Samarbejdsaftalens bilag 10 Databehandleraftale mellem partnerskoler og Gymnasiefællesskabet

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger mellem den enkelte partnerskole som dataansvarlig og Gymnasiefællesskabet ved Roskilde Gymnasium, Skolegade 3, Roskilde 4000, CVR. nr.: 29545758, som databehandler, som 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 den dataansvarliges deltagelse i de samarbejdsområder, der fremgår af oversigtsbilaget på sidste side i Samarbejdsaftalen, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser. Samarbejdsaftalen og oversigtsbilaget findes på GF's intranet[1].

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

[1] http://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/samarbejdsaftaler

24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[2] 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.

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.

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

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 og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne

ændringer inden brugen af de(n) omhandlede underdatabehandler(e). 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 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 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 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 så betids 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 tilbagelevere alle personoplysningerne og slette eksisterende kopier, 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. Bogføringsloven jfr. bilag c

    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.

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.

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 når styregruppen har godkendt aftalen

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 skriftligt varsel af begge parter.

5. Underskrift

   Da databehandleraftalen er et underbilag til samarbejdsaftalen, underskrives denne aftale ikke særskilt.

Kontaktoplysninger Databehandler:

Navn	Camilla Schaldemose
Stilling	Direktør
Telefonnummer	2129 2043
E-mail	cas@gfadm.dk

Kontaktoplysninger DPO:

Navn	Pernille Frimann
Stilling	DPO
Telefonnummer	4114 7862
E-mail	dpo@gfadm.dk

Bilag A Oplysninger om behandlingen

Databehandleren tilbyder den dataansvarlige følgende samarbejdsområder, særydelser og systemer:

a) Sekretariat og Jura
b) Datasikkerheds- og DPO-samarbejde
c) Løn- og Personaleadministration
d) Kreditorbogholderi
e) IT
f) Bygning
g) Indkøb.

Systemer:
h) HR-Database
i) Gymbetaling (web-baseret system til køb af billetter, online-betaling, samtykkeblanketter)
j) DocuNote ESDH (opsætning, hosting, drift, vedligehold og support)
k) EveryonePrint – Printløsning til sikker print (”follow me-print”) (opsætning, hosting, drift, vedligeholdelse)
l) GatewayApi – Forsendelse og modtagelse af SMS via SMS-API-gateway (opsætning, hosting, drift, vedligeholdelse)

Det fremgår af oversigtsbilaget sidst i Samarbejdsaftalen[3], hvilke ydelser den dataansvarlige aftager fra den dataansvarlige.

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

Ad a) Sekretariat og Jura, herunder Whistleblowerordning, samt b) Datasikkerheds- og DPO-samarbejde.

Formålet med behandling af personoplysninger er rådgivning og sagsbehandling (inkluderer sagsbehandling af indberettede Whistleblowersager).

Ad c) Løn- og Personaleadministration

Formålet med behandling af personoplysninger er

- Oprettelse og vedligehold af personalesag i ESDH
- Oprettelse af ansættelsesbrev, tillæg til ansættelsesbrev og lønaftale
- Beregning, udbetaling, afregning og postering af løn og andre ydelser i statens lønsystemer
- Beregning, fradrag og afregning af fx. kildeskat og pensionsbidrag i statens systemer
- Lønbudgettering og styring af lønbudgetter
- Ferie- fraværs- og afspadseringsadministration
- Statistik.

Ad d) Kreditorbogholderi

Formålet med behandling af personoplysninger er godkendelse og gennemførelse af betalinger via statens økonomisystemer.

Ad e) IT

[3] https://www.gymnasiefaellesskabet.dk/gym/images/docs/ydelseskatalog/Samarbejdsaftale_gldende_pr_1_oktober_2020.pdf

Formålet med behandling af personoplysninger er opsætning, vedligehold og support af netværk, servere (inkl. hosting), pc'ere samt mail-løsning.

Ad f) Bygning og g) Indkøb
Formålet med behandling af personoplysninger er dokumentation af konkurrenceretlige forhold ifbm. tilbudsindhentning samt og skatteretlige forhold hos leverandører (forebyggelse af sort arbejde og ulovlig arbejdskraft).

