Indhold

1 Indledning

Denne persondatahåndbog (PDH) kan bruges som et opslagsværk for alle medarbejdere på Ingrid Jespersens Gymnasieskole, der behandler personlige oplysninger.

Skolen er dataansvarlig overfor alle personlige data, der er indhentet fra det tidspunkt eleven/medarbejderen søger om optagelse/ansættelse.

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, og gøre rettighederne nemmere at håndhæve. 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 – skal overholde forordningen med effekt fra og med den 25. maj 2018.

Denne persondatahåndbog er godkendt af skolens ledelse som dokumentation for, at reglerne (GDPR) om behandling af personlige oplysninger overholdes.

Håndbogen opdateres af skolens ledelse i samarbejde med datasikkerhedsrådgiveren og vil være tilgængelig elektronisk på First Class under Personalehåndbog 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 0):	Skolens ledelse (ansvarlig for håndtering af de personlige oplysninger, du "låner" til skolen, mens du er tilknyttet).
Databehandlere (se 1.2.2):	Systemleverandører og hosting-virksomheder (opbevarer og behandler dine data på skolens vegne, f.eks. Diskos, Skoleintra, Lectio og Microsoft).
De registrerede (se 1.2.3):	Personer som skolen "låner" nødvendige og i studiesammenhæng relevante personlige oplysninger fra.
Datasikkerhedsrådgiver (se 1.2.4)	Rådgiver i spørgsmål og klager vedr. skolens behandling af personlige data - referer direkte til skolens ledelse og myndighederne (Datatilsynet).

1.2.1 Den dataansvarlige (skolen)

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.

Skolen har en datasikkerhedsrådgiver, og det er stadig den dataansvarlige, der har ansvaret for overholdelse af persondataforordningen.

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

1.2.2 Databehandlere

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

Betegnelsen *de registrerede* dækkerover tre kategorier af personer:

1. Medarbejdere (ansøgende, nuværende og tidligere)
2. Elever (ansøgende, nuværende og tidligere)
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 Datasikkerhedsrådgiver (it-chef)

Datasikkerhedsrådgiveren rådgiver ledelsen, således at reglerne bliver overholdt, at personalet uddannes i forordningens krav, at datasikkerheden efterses og er kontaktled mellem skolens ledelse og Datatilsynet.

Rådgiveren skal være til rådighed for alle de registrerede personer med rådgivning om skolens brug af deres personlige oplysninger.

Kontaktoplysninger til skolens datasikkerhedsrådgiver (it-chef) findes i tillægget **Kontaktoplysninger** til denne håndbog.

2 De registreredes rettigheder[3]

2.1 Elevers og forældres/værgers rettigheder

Grundskolen:
Når forældre opskriver deres barn til skolen, afgiver de personlige oplysninger. Når eleven optages på skolen, indsamler og behandler skolen forskellige andre oplysninger, der enkeltvis eller samlet set er personfølsomme oplysninger.

Ved optagelse af eleven udfylder forældrene en skriftlig samtykkeerklæring vedrørende behandling af visse oplysninger, f.eks. brug af billeder m.v. Samtykkeerklæringen opbevares i mappe på skolens kontor.

Gymnasiet:
Når eleven tilmelder sig gymnasiet 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 skolen udfylder eleven/forældre/værge en skriftlig samtykkeerklæring vedrørende behandling af visse oplysninger, f.eks. brug af billeder. Se afsnit 4 samt elevbrev. Samtykkeerklæringen opbevares i mappe på skolens kontor.

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 datasikkerhedsrådgiver (it-chef).

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.

I tillægget **Skabeloner** til denne manual er elevbrev, gymnasiet samt forældre/elevbrev, grundskolen.

I tillægget **Checklister** til denne manual findes en checkliste, der benyttes til sikring af, at alle informationer og samtykker indhentes og dokumenteres.

2.2 Medarbejdernes rettigheder

Denne håndbog er udviklet for at sikre dine rettigheder og skolens overholdelse af GDPR. Et af kravene er, at du som medarbejder på skolen løbende instrueres i, hvordan du skal sikre, at personlige data, som skolen behandler, bliver benyttet forsvarligt.

