DATABEHANDLERAFTALE

Mellem

Favrskov Gymnasium

Gymnasium

Ellemosevej 30

Adresse

8370 Hadsten

Postnr. og by

29 54 82 85

CVR. nr.

(herefter "Skolen")

og

OPENING a/s
Nørrebrogade 24A
7100 Vejle
CVR. nr.: 27126537
(herefter "Databehandleren")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Databehandlerens behandling af personoplysninger på vegne af Skolen:

1. Generelt

1.1 Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.

1.2 Aftalen 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), som stiller specifikke krav til indholdet af en databehandleraftale.

1.3 Ønsker Skolen, at Databehandleren skal leve op til principper og anbefalinger i ISO27001, kan der indsættes et krav om dette her.

1.4 Databehandleren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

1.5 Ønsker Skolen, at Databehandleren skal forpligte sig til at gøre sig bekendt med Skolens it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de eventuelle, dertilhørende uddybende it-sikkerhedsregler, som vedlægges Aftalen som bilag [4-6], kan der indsættes et krav om dette her. Et krav om dette forudsætter også et yderligere krav om, at Skolen er forpligtiget til at orientere Databehandleren om ændringer af politikker, regler m.v. under pkt. 3.4.

2. Formål

2.1 Databehandleren behandler i medfør af aftale med Skolen, Skolens oplysninger til brug for Gymnasiejob.dk (herefter kaldet "Systemet") og tilhørende e-rekrutteringssystem ifm stillingsannoncering og rekrutteringsprocesser, jf. Hovedaftalen: "Kontrakt for opgradering, abonnement og support af gymnasiejob.dk for danske gymnasier" af 06.01. 2015., personoplysninger for Skolen.

3. Skolens rettigheder og forpligtelser

3.1 Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

3.2 Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3.3 Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

3.4 Skolen er forpligtet til at orientere Databehandleren i tilfælde af Skolens eventuelle skærpede it-sikkerhedsregler og ved ændringer i Skolens it-sikkerhedspolitik og it-sikkerhedsregulativ, jf. bilag [4-6].

4. Databehandlerens forpligtelser

4.1 Databehandleren er databehandler for de personoplysninger, som Databehandleren behandler på vegne af Skolen, jf. pkt. 6 og bilag 3. Databehandleren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4.2 Databehandleren behandler alene de overladte personoplysninger efter instruks fra Skolen, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.

4.3 Databehandleren skal løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.

4.4 Databehandleren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen og Databeskyttelsesforordningen, jf. bilag 1 – Sikkerhed.

4.5 Databehandleren skal på opfordring fra Skolen hjælpe med at opfylde Skolens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Skolens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

4.6 Databehandleren skal hjælpe Skolen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36, jf. pkt. 11.

4.7 Databehandleren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Databehandlerens behandling af Skolens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

4.8 Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor Skolens personoplysninger opbevares, jf. bilag 2. Databehandleren skal ajourføre oplysningerne over for Skolen ved enhver ændring.

4.9 Hvis Databehandleren er etableret i en anden EU-medlemsstat, skal Databehandleren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

5.1 Ved underdatabehandler forstås en underleverandør, til hvem Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af Skolen.

5.2 Databehandleren må ikke uden udtrykkelig skriftlig godkendelse fra Skolen anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Skolen har overladt til Databehandleren i medfør af Hovedaftalen. Skolen kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor.

5.3 Hvis Databehandleren overlader behandlingen af personoplysninger, som Skolen er dataansvarlig for, til underdatabehandlere, skal Databehandleren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Databehandleren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5 Når Databehandleren overlader behandlingen af personoplysninger, som Skolen er dataansvarlig for, til underdatabehandlere, har Databehandleren over for Skolen ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.

5.6 Skolen kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Skolen.

5.7 Al kommunikation mellem Skolen og underdatabehandleren sker via Databehandleren.

6. Instrukser

6.1 Databehandlerens behandling af personoplysninger på vegne af Skolen sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Databehandlerens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt. 5.3, får tilsendt Skolens instruks, jf. bilag 3.

6.2 Databehandleren giver omgående besked til Skolen, hvis en instruks efter Databehandlerens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Databehandleren skal, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

7.2 Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 og 7.2, samt bilag 1.

7.3 Databehandleren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

7.4 Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Skolens personoplysninger, om Databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt. 9.

7.5 Databehandleren er forpligtet til straks at underrette Skolen om ethvert sikkerhedsbrud samt ved

(i) enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Skolen er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,

(ii) anden manglende overholdelse af Databehandlerens, samt eventuelle underdatabehandleres forpligtelser

uanset, om dette sker hos Databehandleren eller hos en underdatabehandler.

7.6 Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt. 7.5, uden forudgående skriftlig aftale med Skolen om indholdet af en sådan kommunikation, medmindre Databehandleren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

8.1 Databehandlerens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Skolens instruks herfor, jf. bilag 3.

8.2 Ved overførsel til tredjelande er Databehandleren og Skolen i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

8.3 Hvis Skolens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Databehandlerens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

8.4 Databehandleren må ikke overføre eller tillade overførsel af personoplysninger til udlandet.

9. Tavshedspligt og fortrolighed

9.1 Databehandleren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.

9.2 Databehandleren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1 Databehandleren er forpligtet til uden ugrundet ophold at give Skolen nødvendige oplysninger til, at Skolen til enhver tid kan sikre sig, at Databehandleren overholder de krav, der følger af denne Aftale.

