PDH

PERSONDATAHÅNDBOG

Gældende for:

Fjerritslev Gymnasium

28. november 2019

Indhold

1 Indledning

Denne persondatahåndbog (PDH) kan bruges som et opslagsværk for alle de personer, som gymnasiet har registreret personlige oplysninger om.

Gymnasiet er dataansvarlig overfor alle personlige data, der er indhentet fra det tidspunkt, eleven/medarbejderen søger om optagelse/ansættelse og indtil de ikke længere er tilknyttet gymnasiet ved ansættelse eller skolegang.

1.1 Lovgrundlag (GDPR)[1]

EU ønsker med persondataforordningen (General Data Protection Regulation - GDPR) at skærpe EU-borgernes rettigheder i forbindelse med beskyttelse af deres data. Samtidig ønsker man en mere ensartet håndtering af EU-borgernes data på tværs af medlemslandene. Resultatet blev vedtagelse af en forordning, der tager højde for globalisering og ændringer i teknologiske løsninger, der gør handel med personlige data til en lukrativ forretning. Alle EU-lande – og alle lande, der handler med EU-borgere – skal overholde forordningen med effekt fra og med den 25. maj 2018.

Denne persondatahåndbog er godkendt af gymnasiets ledelse som dokumentation for, at reglerne (GDPR og dansk persondatalov) om behandling af personlige oplysninger overholdes. Se afsnit 18.1 i denne håndbog for overblik over den samlede dokumentation til overholdelse af GDPR.

Håndbogen opdateres af gymnasiets ledelse/administration i samarbejde med databeskyttelsesrådgiveren og vil være tilgængelig elektronisk på gymnasiets interne netværk samt i fysisk form på skolens kontor.[2]

1.2 Hvem er hvem?

I forbindelse med behandling af personlige oplysninger skelnes mellem tre forskellige personer eller grupper:

Dataansvarlige (se 1.2.1)	Gymnasiets ledelse (ansvarlig for håndtering af de personlige oplysninger, gymnasiet "låner" fra de registrerede.
Databehandlere (se 1.2.2)	Systemleverandører og hosting-virksomheder (opbevarer og behandler personlige oplysninger på gymnasiets vegne, f.eks. Lectio og Microsoft).
De registrerede (se 1.2.3)	Personer som gymnasiet "låner" nødvendige og i studiesammenhæng relevante personlige oplysninger fra.
Databeskyttelsesrådgiver (se 1.2.4)	Ansvarlig for rådgivning, spørgsmål og klager vedr. skolens behandling af personlige data - referer direkte til skolens ledelse og myndighederne (Datatilsynet).

1.2.1 Den dataansvarlige (gymnasiet)[3]

Den dataansvarlige afgør formålet med behandlingen af personoplysninger, hvorfor de fleste regler i persondataforordningen er rettet mod den dataansvarlige, der som central aktør skal sikre de registreredes rettigheder.

Selvom skolen har en databeskyttelsesrådgiver (DPO), er det stadig den dataansvarlige, der har ansvaret for overholdelse af persondataforordningen.

Kontaktoplysninger på den dataansvarlige findes i tillægget **Kontaktoplysninger** til denne håndbog og på skolens hjemmeside.

1.2.2 Databehandlere[4]

Opgaver, den dataansvarlige ikke selv kan løse inden for rimelige teknologiske og økonomiske grænser, kan løses af databehandlere.

Den dataansvarlige skal regulere databehandlerens opgaver i en databehandleraftale.

Se tillægget **Databehandleraftaler** til denne håndbog for en liste over benyttede databehandlere og de dertil indgåede databehandleraftaler.

1.2.3 Kategorier af registrerede personer[5]

Betegnelsen *de registrerede* dækker over tre kategorier af personer:

1. Medarbejdere (ansøgende, nuværende og tidligere)
2. Elever (ansøgende, nuværende og tidligere samt brobygnings elever)
3. Forældre/værger til elever under 18 år

De registrerede har en række rettigheder, som er angivet under **punkt 2** i denne håndbog.

1.2.4 Databeskyttelsesrådgiver (DPO)[6]

Denne rådgiver skal påse, at reglerne bliver overholdt, overvåge personalets uddannelse i forordningens krav, efterse datasikkerheden og være kontaktled mellem gymnasiets ledelse og Datatilsynet.

Rådgiveren skal være til rådighed for alle de registrerede personer med rådgivning om gymnasiets brug af deres personlige oplysninger, og fungerer derfor uafhængigt af skolens ledelse og med tavshedspligt.

Kontaktoplysninger til skolens DPO findes i tillægget **Kontaktoplysninger** til denne håndbog samt på skolens hjemmeside**.**

2 De registreredes rettigheder[7]

Oplysningspligten til de registrerede (*GDPR kap. 3, artikel 13-22*) opfyldes ved en kombination af elev- og medarbejderbrev med overordnet beskrivelse af de registreredes rettigheder, denne uddybende Persondatahåndbog samt skolens IT- og Datapolitik.

Persondatahåndbogen er tilgængelig på skolens hjemmeside, og elever, værger og personale kan ved henvendelse på skolens kontor få adgang til IT- og Datapolitikken.

2.1 Elevers og forældres/værgers rettigheder

Når eleven tilmelder sig en uddannelse på skolen, afgiver eleven personlige oplysninger. Derudover indsamler og behandler skolen forskellige andre oplysninger, der enkeltvis eller samlet set er personfølsomme oplysninger.

Ved optagelse på gymnasiet udfylder eleven en skriftlig samtykkeerklæring vedrørende behandling af visse oplysninger, f.eks. brug af billeder. Se afsnit 4 samt elevbrev, som det fremgår af tillæg. Samtykkeerklæringen opbevares i elevens elektroniske elevmappe. Præcis placering er angivet i skolens *IT- og Datapolitik*. Det skal klart fremgå, hvilke personoplysninger skolen behandler, og til hvilket formål. I alle tilfælde bliver registrerede orienteret om følgende:

- Formålet med og retsgrundlaget for behandlingen
- De legitime interesser som skolen behandler oplysningerne ud fra
- Hvor lang tid skolen opbevarer de pågældende personoplysninger
- At den registrerede har ret til at anmode om indsigt i, berigtigelse af eller sletning af disse personoplysninger
- Retten til at indgive klage til datatilsynet
- Evt. forekomst af automatiske afgørelser, dvs. kategoriseringer på baggrund af overførte oplysninger.
- Kontaktoplysninger på dataansvarlige og databeskyttelsesrådgiver (DPO)

På skolens samtykkeerklæringer er følgende desuden angivet:

- At samtykket til enhver tid kan trækkes tilbage – dog ikke med tilbagevirkende kraft

Det gælder for alle de registrerede, at man til enhver tid vil kunne henvende sig på skolens kontor og få en kopi (fysisk eller elektronisk) af egne personoplysninger, som skolen behandler (*GDPR artikel 15, stk. 3*). Kopien vil kunne udleveres efter anmodning inden for en uge. Vær opmærksom på, at skolen - efter den første kopi er udleveret - er berettiget til at opkræve et administrationsgebyr, såfremt der fremsættes ønske om yderligere kopier af egne personoplysninger.

2.2 Medarbejdernes rettigheder

Et af kravene i Persondataforordningen er, at medarbejderne på gymnasiet løbende instrueres i, hvordan de skal medvirke til at sikre, at personlige data, som gymnasiet behandler, bliver benyttet forsvarligt.