Ad h) HR-Databasen
Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er, at den dataansvarlige kan få opsat, driftet, hostet, supporteret og udviklet et HR-system (et ledelsesværktøj), som kan samle og vise relevante data fra eksisterende systemer (SLS og Lectio) med henblik på at understøtte lokale HR-processer f.eks. MUS.

Ad i) Gymbetaling
Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er, at den dataansvarlige kan få opsat, driftet, hostet, supporteret og udviklet et digitalt redskab til administration af elevers tilmeldinger og betaling til skolerelaterede aktiviteter, fx studieture, fester, elevskabe, ekskursioner mv. GymBetaling anvendes også til alle former for samtykkeerklæringer fra elever eller deres værger.

Ad j) DocuNote ESDH
Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er, at den dataansvarlige kan få opsat, driftet, hostet, supporteret og udviklet et system til behandling og opbevaring af vigtige data og personoplysninger, der er driftskritiske og som skolerne har pligt til at opbevare på en måde, der sikrer fortrolighed, tilgængelighed og ægthed. Endvidere rummer ESDH'et en integration til Digital Post, som muliggør krypteret ekstern mail-kommunikation.

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

Alle bilag findes på: https://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/samarbejdsaftaler

Ad a) Sekretariat og Jura samt b) Datasikkerheds- og DPO-samarbejde
Databehandleren udfører rådgivning og sagsbehandling. Der henvises til følgende bilag til samarbejdsaftalen:
- Bilag 1 Sekretariat og Jura Ydelseskatalog
- Bilag 1.1 Bilag 1.1. Datasikkerhedssamarbejde og DPO-samarbejde Ydelseskatalog

Ad c) Løn- og Personaleadministration
Databehandleren udfører lønsagsbehandling og personaleadministration samt arkivering på vegne af den dataansvarlige. Der henvises til følgende bilag til samarbejdsaftalen:
- Bilag 2 Løn og Personale Ydelseskatalog

Ad d) Kreditorbogholderi
Databehandleren udfører kreditorbogholderi på vegne af den dataansvarlige. Der henvises til følgende bilag til samarbejdsaftalen:
- Bilag 4 Kreditorbogholderi Ydelseskatalog

Ad e) IT
Databehandleren udfører IT-drift på vegne af den dataansvarlige og behandling af personoplysninger i forekommer, når der indgår personoplysninger som led i databehandlerens opgaver som driftsenhed, administrator, supporter og udvikler af den dataansvarliges it-netværk, mailsystemer, PC'ere, printere, mv. Der henvises til følgende bilag til samarbejdsaftalen:

- Bilag 3 IT Ydelseskatalog
- Bilag 3.1 IT SLA backend
- Bilag 3.2 IT SLA frontend

Ad f) Bygning og g) Indkøb
Databehandleren udfører rådgivning og sagsbehandling på vegne af den dataansvarlige. Der henvises til følgende bilag til samarbejdsaftalen:

- Bilag 5 Bygning Ydelseskatalog
- Bilag 6 Indkøb Ydelseskatalog

Ad h) HR-Databasen, i) GymBetaling og j) DocuNote ESDH
Der foretages følgende typer af behandlinger fra databehandlerens side:

- Adgangsstyring via NemID
- Hosting, administration, support og udvikling af systemet
- Automatiseret sletning via kassationsfunktion

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede
Databehandleren tilstræber og støtter den dataansvarlige i dataminimering i videst muligt omfang.

Ad a) Sekretariat og Jura samt b) Datasikkerheds- og DPO-samarbejde
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder fortrolige personoplysninger i form af cpr-numre, samt i begrænset omfang følsomme personoplysninger (art. 9).

Konkret er der tale om oplysninger ang. ansættelsesforholdet, varetagelse af tjenesten, uddannelsen, skolegangen fx oplysninger om fravær, handlinger som strider mod skolens studie- og ordensregler, eksamenssnyd mv. af relevans for rådgivningen samt i begrænset omfang helbredsdiagnoser og oplysninger om fagforeningsmæssige tilhørsforhold, hvis en medarbejder lader sig bistå af sin faglige organisation i en tjenstlig sag.

Ad c) Løn- og Personaleadministration
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre, samt i begrænset omfang helbredsoplysninger, herunder som led i § 56-aftaler og fleksjob-ordninger (art. 9).