10.2 Skolen, en repræsentant for Skolen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Databehandleren, få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Databehandleren overholder de krav, der følger af denne Aftale.

10.3 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger m.v. er truffet. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering. I tilfælde af, at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion (audit) af de foranstaltninger, som Databehandler foretager i medfør af Databehandleraftalen, forpligter Databehandleren sig til - med et rimeligt varsel - at stille tid og ressourcer til rådighed herfor.
Underdatabehandleren Microsoft, som med cloudplatformen Microsoft Azure, varetager hosting, attesteres årligt af ekstern revisor efter SOC 1/SSAE 16/ISAE 3402 og SOC 2 standarder. Erklæringerne kan fremsendes efter anmodning fra den Dataansvarlige.

10.4 I tilfælde af, at Skolen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Databehandleren og Databehandlerens underleverandører sig til uden yderligere omkostninger for Skolen at stille tid og ressourcer til rådighed herfor.

11. Bistand til den dataansvarlige

11.1 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 3.

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) Den registreredes indsigtsret

d) Retten til berigtigelse

e) Retten til sletning (»retten til at blive glemt«)

f) Retten til begrænsning af behandling

g) Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h) Retten til dataportabilitet

i) Retten til indsigelse

j) Retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

11.2 Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen

b) Forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

c) Forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

d) Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

e) Forpligtelsen til at høre tilsynsmyndigheden (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

12. Ændringer i Aftalen

12.1 Skolen kan til enhver tid, med et forudgående varsel på mindst 10 dage, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne aftales skriftligt mellem Skolen og Databehandleren i Hovedaftalen. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.

12.2 I det omfang ændringer i lovgivningen, jf. pkt. 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Skolen med et varsel på 10 dage og uden at dette medfører krav om betaling fra Databehandleren, berettiget til at foretage ændringer i Aftalen.

13. Sletning af data

13.1 Skolen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.

13.2 Skolen skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Databehandleren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Skolen. I det tilfælde, hvor personoplysningerne tilbageleveres til Skolen, skal Databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Skolens meddelelse.

13.3 Databehandleren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 13.2, er foretaget.

13.4 Databehandleren skal foretage den påkrævede sletning, jf. pkt. 13.2, i henhold til [*angiv den ønskede etablerede internationale standard for sletning, f.eks. NIST 800-88*]

14. Misligholdelse og tvistigheder

14.1 En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af Hovedaftalen.

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parters underskrift og løber indtil ophør af Hovedaftalen.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Skolen og Databehandleren.

17. Forrang

17.1 I tilfælde af uoverensstemmelse mellem denne databehandleraftale og Hovedaftalen skal bestemmelserne i databehandleraftalen have forrang.

For Skolen

Dato 28/5 2018

FAVRSKOV GYMNASIUM
Ellemosevej 30
8370 Hadsten

For Databehandleren

Dato: 30.04. 2018

Niels Henrik Duevang

OPENING a/s

OPENING®
HAVNEPARKEN, JYLLANDSGADE 8
DK-7100 VEJLE

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

Bilag 3 – Instruks

[Bilag 4 – Skolens it-sikkerhedsregulativ]

[Bilag 5 – Skolens it-sikkerhedspolitik]

[Bilag 6 – Skolens supplerende it-sikkerhedsregler]

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav indtil 25. maj 2018

Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- Tilintetgøres, mistes, ændres eller forringes,
- Kommer til uvedkommendes kendskab eller misbruges,
- Eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

Generelle sikkerhedsforanstaltninger
Systemet hostes i et lukket miljø på Microsoft Azure (ISO 27001 certificeret) med redundans i Europa.
(https://www.bsigroup.com/en-US/Our-services/Certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=standard=ISO/IEC+27001:2005&licence=577753&company=microsoft&scope=management&licencenumber=IS%205777537753)
Data opbevares i region Nordeuropa. (adresse kan oplyses til den dataansvarlige efter behov)
Backupdata opbevares i region Vesteuropa. (adresse kan oplyses til den dataansvarlige efter behov)
Hosting leveres ud fra de altid gældende Service Level Agreements for Microsoft Azure

- https://azure.microsoft.com/da-dk/support/legal/sla/
- https://azure.microsoft.com/da-dk/support/legal/sla/virtual-machines/v1_5/
- https://azure.microsoft.com/da-dk/support/legal/sla/cdn/v1_0/
- https://azure.microsoft.com/da-dk/support/legal/sla/storage/v1_1/
- https://azure.microsoft.com/da-dk/support/legal/sla/backup/v1_0/
- https://azure.microsoft.com/da-dk/support/legal/sla/sql-database/v1_1/

Autorisation og adgangskontrol
Medarbejdere hos Databehandler, der varetager support eller har teknisk adgang til systemerne, har underskrevet fortrolighedsaftaler.