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

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

Persondataforordningen (*kap. 3, artikel 13-16*) giver dig bestemte rettigheder i forbindelse med, at skolen behandler dine personlige oplysninger.

Du har:

- Ret til at modtage oplysning om en behandling af dine personoplysninger.
- Ret til at få indsigt i dine personoplysninger, dvs. ret til at se, hvad skolen har registreret om dig.
- Ret til at få urigtige personoplysninger berigtiget.
- Ret til at få dine personoplysninger slettet, også kaldet "retten til at blive glemt", når din tilknytning til skolen ophører.
- Ret til at flytte dine personoplysninger (dataportabilitet)
- Ret til at indgive klage til databeskyttelsesrådgiveren eller Datatilsynet, hvis du mener, at skolen ikke følger reglerne på området.

Desuden har du:

- Ret til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
- Ret til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering

Skolen skal kunne dokumentere, at vi behandler dine personlige data i henhold til ovenstående rettigheder. Denne håndbog er en vigtig del af denne lovkrævede dokumentation.

Du vil opleve, at din underskrift til tider er påkrævet i forskellige sammenhænge for at sikre dokumentation af, at du har modtaget den krævede instruktion og eventuelt har givet samtykke til visse behandlinger af dine personlige oplysninger.

3 Hvilke data behandles[4]

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 på barnet tillige fødselsdato og opskrivningsdato til brug for udregning af anciennitet på ventelisten, når forældre søger optagelse af deres barn på skolens ansøgerliste via skolens web-butik.
- Fulde navn, adresse, telefonnummer og e-mailadresse på forældre/værger og elever fra det tidspunkt en elev søger optagelse på skolen gennem *optagelse.dk*.
- Fulde navn, adresse, telefonnummer og e-mailadresse på medarbejdere fra det tidspunkt vedkommende ansøger om ansættelse på skolen.

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.
- Vidensoverdragelse fra kommende børnehaveklasseelevs børnehave
- Elevernes karakterer, besvarelser fra skriftlige eksaminer samt klagesager.

3.1 TV-overvågning

Der foretages TV-overvågning af visse arealer og områder af skolen ud fra et kriminalpræventivt formål med henblik på at undgå hærværk og vold. Der foretages ikke tv-overvågning af områder med adgang for almindelig færdsel. Optagelserne opbevares i et aflåst rum og slettes efter 8-10 dage, afhængig af aktivitet i overvåget område.

4 Samtykkeerklæring[5]

Visse oplysninger, f.eks. brug af billeder i sammenhæng med markedsføring af skolen og i Den Grønne Bog, 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.

Samtykke er:

Frivillig, specifik, informeret og utvetydig viljetilkendegi-velse, der bekræfter at personoplysninger må behandles. Se tillægget Skabeloner for eksempler.

Samtykket gemmes i den registreredes elev- eller medarbejder-mappe på skolens kontor eller i skolens arkiv indtil fem år efter den

registrerede har forladt skolen.
Billederne befinder sig på skolens krypterede server i relevante mapper.
Samtykket kan til hver tid tilbagekaldes ved henvendelse på kontoret.

