

Håndbog i behandling af personoplysninger

Varde Handelsskole og handelsgymnasium

Indledning

Personoplysninger

Behandling af personoplysninger

Almindelige personoplysninger

Følsomme personoplysninger

Fortrolige personoplysninger

Den registreredes rettigheder

- **Orientering om behandling af personoplysninger**
- **Indsigtsret**
- **Retten til indsigelse**
- **Retten til sletning**

Betingelser for gyldigt samtykke

Dataansvarlig

Databehandler

Databehandleraftale

Sletning

- **Elevoplysninger**
- **Medarbejder**

Fortegnelser over skolens behandlingsaktiviteter

Orientering om læk til den registrerede person

Databeskyttelsesrådgiveren

Behandlingssikkerhed

Indledning

Denne håndbog tjener flere formål. For det første skal den sikre, at de ansatte på Varde Handelsskole og handelsgymnasium kender kravene og skolens retningslinjer for behandling af persondata - både ift. elever, ansatte og personer, som er i kontakt med Varde Handelsskole og handelsgymnasium. For det andet skal håndbogen sikre, at Datatilsynet kan få et indblik i, hvordan persondata behandles på Varde Handelsskole og handelsgymnasium.

På Varde Handelsskole og handelsgymnasium skal vi for at overholde behandlingen af personoplysninger efter reglerne nikke til nedenstående punkter:

- Vi sikrer, at vi kun indsamler de personoplysninger, der er hjemmel til i lovgivningen, i overenskomsterne eller i form af samtykke fra den registrerede person selv eller væрге
- Vi orienterer den registrerede person om, at vi behandler dennes personoplysninger og vi støtter vedkommende i at udøve retten til indsigt, berigtigelse, sletning eller klage
- Vi sikrer, at personoplysninger kun kan ses/tilgås af de medarbejdere eller andre personer, der aktuelt har en jobfunktion på Varde Handelsskole og handelsgymnasium eller en rolle (fx forældre), der berettiger til dette
- Vi sikrer, at vores it-leverandører (databehandlere) kun behandler personoplysninger efter instruks fra os, hvilket kræver, at der indgås en kontrakt med tilhørende databehandlaftale og at der sker kontraktopfølgning - samt at vi i det hele taget kun indgår aftaler med de leverandører, der har en sikkerhed og dataetik, der bidrager til at beskytte vores personoplysninger.
- Vi sikrer at personoplysninger slettes, når de ikke længere er nødvendige for vores opgave
- Vi har ajourførte og kendte retningslinjer, som på en klar og letforståelig måde fortæller vores medarbejdere, hvordan de skal håndtere personoplysninger korrekt
- Vi fører en fortegnelse over hovedområderne for vores persondatabehandling
- Vi har en databeskyttelsesrådgiver. Denne funktion varetages af Peter Martin Pedersen fra Herningsholm Erhvervsskole

Overordnet set er det Varde Handelsskole og handelsgymnasiums ansvar, at de personoplysninger, som vi behandler på skolen, som led i elev- og medarbejderadministrationen, sker efter reglerne. Og eftersom alle medarbejdere på skolen i større eller mindre omfang beskæftiger sig med personoplysningerne i de forskellige arbejdsopgaver, er det en fælles daglig opgave, at passe godt på personoplysningerne i de forskellige medier, it-systemer og sammenhænge, som de indgår i.

Personoplysninger

Personoplysninger nævnes mange gange i denne håndbog og her ser du en samlet oversigt over de forskellige kategorier af personoplysninger, som inddeles i forskellige grader af følsomhed (almindelige, fortrolige, semifølsomme og følsomme).