Konkret er der tale om cpr.nr., initialer, navn, adresse, overenskomst, uddannelse, timetal, ansættelsesbrøk, aflønningsform, evt. begrundelse for tidsbegrænsning, anciennitet, stillingsområde, stilling, evt. oplysninger om pædagogikum og tilhørende fag, skattekort, NEM-konto, fri telefon, antal omsorgsdage, fravær, ferie, særlige vilkår, oplysninger vedr. barsel, orlov (periode, formål), tjenstlige forhold og evt. tjenstlige sanktioner.

Ad d) Kreditorbogholderi
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre.

Konkret er der tale om navn, adresse, cpr.nr., NEM-konto, årsag til udgiften.

Ad e) IT
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre.

Konkret er der tale om navn, titel, cpr.nr., skoletilknytning, UNI-login, brugernavn, udleveret password, logon informationer (tidspunkt, IP-adresse, netværk)

Ad f) Bygning og g) Indkøb
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder oplysninger om strafbare forhold (sidstnævnte kun hos ledende medarbejdere i tilbudsgiverens virksomhed, jf. konkret hjemmel.

Hvis databehandleren bistår den dataansvarlige med udbud af serviceydelser, hvor den dataansvarlige hidtil selv har haft medarbejderne ansat, vil der blive behandlet følgende personoplysninger: stilling, overenskomst, timetal, ansættelsesbrøk og aflønningsform.

Ad h) HR-Databasen
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre.

Konkret er der tale om cpr.nr., navn, adresse, tlf.nr., ansættelsesdato, jubilæumsdato, lønanciennitetsdato, nærmeste leder, stilling, pårørende, løn/ferie/fravær, lønsammensætning – fast løn + pension, omsorgsregnskab, opgaveportefølje (fra Lectio), holdelementer, øvrige opgaver, evt. notater og filer ang. opgavefordelingen, kompetencer (fra Lectio), undervisningskompetencer (fag), censorkompetencer (fag), evt. CV, specielle kompetencer, kursusbeviser, MUS-skema, rejseafregningsblanket, udlæg og kørselsgodtgørelse.

Ad i) GymBetaling
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre og i begrænset omfang helbredsoplysninger (art. 9), hvis eleven selv har inddateret dem.

Konkret er der tale om stamklasse, cpr.nr., elev-ID, årgang, navn, fødselsdato, studiekort-ID, telefon, adresse, kommune, land, hold, e-mail, brugernavn - UniLogin username, indmeldt pr., udmeldt pr., værgers data fra Lectio (cpr. nr., telefon, mail, adresse), lærerdata fra Lectio (cpr.nr., navn, telefon, mail), elevens egne oplysninger som tilføjes i systemet (allergier, tilmeldte skolearrangementer, pasnr. hvis eleven tilmeldes studieture til udlandet, besvarelse af samtykkespørgsmål (ifbm. studieture, offentliggørelse af fotos og videoer op skolens hjemmeside mv.)

Ad j) DocuNote ESDH
Behandlingen omfatter almindelige personoplysninger (art. 6), herunder CPR-numre og i begrænset omfang helbredsoplysninger (art. 9), hvis den dataansvarlige selv har inddateret dem.

Konkret er der tale om følgende personoplysninger om:

Medarbejdere: Stamdata: Cpr.nr., navn, adresse, mailadresse, tlf.nr., ansøgning, CV, ansættelsesdato, jubilæumsdato, lønanciennitetsdato, stilling. Ansættelseskontrakt, og herunder oplysninger om lønsammensætning (fast løn + pension), tillæg til ansættelseskontrakt. Evt. oplysninger på børn, hvis medarbejderen er berettiget til at holde orlov/omsorgsdage samt evt. oplysninger om navn og telefonnr. på nærmeste pårørende, hvis medarbejderen har oplyst det. Kompetencer: kursusbeviser, eksamensdokumenter. Eventuelt: MUS-referater, referater af fraværssamtaler og tjenstlige samtaler, ansættelsesretlige sanktioner, oplysninger om hvilke systemer medarbejderen har adgang til og dokumentation for opsigelse.

Bestyrelsesmedlemmer:
Stamdata: Cpr.nr., navn, adresse, mailadresse, tlf.nr.