5 Formål og tidspunkt for registrering af personlige oplysninger[6]

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:
Anmeldelsesblanket om optagelse i gymnasiet: ***Ved afslag på optagelse på skolen slettes oplysningerne straks***	**GYMNASIET:** 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, telefonnumre og e-mailadresser. Ansøgningen hentes via gymnasiets administrationsprogram, Lectio, hvor den indlæses og oplysningerne arkiveres i et såkaldt "ansøgermodul". Ansøgningen printes desuden og lægges fysisk i et skab på skolens kontor, som er aflåst og med alarm, når skolen er lukket.
Optagelse:	Ved optagelse flyttes oplysningerne elektronisk i Lectio fra ansøgermodulet til elevmodulet. Samtidig overføres elev og forældreoplysninger til administrationssystemet Diskos med henblik på opkrævning af skolepenge.
Under uddannelsesforløbet:	På skolens kontor har hver klasse i et arkivskab en hænge-mappe, hvor hver elev har et omslag med bl.a. den fysiske ansøgning og samtykkeerklæringer. I omslaget 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.
Karakterer	Standpunktskarakterer gemmes i elevmappen, mens eksamenskarakterer gemmes i pengeskab.
Udmeldelsesmappen:	Ved udmeldelse (dimission) flyttes hele årgangen af elevmapper til en kasse, som arkiveres i skolens aflåste arkivrum. Ved udmeldelse "i utide" (før dimission) flyttes elevmappen til en ny hængemappe med "årets udmeldte". Disse mapper flyttes ved årets udgang til det aflåste arkivrum.

Sletning af data for udgåede elever:	Standpunktskarakterer slettes efter 10 år. Eksamenskarakterer sendes efter 30 år til Rigsarkivet, hvor det opbevares uendeligt. Besvarelser fra skriftlige eksaminer slettes efter 5 år. Samtykkeerklæringer slettes efter 5 år. Elevmapper bliver løbende gennemgået for irrelevant information, men gemmes ellers på ubestemt tid af historiske årsager. Elever/forældre slettes i Diskos efter elevens udmeldelse, og når økonomiske udeståender er afsluttet. Informationer vedrørende SU og SPS opbevares i aflåst arkiv.
Ansøgning om optagelse i grundskolen: ***Indtil der eventuelt opnås optagelse på IJG, gemmes ansøgningen så længe barnet er skolesøgende (det vil sige til og med 9. klasse). Herefter slettes alle oplysninger.***	**GRUNDSKOLEN**: Der søges om optag på skolens ansøgerliste via skolen web-butik. Ansøgningen indeholder barnets fødselsdato, navn, adresse samt forældre/værges navne, adresser, telefonnumre og e-mailadresser. Ansøgningen overføres til skolens administrationssystem Diskos. Ansøgningen printes desuden og arkiveres fysisk i mappe, i skab på skolens kontor, som er aflåst og med alarm, når skolen er lukket.
Optagelse:	Ved optagelse flyttes oplysningerne elektronisk i Diskos fra ansøgermodulet til elevmodulet. Samtidig overføres oplysningerne også elektronisk til STIL med henblik på oprettelse af unilogin til elever/forældre, hvorfra de synkroniseres videre til databehandlere, bl.a. Skoleintra.
Under skoleforløbet:	På skolens kontor har hver klasse en mappe, hvor hver elev har et datablad. Her noterer elevens lærere informationer om eleven, Hvad med f.eks. korrespondance med forældre?, lægeerklæringer? ifm. idræts- og andet fravær?, informationer om faste aftaler med psykolog??
Karakterer	Indskrives i Diskos Standpunkt. I 8.-9. klasse får eleverne standpunktskarakterer. Disse indskrives i Diskos Standpunkt af lærerne. Herefter udskrives karakterblad til eleverne. Karaktererne gemmes i Diskos Standpunkt. 9. klasses eksamenskarakterer Afgangsprøven gemmes i mappe i stålskab.
Sletning af data for udgåede elever:	Standpunktskarakterer slettes efter 10 år. Eksamenskarakterer sendes efter 30 år til Rigsarkivet, hvor det opbevares uendeligt. Besvarelser fra skriftlige eksaminer slettes efter 5 år. Samtykkeerklæringer slettes efter 5 år. Elevmapper bliver løbende gennemgået for irrelevant information, men gemmes ellers på ubestemt tid af historiske årsager. Informationer vedrørende SPS opbevares i aflåst arkiv. I tilfælde hvor elever meldes ud uden for gængse tidsperioder gemmes bilag 2-3 år

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***, ***www.skolejobs.dk***, ***lærerjob.dk***, ***www.jobindex.dk*** *m.v. og evt.*