Stigende grad af følsomhed og strengere betingelser for behandling	Kategori	Elev	Forældre	Medarbejder
	<u>Følsomme personoplysninger</u> (kræver evt. samtykke for at oplysningen kan registreres, skal sendes via Sikker Mail og skal overføres til et it-system med systemlogning senest 1 måned efter sagsbehandlingen er afsluttet)	Helbredsoplysninger, foreningsmæssigt tilknytning, politisk, religiøs eller filosofisk overbevisning, oplysninger om race, etnicitet, oplysninger om seksuel orientering	Helbredsoplysninger, foreningsmæssigt tilknytning, politisk, religiøs eller filosofisk overbevisning, oplysninger om race, etnicitet, oplysninger om seksuel orientering	Helbredsoplysninger, foreningsmæssigt tilknytning, politisk, religiøs eller filosofisk overbevisning, oplysninger om race, etnicitet, oplysninger om seksuel orientering
	<u>Semifølsomme personoplysninger</u>	Straffedomme og lovovertrædelser	Straffedomme og lovovertrædelser	Straffedomme og lovovertrædelser
	<u>Fortrolige oplysninger</u> (hører til de almindelige personoplysninger, men er omfattet af tavshedspligt, skal sendes via Sikker Mail og skal overføres til et it-system med systemlogning senest 1 måned efter sagsbehandlingen er afsluttet)	CPR, portrætbilleder (offentliggørelse på internet kræver samtykke) karakterer, studievejledning, oplysninger om væsentlige sociale problemer, sanktioner, eksamensbeviser, økonomiske oplysninger og andre private forhold	CPR, oplysninger om væsentlige sociale problemer, økonomiske oplysninger og andre private forhold	CPR, foto (både portræt og situationsbilleder - offentliggørelse på internettet kræver samtykke) karakterer, oplysninger om væsentlige sociale problemer, økonomiske oplysninger og andre private forhold, personlighedstest, logning af internettrafik og kontrol med e-mails, disciplinære foranstaltninger, afskedigelse, fratrådte medarbejders e-mails
	<u>Almindelige personoplysninger</u>	Ansøgning, stamdata/kontaktdata, optagelse, indskrivning, udlån af bøger/bærbar, valg af studieretning, hold/fag, skema, lektiegivning, situationsbilleder fra skolens hverdag, logning af internettrafik/korrespondance på UDDATA+/Fronter, deltagelse i arrangementer, rejser fremmøde/fravær, udskrivning	Stamdata/kontaktdata, civilstand, forældremyndighed	Stamdata/kontaktdata, rekruttering, cv, ansættelse, løn, kontooplysninger, beskatning, fri telefon og pc, hjemmeopkobling, arbejdsopgaver, kurser, meritter, fremmøde og fravær, referat fra MUS/GRUS samtaler, sletning af oplysninger

Personoplysninger er enhver form for information om en fysisk person (fx ansatte, elever forældre og fysiske samarbejdspartnere) Personoplysningerne kategoriseres i forskellige grader af fortrolighed og følsomhed jf. ovenstående figur. Jo mere fortrolig eller følsom en personoplysning er, jo bedre skal skolen passe på den.

Behandling af personoplysninger

Begrebet "behandling af personoplysninger" dækker over alt, hvad man kan udsætte en personoplysning for med skriftlige og digitale redskaber, dvs. indsamling, registrering, systematisering, læsning, søgning, redigering, kopiering, kryptering og sletning.

Almindelige personoplysninger

De "almindelige personoplysninger" (som kan ses i ovenstående tabel) må behandles af skolen, hvis mindst en af følgende betingelser er opfyldt:

- Den registrerede elev eller medarbejder har givet samtykke til det
- Behandling er nødvendig for indgåelse eller opfyldelse af en ansættelseskontrakt
- Behandling er nødvendig for overholdelse af en retlig forpligtelse, som påhviler skolen, fx indgåelse af en kontrakt
- Behandling er nødvendig for beskyttelse af vitale interesser (i en situation, hvor den pågældende person selv er ude af stand til dette)
- Behandling er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som skolen har fået pålagt (fx. Skolens kerneopgave med undervisning og den tilhørende elevadministration)

Som hovedregel kan de almindelige personoplysninger om medarbejdere, jobansøgere, elever og forældre behandles med hjemmel i en af punkterne ovenfor. Det vil sige at behandlingen kan ske uden den registrerede persons udtrykkelige samtykke.

Et eksempel kunne være at for at kunne skolen kunne varetage sin kerneopgave, registrerer skolen digitalt elevernes deltagelse i undervisningen, herunder aflevering af skriftlige opgaver.

Et andet eksempel kunne være at i et ansættelsesforhold har arbejdsgiveren ifølge skattelovgivningen indberetningspligt overfor SKAT om lønoplysninger. Dermed er det nødvendigt at videregive oplysninger til SKAT om medarbejderens identitet (herunder cpr-nr.) bopælskommune og lønnens sammensætning og størrelse. Dette kan dermed ske uden samtykke.

Følgende behandlinger af almindelige personoplysninger kræver dog samtykke, idet behandlingen går ud over det "nødvendige"

- Offentliggørelse af fotos og levende billeder af medarbejdere og elever på det åbne internet
- Offentliggørelse af fotos og kontaktoplysninger af medarbejdere og elever i trykte publikationer (fx markedsføringsmateriale)
- Registrering og opbevaring af visse helbredsdiagnoser om medarbejdere og elever
- Videregivelse af oplysninger om elev til ny modtager skole, hvis eleven forlader skolen
- Videregivelse af oplysninger om medarbejdere og elever til ekstern part fx markedsføring
- Opbevaring af jobansøgers ansøgning i mere end 6 måneder
- Indhentning af straffeattest, referencer og helbredsoplysninger som led i rekrutteringsproces
- Videregivelse af cpr-nummer til en faglig organisation, som medarbejderen ikke er medlem af

Følsomme personoplysninger

Følsomme personoplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Det er som udgangspunkt *forbudt* at registrere og behandle de følsomme personoplysninger.