STX-/HF-ansøgere:
Navn og cpr.nr. på ansøgere og de bilag, som ansøgere har sendt i forbindelse med optagelsesproceduren samt evt. klagesager.

Elever:
Navn og cpr.nr. på elever, referatet fra samtale med studievejledere, lægeerklæringer, oplysninger om fraværsårsager, eksamensbeviser, navn og cpr.nr. på værger. Eventuelt: korrespondance mellem elev/værger og skole, elevsanktioner, SPS-sager og SU-sager, klagesager, samtykkeerklæringer.

A.4. Behandlingen omfatter følgende kategorier af registrerede
Ad a) Sekretariat og Jura samt b) Datasikkerheds- og DPO-samarbejde
Personoplysningerne angår medarbejdere, elever, værger (i få tilfælde), leverandører, skadevoldere.

Ad c) Løn- og Personaleadministration
Personoplysningerne angår medarbejdere.

Ad d) Kreditorbogholderi
Personoplysningerne angår elever, medarbejdere.

Ad e) IT
Personoplysningerne angår medarbejdere, elever, værger.

Ad f) Bygning og g) Indkøb
Personoplysningerne angår medarbejdere (ved virksomhedsoverdragelse som led i udliciteringen) samt tilbudsgiveres ledende medarbejdere.

Ad h) HR-Databasen, i) GymBetaling og j) DocuNote ESDH
Personoplysningerne angår medarbejdere, elever, værger.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed
Behandlingen er ikke tidsbegrænset og varer, indtil samarbejdsaftalen opsiges, eller den dataansvarlige udtræder af et af samarbejdsområderne eller særydelserne, jf. bilag C.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Global Connect	26759722	Hørskætten 6c 2630 Tåstrup	Placering af servere samt backup (selve serveren ejes og vedligeholdes af GF)
Vipre	28117833	Spotorno allé 12 2630 Høje Taastrup	Sikker mail Ophører ultimo november
IntraNote	25797620	Papirfabrikken 20a Silkeborg	Support og konsulentopgaver på ESDH
DBVision	25832663	Fensmarkgade 3, 2200 København	Udvikling, konsulentopgaver/support på HR-Database og Gymbetaling
GatewayAPI	27364276	Buchwaldsgade 50 5000 Odense C	Levering af SMS Gateway
SAC•IT	28892977	Frydenslundsvej 30 2950 vedbæk	Sikker mail Opstart ultimo oktober

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

B.2. Varsel for godkendelse af underdatabehandlere

Den i punkt 7.3 nævnte underretning til den dataansvarlige om planlagte ændringer (tilføjelser eller udskiftning) i underdatabehandlere sker til Gymnasiefællesskabets Forretningsudvalg for det pågældende fagområde, jf. Samarbejdsaftalens Bilag 9.

Forretningsudvalget modtager underretningen på vegne af styregruppen. Hvis forretningsudvalget tager den planlagte ændring til efterretning, gennemfører databehandleren den planlagte ændring. Forretningsudvalget orienterer om ændringen på førstkommende styregruppemøde.

Forretningsudvalget kan fremsætte rimelige og konkret begrundede indsigelser imod en foreslået ændring og om nødvendigt henskyde emnet til styregruppen, hvis det vurderes nødvendigt.

B.3 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

GF skal én gang årligt indhente en revisionserklæring eller en ledelseserklæring fra en uafhængig tredjepart om underdatabehandlerens overholdelse af denne databehandleraftale med tilhørende bilag.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandleren (Gymnasiefællesskabet (GF)) er et administrativt fællesskab mellem 25 statsligt selvejende gymnasieskoler på Undervisningsministeriets ressortområde (Partnerskoler). Databehandleren har til huse i rektorboligen på Roskilde Gymnasium, som er værtsinstitution for det administrative fællesskab. Grundlaget for samarbejdet fremgår af en samarbejdsaftale med tilhørende bilag, som findes på GF's hjemmeside https://www.gymnasiefaellesskabet.dk/gym/.

Formålet med den dataansvarliges deltagelse i det administrative fællesskab er effektivt at få løst administrative og tekniske opgaver med høj kvalitet og forsyningssikkerhed.