Arkiveres elektronisk på First Class	*via dag- og fagblade.* Ansøgningerne sendes digitalt til job@ijg.dk, hvorfra de kan læses af ansættelsesudvalget. Ansøgere, der indkaldes til samtale, udskrives til ansættelsesudvalget.
Ansættelse:	Personen, der ansættes, får en ansættelseskontrakt på papir. Når denne modtages retur i underskrevet stand, opbevares den i et brandsikret og aflåst stålskab, placeret i skolens administration, i en personalemappe. Administrationen er uden for åbningstid aflåst og med alarm. Personalemapperne er sorteret efter cpr.nr. ?? Til lønindberetning opbevares time-dagpenge formularer og diverse oplysninger om honorarer og tillægsgivende kvalifikationer.??
Under ansættelse:	Der informeres om persondataforordningen og indhentes samtykke til brug af billeder af lærerne, Samtykkeerklæringer opbevares i mappe på skolens kontor. Samtykke vil fremadrettet blive opbevaret i personalemapperne. 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. ??
Opbevaring af oplysninger om fratrådte ansatte:	Ved fratrædelse gemmes personalemapperne i skolens aflåste arkivrum i maksimalt 20 år. Billeder opbevares dog på ubegrænset tid af historiske årsager.
Sletning af data efter ansættelsens ophør:	Samtykkeerklæringer, dagpengeskemaer, sygemeldinger og personalesager makuleres efter 5 år. Alle ansøgninger, som ikke fører til ansættelse, slettes straks. Dog kan ansøgninger fra personer, der senere ved behov kan tilbydes ansættelse, opbevares i en længere periode. Ansættelsesbreve opbevares uendeligt af historiske årsager. Uopfordrede ansøgninger gemmes efter indhentning af Samtykke.

6 Hvem behandler dine personlige oplysninger?[7]

Følgende medarbejdergrupper har adgang til at se og behandle de indsamlede personlige oplysninger.

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 tillægget **Databehandleraftaler**.

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, vicerektor, afdelingsinspektør og viceafdelingsinspektører)	Dataansvarlige
Administrative personale (sekretærer og uddannelsesledere)	Studieadministration
Studievejledere/skolepsykologer	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, vicerektor, afdelingsinspektør og viceafdelingsinspektører)	Dataansvarlige
Administrative personale (sekretærer)	Studieadministration
Studievejledere/skolepsykologer	Rådgivning

OBS: Databehandlere benyttes

6.2 De pårørendes personlige oplysninger (inklusive CPR-numre)

Hvem har adgang til oplysningerne:	Formål/noter:
Skolens ledelse (rektor, vicerektor, afdelingsinspektør og viceafdelingsinspektører)	Dataansvarlige
Administrative personale (sekretærer)	Skole og studie-administration
Studievejledere/skolepsykologer	Kun kontaktoplysninger
Lærere	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, vicerektor, afdelingsinspektør og viceafdelingsinspektører)	Dataansvarlige
Administrative personale (sekretærer)	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, vicerektor, afdelingsinspektør og viceafdelingsinspektører)	Dataansvarlige
Administrative personale (sekretærer)	Personaleadministration
IT-medarbejdere	Systemvedligeholdelse

6.4 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 skolens ledelse detaljeret og præcist har definerer 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.

Den egentlige procedure herfor, inklusive hvem der har nøgler til aflåste rum og pengeskab, er beskrevet i **afsnit 16** samt i tillægget *IT- og datapolitik*.

7 Hvor længe opbevarer vi dine data?[8]

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.

Du finder en mere detaljeret beskrivelse af slettefristerne i tabellerne i **afsnit 5.**

Visse data skal opbevares til arkivformål, videnskabelige eller historiske formål i samfundets interesse, hvilket betyder at skolen 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 skolen at opbevare.

Af historiske hensyn forbeholder skolen 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.

I tilfælde hvor elever meldes ud uden for gængse tidsperioder gemmes bilag 2-3 år

8 Bibliotekssystemer

Skolen har eget bibliotek, hvor bøgernes udlån styres gennem to elektroniske bibliotekssystemer: BOSS Infomatik til gymnasiet, som er et internt system og Cicero (Bibliomatic) til grundskolen, som er et eksternt system med dataaftale.