Dog kan der behandles følsomme personoplysninger, hvis en af følgende betingelser er opfyldt:

- a) Den registrerede har givet udtrykkeligt *samtykke* til specifikke formål fx studievejledning
- b) Behandling er *nødvendig* for skolens overholdelse af arbejds- og socialretlige forpligtelser ifølge lovgivningen eller kollektiv overenskomst
- c) Behandling er *nødvendig* for beskyttelse af vitale interesser (i en situation, hvor den registrerede person selv er ude af stand til dette)
- d) Behandling vedrører personoplysninger, som tydeligvis er *offentliggjort* af den registrerede person
- e) Behandling er *nødvendig* for at retskrav kan fastlægges, gøres gældende eller forsvares
- f) Behandlingen har udtrykkelig hjemmel i *speciallovgivning* fx SU-bekendtgørelsen

Hvad der er "*nødvendigt*" skal fremgå udtrykkeligt af lovgivningen på uddannelsesområdet, eksempelvis omkring optagelseskrav og i denne situation, skal der ikke indhentes samtykke til behandlingen.

I ansættelsesforhold kan der uden samtykke behandles følsomme personoplysninger om overenskomstmæssige (fagforeningsmæssige) tilhørsforhold, hvis overenskomsten pålægger arbejdsgiveren en pligt til behandling. Dette kan eksempelvis være pligten til at underrette den faglige organisation ved afskedigelser eller hvis overenskomsten forudsætter videregivelse af personoplysninger til tillidsrepræsentanten eller den faglige organisation som led i lønforhandlinger eller fagretlige konfliktløsning. Dette gælder uanset om medarbejderen er medlem af den pågældende faglige organisation eller ej, så længe ansættelsesforholdet er omfattet af den pågældende overenskomst.

I ansættelsesforhold kan der også uden samtykke behandles følsomme oplysninger om helbredsdiagnoser, hvor det er nødvendigt eksempelvis i forbindelse med et flex-job.

Hvis følsomme personoplysninger sendes via e-mail, skal det ske via en krypteret mailforbindelse fx Sikker Mail eller e-boks.

Eksempler på følsomme personoplysninger om elever og medarbejdere:

Elever:

Situation	Nødvendig oplysning ifølge hjemmelsgrundlaget	Kategori	Skolen får oplysningerne fra	Behandlingshjemmel i lovgivning	Krav om samtykke	Dataansvarlig
Uddannelsesparathedsvurdering	Karakterer, sociale og personlige forudsætninger	Almindelige fortrolige følsomme	www.optagelse.dk		Nej	UU center
Optagelse på særlige vilkår	Lægeerklæring der omfatter diagnose indenfor autismespektrum forstyrrelser og en anbefaling om særundervisning	Almindelige fortrolige følsomme	Elevens ansøgning		Nej	Skolen som eleven har som 1. prioritet
Studievejledning		Almindelige fortrolige følsomme		HHX bekendtgørelse "for at fastholde"	Ja	Skolen
Videregivelse til Studievalg				Samtykke jf. bkg. Om studievalg	Ja	Skolen og regionalt studievalgscenter
Specialundervisning og anden specialpædagogisk bistand	Oplysninger om særlige behov på baggrund af sagkyndige oplysninger og udtalelser herom	Almindelige fortrolige følsomme	Eleven selv		Ja	Skolen
SPS	Oplysninger om fysisk eller psykisk funktionsnedsættelse som giver et fagligt velbegrunder behov for bistand	Almindelige fortrolige følsomme	Eleven selv	SPS bkg. §4	Ja	Skolen
Sygeundervisning	"oplysningen om sygdom, der medfører at eleven i længere tid ikke kan følge den almindelige undervisning"	Almindelige fortrolige følsomme	Eleven selv		Nej	Skolen
Udeboende SU	Dokumentation for de betingelser, der er nævnt (om, at ganske særlige forhold i hjemmet, fx sygdom skal indhentes af skolen)	Almindelige fortrolige følsomme	Eleven selv og de sociale myndigheder	SU bkg. §19	Nej	Skolen og SU styrelsen
Sygeeksamen	"Dokumenteret sygdom"	Almindelige fortrolige følsomme	Eleven	Alm. Eksamens bkg. §9	Nej	Skolen

Medarbejdere:

