det er kun personer, som har et kontraktmæssigt forhold til Coding Pirates Denmark og som har en relevant funktion, der kan få adgang til at læse og ændre alle personoplysninger, enten som administrativ bruger eller system administrator.

Der foretages screening af alle nye personer, som får et kontraktmæssigt forhold til Coding Pirates Denmark, og de underskriver en fortrolighedsaftale ved kontraktindgåelse.

Adgangen fjernes når personen stopper i sin funktion.

Lokalforeninger kan få adgang til at læse og ændre oplysninger om personer, der har en relation til foreningen via for eksempel venteliste eller deltagerliste. En person kan godt være relateret til flere foreninger, og foreningerne vil så have delt dataansvar.

Revisor har adgang til at læse alle personoplysninger, som anvendes til revision af regnskab og dokumentation over for donorer.

Det er kun systemadministratorer, som har adgang til hele systemet.

Der anvendes ikke fælles log-in, så det vil altid være muligt at identificere den person, der har foretaget en aktivitet.

Der stilles vejledning til rådighed vedrørende IT-sikkerhed og behandlingssikkerhed for personoplysninger.

Opdatering, logning og drift

Coding Pirates Danmarks Medlemssystem er udviklet i open source og bruger via Github Dependabot, der fortæller, når der er opdateringer/patches i de eksterne moduler. De medtages i førstkomende release/opgradering af medlemssystemet. Der er en fastlagt procedure for at verificere og godkende både rettelser og opdateringer, inden de lægges ind i medlemssystemet.

Source koden opbevares i GitHub. Alle releases bliver dokumenteret automatisk i GitHub.

Administrative adgange:

Der er adgang til Coding Pirates Danmarks Medlemssystem via brugergrupper i administrationsmodulet:

1. Der er 2 superbrugere, der kan alt.
2. Brugergruppen "Sekretariat" giver rettigheder til at arbejde med personoplysninger fra alle afdelinger og foreninger herunder:
 - a. adgang til alle kontaktoplysninger for personer
 - b. rettigheder til at anonymisere personer.
 - c. adgang til alle deltagere, aktiviteter og ventelister
 - d. at oprette/ændre afdelinger og foreninger.
 - e. at give/fjerne administrator adgang for brugere.
 - f. at tilføje bruger til en brugergruppe og fjerne bruger fra brugergruppe.
3. Brugergruppen "Revisor" har læseadgang til det samme som "Sekretariat", men kan ikke ændre noget..
4. Brugergruppen "Afdelingsleder" er for afdelingskaptajner og personer fra lokalforeningerne. "Afdelingsleder" giver en bruger administratorrettigheder til en eller flere afdelinger eller foreninger. Brugeren kan kun tilgå personoplysninger om personer og familier, der er tilknyttet en af de pågældende afdelinger eller foreninger gennem for eksempel et medlemskab, har deltaget i en aktivitet eller står på venteliste. "Afdelingsleder" kan kun se en persons postnummer, e-mail og telefon.

Når en bruger er logget ind i administrationsmodulet, via en af de 4 brugergrupper, så logges ændringerne automatisk i systemet med tid, bruger og handling.

Der er løbende overvågning af systemets drift herunder oppetid.

C.3 Bistand til den dataansvarlige

Der er ingen særlige tiltag i forhold til de almindelige GDPR-rettigheder som anført i Bestemmelserne 9.1.

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:

Databehandleren skal så vidt muligt bistå den dataansvarlige med guides og support til behandling af data i Coding Pirates Denmarks Medlemssystem.

C.4 Opbevaringsperiode

Ved ophør af den dataansvarlige lokalforening fjernes personer fra venteliste, og Coding Pirates Denmark bliver dataansvarlig. Dette ansvar deles med de lokalforeninger, som allerede er tilknyttet personoplysningerne.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren anonymisere personoplysningerne i overensstemmelse med bestemmelse 11.1.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end hos databehandleren i Danmark, samt hos de underdatabehandlere som er anført i aftalens B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Mailchimp anvendes til at sende mails til medlemmer, for eksempel invitationer.

Intuit Inc (USA), Mailchimp

- E-mail og navn.

Overførselsgrundlag:

- Virksomheden er certificeret under EU-U.S. Data Privacy Framework.

I det omfang det er nødvendigt, anvendes EU Kommissionens Standardkontraktbestemmelser (EU SCC's).

Heroku hoster Coding Pirates Denmarks Medlemssystem

Salesforce (USA), Heroku med Postgresql database. Personoplysningerne behandles og opbevares krypteret i EU, men er underlagt amerikansk lovgivning.

- Navn, adresse, mail, telefon, fødselsdato, køn, dato for indmeldelse, opskrivning,

Overførselsgrundlag:

- Virksomheden er certificeret under EU-U.S. Data Privacy Framework.

I det omfang det er nødvendigt, anvendes EU Kommissionens Standardkontraktbestemmelser (EU SCC's).

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