NØRREBROGADE 24A
DK-7100 VEJLE
+45 75 72 21 12
opening.dk

Databehandleraftale for Gymnasiejob.dk

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

mellem

Skole: _____

CVR: _____

Adresse: _____

Land: _____

herefter "den dataansvarlige"

og

OPENING a/s
CVR 27126537
Nørrebrogade 24A
7100 Vejle
Danmark

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

1. Indhold

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 hosting, drift og videreudvikling af Gymnasiejob.dk annonceringsportal og e-rekruttering, herunder support til Jobsøgere (JS) og Skoler (AG), 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.

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 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.

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.

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

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 1måneds 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. Databehandleren skal i sin aftale med underdatabehandleren indføje 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, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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

9. Bistand til den dataansvarlige

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.

10. 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 36 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. 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 dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

a. Ikke relevant for denne databehandleraftale

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

12. Revision, herunder inspektion

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. Eventuelle omkostninger forbundet hermed afholdes af dataansvarlige.

2. Procedurerne 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 lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation. Eventuelle omkostninger forbundet hermed afholdes af dataansvarlige.

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 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

   Navn
   Stilling
   Telefonnummer
   E-mail

   Underskrift

   På vegne af databehandleren

Navn	Niels Henrik Duevang
Stilling	Kontaktchef
Telefonnummer	2819 333
E-mail	nh@opening.dk

   

   Underskrift

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.

   Navn
   Stilling
   Telefonnummer
   E-mail

Navn	Niels Henrik Duevang
Stilling	Kontaktchef
Telefonnummer	2819 333
E-mail	nh@opening.dk

Bilag A Oplysninger om behandlingen

OPENING a/s varetager følgende behandling af følgende data

- Hosting og support af personhenførbare data på Gymnasiejob.dk, annonceringsportal og e-rekrutteringssystem for hhv.
    - Jobsøgere (JS)
    - Skolers systembrugere (AG)

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

Formål med behandling af ovenstående data er hosting, drift og videreudvikling af Gymnasiejob.dk, annonceringsportal og e-rekrutteringssystem, herunder support til JS og AG.

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

Karakteren af OPENING a/s' adgang til og behandling af ovenstående data er hosting og support til JS og AG.

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

Type af ovenstående data er

- Jobsøgere (JS):
    - Fornavn
    - Efternavn
    - E-mail
    - Telefon
    - Billede (hvis uploadet)
    - Adresse
    - Postnummer/by
    - Undervisningsfag, herunder også hvorvidt JS har undervisningserfaring og/eller pædagogikum
    - Svar på screeningspørgsmål
    - Vedhæftede filer
    - Noter skrevet af ansættelsesudvalg (Skoles systembrugere)
    - Anvendelseshistorik
- Skolers systembrugere (AG)
    - Fornavn
    - Efternavn
    - E-mail
    - Anvendelseshistorik

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kategorier af registrerede er

- JS: Jobsøgere, der opretter profil, Jobmatchagent og ansøger stillinger, opslået af AG.
- AG: Skolers systembrugere, der hhv. kan administrere brugere, oprette rekrutteringer, annoncere stillinger eller indgår i ansættelsesudvalg.

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

Varighed af databehandlers behandling af personoplysninger for dataansvarlige følger drift-, service- eller supportaftale vedr. de i Præambel, punkt 2.3 nævnte systemer. Såfremt der ikke forefindes en aktiv drift-, service- eller supportaftale kan databehandler ikke behandle personoplysninger som beskrevet i Bilag A.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Curanet A/S	29412006	Højvangen 4 8660 Skanderborg Danmark	Hosting

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 ved, at databehandleren udfører følgende:

- Hosting, drift og videreudvikling af Gymnasiejob.dk, annonceringsportal og e-rekrutteringssystem, herunder support til JS og AG.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:
Behandlingen omfatter en større mængde personoplysninger, hvorfor der etableres et "højt" sikkerhedsniveau.

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 for systemer omfattet af denne databehandleraftale – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger for, som er aftalt med den dataansvarlige:

Adgangsstyring
Fysisk
Der er etableret fysisk adgangskontrol, således at kun autoriserede personer, der har et arbejdsrelateret behov for adgang, kan opnå adgang med nøglekort og kode. Adgangsrettighederne til sikre områder gennemgås og ajourføres i en kontrolliste. Hvis ansatte mister nøgler eller adgangskort, er der indarbejdet procedure for skift af nøgler og koder.

Digitalt
Medarbejdere hos databehandleren kan kun tilgå systemerne gennem beskyttet adgangsinformation tildelt via OPENINGs centrale brugeradministration. Ved adgang fra hjemmearbejdsplads sker dette via vpn og beskyttet adgangsinformation tildelt via OPENINGs centrale brugeradministration. Medarbejderes adgang via OPENINGs centrale brugeradministration sker ved biometrisk eller password beskyttet 2-faktor login.