Der er altså tale om sikring af medarbejdernes og elevernes personlige data. Intet i denne håndbog har til hensigt at begrænse den enkeltes frihed til at fungere i dagligdagen, men bygger på en lovgivning, vi alle skal følge.

I bund og grund bygger reglerne på brugen af sund fornuft og ansvarlighed.

Medarbejderen har:

- Ret til at modtage information om en specifik behandling af sine personlige oplysninger.
- Ret til at få indsigt i hvilke personoplysninger, gymnasiet har registreret.
- Ret til at få urigtige personoplysninger berigtiget.
- Ret til at få sine personoplysninger slettet, også kaldet "retten til at blive glemt", når medarbejderens tilknytning til gymnasiet ophører.
- Ret til at flytte sine personoplysninger (dataportabilitet)
- Ret til at indgive klage til databeskyttelsesrådgiveren eller Datatilsynet, hvis medarbejderen mener, at gymnasiet ikke følger reglerne på området.

Desuden har medarbejderen:

- Ret til at gøre indsigelse mod, at personoplysninger anvendes til direkte markedsføring.
- Ret til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering (f.eks. automatisk selektering af medarbejdere / elever alene ud fra ansøgninger).

Gymnasiet skal kunne dokumentere, at behandlingen af medarbejderens personlige data sker i henhold til ovenstående rettigheder. Denne håndbog er en vigtig del af denne lovkrævede dokumentation.

Medarbejderens underskrift vil til tider være påkrævet i forskellige sammenhænge for at sikre dokumentation af, at den krævede instruktion er modtaget, eventuelt med afgivet samtykke til visse behandlinger af medarbejderens personlige oplysninger.

3 Hvilke data behandles[8]

Skolen behandler personlige oplysninger, der primært er nødvendige og relevante til personaleadministration og for at skolen kan efterleve Undervisningsministeriets krav til elevernes gennemførelse af studiet. Desuden benytter skolen billeder af elever og lærere i undervisnings-situationer til markedsføring af skolen og dens aktiviteter.

Behandling er:

Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling, sammenkøring, begrænsning, sletning eller tilintetgørelse.

Følgende personoplysninger behandles:

- Fulde navn, adresse, telefonnummer og e-mailadresse på forældre/værger og elever fra det tidspunkt en elev søger optagelse på skolen gennem *optagelse.dk* eller vælger brobygning på gymnasiet gennem kommunens UU-vejleder.
- Fulde navn, adresse, telefonnummer og e-mailadresse på medarbejdere fra det tidspunkt vedkommende ansøger om ansættelse på skolen.
- Personnummer på brobygningselever, elever, forældre/værger og medarbejdere.

Desuden behandles følgende personfølsomme oplysninger:

- Helbredsoplysninger i form af sygefravær og sygeårsag for elever og lærere.
- Væsentlige sociale forhold for elever i forbindelse med dialogmøder om børns mistrivsel samt kommunikation med kommunen.
- Elevernes karakterer, besvarelser fra skriftlige eksaminer samt klagesager.

3.1 TV-overvågning

Finder pt. ikke sted på Fjerritslev Gymnasium

4 Samtykkeerklæring[9]

Visse oplysninger, f.eks. brug af billeder i sammenhæng med markedsføring af skolen, kræver den registreredes samtykke inden behandlingen af disse data påbegyndes, hvilket i praksis vil sige i forbindelse med optagelse eller ansættelse på skolen. Specifikt samtykke skal indhentes for hvert formål, billederne bruges til.

Samtykket gemmes i elev- eller medarbejder-mapperne på skolens kontor eller i skolens aflåste arkiv indtil behandlingen af oplysningerne, hvortil der er indhentet samtykke, ikke længere er relevant.

Benytter gymnasiet elektronisk dokumenthåndtering, befinder billederne sig på skolens krypterede server i relevante mapper. Samtykket kan til hver tid tilbagekaldes ved henvendelse på kontoret, dog kan samtykket ikke gælde med tilbagevirkende kraft.

5 Formål og tidspunkt for registrering af personlige oplysninger[10]

Benytter gymnasiet elektronisk dokumenthåndtering, befinder dokumentationen sig på skolens krypterede server i en overskuelig mappestruktur med adgangsrettigheder som angivet under **punkt 6**. Ref. tillægget *IT- og Datapolitik* for yderligere beskrivelse heraf.

5.1 Behandling af elevernes personlige oplysninger

Det overordnede formål med behandlingen: Behandling er nødvendig for at opfylde forpligtelser og lovkrav fra myndighederne (Undervisningsministeriet)	
Tidspunkt:	Hvorfor, hvor og hvor længe opbevares oplysningerne:
Ansøgning om optagelse: ***Ved afslag på optagelse på skolen gemmes ansøgningen i indeværende år samt 1 år tilbage, hvorefter den slettes.***	Der søges om optagelse via UVM's ansøgningsplatform ***www.optagelse.dk*** i henhold til *Bekendtgørelsen om optagelse på ungdomsuddannelser.* Ansøgningen indeholder elevens CPR-nr., navn, adresse, telefonnumre og e-mailadresser samt uddannelsesønske med hertil knyttede oplysninger mht. sprogønske og/eller ønske om kunstnerisk fag. Ansøgningen indeholder desuden forældres/værges navne, adresser, CPR-nr., telefonnumre og e-mailadresser. Ansøgningen hentes via gymnasiets administrationsprogram, Lectio, hvor den indlæses og oplysningerne arkiveres i et såkaldt "ansøgermodul".
Optagelse:	Ved optagelse kopieres oplysningerne elektronisk i Lectio fra ansøgermodulet til elevmodulet.
Under uddannelsesforløbet:	På gymnasiets server har hver elev en mappe, med bl.a. ansøgning og samtykkeerklæringer. I mappen lægges diverse beskeder, f.eks. korrespondance med forældre, lægeerklæringer ifm. idræts- og andet fravær, informationer om faste aftaler med psykolog samt underskrevne kopier af advarsler for højt fravær og plagiat. Oplysninger om SPS og SU gemmes i aflåst fysisk arkiv mens eleven går på skolen. Herefter scannes dokumenterne til elevens mappe på serveren. Oplysningerne slettes 10 år efter eleven stopper på skolen.
Standpunktskarakterer	Standpunktskarakterer gemmes i Lectio i 10 år, mens eksamenskarakterer gemmes i pengeskab i minimum 30 år.
Udmeldelse før tid:	Ved udmeldelse "i utide" (før dimission) gemmes udmeldelsesblanketten og en oversigt over protokollinjer i elevmappen.
Sletning af data for udgåede elever: **Vedrørende arkiveringsregler henvises til håndbogens afsnit 14.**	Standpunktskarakterer slettes som hovedregel efter 10 år. Eksamenskarakterer sendes efter 30 år til Rigsarkivet, hvor det opbevares uendeligt. Besvarelser fra skriftlige eksaminer uploades til netprøver og gemmes således ikke på skolen. Samtykkeerklæringer samt informationer vedrørende SU og SPS slettes senest efter 10 år. Elevmapper bliver efter endt uddannelsesforløb gennemgået for overflødig information såsom lægeerklæringer, advarsler m.m., men gemmes ellers på ubestemt tid af historiske årsager.