Det er alene bibliotekarerne, der har adgang til bibliotekssystemet.

9 Fysisk opbevaring af personlige oplysninger[9]

Skolen 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 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 tillægget ***IT- og datapolitik*** til denne håndbog for nærmere beskrivelse af såvel de almindelige som de følsomme personoplysningers fysiske opbevaring.

9.1 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 systemer Diskos, Skoleintra, Lectio og Microsoft Sharepoint.

9.2 Forældres og værgers personlige oplysninger

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

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

9.3 De ansattes personlige oplysninger

Alle medarbejdernes personlige oplysninger – udover almindelige kontaktinformationer – opbevares udelukkende på skolens krypterede servere. Ansættelseskontrakter opbevares i brandsikkert pengeskab på skolens aflåste kontor.

Liste over personer med adgang til disse oplysninger findes i **afsnit 6.3**.

10 Instruktion til medarbejdere[10]

Den nyansatte skal på ansættelsestidspunktet informeres og instrueres i skolens 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.
- Kontaktoplysninger på dataansvarlige og datasikkerhedsrådgiver.

På skolens samtykkeerklæringer til såvel forældre, 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.

Det gælder for såvel forældre, 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.

Medarbejderbrev med samtykkeerklæring udleveres ved ansættelse.

For information om, hvor oplysningerne fysisk opbevares henvises til skolens *IT- og datapolitik*. ?

Checkliste benyttes til sikring af, at alle informationer og samtykker indhentes og dokumenteres.

11 Behandlingssikkerhed

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.

11.1 Interne retningslinjer

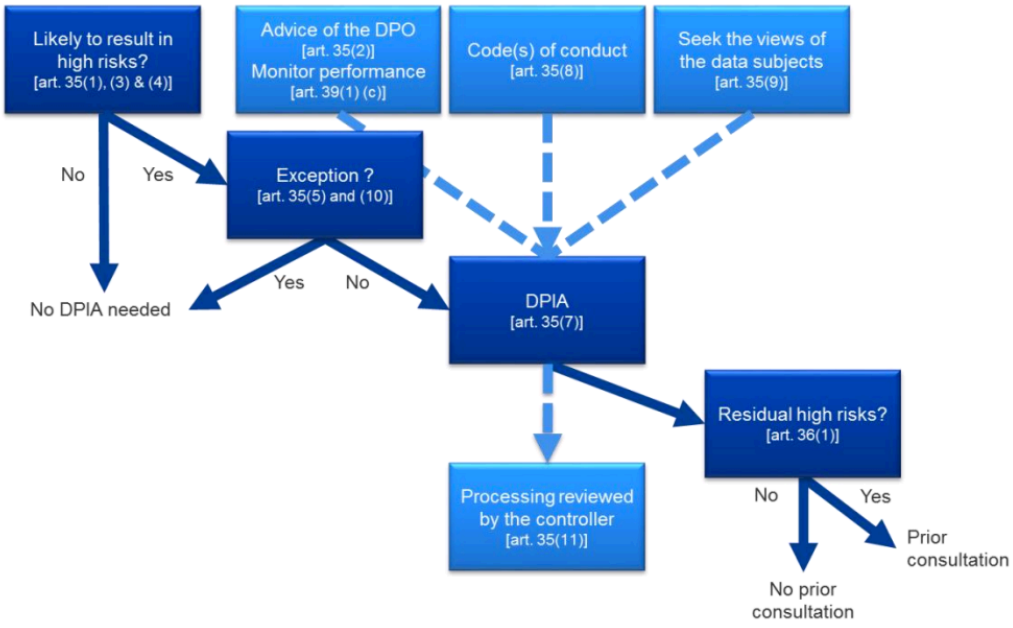
Behandlingssikkerheden på skolen er beskrevet i et tillæg til denne håndbog, *IT- og datapolitik*. Denne indeholder af beskrivelse procedurer for data backup og regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden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

Se **afsnit 16** for retningslinjer ved brud på persondatasikkerheden.