Situation	Nødvendig oplysning ifølge hjemmelsgrundlaget	Kategori	Skolen får oplysningerne fra	Behandlingshjemmel i lovgivning	Krav om samtykke	Dataansvarlig
Oplysninger om fagforeningsmæssig tilknytning	Arbejdsgiver er iflg statslige overenskomster forpligtet til at oplyse om overenskomstgrundlag i jobopslag, lønindplacering i overenskomst med organisationsaftalerne, underrette den forhandlingsberettigede organisation om lønaftaler samt om opsigelse og bortvisning	Oplysninger om fagforeningsmæssig tilknytning er en følsom personoplysning	Indirekte via ansættelsesprocesses	Fx OAO-fællesoverenskomst	Nej	Arbejdsgiver
Helbredsoplysninger i lægeerklæring	Arbejdsgiver har ikke krav på at vide, hvad en medarbejder fejler	Helbredsoplysninger er følsomme personoplysninger	Medarbejderen	Ingen hjemmel	Ja	Arbejdsgiver
Helbredsoplysninger som led i §56 ordning	§56 aftalen skal indeholde oplysning om sygdommens art	Helbredsoplysninger er følsomme personoplysninger	Medarbejderen	Sygedagpenge loven §56	Nej	Arbejdsgiver
Helbredsoplysninger som led i fleksjob	Fleksjobbeviset skal indeholde en beskrivelse af flexjobberens "særlige behov"	Helbredsoplysninger og de af følgende "særlige behov" er fortrolige og /eller følsomme personoplysninger	Medarbejderen og kommunen	Lov om aktiv beskæftigelsesindsats	Nej	Arbejdsgiver

Fortrolige personoplysninger

Fortrolige oplysninger er oplysninger, som efter den almindelige opfattelse i samfundet bør unddrages offentlighedens kendskab. Fortrolige oplysninger kan både være almindelige og følsomme personoplysninger.

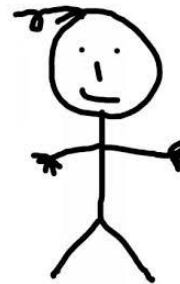
De følsomme personoplysninger er altid fortrolige.

Følgende almindelige personoplysninger er også fortrolige:

- CPR-nummer
- Oplysninger om interne familieforhold
- Mistrivsel
- Karakterer (både top-, dumpe, års- og eksamenskarakterer)
- Oplysninger om private stridigheder
- Begrundelser for tildeling eller afslag på løntillæg
- Begrundelse for afslag på ansættelse
- Mus referater
- Logning eller videooptagelse af medarbejdere og elevers trafik ind og ud af skolens bygninger

Hvis fortrolige personoplysninger skal sendes via e-mail skal det ske via en krypteret mailforbindelse fx Sikker Mail eller e-boks

Den registreredes rettigheder



På skolens initiativ

Medarbejderen/eleven har ret til at få **orientering** om, at hans personoplysninger behandles

Medarbejderen/eleven har ret til at blive **orienteret om brud** på datasikkerheden, hvis det berører dennes data.

På den registrerede persons initiativ

Medarbejderen/eleven har ret til **indsigt** i, hvilke personoplysninger, der konkret behandles om vedkommende.

Medarbejderen/eleven har ret til at få **berigtiget** urigtige personoplysninger om denne

Medarbejderen/eleven har - i visse (få) tilfælde - ret til at få sine personoplysninger **slettet**

Denne dataansvarlige skole skal tilrettelægge sin administration på en måde, så det er enkelt, gennemsigtigt, letforståeligt og let til gængeligt for den registrerede person, at udøve sine rettigheder

Oplysningerne til den registrerede person skal gives i et klart og enkelt sprog og som udgangspunkt skriftligt

Orientering om behandling af personoplysninger

Den dataansvarlige skal på eget initiativ orientere den registrerede person (som kan være en jobansøger, medarbejder, brobygningselev, ansøger om optagelse på skolen, elev samt værge) om følgende:

- At Varde Handelsskole er dataansvarlig
- Kontaktoplysninger på databeskyttelsesrådgiveren
- Formålet med behandlingen af de personoplysninger og det retlige grundlag for behandlingen (lovhenvielse eller samtykke)
- Eventuelle modtagere af personoplysningerne (ikke data behandlere - kun nye dataansvarlige)
- Tidsrummet (eller kriterierne for fastlæggelse af tidsrummet) for opbevaringen

- Den registreredes persons egen ret til at bede skolen om indsigt i, berigtigelse eller sletning af personoplysningerne eller begrænsning af behandlingen af personoplysningerne
- Den registreredes egen ret til at trække et samtykke tilbage på ethvert tidspunkt
- Muligheden for at klage over behandlingen til Datatilsynet
- Hvorvidt meddelelse af personoplysninger er lovpligtigt eller et krav mht. en kontrakt, indgået mellem dataansvarlige og registrerede. Yderligere skal den dataansvarlige informere den registrerede om konsekvenserne ved ikke, at give dataansvarlige disse oplysninger.
- Hvilke kategorier af personoplysninger, der behandles*
- Hvilken kilde personoplysningerne stammer fra*

De med * markerede oplysninger skal kun gives, hvis oplysningerne er indsamlet fra en anden end den registrerede person selv.