Kryptering og sikring af eksterne kommunikationsforbindelser
Der anvendes kryptering på al ekstern kommunikation til og fra datacentreret. Der anvendes enten IPsec VPN eller SSL.
Transmissioner sker via SSL kryptereret dataforbindelse fra klient til server. Servere er adgangsbeskyttet via IP-restriktioner på alle porte undtaget standard http og https (80,81 og 443)

Driftssikkerhed
Tilgængeligheden af systemer og data sikres gennem en fortsat drift i tilfælde af mulige forstyrrelser. Dette sikres bl.a. gennem kontroller, der er forebyggende, detektive og korrigerende. Kontrollerne ligger inden for procedurekontroller, tekniske kontroller og lovmæssigt styrede kontroller. Disse kontroller dækker bl.a. over følgende: autentifikation, antivirus, firewall, incident management, monitorering, backup og beredskabsplaner.

Der er indarbejdet adgangsstyring for håndtering og godkendelse af såvel interne som kundens bruger id'er. Der er fastlagte passwordpolitikker for autentifikation og to-faktor autentifikation.
Der er udarbejdet formelle forretningsgange for ændringsstyring med formålet, at risikoen for kompromittering af virksomhedens og kundernes informationer minimeres. Introduktionen af nye systemer og større ændringer til de eksisterende systemer følger en formel proces med dokumentation, specifikation og styret implementering.
Effektiv monitorering af processer giver vigtige oplysninger til både proaktivt og reaktivt at kunne undgå events, der ville have påvirket kundens systemer. Målet er at minimere den tid, det tager at genetablere normal drift.
For at imødegå dette arbejder OPENING med forebyggende monitorering og korrigerende handlinger. Ved denne metode sker der ingen eller minimal påvirkning af kundens systemer.
OPENING anvender event management værktøj til at varetage automatisk monitorering af servere, systemsoftware og applikationssoftware. Monitoreringen dækker typisk ram, diskplads, CPU-forbrug, eller om specifikke applikationer er kørende.
For systemer, der ikke kan monitoreres automatisk, er der etableret fastlagte manuelle driftsrutiner og backuprutiner. Ved fejl eskaleres disse til den ansvarlige.

Sikring af logning
For e-rekrutteringssystem gælder, at der er følgende logning på systemerne:

- Aktivitetslog: Der findes aktivitetslog, der registrerer handlinger på systemerne. Aktivitetslog kan tilgås af dataansvarlige og databehandler.
- Systemlog: Der findes systemlog, der registrerer handlinger og fejl på systemerne. Systemlog kan tilgås af databehandler og fremsendes til dataansvarlige efter ønske. Eventuelle omkostninger forbundet hermed for databehandleren dækkes af dataansvarlige.
- Web hændelseslog: Der findes web hændelseslog, der registrerer og logger alle forespørgsler til systemerne. Web hændelseslog kan tilgås af databehandler og fremsendes til dataansvarlige efter ønske. Eventuelle omkostninger forbundet hermed for databehandleren dækkes af dataansvarlige. Web hændelseslog gemmes 1 år tilbage

Kommunikationssikkerhed
Vores kommunikation til kunderne i forbindelse med drifts- og datasikkerhed aftales med den individuelle kunde. I forbindelse med eventuelle sikkerhedshændelser kontaktes berørte kunder så hurtigt som muligt pr. telefon.
Informationssikkerhed vedrører virksomhedens samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte OPENING's informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Alle medarbejdere uddannes i informationssikkerhed i relevant omfang.

Som brugere af OPENING's informationer skal alle medarbejdere følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende virksomhedens informationer i overensstemmelse med det arbejde, de udfører i virksomheden, og de skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed og særlige og/eller kritiske natur.
Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsniveau.

Anskaffelse, udvikling og vedligeholdelse af systemer
Vi udfører patch management på systemer i datacentrene. Formålet er at sikre, at der sker sikkerhedsopdatering af kritiske systemer.

Udrulning af opdateringer
Curanet a/s frigiver løbende opdateringer. Opdateringer udrulles til produktionsmiljøet ud fra de fastdefinerede servicevinduer. Det tilstræbes, at frigivne patches installeres inden for 2 måneder.

Styring af sikkerhedshændelser
Hvis der konstateres en sikkerhedshændelse, adviseres de berørte kunder så hurtigt som muligt, og samtidigt tages der skridt til at sikre data og systemer. Efterfølgende kan udarbejdes en "root cause analysis"-rapport til kunden, for så vidt muligt at sikre at hændelsen ikke kan optræde igen.
Er der tale om en intern medarbejder, der har overtrådt, eller forsøgt at overtræde, sikkerhedsreglerne uforsætligt, gives vedkommende ved første tilfælde en mundtlig advarsel og ved andet tilfælde en skriftlig advarsel. Sker det tredje gang, tages der skridt til afskedigelse af den pågældende medarbejder.
Hvis medarbejdere forsætligt overtræder, eller forsøger at overtræde, sikkerhedsreglerne, tages der straks skridt til afskedigelse, og i særligt grove tilfælde vil der være tale om bortvisning.
Alle sikkerhedshændelser rapporteres til OPENINGs ledelse.