5.2 Behandling af medarbejdernes personlige oplysninger

Det overordnede formål med behandlingen: Behandling er nødvendig for at føre personaleadministration iht. gældende lovgivning.	
Tidspunkt:	Hvorfor, hvor og hvor længe opbevares oplysningerne:
Modtagelse af ansøgninger (lærerne):	Rekruttering af lærerne sker via ***www.gymnasiejob.dk*** og enkelte via ***www.jobnet.dk.*** Ansøgningerne behandles af ledelsen og evt. af ansættelsesudvalget/faggrupperepræsentanten. Ansøgninger der ikke fører til ansættelse slettes senest 6 måneder efter ansøgningsfristens udløb. Ansøgeren kan give samtykke til at ansøgningen gemmes længere. Uopfordrede ansøgninger slettes umiddelbart efter læsning, men gemmes i op til 6 måneder, hvis ansøgeren giver samtykke til det. Ansøgningerne gemmes i rektors mailbox.
Ansættelse:	Personen, der ansættes, får en ansættelseskontrakt. Når denne modtages retur i underskrevet stand, opbevares den i kælderen i aflåst skab, i en personalemappe. Oplysningerne indscannes også og gemmes på kontorets server. Til lønindberetning opbevares diverse oplysninger om honorarer og tillægsgivende kvalifikationer.
Under ansættelse:	Der informeres om persondataforordningen og *IT- og Datapolitik*ken, og der indhentes samtykke til brug af billeder af lærerne. I tilfælde af en medarbejders længere tids sygdom udarbejdes der en mulighedserklæring, som udleveres til medarbejderen. Kopi af disse gemmes i personalemappen og fjernes ikke herfra. Personalesager opbevares også i mappen.
Sletning af data efter ansættelsens ophør:	Ved fratræden gemmes personfølsomme oplysninger fra personalemapperne i gymnasiets arkivsystem eller aflåste arkivrum. Samtykkeerklæringer, dagpengeskemaer, sygemeldinger og personalesager makuleres senest efter 5 år. Ansættelsesbreve og billeder opbevares uendeligt af historiske årsager. Derfor opbevares samtykkeerklæringer til behandling af billeder også på ubegrænset tid. Dokumenter i forbindelse med afskedigelse / opsigelse opbevares i op til 20 år efter fratrædelsen.

5.3 Specielle forhold jævnfør Statens Arkivsystem

Speciel registrering:	Hvorfor, hvor og hvor længe opbevares oplysningerne:
Data om personer født den 01. i hver måned samt ansatte i chefstillinger	Formål med at registrere disse data er af ren statistisk karakter eller i samfundets interesse og er krævet af gældende lovgivning.
Hvor opbevares dataene:	Gemmes i dertil oprettede mapper på skolens server.
Varighed:	Gemmes på ubestemt tid.

Gymnasiet har i sin *IT- og Datapolitik* beskrevet, hvordan disse tidsfrister sikres, og hvor ofte en periodisk evaluering af nødvendigheden af den fortsatte

opbevaring af de behandlede personlige oplysninger foretages.
Urigtige oplysninger skal straks korrigeres.

5.4 Brobygnings-kursus elever

Elever i 8. til 10. klasse skal ifølge loven deltage i brobygnings-kurser med det formål at give de unge en konkret fornemmelse for den ungdomsuddannelse, som de muligvis vil søge ind på.

Da behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som gymnasiet har fået pålagt, kræves ingen samtykke selvom barnet er under 15 år gammel.

Barnet tilmelder sig brobygnings-kurserne gennem Uni-Login og bliver sendt til gymnasiet af kommunens UU-vejleder.

5.4.1 Hvilke personlige oplysninger behandles

Dataene er almindelige kontaktoplysninger (navn, adresse, telefonnummer) samt CPR-nummer, folkeskolens navn og UU-vejlederens navn.

Tidspunkt:.	Hvorfor, hvor og hvor længe opbevares oplysningerne:
Når eleven har valgt brobygning i folkeskolens 8. til 10. klasse	Oplysningerne er lovpligtige og bliver leveret fra kommunens UU-funktion (Ungdommens Uddannelsesvejledning).
Under brobygningsforløbet	Oplysningerne skal opbevares i mapper på kontoret og indtastes i Lectio. Her gemmes de indtil brobygningsforløbet er slut og indberetning til Undervisningsministeriet er foretaget. Lærerne modtager elevernes kontaktinformationer, ligesom skolens revisor kan få en oversigt over eleverne, hvis de beder herom.
Efter brobygningsforløbet	Når den økonomiske ydelse for elevens deltagelse i brobygnings-forløbet er udbetalt til gymnasiet, er behandlingen i princippet slut. Hvert år i september slettes alle fysiske oplysninger og oplysninger i Lectio om UNI-login og CPR-nummer for brobygningselever fra forrige skoleår. Fx slettes oplysninger fra skoleåret 2017/18 i september 2019.

5.4.2 Begrænsning i lovhjemmel

Ønsker gymnasiet at tage billeder af brobyggereleverne mens de er på gymnasiet, skal der indhentes skriftligt samtykke herfor. Er eleven under 15 år skal dette samtykke indhentes hos barnets forældre eller værge. Samtykket skal være tidsbegrænset og kun omhandle den konkrete situation eller omstændighed, der ønskes fotograferet.

6 Hvem behandler de personlige oplysninger?[11]

Følgende medarbejdergrupper har adgang til at se og behandle de indsamlede personlige oplysninger. Hvis nedenstående skemaer ændres eller opdateres, skal de registrerede informeres herom inden ændringen træder i kraft.

Forklaring til benævnelserne i anden kolonne af skemaerne under **punkt 6.2**:

Hvem/hvad:	Årsag til behandling af personlige oplysninger:
Dataansvarlige	Overordnet ansvar for alle behandlinger.
Rådgivning	Nødvendig for at udøve relevant målrettet uddannelsesvejledning.
Studieadministration	Nødvendig for at håndtere elevernes skolegang samt registerloven.
Personaleadministration	Nødvendig for at styre ansættelsesforhold, løn, pension m.v.
Studierelateret	Lærernes adgang til relevante elevers stamdata.
Systemvedligeholdelse	Kan medføre adgang til alle data for alle registrerede personer.
Kræver samtykke	Når behandling falder udenfor det egentlige formål kræves samtykke.
Kontaktoplysninger	Nødvendige for at kontakte forældre/værger til elever under 18 år.

Benyttelse af databehandlere er, hvor det er relevant, indikeret ved en lille note efter hvert af følgende skemaer. Se

6.1 Elevernes personlige oplysninger

Der behandles både almindelige og følsomme personoplysninger for eleverne.

6.1.1 Ikke følsomme oplysninger

Hvem har adgang til oplysningerne:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Studieadministration
Studievejledere	Rådgivning
Lærere	Studierelateret
IT-medarbejdere	Systemvedligeholdelse
Den eksterne omverden (markedsføring)	Kræver samtykke

OBS: Databehandlere benyttes

6.1.2 Følsomme oplysninger (inklusive CPR-numre)

Hvem har adgang til oplysningerne:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Studieadministration
Studievejledere	Rådgivning
IT-ansvarlige	Systemvedligeholdelse

OBS: Databehandlere benyttes

6.2 Værgers personlige oplysninger (inklusive CPR-numre)

Hvem har adgang til oplysningerne:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Studieadministration
Studievejledere	Kun kontaktoplysninger
IT-medarbejdere	Systemvedligeholdelse

OBS: Databehandlere benyttes

6.3 De ansattes personlige oplysninger

Al behandling af de ansattes personlige oplysninger, følsomme som almindelige, sker udelukkende for at kunne varetage personaleadministration, f.eks. håndtering af løn, pension, ferier, sygefravær osv.

Dertil kommer markedsføring af skolens aktiviteter på sociale medier og trykte medier, hvilket der indhentes samtykke til i forbindelse med ansættelse på skolen.

