



Notat

Vedrørende: Opgaver og ansvar for den dataansvarlige i forbindelse med anvendelse af private leverandørers digitale monitoreringsværktøjer

Skrevet af: Hany Dughaim

Fordeling: Lederforeninger

Baggrund

Under afvikling af gymnasiernes eksamener og prøver skal institutionerne sikre, at prøverne gennemføres under forhold, der er egnede til at udelukke, at eksaminanden kommunikerer utilsigtet jf. § 14 i *Bekendtgørelse om prøver og eksamen i de almene og studieforberedende ungdoms- og voksenuddannelser*. I den forbindelse kan institutionerne fastsætte lokale retningslinjer for anvendelse af digitale monitoreringsværktøjer som hjælp til at sikre, at eksamensreglerne overholdes jf. § 6.

Anvendelse af digitale monitoreringsværktøjer indebærer registrering af personhenførbare oplysninger om elever. Institutionerne skal derfor være opmærksomme på databeskyttelsesforordningens regler om behandling af personoplysninger.

Ved anvendelse af monitoreringsværktøjer, som er indkøbt hos private leverandører, gælder opgaver og ansvar for den dataansvarlige og databehandleren alene i relationen mellem institutionen og den private leverandør. Dette notat giver en redegørelse for de overordnede opgaver og forpligtelser som er pålagt den dataansvarlige i forbindelse med anvendelse af private leverandørers monitoreringsværktøjer.

Indhold

Hvem er dataansvarlig?

I henhold til databeskyttelsesforordningens artikel 4 nr. 7 er den dataansvarlige den, der *"alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger"*.

Dataansvaret for behandling af personoplysninger i monitoreringsværktøjet er hos de enkelte institutioner for gymnasiale uddannelse, fordi behandlingen af elevers oplysninger til brug for monitorering under prøveafviklingen sker til institutionens formål og på institutionens vegne. Monitoreringsværktøjet er således et værktøj, som kan hjælpe den enkelte institution, hvis institutionen konkret oplever, at der ved skriftlige stedprøver på den enkelte institution er mistanke om snyd. 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 monitoringsløsningen til at foretage stikprøver, altså

Styrelsen for It og Læring
Afdelingen for Data og
Digitalisering

Vester Voldgade 123
1552 København V
Tlf.: 35 87 88 89
E-mail: stil@stil.dk
www.stil.dk
CVR-nr.: 13223459

15. april 2019

Sagsnr.: [Click here to enter text.](#)

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.

Hvad er behandlingens hjemmel?

Institutionernes behandling af personoplysninger i monitoreringsværktøjet har hjemmel i databeskyttelsesforordningens artikel 6 stk. 1 litra e (offentlig myndighedsudøvelse).

Institutionernes offentlige myndighedsudøvelse i forbindelse med kontrol mod snyd og anden overtrædelse af eksamensreglerne er udfoldet i dansk lovgivning som angivet neden for. Det er muligt for institutioner at kræve af eleverne, at de skal anvende en monitoreringsløsning, når kravet fremgår af skolens lokale retningslinjer for prøvernes tilrettelæggelse og planlægning.

Hjemlen er i § 5 i *bekendtgørelse om visse regler om prøver og eksamen i de gymnasiale uddannelser* (Bekg. nr. 1276 af 27. november 2017). For elever, der er omfattet af reglerne før gymnasireformen, herunder de fleste af de elever, der pt. går i 3.g., er der hjemmel i § 6, stk. 4, i *den almene eksamensbekendtgørelse* (Bekg. nr. 343 af 8. april 2016) om institutionernes mulighed for at fastsætte yderligere retningslinjer for tilrettelæggelse og planlægning af prøver. Det er i begge tilfælde et krav, at det fremgår af institutionens retningslinjer, at der anvendes monitorering ved prøverne. Institutionerne kan bestemme, om de vil pålægge eleverne at anvende monitoreringsløsningen eller om det skal være frivilligt.

Databehandleren

Leverandøren bag det monitoreringsværktøj, som institutionen vælger at anvende, er databehandler, fordi leverandøren indsamler og opbevarer personoplysninger på eleverne i monitoreringsværktøjet på vegne af den dataansvarlige institutions formål.

Institutionerne er som dataansvarlige forpligtet til at indgå en databehandleraftale med leverandøren forud for behandlingen af personoplysninger. Databehandleraftalen skal opfylde minimumskravene til indholdet af en databehandleraftale som fremgår af databeskyttelsesforordningens artikel 28 stk. 3.