11.1.1 Konsekvensanalyse (DPIA)

Hvis et brud på datasikkerheden vil resultere i en høj risiko for den registreredes frihedsrettigheder, skal skolen 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:



11.1.2 Behandlinger med særlig høj risiko

Håndtering og opbevaring af personlige oplysninger uden for 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 = skolen)
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.

11.1.3 Brug af pseudonymisering

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.

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

11.2 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.

11.3 Sikkerhedsbevidsthed (Awareness)[11]

Skolen 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 skolen.

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

Opmærksom 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 afholdes løbende kampagner med det formål at understøtte medarbejdernes fokus på datasikkerhed.

I lyset af skolens 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 13** for information om medarbejderuddannelse.

12 Når den ansatte ikke er på skolen

12.1 Hjemmearbejdsplads

Der gælder følgende regler og retningslinjer for ansatte på skolen om omgang med skolerelaterede personfølsomme data såvel i fysisk form som i digital form fra hjemmearbejdsplads:

- 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 skiftes hver 3. 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.
- Elektronisk udstyr skal benyttes og opbevares ansvarligt, så andre ikke kan misbruge det.
- Det er ikke tilladt at udveksle skolerelaterede 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. Se endvidere afsnit 14.

12.2 Offentlige netværk

Det er ikke tilladt at håndtere skolerelaterede personfølsomme data på elektronisk udstyr, der har netadgang via offentligt tilgængelige netværk, og der skal altid udvises særlig opmærksomhed på de risici, der er forbundet med brug af offentlige netværk. Herunder om uvedkommende personer kan se computer-skærmen, f.eks. via spejling i vinduer m.m.

12.3 Mistanke om misbrug

Hvis man får mistanke om, at der er sket misbrug af skolerelevant data fra det benyttede elektroniske udstyr, hvad enten det er ens private udstyr eller udlånt af skolen, skal skolen ledelse orienteres uden unødig forsinkelse.

Ledelsen vil derefter informere skolens datasikkerhedsrådgiver (it-chef), der tager initiativ til udfærdigelse af en DPIA (risikoanalyse), og vurderer om tilsynsmyndigheden skal involveres.

Ledelse og datasikkerhedsrådgiver analyserer derefter situationen ved hjælp af den udfærdigede DPIA og indfører – hvis relevant – ændringer i skolens procedurer eller systemer, så lignende databrud i fremtiden kan undgås.

13 Medarbejder uddannelse

De ansatte på skolen, der har adgang til personlige og personfølsomme data, skal ifølge loven uddannes i persondataforordningen og skolens 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 skolens ansvar at opdatere håndbogen og sikre, at de ansatte hurtigt muligt bliver informeret om ændringer i håndbogens indhold og gymnasiets procedurer vedrørende datasikkerhed.

14 Brug af Cloud-løsninger

Skolen tilbyder visse cloudløsninger til arkivering og deling af information. Selvom disse løsninger ikke alle 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 og på sikkert SharePoint. Manglende overholdelse af denne regel vil blive betragtet som brud på datasikkerheden. Ved tvivlstilfælde skal skolens kontor eller datasikkerhedsrådgiver straks kontaktes.

Se endvidere **afsnit 12.1** for regler vedrørende hjemmeplads.

15 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 elektronisk 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 giver samtykke til dette. Disse billeder opbevares på ubestemt tid i skolens aflåste arkivrum.

Ligeledes opbevares Den Grønne Bog, brochurer og andre publikationer af historiske årsager i skolens aflåste arkivrum på ubestemt tid.

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

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

16 Databehandlere[12]

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

Skolen 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 skolen. Skolen skal underrettes om planlagt brug af databehandlere, der ikke er angivet i databehandleraftalen, og derved give skolen 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 skolen for opfyldelsen af denne anden databehandlers forpligtelser.