Orienteringen gives samtidig med at oplysningerne indsamles. Hvis oplysningen er indsamlet hos en anden end den registrerede person selv, skal orienteringen gives senest 1 måned efter data er indsamlet.

Hvis den dataansvarlige har planer om at viderebehandle personoplysningerne til et andet formål, end oplysningerne oprindeligt var tiltænkt, skal den registrerede person orienteres herom forud for viderebehandlingen.

Indsigtsret

Ved indsigtsret opnår den registrerede person (som kan være en jobansøger, medarbejder, brobygningselev, ansøger om optagelse på HHX, elev eller væрге) indsigt i behandlingen af dennes personoplysninger gennem en forespørgsel til skolen.

Den registrerede person har ret til at få skolens bekræftelse på, om personoplysninger om ham/hende behandles, få en kopi af eller adgang til oplysningerne og få en orientering om følgende:

- Formålet med behandlingen
- Kategorierne af personoplysninger
- Hvem personoplysningerne videregives til
- Tidsrum for opbevaring af oplysningerne
- Retten til at anmode om berigtigelse
- Sletning
- Begrænsning og indsigelse
- Muligheden for at klage over behandlingen til Datatilsynet
- Kilden til oplysningerne, hvis de ikke kommer fra registrerede selv

Bemærk at skolens efterkommelse af en anmodning om indsigt helt grundlæggende forudsætter, at man som skole kan finde oplysningerne frem. Dette lægger op til, at skolen overfor sine medarbejdere kommunikerer klart om, hvilke systemer og medier, personoplysninger må/skal gemmes i.

Inden der udleveres oplysninger til en elev eller medarbejder, der har bedt om indsigt i egne oplysninger, skal skolens sikre sig den pågældendes identitet. Hvis anmodningen fx skal sendes fra en mailadresse, som tilhører den pågældende elev eller medarbejder, må dette være tilstrækkelig sikkerhed.

Indsigt i elevens oplysninger, kan den forælder der har forældremyndigheden bede om, samt sine egne oplysninger. Der kan ikke bedes om indsigt i den anden forældres oplysninger uden samtykke fra den pågældende. Bonus forældre der ikke har formel forældremyndighed, har kun ret til indsigt i elevens oplysninger, hvis den formelle forældremyndighedsindehaver og eleven selv på forhånd giver samtykke.

Oplysninger om andre personer end den elev eller medarbejder, der anmoder om at se sine egne oplysninger, som måtte fremgå af det samme dokument, skal slettes effektivt (blændes eller streges ud) inden dokumentet udleveres.

Indsigten kan gives elektronisk. I praksis betyder det, at en mail med et vedhæftet pdf-dokument, hvori udskriften af elevens eller medarbejderens personoplysninger er samlet, vil opfylde kravet om indsigt.

Bemærk at hvis indsigten gives via mail, skal der anvendes Sikker Mail eller e-boks.

De oplysninger, der skal gives indsigt i, befinder sig fx følgende steder:

Medarbejderoplysninger:

- Personalesagsmappe
- Løndata (alt fremgår af lønsedler)
- Tidsregistrering (medarbejderen kan selv se dette i UDDATA+)
- Mailkorrespondance med skolen, hvori medarbejderens oplysninger indgår

Elevoplysninger:

- Elevsagen (der gives indsigt i referater, breve, lægelige oplysninger, karakterblade, udtalelser fra sociale myndigheder til fx SPS eller SU-dispensationer, tests fx for ordblindhed)
- UDDATA+: udskrift af personoplysninger, som eleven ikke selv kan se
- US2000 hvis eleven har anmodet om dispensation til godkendelse til udeboende SU eller SPS-midler gives der print af elevens oplysninger i systemet
- Bogdepot og BOSS - udskrift af oversigt over udlånt materiale
- Registrering af fremmøde jf. studie- og ordensbekendtgørelsen
- Log af netværkstrafik: der gives udskrift heraf, hvis en sådan log føres
- Mailkorrespondance med skolen, hvori elevens oplysninger indgår: der gives print heraf til eleven
- Diverse interne kommunikationssystemer, hvori skolens lærere kommunikerer om elevens trivsel og resultater: der gives udskrift heraf til eleven.