Dette indebærer, at databehandleraftalen skal indeholde følgende:

- Behandlingens genstand og karakter – *dvs. en beskrivelse af databehandlerens opgave samt formålet med behandlingen af personoplysninger.*
- Typen af personoplysninger – *dvs. hvilke oplysninger, der registreres i monitoreringsværktøjet.*
- Kategorier af registrerede – *dvs. angiv hvilke elever, der er tale om, angiv også lærere, rektor, uddannelsesleder og administrative medarbejdere, hvis oplysninger om disse registreres.*

- En angivelse af behandlingens varighed – *dvs. at der eksplicit skal tages stilling til, hvor længe data skal opbevares i systemet og dermed også hvornår data skal slettes hos databehandleren. De kriterier som kan pålægges vægt er fx den almindelige sagsbehandlingstid ved bedømmelse og vurdering af mistanke om snyd samt eventuel klageperiode.*
- En angivelse af, at databehandleren kun må behandle oplysninger efter dokumenteret instruks fra den dataansvarlige – *det er derfor vigtigt at afgrænse formålet og behandlingens genstand oven for.*
- En angivelse af, at overførsler til tredjelande kun må ske efter dokumenteret instruks, medmindre det er krævet i henhold til lovgivning. I så fald underrettes den dataansvarlige forud for overførslen.
- En angivelse af, at databehandleren sikrer sig, at medarbejdere har forpligtet sig til fortrolighed eller er underlagt passende lovbestemt tavshedspligt.
- En angivelse af, at databehandleren skal iværksætte alle nødvendige og passende sikkerhedsforanstaltninger som krævet i henhold til artikel 32 – *dvs. at den dataansvarlige skal sikre sig, at der i aftalen er konkretiseret, hvilke sikkerhedsforanstaltninger databehandleren skal iværksætte. Det kan fx være krav om logning, kryptering, pseudonymisering osv.*
- En angivelse af databehandlerens eventuelle underdatabehandlere, og hvor disse har adresse – *det skal i aftalen angives, at databehandleren ikke må gøre brug af en anden databehandler uden forudgående specifik eller generel skriftligt godkendelse fra den dataansvarlige. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.*
- En angivelse af at databehandlerens eventuelle underdatabehandlere skal være pålagt de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.
- En angivelse af, at databehandleren forpligtes til at bistå den dataansvarlige med opfyldelse af de registreredes rettigheder i det omfang, det er nødvendigt og relevant, såvel som at bistå med at overholde databeskyttelsesforordningens artikel 32-36.
- En angivelse af, at databehandleren sletter eller tilbageleverer oplysninger til den dataansvarlige efter databehandleraftalens ophør.
- En angivelse af, at databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i artikel 28, til rådighed for den dataansvarlige, *fx ved at give mulighed for og bidrage til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.*

- En angivelse af, at databehandleren omgående underretter den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Både databehandleren og den dataansvarlige skal opbevare en elektronisk kopi af aftalen.

Institutionerne kan med fordel anvende Datatilsynets skabelon for databehandleraftalen (bilag 1), da den tager højde for alle minimumskravene. Hvis leverandøren sender sin egen skabelon, kan institutionen også underskrive denne, men institutionen skal sikre, at den indeholder ovennævnte minimumskrav til en databehandleraftale. Det anbefales, at institutionerne kontakter deres databeskyttelsesrådgiver (DPO), hvis de har en sådan, for at få bistand til indgåelse af databehandleraftalen.

Risikovurdering

Det er i henhold til databeskyttelsesforordningens artikel 32 et krav, at der udarbejdes en risikovurdering af behandlingen af personoplysninger, inden behandlingen starter.

Det betyder, at institutionen skal foretage en risikovurdering af monitoringsværktøjet, inden det tages i brug. Der er ikke nogen formkrav til risikovurderingen, og udarbejdelsen af den behøver ikke være tidskrævende og omfattende. Institutionen skal blot kunne dokumentere, at man har overvejet eventuelle risici, der er mod den registreredes databeskyttelsesrettigheder og øvrige frihedsrettigheder ved anvendelse af monitoringsværktøjet.

Det er derefter op til den dataansvarlige at iværksætte de relevante og nødvendige organisatoriske og tekniske sikkerhedsforanstaltninger, der så vidt muligt imødekommer de identificerede risici. Disse sikkerhedsforanstaltninger skal angives i databehandleraftalen.

For yderligere vejledning kan der henvises til www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf.

Oplysningspligt

Det er krav at oplyse den registrerede om behandlingen af personoplysninger senest samtidig med registreringen jf. databeskyttelsesforordningens artikel 13.

Det betyder, at elever, hvis oplysninger skal registreres og behandles i et monitoringsværktøj, forud for eksamen skal oplyses på en forståelig måde om følgende:

- Hvilke data, der registreres og til hvilket formål.
- Hvad retsgrundlaget for behandlingen (behandlingshjemmel) er.
- Hvem den dataansvarlige og dennes eventuelle DPO er.

