Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Navn: N. Zahles Gymnasieskole
CVR: 62513217
Adresse: Nørre Voldgade 7
Postnummer og by: 1358 København K
Land: Danmark

herefter "den dataansvarlige"

og

ExamCookie ApS
CVR 38463888
Peder Skrams Gade 1, 1. tv.
9000 Aalborg
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

Denne aftale er sidst opdateret d. 23 marts 2024 i forbindelse med Datatilsynets ændringer for standardkontraktsbestemmelser.

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 leveringen af ExamCookie monitorerings software 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.

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

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

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående generelle skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 3 måneder inden anvendelsen af den pågældende underdatabehandler. 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 generel 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, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og 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 24 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, se bilag C punkt 4.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de 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 nærmeret 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 på datoen for begge parters underskrift heraf.

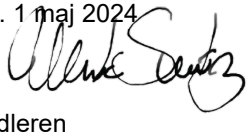
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

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	Ulrik Sieverts
Stilling	IT-ansvarlig
Telefonnummer	33697993
E-mail	us@zahles.dk
Dato	d. 1 maj 2024
Underskrift	

På vegne af databehandleren

Navn	Morten Claudius Jakobsen
Stilling	Direktør
Telefonnummer	27626794
E-mail	Kontakt@examcookie.dk
Dato	d. 1 maj 2024
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.

Den dataansvarlige

Navn	Ulrik Sieverts
Stilling	IT-ansvarlig
Telefonnummer	33697993
E-mail	us@zahles.dk

Databehandleren

Navn	Morten Claudius Jakobsen
Stilling	Direktør
Telefonnummer	27626794
E-mail	Kontakt@examcookie.dk

Bilag A Oplysninger om behandlingen

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

Ved brugen af ExamCookie som monitoreringsværktøj er formålet
- Behandling af eksaminandernes personnummer, jf. databeskyttelseslovens § 11, stk. 1, med henblik på entydig identifikation af eksaminanderne for at forbygge og forhindre eksamenssnyd.
- Mulighed for at få be- eller afkræftet om eksaminanden har kommunikeret utilsigtet, anvender ikke-tilladte hjælpemidler eller i øvrigt overtræder eksamensbestemmelserne.
- At eksaminandens besvarelse ikke er udarbejdet af tredjemand.

Institutionen vil her have mulighed for at kunne få be- eller afkræftet en sådan formodning og i situationen agere over for egne elever. Institutionerne vil oftest også anvende monitoreringsløsningen til at foretage stikprøver, altså undersøge om elever har snydt, men uden at der på forhånd er mistanke om at eleven har snydt. Værktøjet vil herved udgøre et supplement til det tilsyn, som institutionerne allerede fører med de skriftlige prøver.

Institutionens behandling af personoplysninger i monitoreringsværktøjet har hjemmel i databeskyttelsesforordningens artikel 6 stk. 1 litra e (offentlig myndighedsudøvelse), som er udmøntet i (retsinformation.dk):
- §14, §15 og §20 i ” Bekendtgørelse om prøver og eksamen i de almene og studieforberedende ungdoms- og voksenuddannelser” (bek. nr. 343 af 08/04/2016)
- §5 i bekendtgørelse om visse regler om prøver og eksamen i de gymnasiale uddannelser (bek. nr. 1276 af 27. november 2017)
- §1 i ”Bekendtgørelse om adgangen til at medbringe og anvende udstyr, herunder digitale hjælpemidler, under prøver i de gymnasiale uddannelser” (bek. nr. 224 af 19/03/2018)

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

Data der behandles af Databehandleren i ExamCookie opdeles i 2 kategorier:
A. 2.2 Indsamlet data fra ExamCookie klienten der indsamles under eksamen, og udelukkende i den tidsramme eksamen er angivet til af institutionen, disse opbevares i op til 3 måneder efter eksamen se bilag C punk 4:
- Relevante skærmbilleder
- Procesliste
- Ny kopieret tekst og billeder i computerens clipboard
- Programmer anvendt i front på computeren
- URL-adresser anvendt under eksamen
- Netværkskort

Eksamensdata indsamlet fra klienten er krypteret og psedonymiseret således data ikke kan tilkobles den konkrete person data er indsamlet fra. Data kan derimod tilkobles en konkret person efter en dekryptering, som gøres med henblik på at påvise eksamenssnyd som beskrevet i hjemmel for at indsamle data. Data er krypteret med en unik krypteringsnøgle.