Den enkelte partnerskole er dataansvarlig for den behandling af personoplysninger, der er forbundet med skolens deltagelse i et konkret samarbejdsområde. Partnerskolen – den dataansvarlige – vælger selv, hvilke samarbejdsområder, skolen ønsker at deltage i. Samarbejdsområderne er beskrevet i bilag A.

Den til samarbejdsområdet hørende behandling af personoplysninger er omfattet af denne databehandleraftaleinstruks.

Den dataansvarlige instruerer hermed databehandleren om at foretage behandling af de beskrevne personoplysninger til brug for drift og levering af de i Samarbejdsaftalen aftalte ydelser. Databehandleren må ikke anvende personoplysningerne til andre formål på vegne af den dataansvarlige.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen som altovervejende udgangspunkt omfatter "almindelige personoplysninger", jf. databeskyttelsesforordningens art. 6, herunder en større mængde fortrolige personoplysninger i form af cpr-numre.

Kun i begrænset omfang er der tale om personoplysninger, der er omfattet af databeskyttelsesforordningens art. 9 om "særlige kategorier af personoplysninger. Der skal derfor ikke 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 – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Overordnet set har databehandleren indført en række politikker og procedurer, der sikrer, at databehandleren kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

Databehandleren har etableret en organiseringen af persondatasikkerheden samt udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.

C.2.1 Databehandlerens medarbejdere

Opmærksomhed på databeskyttelse i hele ansættelsesforløbet og i det daglige arbejde
Databehandleren har procedurer for rekruttering og fratrædelse af medarbejdere samt retningslinjer for uddannelse og instruktion af medarbejdere, der behandler personoplysninger, herunder gennemførelse af løbende awareness-træning i form af informationsmails, læringsvideoer, opslag og husmøder med drøftelser om konkrete emner med relevans for databeskyttelsen.

Tværgående team
Databehandleren har etableret et tværgående team i organisation, som mødes ca. hver 6. uge til drøftelse af aktuelle emner vedr. databeskyttelse, fx videndeling om myndighedskrav og drift samt koordinering og forankring af konkrete opgaver af relevans for databeskyttelse og it-sikkerhed. Der holdes ikke møder i ferieperioderne.

Fortrolighed og lovbestemt tavshedspligt
Databehandleren har indført politikker og procedurer, der sikrer fortrolighed ved behandlingen af personoplysninger. Alle medarbejdere hos databehandleren har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed.

C.2.2 Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering
Databehandleren har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed.

Databehandlerens risikovurderinger afdækker fx behovet ift. tekniske og organisatoriske sikkerhedsforanstaltninger, at der er funktioner til adgangskontrol, overvågning af autoriserede brugeres trafik i systemet, struktureret og målrettet sletning mv., og at funktionerne bruges aktivt.

Beredskabsplaner
Databehandleren har etableret beredskabsplaner, således at databehandleren rettidigt kan genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. GF har etableret et kriseberedskab, der træder i kraft i disse tilfælde.

Databehandleren har udformet detaljerede beredskabsplaner og planer for retablering af systemer og data, der blandt andet sikrer personuafhængighed i forbindelse med aktivering af beredskabet og retableringen. Planerne er i kopi opbevaret sikret uden for databehandlerens it-systemer. Planerne afprøves og revideres løbende i forbindelse med ændringer i systemer mv.

Håndtering af inddata- og uddatamaterialer
Databehandleren har indført procedurer for håndtering af inddata, der sikrer, at inddatamateriale kun må anvendes af de medarbejdere, der er beskæftiget med opgaver, der relaterer sig til inddatamaterialet/behandlingen af personoplysninger. Inddatamateriale opbevares aflåst, når det ikke anvendes. Inddatamateriale slettes eller tilintetgøres, når det ikke længere anvendes til behandlingens formål eller til kontrol.

Databehandleren har indført procedurer for håndtering af uddata, der sikrer, at uddatamateriale kun må anvendes af de medarbejdere, er er beskæftiget med behandlingen af personoplysninger. Uddatamateriale opbevares aflåst, når det ikke anvendes, således at uvedkommende ikke kan tilgå eller gøre sig bekendt med de behandlede personoplysninger. Uddatamateriale slettes eller tilintetgøres, når det ikke længere anvendes til behandlingens formål.