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

Denne kontrakt fastsætter navnlig, at databehandleren:

a) kun må behandle personoplysninger efter dokumenteret instruks fra skolen, 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 skolen 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 skolen med opfyldelse af skolens forpligtelse til at besvare anmodninger om udøvelse af behandlingssikkerhed og de registreredes rettigheder.

d) efter skolens valg sletter eller tilbageleverer alle personoplysninger til skolen 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 skolen og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af skolen eller en anden revisor, som er bemyndiget af skolen.

f) omgående skal underrette skolen, 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 skolen efter at være blevet bekendt med brud på persondatasikkerheden.

16.1 Skolens databehandlere

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

16.2 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. Hvilket informationer de forskellige kategorier af medarbejdere har adgang til fremgår af **afsnit 6** i denne håndbog. Der føres log over afviste adgangsforsøg. Skolens *IT- og datapolitik* beskriver nærmere, hvordan skolens forholder sig til personer, der gentagne gange bliver afvist af Lectios login procedure.

⚠ **Vigtig information om tidsbegrænset brug af Lectio:**

Lectio kan for nærværende ikke opfylde persondataforordningens krav til sikker behandling af personlige oplysninger.

Der findes imidlertid ikke et brugbart alternativ på markedet på nuværende tidspunkt, hvorfor skolen ser sig nødsaget til at fortsætter med at benytte programmet, med øget forsigtighed og med streng login-kontrol, frem til og med 31. december 2018, hvor det forventes at et alternativ kan indfases som nyt administrativt program med fuld overholdelse af persondataforordningen.

16.2.1 Risikovurdering

17 Samarbejdspartnere (tavshedspligtserklæring)[13]

Samarbejdspartnere (ikke databehandlere) pålægges tavshedspligt, hvis de modtager 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, skolen har leveret uanset tidspunkt herfor.
- at alle persondata på anmodning fra skolen slettes ved aftalens ophør.

18 Brud på datasikkerheden[14]

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.

18.1 Udvisning af rettidigt 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 11.1.1** og **18.3**).

18.2 Hvis databruddet sker

Ved brud på persondatasikkerheden skal skolen 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 18.3)

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 datasikkerhedsrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- beskrive de sandsynlige konsekvenser af bruddet.
- beskrive de foranstaltninger, som skolen har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Skolen skal kunne fremvise en samlet liste over alle brud på persondatasikkerheden. Se **afsnit 18.5** for krav til denne oversigt.

18.3 Underretning af den registrerede

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter skolen 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:

- skolen 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.
- skolen 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 18.2**).

18.4 Datasikkerhedsrådgiveren

Skolens datasikkerhedsrådgiver (it-chef) skal altid inddrages, når der sker et brud på persondatasikkerheden uanset omfanget af den vurdere risiko.

18.5 Oversigt over databrud

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.

19 Oversigt over tillæg til håndbogen

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

Den samlede dokumentation består således af følgende dokumenter:

Dokument:	Indhold:
Persondatahåndbogen (PDH)	Denne håndbog med generel beskrivende tekst
Kontaktoplysninger	Oplysninger om den dataansvarlige og datasikkerhedsrådgiver.
Skabeloner	Skabeloner over nødvendig dokumentation, som forventes gentaget (typisk minimum ved start af et nyt skoleår eller ved ansættelse af personale).
Checklister	Sikrer overholdelse af oplysningspligt og indhentning af nødvendige samtykker samt rapporteringspligt ved brud på persondata sikkerheden.
Databehandleraftaler	Kopier af samtlige databehandleraftaler, som dem, dataansvarlige angivet i tillægget **Kontaktoplysninger,** benytter sig af.
It- og datapolitik	Indeholder rammerne for styring af datasikkerheden på IJG.

20 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 12 (regler for udøvelse af den registreredes rettigheder). Artikel 13 til og med 22 (regler der skal sikre den registreredes rettigheder).

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

[5] GDPR artikel 7 (betingelser for samtykke)

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

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

[8] 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).

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

[10] 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).

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

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

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

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