6.3.1 Ikke følsomme oplysninger

Hvem:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Personaleadministration
IT-medarbejdere	Systemvedligeholdelse
Den eksterne omverden (markedsføring)	Kræver samtykke

OBS: Databehandlere benyttes

6.3.2 Følsomme oplysninger (inklusive CPR-numre)

Hvem:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Personaleadministration
IT-medarbejdere	Systemvedligeholdelse

6.4 Brobygnings-elever

Disse elever har kun kortvarig berøring med nedenstående personer.

Hvem:	Formål/noter:
Skolens ledelse (rektor og vicerektor)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Studieadministration
Uddannelsesleder	Studieadministration
Lærere	Kun navn
IT-ansvarlige	Systemvedligeholdelse

6.5 Pedeller

På visse gymnasier har pedellerne adgang til alle områder på skolen, de sørger for makulering af store mængder personfølsomme data, og de har adgang til tv-overvågning. Dette vil i så fald fremgå af skolens interne *IT- og Datapolitik*.

6.6 Videregivelse af personlige oplysninger

Ved benyttelse af databehandlere, der kan have adgang til både ikke følsomme og følsomme personlige oplysninger, reguleres dette gennem en databehandler-aftale, hvori gymnasiets ledelse detaljeret og præcist har defineret omfang og formål med databehandlingen. Se endvidere tillægget **Databehandleraftaler**. Hvis personlige oplysninger videregives til uberettigede modtagere, skal disse data straks slettes eller afhentes/returneres, herunder data fra internettet.

Se endvidere **afsnit 15** samt i skolens *IT- og Datapolitik*.

6.7 Fællesstatslige IT-systemer

Moderniseringsstyrelsen tilbyder en række IT-løsninger, der er reguleret gennem et cirkulære: https://www.retsinformation.dk/Forms/R0710.aspx?id=200442.

Gymnasier er ifølge styrelsen og Datatilsynet omfattet af samme vilkår, som gælder for de institutioner, der er forpligtet til at anvende systemerne, hvorfor henvisning til ovenstående cirkulære er tilstrækkelig dokumentation til overholdelse af persondataforordningen.

7 Hvor længe opbevarer vi de registreredes data?[12]

Fælles for alle personlige informationer er, at de slettes, når de ikke længere er relevante til at opfylde de formål, hvortil de blev indsamlet eller på anden vis behandlet.

Se tabellerne i **afsnit 5** for en mere detaljeret beskrivelse af slettefristerne**.**

Visse data skal opbevares til arkivformål, videnskabelige eller historiske formål i samfundets interesse, hvilket betyder, at gymnasiet ifølge gældende lovgivning skal opbevare disse oplysninger ud over formålets rækkevidde. Endvidere skal visse oplysninger overføres til Rigsarkivet, når de ikke længere er relevante for gymnasiet.

Af historiske hensyn forbeholder gymnasiet sig ret til at opbevare klassebilleder i ubegrænset tid, så de kan benyttes til jubilæer m.v.

De opbevarede data gennemgås med mellemrum for at sikre, at der ikke opbevares oplysninger unødigt.

8 Fysisk opbevaring af personlige oplysninger[13]

Gymnasiet opbevarer alle personlige oplysninger på en måde, hvor uvedkommende ikke kan få adgang til dem. Personfølsomme oplysninger opbevares under særligt sikre forhold, og der føres i Lectio log til dokumentation af hvorfor og hvornår, dataene er blevet set eller på anden måde behandlet med angivelse af hvem, der har tilgået dem.

Se skolens IT- og Datapolitik for nærmere beskrivelse af såvel de almindelige som de følsomme personoplysningers fysiske opbevaring.

Benytter gymnasiet elektronisk dokumenthåndtering, befinder dokumentationen sig på skolens krypterede server i en overskuelig mappestruktur med adgangsrettigheder som angivet under **punkt 6**.

8.1 Elevernes personlige oplysninger

De personer, der har adgang til disse oplysninger, er særligt instrueret i hvordan oplysningerne behandles sikkert. Liste over disse personer / persongrupper findes i **afsnit 6.1**.

Personfølsomme oplysninger gemmes udelukkende på skolens krypterede servere, på skolens aflåste kontor og i skolens administrative system, Lectio.

8.2 Forældres og værgers personlige oplysninger

Udelukkende almindelige kontaktoplysninger med tillæg af CPR-numre opbevares om forældre og værger. Disse opbevares på skolens aflåste kontor samt i skolens administrative system, Lectio.

Liste over personer med adgang til disse oplysninger findes i **afsnit 6.2**.

8.3 De ansattes personlige oplysninger

Udover opbevaring af oplysninger hos databehandlere (se tillægget **Databehandleraftaler** for nærmere information herom), opbevares almindelige og følsomme personoplysninger på skolens krypterede servere.

Der ud over opbevares ansættelseskontrakter og andre relevante dokumenter for nuværende ansatte i brandsikkert arkivskab i skolens kælder, som rektor, vicerektor samt administrationen har nøgle til. Disse forhold er angivet i skolens *IT-og datapolitik.*

Komplet liste over personer med adgang til de ansattes personlige oplysninger findes i **afsnit 6.3** og i skolens *IT-og datapolitik*.

8.4 Brobygnings elever

Som beskrevet under **punkt 8.1** med undtagelse af, at der ikke behandles følsomme personlige oplysninger for denne kategori.

9 Instruktion til medarbejdere[14]

Den nyansatte skal på ansættelsestidspunktet informeres om og instrueres i gymnasiets procedurer samt afgive samtykkeerklæring.

Det skal klart fremgå, hvilke personoplysninger skolen behandler og til hvilket formål.

I alle tilfælde bliver registrerede orienteret om følgende:

- Formålet med og retsgrundlaget for behandlingen
- De legitime interesser som skolen behandler oplysningerne ud fra
- Hvor lang tid skolen opbevarer de pågældende personoplysninger
- At den registrerede har ret til at anmode om indsigt i, berigtigelse af eller sletning af disse personoplysninger
- Retten til at indgive klage til datatilsynet
- Evt. forekomst af automatiske afgørelser, dvs. kategoriseringer på baggrund af overførte oplysninger (f.eks. kategorisering i forbindelse med jobansøgning).
- Kontaktoplysninger på dataansvarlige og databeskyttelsesrådgiver (DPO)

På skolens samtykkeerklæringer til såvel elever som ansatte er følgende desuden angivet:

- At samtykket til enhver tid kan trækkes tilbage – dog ikke med tilbagevirkende kraft

Samtykkeerklæringen skal opbevares i medarbejderens personalemappe.

Benytter gymnasiet elektronisk dokumenthåndtering, befinder dokumentationen sig på skolens krypterede server i en overskuelig mappestruktur med adgangsrettigheder som angivet under **punkt 6**.

Det gælder for såvel elever som ansatte (GDPR artikel 15, stk. 3), at man til enhver tid vil kunne henvende sig på skolens kontor og få en kopi (fysisk eller elektronisk) af egne personoplysninger, som skolen behandler. Kopien vil kunne udleveres efter anmodning inden for en uge. Vær opmærksom på, at skolen - efter den første kopi er udleveret - er berettiget til at opkræve et administrationsgebyr, såfremt der fremsættes ønske om yderligere kopier af egne personoplysninger.