Opbevaring af personoplysninger
Databehandleren har indført procedurer, der sikrer, at opbevaring af personoplysninger alene foretages i overensstemmelse med samarbejdsaftalen med den dataansvarlige og listen over lokationer i den tilhørende databehandleraftale.

Fysisk adgangskontrol
Databehandleren har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Gæster, leverandører og andre besøgende ledsages.

Databehandleren har indført procedurer, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov. Serviceleverandører, der har behov for adgang for at varetage opsyn eller vagt, er godkendt af ledelsen. Tildelte adgange til serverrum gennemgås og revideres ved ændringer og mindst én gang årligt.

Fysisk sikkerhed
Databehandleren har indført procedurer, der sikrer, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger. Servere er således opbevaret i et særligt indrettet serverrum med fysisk og elektronisk adgangskontrol og logning af adgange. Serverrummet er sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald og overspænding. Systemer til miljømæssig sikring af driftsfaciliteter er serviceret og vedligeholdt løbende efter de respektive leverandørers forskrifter. Driftsmiljøet er overvåget.

Logisk adgangssikkerhed
GF har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages hver 6. måned en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Fjernarbejdspladser og fjernadgang til systemer og data
Databehandleren har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for databehandlerens lokaler og fjernadgang til systemer og data sker via VPN-forbindelser og tofaktor autentifikation for udvalgte medarbejdere.

Eksterne kommunikationsforbindelser

Databehandleren har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mail og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS.

Kryptering af personoplysninger
Databehandleren har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis. Der er ikke kryptering på databehandlerens fildrev.

Databehandleren har indført procedurer, der sikrer, at data på personlige enheder, der ikke er beskyttet af særlige sikkerhedsforanstaltninger, er krypteret ved ibrugtagning, således at adgang til data alene er mulig for autoriserede brugere. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

De algoritmer og niveauer for kryptering, der er anvendt til kryptering af enheder, servere og data, risikovurderes løbende i forhold til det aktuelle trusselsniveau.

Firewall
Databehandleren har indført procedurer, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Netværkssikkerhed
Databehandleren har indført procedurer, der sikrer, at netværk i forhold til anvendelse og sikkerhed er opdelt i et antal virtuelle netværk (VLAN), hvor trafik mellem de enkelte virtuelle netværk kontrolleres af firewall. Servere med indbygget firewall benytter denne til at sikre, at der kun gives adgang til nødvendige services.

Antivirusprogram
Databehandleren har indført procedurer, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer i forhold til det aktuelle trusselsniveau, og der er opsat en løbende overvågning af disse systemer, herunder periodisk test for funktionalitet.

Sårbarhedsscanning og penetrationstests
Databehandleren har indført procedurer, der sikrer, at systemer er indført med henblik på at identificere og imødegå tekniske sårbarheder i applikationer, services og infrastruktur, således at tab af fortrolighed, integritet og tilgængelighed af systemer og data undgås.

Sikkerhedskopiering og retablering af data
Databehandleren har indført procedure, der sikrer, at systemer og data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud. Sikkerhedskopier opbevares på alternativ lokation. Sikkerhedskopier er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerhedskopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Vedligeholdelse af systemsoftware

Databehandleren har indført procedurer, der sikrer, at systemsoftware opdateres løbende efter leverandørernes forskrifter og anbefalinger. Procedurer for Patch Management omfatter operativsystemer, kritiske services og software installeret på servere og arbejdsstationer.

Logning i systemer, databaser og netværk
Databehandleren har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data, og logdata gennemgås løbende for anvendelighed og unormal adfærd. Logdata er sikret mod tab og sletning.

Overvågning
GF har indført procedurer, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Reparation og service samt bortskaffelse af it-udstyr
Databehandleren har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier og diske registreres og destrueres in-house eller af certificeret leverandør.

Afprøvning, vurdering og evaluering
Databehandleren har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

C.2.3 Databeskyttelse gennem design og standardindstillinger
Der er udarbejdet forretningsgangsbeskrivelser og setup-beskrivelser, der sikrer styring af udviklings- og ændringsopgaver af databehandlerens ESDH, HR-databasen og Gymbetaling, dvs. de systemer, som databehandleren er ansvarlig for, skal understøtte databeskyttelse gennem design og standardindstillinger.