Alle systemadgange er beskyttet via 2-faktor godkendelse.
Medarbejdere kan kun tilgå Systemet gennem beskyttet adgangsinformation tildelt via OPENINGs centrale brugeradministration. Medarbejderen kender således ikke sin specifikke adgangsinformation til Systemet.

Inddatamateriale som indeholder personoplysninger
Der er på Systemet opbygget følgende til sikring af inddaterede personoplysninger

Aktivt samtykke til Skolens vilkår for behandling af ansøgning

- Ansøger bekræfter ved tjekmark at have læst skolens vilkår for behandling af persondata ved ansøgning af konkret stillingsopslag.

Automatisk sletning af ansøgninger
Systemet sletter automatisk jobsøgers ansøgninger incl. tilhørende dokumenter 6 mdr. efter sidste ansøgningsfrist.
Mulighed for at samtykke til opbevaring af personoplysninger i 6 mdr.

Uddatamateriale som indeholder personoplysninger
Skolen kan udtrække data fra Systemet. Databehandler har ikke kontrol over disse uddata og ansvaret herfor er alene Skolens.

Eksterne kommunikationsforbindelser
Transmissioner til Systemet sker via SSL kryptereret dataforbindelse fra klient til server.
Systemets servere er adgangsbeskyttet via IP-restriktioner på alle porte undtaget standard http og https (80,81 og 443)

Logning
Der er følgende logning på Systemet:

Systemlog
Der findes systemlog, der registrerer alle fejl på Systemet.
Systemlog kan kun tilgås af Databehandler

Hændelseslog
Der findes brugeridentificerbar aktivitets- og hændelseslog for Skolen på Systemet.
Aktivitets- og hændelseslog indeholder

- Opsummeret handlingslog for alle handlinger for Skolen
- Handlingslog på detaljeside for rekruttering (stillingsopslag)
- Handlingslog på detaljeside for ansøger

Aktivitets- og hændelseslog kan tilgås af Skolens administrator på Systemet.

Hjemmearbejdspladser

Databehandlerens adgang til Systemet kan ske ved anvendelse af hjemmearbejdspladser.

Ved adgang fra hjemmearbejdsplads sker dette via vpn og beskyttet adgangsinformation tildelt via OPENINGs centrale brugeradministration.

Adgangsrettigheder på skolen

Det er skolen selv, der administrerer egne medarbejderes adgang til Systemet. Hver skole, der er oprettet med konto på Systemet har som minimum én bruger med rolle "Superbruger". Superbrugeren kan administrere brugere på skolens konto, herunder oprette, redigere og slette brugere med hhv. "Superbruger"- og "Bruger"-rolle.

Sikkerhedskrav fra 25. maj 2018

Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
   a. tilintetgørelse af oplysningerne
   b. tab af oplysningerne
   c. ændring af oplysningerne
   d. uautoriseret videregivelse af oplysningerne
   e. uautoriseret adgang til oplysningerne

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen
   Data på Systemet behandles på Databehandlers fysiske adresse: Nørrebrogade 24A, 7100 Vejle eller fra hjemmearbejdspladser via VPN til Databehandlers adresse.

2. Underdatabehandlere
   Underdatabehandler er Microsoft, som hoster data med redundans i Europa. Data opbevares i region Nordeuropa og backupdata opbevares i region Vesteuropa. Microsoft repræsenteres i Danmark af Microsoft Danmark ApS, Kanalvej 7, 2800 Kongens Lyngby med CVR nr. 13612870

Adresse kan oplyses til den dataansvarlige efter behov.

Bilag 3 – Instruks

Instruks
Skolen instruerer hermed Databehandleren om at foretage behandling af Skolens oplysninger til brug for Gymnasiejob.dk (herefter kaldet "Systemet") og tilhørende e-rekrutteringssystem ifm stillingsannoncering og rekrutteringsprocesser, jf. Hovedaftalen "Kontrakt for opgradering, abonnement og support af gymnasiejob.dk for danske gymnasier" af 06.01. 2015.

Overlader Databehandleren behandling af Skolens oplysninger til underdatabehandlere, er Databehandleren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt. 5.3. Databehandleren er ansvarlig for, at Skolens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål

Behandling af Skolens oplysninger sker i henhold til formålet i Hovedaftalen.

Databehandleren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Skolen.

1.2 Generel beskrivelse af behandlingen

Databehandler varetager drift og hosting af Systemet, herunder support for jobsøgere til Skolens stillingsopslag og Skolens egne systembrugere.

1.3 Typen af personoplysninger

Databehandlerens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om "at databehandleren stiller Systemet til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges jobsøgere på Systemets servere".

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Fornavn
- Efternavn
- Email

- Telefon
- Billede (hvis uploadet)
- Adresse
- Postnummer/by
- Undervisningsfag, herunder også hvorvidt jobsøger har undervisningserfaring og/eller pædagogikum
- Svar på screeningspørgsmål
- Vedhæftede filer
- Noter skrevet af ansættelsesudvalg (Skoles systembrugere)

Behandlingen omfatter følgende kategorier af registrerede:

- Skolens jobsøgere og ansatte

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.