I tillægget **Skabeloner** til denne manual er et eksempel på formuleringen af et medarbejderbrev med samtykkeerklæring, hvor markeringerne med [X] ændres til pågældende gymnasies navn. Eksemplet indeholder et minimum af information, så det står det enkelte gymnasium frit for at tilføje mere tekst, f.eks. regler for adgang til gymnasiet.

For information om, hvor oplysningerne fysisk opbevares henvises til gymnasiets *IT- og Datapolitik*.

10 Behandlingssikkerhed[15]

Personlige oplysninger skal behandles sikkert og med respekt for den person, der har udleveret oplysningerne.

Selvom denne håndbog på en proaktiv måde forsøger at tage højde for alle forhold vedrørende behandling af personlige oplysninger, kan det dog ikke garanteres, at håndbogen tager hensyn til alle situationer. Brug af sund fornuft vil derfor være uundværlig til sikring af behandlingssikkerhed.

Desuden skal den dataansvarlige sikre, at alle interne IT-systemer altid lever op til den højest mulige standard, hvad sikkerhed og beskyttelse angår, inden for skolens økonomiske rammer.

10.1 Interne retningslinjer

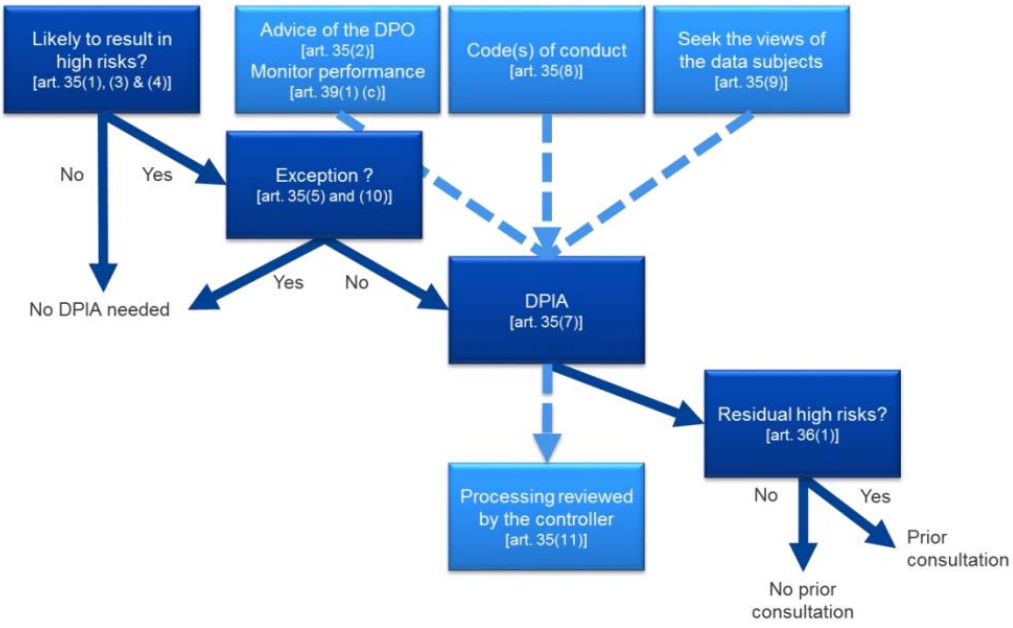
Behandlingssikkerheden på gymnasiet er beskrevet i et tillæg til denne håndbog, *IT- og Datapolitik*. Denne indeholder beskrivelse af procedurer for data backup og regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden med behørig hensyntagen til risici. Endvidere beskrives styring af adgangskontrol og sikkerhedsindstillinger på de anvendte sociale medier.

Se **afsnit 17** for retningslinjer ved brud på persondatasikkerheden.

10.1.1 Konsekvensanalyse (DPIA)[16]

Hvis et brud på datasikkerheden vil resultere i en høj risiko for den registreredes frihedsrettigheder, skal gymnasiet gennemføre en risikoanalyse (Data Protection Impact Assessment, DPIA).

Skabelon til udfærdigelse af en DPIA findes i tillægget **Skabeloner** til denne mappe, og processen kan illustreres således:



10.1.2 Behandlinger med særlig høj risiko[17]

Håndtering og opbevaring af personlige oplysninger udenfor skolens netværk er særligt udsat for risiko. Eksempler kan være brug af bærbare computere uden tilstrækkelig sikkerhed (kryptering m.v.), brug af disse computere på offentlige steder, f.eks. logge på åbne netværk på cafeer, biblioteker, bus og tog med videre.

I sådanne tilfælde skal der udføres en risikoanalyse (DPIA). Såfremt tilstrækkelig datasikkerhed ikke kan sikres, skal Datatilsynet orienteres.

Denne DPIA skal være tilstrækkelig omfattende og f.eks. indeholde følgende stillingtagen:

1. Hvilke personoplysninger vil blive behandlet? (f.eks. navn, adresse, e-mail, telefonnummer, IP-adresse, metadata, adfærd)
2. Hvilke typer af teknologier anvendes? (f.eks. webportaler, sociale medier, biometri, RFID eller TV-overvågning)
3. Hvordan foregår indsamlingen af personoplysninger? (f.eks. egne eksisterende data, data fra individ eller data fra tredjepart)
4. Til hvilket formål behandles personoplysningerne? (f.eks. profilering)
5. Sikres det, at der ikke indsamles flere data end formålet tilsiger?
6. Sikres det, at data ikke anvendes til andre formål?
7. På hvilket retligt grundlag foretages databehandlingen (f.eks. samtykke)?
8. Hvilken behandling finder sted? (f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)
9. Hvem har adgang til data? (f.eks. hvilke personalegrupper)
10. Hvem har ansvaret for personoplysningernes sikkerhed? (f.eks. dataansvarlige = gymnasiet)
11. Hvordan ser dataflowet ud efter personoplysninger er indsamlet? (f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre formål (og hvis de gør, efter hvilken procedure det så sker) og hvornår de slettes; en livscyklusbetragtning for data)
12. Hvordan organiseres personoplysningerne? (f.eks. kundenummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))
13. Videregives data til andre? (f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)

Daglig behandling af almindelige personlige oplysninger gennem skolens interne sikre netværk kræver ikke risikoanalyse.

10.1.3 Brug af pseudonymisering[18]

Der kan i særlige tilfælde ved henvendelse fra andre offentlige myndigheder (f.eks. politiet) oprettes anonyme brugere (pseudonymer) i Lectio og andre af skolens systemer, der giver bred adgang til personlige oplysninger. Formålet med dette er alene at sikre den anonymiserede mod kriminelle handlinger, f.eks. vold.

Gymnasiets ledelse, administration og IT-administratorer vil kende vedkommendes rigtige personlige oplysninger, og er underlagt streng tavshedspligt herom.

10.2 Skolens udleverede udstyr

Computere, som er udleveret af skolen, er sikret med antivirusprogram, kryptering af harddisk og bliver ved udlevering sikret med en sikker adgangskode, som den ansatte selv definerer efter nærmere instruks.

Det er ikke tilladt at installere andre programmer end de af skolen testede og godkendte programmer, og det er ikke tilladt at ændre sikkerhedsindstillinger i computerens opsætning, herunder i internet-browserne.

Når en ansat leverer udstyret tilbage til skolen, f.eks. ved ophør af ansættelse, bliver udstyret nulstillet (sikker sletning) af skolens it-medarbejdere.

Alternativt destrueres harddisken fysisk inden kassering.