Udviklings-, test- og produktionsmiljø er adskilte, og der er etableret funktionsadskillelse mellem medarbejdere, som arbejder i udviklingsafdelingen og i drifts- og supportafdelingen. Idet databehandleren har få medarbejdere ansat, sker al udvikling – for at opnå funktionsadskillelse – via eksterne konsulenter. Enhver udviklings- og ændringsopgave gennemløber et testforløb, og der anvendes anonymiserede produktionsdata som i HR-databasen og Gymbetalingsdatabasen. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, således at det er muligt at geninstallere tidligere versioner.

Sletning og tilbagelevering af personoplysninger
Databehandleren har indført politikker og procedurer, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

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:

Databehandlerens medarbejdere skal være uddannet i korrekt håndtering af data, understøttelse af de registreredes rettigheder og håndtering af sikkerhedshændelser i henhold til gældende lovgivning.

Databehandleren har implementeret procedurer for håndtering af sikkerhedshændelser, som ajourføres efter behov. Den dataansvarlige kan få indsigt i disse ved henvendelse.

Ved sikkerhedshændelser, der kræver anmeldelse til Datatilsynet, har databehandleren procedurer og ressourcer til at assistere den dataansvarlige i udfyldelsen af følgende punkter til en anmeldelse af til Datatilsynet:

- databruddets karakter.
- beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden.
- beskrive de foranstaltninger, som der har været truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Omfanget af databehandlerens assistance i henhold til databrud vil afhænge af, i hvilken grad denne har adgang til de personoplysningerne, som den dataansvarlig behandler.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i følgende perioder, hvorefter de slettes hos databehandleren:

- I rådgivningssager: senest 3 år fra udgang af det kalenderår, hvori sagen er afsluttet (Sekretariat, Jura, Datasikkerhed, DPO, Indkøb og Bygning)
- 5 år fra udgang af det kalenderår, som lønbilag eller bogføringsbilag vedrører (Løn og Bogholderi)
- 90 dage i back up (IT)
- 1 år i logningsrapporter (ESDH).

Sletterutinerne for personoplysninger i DocuNote, HR-databasen og Gymbetaling fremgår af GF's forretningsgang og setup for de to systemer.[4]

Ved den dataansvarliges udtræden af et eller flere samarbejdsområder skal databehandleren enten slette eller tilbagelevere de af samarbejdsområdet omfattede personoplysningerne, jf. pkt. 11.1.

Den dataansvarlige skal senest 45 dage inden tidspunktet for udtræden skriftligt meddele databehandleren, om alle personoplysningerne skal slettes eller tilbageleveres til den dataansvarlige. Hvis databehandleren ikke modtager en sådan skriftlig meddelelse, skal databehandleren af egen drift slette personoplysningerne hurtigst muligt efter tidspunktet for udtræden. I det tilfælde, hvor personoplysningerne tilbageleveres til den dataansvarlige, skal databehandleren ligeledes slette eventuelle kopier.

Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever den datasvarliges meddelelse. Evt. omkostninger forbundet med tilbageleveringen betales af den dataansvarlige.

[4] Disse findes på https://www.gymnasiefaellesskabet.dk/gym/index.php, under fanen Intranet.

Hvis myndighedskrav eller særlovgivning pålægger databehandleren fortsat opbevaring af personoplysninger, bevarer databehandleren personoplysningerne i det krævede antal åremål. Dette gør sig eksempelvis gældende på med bogføringsmateriale.

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:

- Skolegade 3, Domkirkepladsen, 4000 Roskilde
- På de i bilag B nævnte lokaliteter.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
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.

Hvis den dataansvarlige ønsker at overføre personoplysninger til et tredjeland, skal databehandleren underrette den dataansvarlige som anført i pkt. 8 ovenfor, og den dataansvarlige kan gøre eventuel indsigelse. Ved indsigelse skal den dataansvarlige komme med en saglig begrundelse herfor, herunder opstille betingelser for overførslen.

Den dataansvarlige indestår for, at der findes et gyldigt overførselsgrundlag for den konkrete dataoverførsel, jf. databeskyttelsesforordningens kap. V.

Databehandleren er opmærksom på, at support i enhver form, der er tiltænkt at ske fra en fysisk lokalitet i et tredjeland, og hvor der vil være mulighed for, at supportmedarbejderne kan tilgå personoplysninger, er en overførsel af personoplysninger til et tredjeland.