Nød-, beredskabs- og reetableringsstyring
Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici imod sikringsomkostninger.

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:

- Sikre databehandlers overholdelse af oplysningspligt ved indsamling af personoplysninger i form af brugeres afgivelse af samtykke til databehandlers persondatapolitik ved selvbetjent afgivelse af personoplysninger på systemerne denne databehandleraftale omfatter.
- Stå til rådighed 24/7 for at dataansvarlige kan overholde øvrige forpligtelser i Bestemmelse 9.1. Eventuelle omkostninger hertil afholdes af Dataansvarlige.

- Sikre at dataansvarlig uden unødig forsinkelse oplyses om alle brud på persondatasikkerhed databehandler bliver bekendt med på systemerne denne databehandleraftale omfatter.

C.4 Opbevaringsperiode/sletterutine
Systemet sletter automatisk jobsøgers ansøgninger incl. tilhørende dokumenter 12 mdr. efter sidste ansøgningsfrist.
Personoplysninger på de systemer databehandleraftalen omfatter, opbevares i den periode, registrerede har afgivet samtykke til ved registrering. Medmindre der sker fornyet samtykke fra registrerede, slettes personoplysninger fuldstændigt ved automatisk systemproces

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

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 følgende:

- OPENING a/s, Nørrebrogade 24A, 7100 Vejle, Danmark eller ved VPN forbindelse hertil.
- Fysiske lokationer for underdatabehandlere nævnt i Bilag B, B1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Hosting for systemer omfattet af denne databehandleraftale sker i Danmark hos underdatabehandlere nævnt i Bilag B, B1. Der sker således ingen overførsel af personoplysninger til tredjelande.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Databehandleren skal, på den dataansvarliges opfordring og uden yderligere omkostning, skriftligt bekræfte, at alle krav i databehandleraftalen fortsat efterleves, herunder:

- At databehandlerens medarbejder, der behandler personoplysninger, har underskrevet en fortrolighedsaftale eller er underlagt en passende lovbestemt tavshedspligt.
- At databehandleren, i forhold til den behandling af personoplysninger, som databehandleren foretager på vegne af den dataansvarlige, gennemfører passende tekniske og organisatoriske sikkerhedsforanstaltninger med fokus på risikoen for de registrerede samt gennemfører eventuelle særlige aftalte sikkerhedskrav.
- At databehandleren ikke gør brug af en underdatabehandler uden den dataansvarliges godkendelse.
- At databehandleren pålægger eventuelle underdatabehandlere samme forpligtigelser som i databehandleraftalen mellem den dataansvarlige og databehandleren, herunder at databehandleren fører tilsyn med eventuelle underdatabehandlere.

- At databehandleren så vidt muligt bistår den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, så den dataansvarlige kan opfylde sine forpligtigelser til at besvare anmodninger om at udøve de registreredes rettigheder.
- At databehandleren bistår den dataansvarlige f.eks. i forhold til den dataansvarliges forpligtigelse til at anmelde brud på personsikkerheden til Datatilsynet, herunder at databehandleren underretter den dataansvarlige uden unødig forsinkelse om brud på persondatasikkerheden, som berører den behandling, som databehandleren foretager på den dataansvarliges vegne.
- At databehandleren sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, når databehandlerens service til den dataansvarlige ophører.
- At databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i databehandleraftalen, til rådighed for dig, og at databehandleren giver mulighed for og bidrager til revision, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Omkostninger forbundet hermed for databehandleren dækkes af den dataansvarlige.

Har den dataansvarlige begrundet mistanke om, at der er noget galt hos databehandleren, f.eks. fordi Datatilsynet har indstillet databehandleren til en bøde, skal databehandleren, på den dataansvarliges forlangende, indhente revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen. Omkostninger forbundet hermed dækkes af dataansvarlige.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
For de i denne databehandleraftale omfattede systemer gælder, at

- Hosting hos Curanet a/s drives efter ISO 27001-standarder for informationssikkerhed og risikostyring. Revisioner gennemføres årligt efter ISAE 3000 og ISAE 3402 Type 2. Erklæringer for dette kan fremsendes til dataansvarlige efter ønske.

Såfremt den dataansvarlige ønsker det, kan databehandleren indhente revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Eventuelle omkostninger forbundet hermed for databehandleren og underdatabehandleren dækkes af dataansvarlige.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt. Eventuelle omkostninger forbundet hermed for databehandleren og underdatabehandleren dækkes af dataansvarlige.

Baseret på resultaterne af inspektioner, revision og erklæringer, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Eventuelle omkostninger forbundet hermed for databehandleren og underdatabehandleren dækkes af dataansvarlige.

Bilag D Parternes regulering af andre forhold