Retten til berigtigelse

Den registrerede person har ret til at få rettet oplysninger, der ikke er korrekte.

Bemærk at dette kræver, at skolen har så meget kontrol over de it-systemer, som personoplysningerne opbevares i, at ændring (herunder sletning af forældede oplysninger og inddatering af aktuelle oplysninger) er muligt.

Bemærk også at skolens eventuelle beslutning om helt eller delvist at afslå en persons anmodning om berigtigelse af dennes personoplysninger er en forvaltningsafgørelse, der kræver høring, begrundelse og klagevejledning.

Retten til indsigelse

Den registreredes person har ret til at få personoplysninger om sig selv slettet af skolen, hvis oplysningerne ikke længere er nødvendige for at opnå det oprindelige formål, hvis den registrerede person kalder et samtykke tilbage (og der herefter ikke er et andet grundlag for behandlingen), hvis den registrerede gør berettiget indsigelse mod behandlingen eller hvis behandlingen i det hele taget er ulovlig.

Retten til sletning

Den registrerede person har ret til at få sine personoplysninger om sig selv slettet af skolen, hvis oplysningerne ikke længere er nødvendige for at opnå det oprindelige formål, hvis den registrerede person kalder et samtykke tilbage (og der herefter ikke er et andet grundlag for behandlingen), hvis den registrerede gør berettiget indsigelse mod behandlingen eller hvis behandlingen i det hele taget er ulovlig.

Bemærk, at der dog ikke skal ske sletning, hvis skolen har fx administreret følsomme personoplysninger på baggrund af et gyldigt samtykke til fx SPS-ansøgning og på denne baggrund har modtaget og administreret midler. Årsagen er at fortsat opbevaring er nødvendig for at skolen kan dokumentere sin lovlige administration af SPS-midlerne.

Hvis skolen har offentliggjort personoplysninger (fx fotos på hjemmesiden) og i henhold til ovenstående er forpligtet til at slette personoplysningerne, skal skolen træffe såkaldt ”rimelige foranstaltninger” for at underrette eksterne parter, som behandler personoplysningerne, om at slette alle links, kopier eller gengivelser af de pågældende personoplysninger.

Sletning af data

Den dataansvarlige skole skal være i stand til at slette de personoplysninger, som ikke længere må behandles.

Når skolens slettepligt indtræder, skal sletning kunne ske effektivt (dvs. for bestandigt) og i alle de systemer og platforme, som medarbejderens/elevens personoplysninger er gemt.

Det er afgørende vigtigt at sletning også sker hos data behandlere, hvilket normalt kræver en udtrykkelig formulering herom i kontrakten eller databehandleraftalen eller en ad hoc sletteinstruks fra skolen til databehandleren.

Fysiske print skal(indsamles) og makuleres.

Skolen skal have beskrivelser til administrative medarbejdere og it-vejledere i, hvordan sletnings ker effektivt og ressourcebesparende, fx ved automatiserede sletteregler.

Elever:

Oplysninger om elever slettes enten, når eleven anmoder (og skolen finder anmodningen berettiget), eller efter følgende retningslinjer

	Slettefrist	Hjemmel/Lov
Identifikationsoplysninger (navn og cpr-nr.), oplysninger om studieretning og indskrivningsperioder	Ingen slettefrist. Dog skal sletning ske ved meddelelse om den studerendes død	
Eksamensbevis samt oplysninger der er nødvendige for at generere et eksamensbevis	30 år	§ 38, stk. 1 i den almene eksamensbekendtgørelse
Oplysninger der er nødvendige for at udstede attestationer for gennemført undervisning (merit)	10 år	Gymnasiebekendtgørelsen
Oplysninger om elever af betydning for årsrapporten (fx oplysninger om elevbetalinger til fester, begivenheder og studieture (beløb, dato og elev))	5 år	Bogføringsloven §10
Oplysninger om SPS (søgning om tilskud til samt administration af midler)	5 år	§14 i SPS - bekendtgørelsen
Oplysninger om SU	5 år	SU-styrelsens udmelding

Alle andre elevoplysninger	Kan (i princippet) slettes når eleven forlader skolen (dog i praksis ved udgangen af kalenderåret)	
Logningsdata af elevers internettrafik på skolens netværk samt it-systemer	6 måneder fra de er registreret	Sikkerhedsbekendtgørelsen
TV-overvågning	30 dage fra optagelsen	

Medarbejdere:

Oplysninger om medarbejderen slettes enten, når medarbejderen selv anmoder om det (og skolen finder anmodningen berettiget) eller efter følgende retningslinjer (åremål regnes fra fratræden)