A. 2.3 Data der anvendes fra UNI-Sync mellem pakke ved UVM tilslutning.dk, anvendes alene til at oprette og identificere den enkelte elev i ExamCookie.
- Kursistens fulde navn
- Kursistens klasse samt eventuelle hold på institutionen
- Kursistens skole & årgang

- Kursistens eksamensplan
- Kursistens UNI-Login bruger ID til identificering af hver kursist som unik bruger (password er krypteret)
- Kursistens personnummer, hvor dette behandles under pseudonymisering og ikke er synligt i backenden
- Personoplysninger opbevares krypteret og pseudonymiseret som en ekstra sikkerhedsforanstaltning, hvor krypteringsnøgler (HASH nøglen) kun er tilgængelig for én betroet medarbejder i ExamCookie.

Data er opdelt i to kategorier, eksamensdata indsamlet fra klienten samt registreringsdata fra UNI-sync aftalen. Disse er krypteret med separate krypteringsnøgler. Alt data er krypteret både i 'in transmission', 'in rest' og 'in motion'.
Data i klar tekst er derfor ikke tilgængeligt for underdatabehandler, Microsoft Azure. Adgang til denne data kræver derfor et login gennem 2-faktor godkendelse, krypteringsnøglen (HASH nøglen) samt én specifik IP adresse, hvor dette igen kun er én betroet medarbejder der har adgang til disse.

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

Der behandles personoplysninger, herunder fortrolige oplysninger, i form af navnlig:
- Skærmbilleder af eksaminandens computer
- Registrering af eksaminandens browserhistorik i de timer, som eksamen varer (browserhistorikken registreres hverken før eller efter eksamen)
- Kursistens personoplysninger til identificering af kursisten fra UNI-Sync mellem pakke beskrevet i punkt A. 2.3 over.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kursister / elever

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

Der henvises til beskrivelsen i punkt 14. i denne Databehandleraftale.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft Azure	Company number 600413485	Holland & Tyskland	Server til opbevaring

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.
Der er i aftalen mellem ExamCookie og Microsoft Azure indgået aftale om at data udelukkende opbevares på sikret datacentre i Holland & Tyskland.
ExamCookie forpligter sig alene til at anvende en dansk siddende Microsoft Azure support, hvis dette skulle blive aktuelt. ExamCookie har udarbejdet TIA for Microsoft Azure.

B.2. Varsel for godkendelse af underdatabehandlere

Se punkt. 7. stk. 3

B.3. Information om GDPR aftale mellem databehandler & underdatabehandler

Link til GDPR information fra underdatabehandleraftale med Micorosoft Azure:
https://docs.microsoft.com/da-DK/compliance/regulatory/gdpr?view=o365-worldwide

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:

Kursistens personoplysninger behandles for at oprette kursisten i softwaren når denne aftale er indgået samt der er oprettet en UVM UNI-Sync aftale gennem tilslutning.dk.
Kursistens monitorerings data fra eksamen indsamles i institutionens personlige backend i ExamCookie og behandles af den Dataansvarlige. Ønsker den Dataansvarlige hjælp til at behandle indsamlet data fra kursisten, skal dette ske efter instruks fra den Dataansvarlige.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

At databehandleren indsamler fortrolige oplysninger mhp. at kunne dokumentere evt. eksamens- snyd. I lyset heraf skal databehandleren løbende fastsætte passende tekniske og organisatoriske sikkerhedsforanstaltninger, herunder efter retningslinjerne i pkt. 6(2) om behandlingssikkerhed.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Databehandleren sikre en høj standard i sikkerhedsniveauet ved eksempelvis at indføre følgende foranstaltninger:

- Det er kun én person i virksomheden der har adgang til data, og denne person er partner i virksomheden og har indgået fortrolighedserklæring i denne sammenhæng.

- Personoplysninger opbevares krypteret og pseudonymiseret som en ekstra sikkerhedsforanstaltning, hvor krypteringsnøgler (HASH nøglen) kun er tilgængelig for den betroede medarbejder i ExamCookie og derfor ikke tilgængelig for Underdatabehandlere.