10.3 Sikkerhedsbevidsthed (Awareness)[19]

Gymnasiet skal ajourføre de interne sikkerhedsbestemmelser mindst én gang om året med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold på gymnasiet. Hvert år i september tager skolens ledelse initiativ til at skolens samlede dokumentation vedrørende GDPR gennemgås og opdateres. I løbet af året opdateres der efter behov. Medarbejderne informeres, når der sker større ændringer ud over sproglige rettelser og lignende.

Alle medarbejdere, der behandler personlige oplysninger, har ansvar for at bidrage til, at gymnasiet behandler disse data i henhold til denne håndbog, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse.

Opmærksomhed på dette sikres gennem jævnlige instruktionsmøder og/eller kurser, hvorved medarbejderne holdes opdaterede og påmindes om procedurer og regler, som denne manual og skolens *IT- og Datapolitik* foreskriver.

Desuden anbefales det, at der løbende afholdes kampagner med det formål at understøtte medarbejdernes fokus på datasikkerhed.

I lyset af gymnasiers feriemønster og perioder med høj arbejdsbelastning, anses et til to årlige opdateringsmøder/kurser for passende, kombineret med

kampagner ved årets start, inden eksamenstiden starter og i starten af et nyt skoleår.

Ved større ændringer i procedurer eller regler skal denne orientering dog gennemføres uden unødig forsinkelse.

Se endvidere **afsnit 12** for information om medarbejderuddannelse.

11 Når den ansatte ikke er på gymnasiet

11.1 Hjemmearbejdsplads

Der gælder følgende regler og retningslinjer for ansatte på gymnasiet om deres omgang med gymnasierelaterede almindelige, fortrolige og personfølsomme oplysninger på hjemmearbejdspladsen:

- Der skal bruges en personlig adgangskode for at få adgang til det elektroniske udstyr.
- Koden skal være en sikker kode, det vil sige består af minimum 8 tegn og indeholde både store og små bogstaver og tal.
- Koden skal som udgangspunkt skiftes hver 6. måned.
- Der må ikke bruges autoudfyldning af koder i programmer og internet-browsere, og det er ikke tilladt at gemme sine adgangskoder på pc'en eller steder, hvor uvedkommende kan få adgang til dem.
- Fysisk papir og elektronisk udstyr skal benyttes og opbevares ansvarligt, så uvedkommende ikke har adgang til det.
- Det er ikke tilladt at udveksle gymnasierelaterede personlige oplysninger til eller fra private mailadresser.
- Private backup løsninger må ikke benyttes til sikkerhedskopiering af skolerelaterede data.
- Der må udelukkende benyttes cloud-løsninger fra udbydere, som skolen har databehandleraftaler med, og disse bør ikke benyttes til opbevaring af personfølsomme oplysninger. Se endvidere afsnit 13.

11.2 Offentlige netværk

Der kan være stor risiko for tab af data, når offentlige netværk benyttes til at sende og modtage data. Det er derfor ikke tilladt at sagsbehandle (sende eller modtage) gymnasierelaterede personlige oplysninger via almindelig e-mail på elektronisk udstyr, der har netadgang via offentligt tilgængelige netværk, f.eks. på hoteller.

Al kommunikation, der involverer personlige oplysninger, som gymnasiet er dataansvarlige for, skal ske via krypterede forbindelser, fx gennem VPN-klient eller Lectio-beskeder. Endvidere skal de benyttede enheder være beskyttet med sikker adgangskode og krypteret lager (harddisk).

Der skal altid udvises særlig opmærksomhed på de risici, der er forbundet med brug af elektronisk udstyr på områder med offentlig færdsel. Herunder om uvedkommende personer kan se computerskærmen, f.eks. via spejling i vinduer.

Der kan være beskrevet specifikke regler og procedurer i de enkelte gymnasiers *IT- og Datapolitik*.

11.3 Mistanke om misbrug

Hvis man får mistanke om, at der er sket misbrug af gymnasierelevante data fra det benyttede elektroniske udstyr, hvad enten det er ens private udstyr eller udlånt af skolen, skal skolens ledelse orienteres uden unødig forsinkelse. Ledelsen vil derefter informere gymnasiets databeskyttelsesrådgiver (DPO), der med udgangspunkt i en DPIA (konsekvensanalyse) vurderer, om Datatilsynet skal involveres, og om de berørte registrerede skal informeres. Ledelse og DPO beslutter derefter, om der skal indføres ændringer i skolens procedurer eller systemer, så lignende databrud i fremtiden kan undgås.

12 Medarbejder uddannelse[20]

De ansatte på gymnasiet, der har adgang til personlige og personfølsomme data, skal ifølge loven uddannes i personforordningen og gymnasiets procedurer omkring sikker håndtering af disse oplysninger.

Tavshedspligten og forsigtighed i omgang med personfølsomme data skrives ind i ansættelsesbreve. For allerede ansatte sker denne orientering ved et tillæg til ansættelsesbrevet.

Der afholdes mindst en gang årligt et instruktionsmøde (med mødepligt) for alle ansatte om dette. For nyansatte drejer det sig om et grundlæggende kursus, for allerede ansatte om ajourføring på området. Ansatte bekræfter ved deres underskrift, at de har deltaget i disse møder og er orienteret om forordningen og om skolens procedurer til overholdelse af reglerne, herunder forventninger til de ansattes håndtering af personfølsomme oplysninger.

Ved persondataforordningens ikrafttræden 25. maj 2018 afholdes grundlæggende kurser for alle relevante medarbejdere for at sikre introduktion af de nye regler og procedurer. Deltagelse på dette kursus er obligatorisk og skal kunne dokumenteres.

Denne persondatahåndbog skal være tilgængelig for alle ansatte, og bør forefindes let tilgængelig i elektronisk form samt i udskrevet form på skolens kontor.

Det er gymnasiets ansvar at opdatere håndbogen og sikre, at de ansatte hurtigt muligt bliver informeret om ændringer i håndbogens indhold og gymnasiets procedurer vedrørende datasikkerhed.

13 Brug af Cloud-løsninger

Gymnasiet tilbyder visse cloudløsninger til arkivering og deling af information. Selvom disse løsninger ikke som udgangspunkt er tænkt til opbevaring og deling af personlig information, kan det ikke udelukkes, at dette vil forekomme.

De enkelte cloud-løsninger er reguleret af databehandleraftaler, der kan findes i tillægget **Databehandleraftaler** til denne håndbog.

Det er ikke tilladt at gemme følsomme personlige oplysninger andre steder end på skolens krypterede servere. Manglende overholdelse af denne regel vil blive betragtet som brud på datasikkerheden. Ved tvivlstilfælde skal skolens kontor eller databeskyttelsesrådgiver straks kontaktes.

Se endvidere **afsnit 11.1** for regler vedrørende hjemmeplads.

14 Arkiveringsregler

Personlige oplysninger må ikke opbevares længere end relevant for opfyldelse af deres formål (se **afsnit 5** for detaljerede slettefrister).

Opbevaring af personlige oplysninger hos de benyttede databehandlere er reguleret i de tilhørende databehandleraftaler.

Ud over de i skemaet i **afsnit 5** angivne slettefrister, sendes elevernes karakteroplysninger fysisk til Rigsarkivet, der opbevarer dem på ubestemt tid. Eleven kan mod et gebyr rekvirere dem herfra.

Endvidere opbevarer skolen billeder af lærere og elever af historiske hensyn, forudsat de ved ansættelse/optagelse på skolen gav samtykke til dette. Disse billeder opbevares på ubestemt tid i skolens aflåste arkivrum.

Ligeledes opbevares årsskrifter og andre publikationer af historiske årsager i gymnasiets aflåste arkivrum på ubestemt tid.