Jobansøgere	Personoplysninger om ansøgere, der ikke blev ansat slettes efter 6 måneder efter rekrutteringsprocessen er afsluttet. <u>Undtagen</u> - hvis samtykke til længere opbevaring
Nuværende medarbejdere	Personoplysninger på personalesagen (og i IT systemer) kan opbevares indtil medarbejderen er fratrådt. <u>Undtagen</u> - hvis medarbejderen beder om sletning af forældede personoplysninger undervejs i ansættelsesforholdet, fx en gammel tjenestelig advarsel, skal skolen forholde sig aktivt til, om fortsat opbevaring er saglig, proportionel og relevant. Skolens afgørelse om afslag på at slette en personoplysning på medarbejderens anmodning er en forvaltningsretlig afgørelse, som skal indeholde en høring, begrundelse og klagevejledning.
Fratrådte medarbejdere	Personoplysninger på personalesagen slettes 5 år efter fratræden. <u>Undtagelse nr. 1</u> - personalesager for ansatte, der er født den 1. i måneden og medarbejdere i chefstillinger slettes ikke, da der kan være afleveringspligt til Statens Arkiver. <u>Undtagelse nr. 2</u> - hvis der verserer arbejdsskadesag, retsag eller arbejdsretlig tvist mellem medarbejderen og arbejdsgiver slettes personalesagen først 3 år efter den pågældende sag er afsluttet.

Betingelser for gyldigt samtykke

For at et samtykke er gyldigt, skal følgende betingelser være opfyldt:

- 1) Det skal afgives inden behandlingen påbegyndes
- 2) Det skal være bekræftet af forældrene, hvis samtykket angår et barns personoplysninger (undtaget fotos)
- 3) Det skal være afgivet frivilligt
- 4) På informeret grundlag
- 5) Det skal kunne tilbagekaldes
- 6) Det skal kunne dokumenteres af den dataansvarlige

Samtykket skal indhentes via det medie, som skolen vælger.

Hvis samtykket tilbagekaldes, skal de personoplysninger, hvis behandlingen samtykket gav hjemmel til, slettes med mindre, der foreligger et andet behandlingsgrundlag.

Dataansvarlig

En dataansvarlig er den ansvarlige for at personoplysninger om elever og medarbejdere behandles i overensstemmelse med lovgivningen.

Når en skole behandler oplysninger om sine elever og medarbejdere, er det normalt skolen der er dataansvarlig.

Den dataansvarlige skole står til ansvar overfor den registrerede medarbejder eller elev og overfor Datatilsynet for behandlingens lovlighed.

Individet/den registrerede person	Den dataansvarlige skole	Databehandler (it-leverandør)
<ul style="list-style-type: none">- Medarbejder- Jobansøger- Elev- Gæst	<p>Beslutter, hvad personens data skal bruges til fx</p> <ul style="list-style-type: none">- Rekruttering og ansættelse, lønadministration- Adgange til it-systemer og bygninger- optagelse af elev undervisning, eksamen- Fraværsregistrering og - håndtering <p>Ansvarlig for</p> <ul style="list-style-type: none">-lovligt grundlag til behandling ad data (lov eller samtykke)-saglighed, proportionalitet, gennemsigtighed-sikring af den registreredes rettigheder, fx orientering, indsigt og sletning-behandlingssikkerheden til forebyggelse af at data mistes, ændres lækkes eller i øvrigt behandles i strid med lovgivningen. <p>Sikkerheden skal være til stede på følgende områder:</p> <ul style="list-style-type: none">-teknisk (back-up, firewall, kryptering, antivirus)-organisatorisk (instrukser, brug af it-systemer, adgange/rettigheder, varighed af opbevaring)-fysisk (adgang til bygningen og kontorer, makulering og brandsikring)	<p>Behandler personoplysninger for/på vegne af skolen i henhold til en kontrakt, aftale eller lignende</p> <p>Skolen afgør, hvilke personoplysninger, fx CPR-nummer, databehandleren må få.</p> <p>Er underlagt skolens instruks om,</p> <ul style="list-style-type: none">-hvilket formål personoplysningerne må bruges til, fx rekruttering, lønadministration, it-administration-hvor (i eller udenfor Danmark)-hvor længe personoplysningerne skal opbevares (dvs. hvornår de må slettes)

For at den dataansvarlige skole kan bevise lovligheden er det nødvendigt med skriftlig og ajourført dokumentation for hvorfor, hvordan og hvor længe personoplysninger behandles hos den dataansvarlige.

Databehandler

Den dataansvarlige skole kan outsource behandlingen af persondata til en databehandler, hvilket er en it-leverandør, der ejer, driver eller vedligeholder de it-systemer, som skolen har valgt at bruge.