- Er det planlagt, at data skal videregives til tredjeparter? Hvis ja, til hvem? *Bemærk, at databehandleren ikke er en tredjepart i denne sammenhæng.*
- Er det planlagt, at data skal overføres til et tredjeland? Hvis ja, hvad er retsgrundlaget herfor?
- Hvor længe skal data opbevares / hvornår bliver data slettet? Hvis en præcis slettedato ikke kan angives, så skal man angive hvilke kriterier, der ligger til grund for sletningen.
- Hvilke rettigheder har den registrerede i forbindelse med monitoreringsværktøjet?
- Retten til at klage til Datatilsynet.
- Hvorvidt det er obligatorisk at lade sine data registrere, og hvad konsekvensen er ved at nægte.

Vedlagt er et eksempel på en tekst, der opfylder oplysningspligten (bilag 2). *"Bemærk, at teksten herunder alene er et eksempel, som er udfærdiget med henblik på at vejlede institutionerne i opfyldelse af deres oplysningspligt. Institutionernes oplysningspligt over for fx elever skal opfyldes ved iagttagelse af de konkrete forhold som gør sig gældende ved den valgte monitoreringsløsning.*

Indsigtsret

Den registrerede har ret til indsigt i egne data jf. databeskyttelsesforordningens artikel 15.

Der kan ikke gøres undtagelser til opfyldelse af den registreredes indsigtsret i behandlingen af personoplysninger i monitoreringsværktøjet, hverken efter databeskyttelseslovgivningen, forvaltningsloven eller offentlighedsloven.

Hvis en elev anmoder om indsigt i egne data i monitoreringsværktøjet, skal institutionen derfor kunne udlevere en kopi af de personoplysninger, der behandles i monitoreringsværktøj. Institutionen bør derfor sikre sig, at det valgte monitoreringsværktøj giver teknisk mulighed for at kunne lave et udtræk – herunder hvordan og hvem der skal foretage udtrækket, er det institutionen selv eller leverandøren (databehandleren)?

Udover en kopi af de behandlede personoplysninger skal den registrerede, som en forlængelse af oplysningspligten oven for, have meddelt følgende:

- Formål med behandlingen.
- Hvilke personoplysninger, der er tale om.
- Om personoplysninger er blevet videregivet til tredjeparter - bemærk at leverandøren (databehandleren) ikke er en tredjepart i denne sammenhæng.
- Hvor længe data opbevares.
- Retten til at anmode om berigtigelse, begrænsning eller sletning (*se dog neden for om opbevaringsperiode*).
- Retten til at klage til Datatilsynet.

- Hvor oplysningerne stammer fra, hvis de ikke er indsamlet hos den registreret selv – dvs. hvis det ikke er oplysninger som den registrerede selv har indtastet.
- Hvorvidt man har brugt oplysningerne til at foretage automatiske afgørelser, herunder profilering.
- Hvis personoplysninger er blevet overført til tredjelande skal eleven oplyses om det retlige grundlag herfor.

Opbevaringsperiode

Det er vigtigt, at institutionen fastsætter en saglig og formålsbegrænset opbevaringsperiode. Denne opbevaringsperiode skal også afspejles i databehandleraftalen.

Hvis institutionen har fastsat en sagligt begrundet og formålsbegrænset opbevaringsperiode, kan man afvise anmodninger om sletning frem til opbevaringsperiodens udløb.

Der er mulighed for forlænget opbevaring udover den fastsatte opbevaringsperiode, hvis der opstår konkret mistanke om snyd og det eventuelt fører til en klagesag. Det er vigtigt, at institutionen dokumenterer sin politikker for opbevaringsperiode ved at skrive dem ned.

Det er også vigtigt at man sikrer sig, hvorvidt monitoreringsværktøjet rent teknisk giver mulighed for at lave en automatisk sletning efter udløbet af opbevaringsperiode. Derudover skal man overveje, hvordan man eventuelt afværger sletning eller forlænger opbevaring af en enkelt elevs data, hvis der for denne elev skulle opstå formodning om snyd eller en eventuel klagesag.

Databeskyttelsesrådgiver (DPO)

Institutionen kan have udpeget sin egen DPO.

DPO'ens funktion er at rådgive institutionen om dens overholdelse af databeskyttelsesforordningen.

Det anbefales derfor, at institutionen rådfører sig hos DPO'en i forbindelse med indgåelse af databehandleraftalen og udarbejdelse af risikovurderingen. DPO'en kan fungere som en person, der sikrer, at databehandleraftalen er indgået korrekt, men DPO'en kan ikke selv underskrive den.

Det anbefales, at DPO'en inddrages så tidligt som muligt i forbindelse med anvendelse af monitoreringsværktøjet, fordi DPO'en rolle også er at rådgive eleverne, hvis de skulle have spørgsmål eller betænkeligheder vedrørende institutionernes behandling af elevernes data.

Bilag

- Bilag 1: Datatilsynets skabelon til en databehandleraftale
- Bilag 2: Eksempel på tekst til oplysningspligten