Det bemærkes, at samtykke til brug af billeder ikke kan trækkes tilbage for allerede udgivne årsskrifter, brochurer og andre publikationer.

Elektronisk dokumentationen befinder sig på skolens krypterede server i en overskuelig mappestruktur med adgangsrettigheder som angivet under **punkt 6**. Ref. skolens *IT- og Datapolitik* for yderligere beskrivelse heraf.

For nærmere information om reglerne for frister og tilgængelighed for arkivalier i Rigsarkivet henvises til:

https://www.sa.dk/da/brug-arkivet/bestil-arkivalier/tilgaengelighedsfrister-paa-arkivalier/

Den fulde arkivbekendtgørelse kan læses på følgende adresse:

https://www.sa.dk/wp-content/uploads/2014/10/Arkivbekendtgoerelsen-Bekendtgoerelse-nr-591-af-26-juni-2003.pdf

15 Databehandlere[21]

Benyttes databehandlere til at løse opgaver på gymnasiets vegne, skal dette reguleres af en databehandleraftale. Denne skal klart beskrive behandlerens rolle og slå fast, at gymnasiet er den dataansvarlige, og at leverandøren behandler data på vegne af gymnasiet i forbindelse med de i aftalen angivne behandlinger af personoplysninger.

Gymnasiet må udelukkende benytte databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger så behandlingen opfylder kravene i GDPR.

Databehandleren må ikke gøre brug af en anden databehandler (underleverandør) uden forudgående specifik eller generel skriftligt godkendelse fra gymnasiet. Gymnasiet skal underrettes om planlagt brug af databehandlere, der ikke er angivet i databehandleraftalen, og derved give gymnasiet mulighed for at gøre indsigelse mod sådanne ændringer.

Denne anden databehandler pålægges samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandlerkontrakten. Hvis denne anden databehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver den oprindelige databehandler fuldt ansvarlig over for gymnasiet for opfyldelsen af denne anden databehandlers forpligtelser.

Behandlingens varighed, karakter, formål samt typen af personoplysninger og kategorierne af registrerede samt gymnasiets forpligtelser og rettigheder skal klart fremgå af kontrakten.

Denne kontrakt fastsætter navnlig, at databehandleren:

a) kun må behandle personoplysninger efter dokumenteret instruks fra gymnasiet, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren gymnasiet om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

b) sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en lovbestemt passende tavshedspligt.

c) under hensyntagen til behandlingens karakter, så vidt muligt bistår gymnasiet med opfyldelse af gymnasiets forpligtelse til at besvare anmodninger om udøvelse af behandlingssikkerhed og de registreredes rettigheder.

d) efter gymnasiets valg sletter eller tilbageleverer alle personoplysninger til gymnasiet efter tjenesterne vedrørende behandling er ophørt. Samtidig skal

eksisterende kopier slettes, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

e) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i aftalen, til rådighed for gymnasiet og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af gymnasiet eller en anden revisor, som er bemyndiget af gymnasiet.

f) omgående skal underrette gymnasiet, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

g) uden unødig forsinkelse skal kontakte gymnasiet efter at være blevet bekendt med brud på persondatasikkerheden.

15.1 Gymnasiets databehandlere

Tillægget **Databehandleraftaler** til denne håndbog indeholder en komplet fortegnelse over benyttede databehandlere med tilhørende databehandleraftaler.

15.2 Specielt om Lectio (MaCom)

Ifølge skolens *IT- og Datapolitik* er alle medarbejderes adgang til Lectio styret gennem tildeling af rettigheder i Lectios administratormodul. Denne autorisation skal med jævne mellemrum revurderes, og programmet anmoder med fastlagte intervaller brugeren om at angive en ny adgangskode. Hvilke informationer de forskellige kategorier af medarbejdere har adgang til fremgår af **afsnit 6** i denne håndbog. Der føres log over afviste adgangsforsøg. Gymnasiets *IT- og Datapolitik* beskriver nærmere, hvordan skolens forholder sig til personer, der gentagne gange bliver afvist af Lectios login procedure.

Håndteringen af personlige oplysninger i Lectio har siden Persondataforordningens ikrafttrædelse 25. maj 2018 været omgærdet af tolkninger og tvivl om lovligheden til sikring af de registreredes rettigheder, som for nuværende hverken kan be- eller afkræftes.

Udskiftning af Lectio til fordel for et alternativt elevadministrativt system, der med sikkerhed overholder persondataforordningen og databeskyttelsesloven, bliver derfor løbende vurderet. Dog er dette forbundet med meget store økonomiske og tidsmæssige omkostninger, hvorfor gymnasierne fortsat ønsker at benytte Lectio på ubestemt tid.

15.2.1 Risikovurdering

Der er udarbejdet en konsekvensanalyse (DPIA) til beskrivelse af de involverede risici for tab eller forkert brug af de registreredes personlige oplysninger. Følsomme og fortrolige oplysninger er i Lectio beskyttet af adgangskoder, ligesom korrespondance imellem brugerne af systemet er sikret ved kryptering. Den it-ansvarlige har etablere sikkerhedsprocedurer og streng login-kontrol til overvågning af programmets fortsatte brug.

Skulle tilsynsmyndigheden (Datatilsynet) komme med anbefalinger og/eller konklusioner vedrørende skolernes brug af Lectio, vil disse straks blive taget til efterretning og hurtigst muligt implementeret hos alle de dataansvarlige gymnasier, som denne persondatahåndbog omfatter.

16 Samarbejdspartnere (tavshedspligtserklæring)[22]

Samarbejdspartnere med delt dataansvar pålægges tavshedspligt, hvis de modtager fortrolige/følsomme personoplysninger eller almindelige personoplysninger i stort omfang. Tavshedspligtserklæringen skal underskrives, inden samarbejdspartneren modtager disse oplysninger, og erklæringen skal minimum indeholde bekræftelse på:

- at samarbejdspartneren udelukkende modtager eller behandler informationer, der er relevante for deres opgave.
- at medarbejdere, der får kontakt med oplysningerne, overholder lovgivningens (herunder straffelovens) regler om tavshedspligt.
- at tavshedspligten gælder både under og efter opgavens udførelse og omfatter alle oplysninger, gymnasiets har leveret uanset tidspunkt herfor.
- at alle persondata på anmodning fra gymnasiet slettes ved aftalens ophør.

Samarbejdspartnere er i den forbindelse andre gymnasier som nærværende gymnasium indgår et administrativt samarbejde med, f.eks.:

16.1 Lønfællesskab

En del af gymnasierne i fællesskabet indgår også i et lønfællesskab, der har til formål at mindske de administrative omkostninger.

De medarbejdere, der administrerer dette fællesskab, befinder sig fysisk på forskellige gymnasier, og er underlagt specielle sikkerhedsregler, herunder en skærpet tavshedspligt og IT-instrukser.

Al behandling af de personlige oplysninger foregår i Silkeborg Datas systemer, som er beskrevet i dennes databehandleraftale.

De nærmere sikkerhedsregler og angivelse af kontaktoplysninger er detaljeret beskrevet i den mellem parterne indgåede kontrakt om delt dataansvar.

Der er udelukkende tale om oplysninger, der er nødvendige for at udføre personaleadministration, herunder lønudbetaling. Ingen andre end det specielt uddannede personale har adgang til disse personlige oplysninger.

Slettefrister følger gymnasiets generelle slettefrister, dog undtaget oplysninger, der er krævet opbevaret af myndighederne.