Det gælder, uanset om personoplysningerne er krypterede, uanset medarbejdernes ansættelsesforhold, uanset det tekniske set up (kiggeadgang, Teamviewer, fjernadgang til server med lokalitet i EU mv.) og uanset supportmedarbejdernes evne til at forstå dansk.

Databehandleren tilstræber i sin dialog med sine underdatabehandlere at skabe fokus på dette problem og sikre, at underdatabehandleres tekniske support i tredjelande ikke får tilsendt/adgang til personoplysninger, men derimod kun fuldt ud anonymiserede oplysninger samt tekniske data.

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

Databehandleren skal hvert år for egen regning indhente følgende:

- en revisionserklæring i henhold til standarden ISAE 3000, som udformes af en uafhængig tredjepart, og som udtaler sig om databehandlerens overholdelse af nærværende databehandleraftale, databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser
- en revisionserklæring i henhold til standarden ISAE 3402, som udformes af en uafhængig tredjepart, og som udtaler sig om databehandlerens it-sikkerhed og evnen til at opretholde fortrolighed, ægthed og tilgængelighed i de systemer, som databehandlingen foretages i.

Begge revisionserklæringer skal være type 2-erklæringer og omfatte en periode på 12 måneder. For ISAE 3402-erklæringens vedkommende skal den aflægges senest den 15. januar, jf. bkg. nr. 2110 af 24/11/2021 om revision og tilskudskontrol m.m. ved institutioner for erhvervsrettet uddannelse, alment gymnasiale uddannelser og almen voksenuddannelse mv., bilag 1, pkt. 2.3. Bekendtgørelsen pålægger administrative fællesskaber mv., der stiller applikationer og infrastruktur til rådighed at indhente en ISAE 3402-erklæring.

Af ressourcehensyn tilstræber databehandleren at aflægge ISAE 3000-erklæringen, så den dækker den samme periode, som ISAE 3402-erklæringen.

Revisionserklæringerne fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringerne og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen, 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.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne, hvorfra databehandleren 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.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Som led i ovennævnte revision indhentes revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer kan anvendes i overensstemmelse med disse bestemmelser:

- ISAE 3402
- ISAE 3000
- Ledelseserklæringer
- ISO 27001-dokumentation.

Erklæringerne kan på forespørgsel fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen/dokumentationen og kan i sådanne tilfælde anmode om en ny revisionserklæring/dokumentation under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen/dokumentationen, 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.

Databehandleren eller en repræsentant for databehandleren 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 databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Bilag D Parternes regulering af andre forhold

Ingen

Changelog

VERSION	ÆNDRINGER
Maj 2021	Konvertering af eksisterende databehandleraftale til nærværende standardbestemmelser.
Maj 2022	Godkendte underdatabehandlere (Bilag B) ajourført: e-Boks til Digital Post tilføjet Heimdal Security A/S Opdateret DPOs kontaktoplysninger.
Juni 2022	Godkendte underdatabehandlere (Bilag B) ajourført: GatewayAPI.
November 2023	Godkendte underdatabehandlere (Bilag B) Ajourført: Vipre (Sikker mail) ophører ultimo november og erstattes af SAC•IT. Bilag c.4 Opbevaringsperiode/sletterutine Bilag C, C.7: bkg. nr. 956 af 6/7 2017 erstattet af bkg nr. 2110 af 24/11/2021.

Solrød Gymnasium	Frederiksværk Gymnasium	Tårnby Gymnasium & HF
Roskilde Katedralskole	Himmelev Gymnasium	Greve Gymnasium
Gladsaxe Gymnasium	Allerød Gymnasium	Rungsted Gymnasium
Rysensteen Gymnasium	Nordfyns Gymnasium	Køge Gymnasium
Aurehøj Gymnasium	Espergærde Gymnasium & HF	Ørestad Gymnasium
Gefion Gymnasium	Roskilde Gymnasium	Virum Gymnasium

Sct. Knuds Gymnasium

Nyborg Gymnasium

Egedal Gymnasium & HF

Borupgaard Gymnasium

Nørre Gymnasium

Helsingør Gymnasium

Gentofte HF