- Databehandleren har ikke data opbevaret fysisk på nogen computer og kan kun tilgå dette gennem tilslutning.dk eller Microsoft Azure. Disse er valgt for at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed. For yderligere information om de sikkerhedsforanstaltninger og certificeringer Microsoft Azure gennemgår, henvises der til deres ”Compliance” rapport: https://azure.microsoft.com/en-us/resources/microsoft-azure-compliance-offerings/

- Databehandleren har etableret logning i systemer, databaser og netværk af følende forhold:
1. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
2. Sikkerhedshændelser omfattende:
    - Ændringer i logopsætninger, herunder de-aktivering af logning.
    - Ændringer i systemrettigheder til brugere.
    - Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.

- Databehandleren har etableret tekniske foranstaltninger til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Dette

- Databehandlerens betroede medarbejder kan kun få adgang til behandlet data gennem en 2-faktor godkendelse for at minimere risiko.

- Udover 2-faktor godkendelse kræver det én specefik IP adresse for at kunne tilgå data, som kun den betroede medarbejder har adgang til.

- Databehandleren har udarbejdet og udleveret informationsmateriale til den dataansvarlige, i forhold til en risiko og konsekvensanalyse af it-sikkerheden for den Dataansvarlige.

- Der foretages flere gange årligt en løbende evaluering og afprøvning af behandlingssikkerhed af Databehandleren.

- Databehandleren sikre at data under transmissions sendes krypteret, låst bag en krypteringsnøgle, som kun er tilgængelig for den betroede medarbejder.

- Adgang til institutionens unikke backend (webinterface), kræver ligeledes login gennem 2-faktor godkendelse.

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:

Databehandleren kan efter instruks fra den Dataansvarlige minimere adgang til data.
Databehandleren kan efter instruks fra den Dataansvarlige bistå med brugerroller, oprettelse og nedlæggelse af disse og heraf adgang til data.
Databehandleren kan efter instruks fra den Dataansvarlige slette specifikt data eller alt data.

Databehandleren bistår den registrerede, i dette tilfælde kursisten/eleven, i at få indsigt i hvilke data der er indsamlet.

Databehandleren sikrer at der i organisationen altid er én betroet medarbejder, der har mulighed for at bistå den dataansvarlige i overensstemmelse med bestemmelse 9.1 og 9.2.
Databehandleren sikrer at der løbende udvikles tekniske foranstaltninger med henblik på at kunne bistå den dataansvarlige.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i 90 dage, hvorefter de slettes hos databehandleren. I særlige tilfælde kan personoplysninger opbevares i op til 3 måneder, fx ved mistanke om snyd eller behandling f en klagesag, hvor oplysningerne indgår i sagsbehandlingen.

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

Sletterutine er følgende:

a. Indsamlet data slettes automatisk efter en 90 dages periode.

b. Indsamlet data kan slettes manuelt af databehandleren indenfor maksimalt 48 timer hvis der skulle være et ønske fra den dataansvarlige om dette.
c. Den dataansvarlige har gennem tilslutning.dk tilkoblet en 'mellem data-pakke', hvor det er givet at denne aftale kan opsiges af den dataansvarlige på tilslutning.dk, på ethvert givent tidspunkt, og derved vil data automatisk blive slettet af databehandleren indenfor maksimalt 48 timer.

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:

Virksomhedens adresse, Peder Skrams Gade 1, 1 TV, 9000 Aalborg, Danmark, indtil virksomheden eventuelt flytter adresse.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Der overføres ikke data til tredjelande. Data bliver som beskrevet i denne aftale bilag B, opbevaret i Holland & Tyskland, efter aftale med Microsoft Azure. Eventuel support fra Microsoft Azure vil ske fra deres danske support i henhold til aftalen med Microsoft Azure. ExamCookie har deaktiveret support funktion i Microsoft Azure for at sikre data ikke kan overføres til tredjelande. ExamCookie har en dansk kontaktperson der kan assistere hvis dette skulle blive nødvendigt, dette vil alene benyttes efter overvejelse og accept af databehandler samt dataansvarlig.

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

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

Databehandleren skal en gang årligt for egen regning indhente en revisionserklæring, ISAE3000 erklæring, fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:
- ISAE3000

Revisionserklæringer fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring for egen regning 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.

Bilag D Parternes regulering af andre forhold

Der er ikke aftalt eller reguleret andre forhold.