17 Brud på datasikkerheden[23]

Persondataforordningen fastsætter en række regler for behandling af brud på datasikkerheden, og arbejdsgruppen *Article 29* under EU har endvidere fremsat nogle retningslinjer i publikationen *WP250* af den 3. oktober 2017.

17.1 Udvisning af rettidig omhu

Dataansvarlige og databehandlere opfordres i disse publikationer til at indføre procedurer, der hurtigt kan opdage og begrænse et databrud, så det ikke griber om sig, og samtidig vurdere risikoen for den registrerede. Er denne risiko stor, skal Datatilsynet kontaktes, og den berørte registrerede skal under visse omstændigheder orienteres i nødvendigt omfang (se **afsnit 10.1.1** og **17.3**).

17.2 Hvis databruddet sker

Ved brud på persondatasikkerheden skal gymnasiet, uden unødig forsinkelse og om muligt senest 72 timer efter bruddet på persondatasikkerheden, anmelde det til Datatilsynet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. I så tilfælde kan anmeldelse udelades.

Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Risici for den registrerede:	Procedure:
Ingen risiko	Ikke anmeldelsespligt til Datatilsynet
Moderat risiko	Anmeldelsespligt til Datatilsynet.
Høj risiko	Anmeldelsespligt til Datatilsynet samt underretningspligt over for den registrerede (se afsnit 17.3)

Denne anmeldelse skal minimum:

- beskrive karakteren af bruddet, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
- angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- beskrive de sandsynlige konsekvenser af bruddet.
- beskrive de foranstaltninger, som gymnasiet har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Gymnasiet skal kunne fremvise en samlet liste over alle brud på persondatasikkerheden. Se **afsnit 17.5** for krav til denne oversigt.

17.3 Underretning af den registrerede[24]

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter gymnasiet uden unødig forsinkelse den registrerede om bruddet. Eksempler på dette kan f.eks. være identitetstyveri eller svindel, skade på omdømme eller økonomisk ulempe.

Ved vurderingen af de sandsynlige konsekvenser skal alle de mulige konsekvenser tages i betragtning. Herunder at den registrerede kan benytte samme adgangskode til flere tjenester.

Det er ikke nødvendigt at underrette den registrerede (medmindre Datatilsynet kræver det), hvis blot en af følgende betingelser er opfyldt:

- gymnasiet har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering.
- gymnasiet har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder sandsynligvis ikke længere er reel, f.eks. ved at den dataansvarlige straks har rettet henvendelse til den uberettigede modtager, forinden vedkommende har haft mulighed for at anvende oplysningerne.
- det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Underretningen af de berørte registrerede skal som minimum indeholde samme informationer som en anmeldelse til Datatilsynet skal (se **afsnit 17.2**).

17.4 Databeskyttelsesrådgiveren

Gymnasiets DPO skal altid inddrages, når der sker et brud på persondatasikkerheden uanset omfanget og den vurderede risiko.

17.5 Oversigt over databrud[25]

Alle brud på persondatasikkerheden skal kunne dokumenteres, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger.

Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at persondataforordningens *Artikel 33* er overholdt, og skal på anmodning forevises tilsynsmyndigheden.

Listen over alle brud på persondatasikkerheden opbevares i tillægget **Skabeloner** til denne håndbog.

18 Oversigt over tillæg til håndbogen

Denne persondatahåndbog er kun fuldstændig, når følgende tillæg medregnes til dokumentation af, at gymnasiet overholder persondataforordningen (GDPR) og anden relevant lovgivning.

18.1 Den samlede dokumentation til overholdelse af GDPR

Følgende dokumentation er tilgængelig for medarbejdere og – på anmodning ved fremmøde til skolens kontor eller via e-mail – for elever og deres værger:

Dokument:	Indhold:
Kontaktoplysninger (også tilgængelig på skolens hjemmeside)	Oplysninger om det dataansvarlige gymnasium og tilknyttede databeskyttelsesrådgiver.
Persondatahåndbogen (PDH)	Denne håndbog med generel beskrivende tekst, der er fælles for alle gymnasier i fællesskabet.
IT- og Datapolitik	Skolens detaljerede opbevaring og håndtering af personlige oplysninger beskrives i dette dokument, der er tilgængelig ved henvendelse på skolens kontor.
Databehandleraftaler	Kopier af samtlige databehandleraftaler, som dem dataansvarlige angivet i tillægget **Kontaktoplysninger** benytter sig af.

18.2 Støttende dokumentation

Udover denne dokumentation er følgende dokumenter udviklet til støtte for det administrative personale, skolernes ledelse og skolernes DPO:

Dokument:	Indhold:
Skabeloner	Skabeloner over nødvendig dokumentation, som forventes gentaget (f.eks. ved start af et nyt skoleår eller ved ansættelse af personale i form af elev- og medarbejderbreve med samtykkeerklæringer).

19 Slutnoter

[1] GDPR artikel 24, stykke 1 og 2 (indførelse af databeskyttelsespolitikker). Artikel 5, 6 & 9 (principperne om lovlig behandling af personoplysninger inklusive følsomme oplysninger)

[2] GDPR artikel 32, stykke 1 (behandlingssikkerhed)

[3] GDPR artikel 4, stykke 7 (definition)

4 GDPR artikel 4, stykke 7 (definition)

5 Datatilsynets "Vejledning om fortegnelse", afsnit 3.1, litra c punkt 1.

[6] GDPR artikel 31 (pligt til samarbejde med tilsynsmyndigheden), artikel 37 (pligt til at udpege en databeskyttelsesrådgiver).

[7] GDPR artikel 12 (regler for udøvelse af den registreredes rettigheder). Artikel 13 til og med 22 (regler der skal sikre den registreredes rettigheder).

[8] GDPR artikel 30 stykke 1 (pligt til at udarbejde fortegnelse over behandlingsaktiviteter)

[9] GDPR artikel 7 (betingelser for samtykke)

[10] GDPR artikel 5 stykke 1 litra b og artikel 6 stykke 1 (legitimt og nødvendigt formål)

[11] GDPR artikel 15 stykke 1 (hvem behandler de personlige oplysninger).

[12] GDPR artikel 5 stykke 1 litra e (opbevaring på en sådan måde, at den registrerede ikke kan identificeres i et længere tidsrum end det, der er nødvendigt til formålet).

[13] GDPR artikel 5 stykke 1 litra f (… sikre tilstrækkelig sikkerhed for de pågældende oplysninger…).

[14] GDPR artikel 5, 24 og 32 stykke 4 (enhver fysisk person, der udfører arbejde for den dataansvarlige, og som får adgang til personoplysninger, må kun behandle disse efter instruks fra den dataansvarlige).

[15] GDPR artikel 32

[16] GDPR artikel 35 (Konsekvensanalyse vedrørende databeskyttelse)

[17] GDPR præambel 84

[18] GDPR artikel 4, stykke 5 (definition)

[19] GDPR artikel 24 (passende organisatoriske foranstaltninger).

[20] GDPR artikel 39, stykke 1, litra b (DPO opgaver)

[21] : GDPR artikel 28 (krav til databehandlere og underdatabehandlere), artikel 29 (behandler oplysninger efter instruks), artikel 33, stk. 2 (underretningspligt ved brud på persondatasikkerheden).

[22] Justitsministeriets og Datatilsynets vejledning om dataansvarlige og databehandlere.

[23] GDPR artikel 33 & 34 (underretning af tilsynsmyndighed og/eller den registrerede).

[24] GDPR præambel 86

[25] GDPR artikel 33, stykke 5