Databehandleren behandler blot personoplysninger på vegne af skolen. Databehandleren må ikke behandle oplysningerne til eget formål, fx statistik eller markedsføring. Det er den dataansvarlige skoles opgave og ansvar at sikre, at databehandleren er bevidst om og overholder dette. Dette styres via en databehandler aftale mellem skolen og it-leverandøren.

Det er væsentligt, at man som skole har gjort sig klart:

- At den dataansvarlige skole har ejerskabet til personoplysninger om elever og medarbejdere og suverænt afgør, hvad oplysningerne skal bruges til og hvor længe
- At skolen står til ansvar for behandlingens lovlighed overfor den registrerede medarbejder eller elev uanset om behandlingen af dennes personoplysninger sker på skolen eller ude hos en databehandler
- At ejerskabet derfor skal håndhæves og behandlingen af personoplysningerne skal kunne kontrolleres - selvom behandlingen sker hos en databehandler.
- At skolen derfor skal overveje nøje, hvilke data behandlere skolen vil have et samarbejde med, idet det kun bør være de data behandlere, der har en tilstrækkelig god it-sikkerhed og dataetik og som vil forpligte sig til at overholde dette via en databehandleraftale.

Databehandleraftale

En databehandleraftale indgås mellem den dataansvarlige skole og den databehandlernde it-leverandør. Databehandleraftalen skal være skriftlig.

Databehandleraftalen er en del af den samlede kontrakt med it-leverandøren. Selve kontrakten fastlægger ydelse, serviceniveau, varighed og pris. Databehandleraftalen (som kan være en integreret del af kontrakten eller fungere som et bilag) fastlægger sikkerhedsniveauet for beskyttelse af personoplysninger hos databehandleren.

Det er særligt vigtigt, at kontrakten eller databehandleraftalen klart og tydeligt pålægger databehandleren at personoplysningerne kun må behandles efter direkte instruks fra skolen, at personoplysningerne kun må bruges til det formål, der følger af kontrakten, fx skolens personalerekruttering, at personoplysningerne opbevares indenfor EU (allerhelst i Danmark), at oplyse skolen om evt. underleverandører før underleverandøren tages i brug, at orientere skolen om evt. datalæk, at føre en fortegnelse over behandlingsaktiviteter straks samt at slette skolens personoplysninger, når skolen beder om det og i øvrigt når formålet med behandlingen (fx rekruttering) er opfyldt.

Når skolen overlader behandling af sine medarbejdere og elevers personoplysninger til en databehandler via NI-login, skal der samtidig indgås en databehandleraftale. Skolen har i den forbindelse mulighed for selv at påvirke, hvilke personoplysninger, databehandleren skal modtage som led i samarbejdet. Dette vælges via forskellige datapakker i UNI-logins administrationsmodul. Det anbefales, at skolen kun åbner den lille pakke, idet de større pakker indeholder CPR-nummer og idet det har formodningen mod sig, at CPR-nummer er nødvendigt for databehandleren.

Skolen skal løbende følge op på, om databehandleren efterlever kontrakten. Dette kan ske ved at indhente en ledelses- eller en revisionserklæring. Kravet om en sådan erklæring skal fremgå af kontrakten eller databehandleraftalen. Erklæringen bør indhentes årligt eller hvert 2. år.

Bemærk at når de personoplysninger, som databehandleren har modtaget fra skolen, ikke længere er relevante at behandle, fx fordi eleven er blevet ikke længere går på skolen eller medarbejderen har forladt skolen, så skal data ikke alene slettes hos skolen, men også slettes hos databehandleren.

Skolen bør derfor have det som en fast del af årshjulet at afgive sletteinstruks til sine data behandlere om afgåede elever og medarbejdere. At databehandleren lukkes ned via Uni-login er ikke i sig selv nogen sikkerhed for sletning af personoplysningerne sker hos databehandleren.

Sletning

Den dataansvarlige skole skal være i stand til at slette de personoplysninger, som ikke længere må behandles. Når skolens slettepligt indtræder, skal sletning kunne ske effektivt (dvs. for bestandigt) og i alle systemer og platforme, som medarbejderens/elevens personoplysninger er gemt i, fx Outlook, UDDATA+ osv.

Det er vigtigt, at sletning også sker hos data behandlere, hvilket normalt kræver en udtrykkelig formulering herom i kontrakten eller databehandleraftalen eller en ad hoc sletteinstruks fra skolen til databehandleren.

Fysiske print skal (indsamles og) makuleres.

Skolen skal have beskrivelser til de administrative medarbejdere og studievejledere i, hvordan sletning sker effektivt og ressourcebesparende, fx ved automatiserede sletteregler.

Elevoplysninger:

Oplysninger om elever slettes enten, når eleven anmoder (og skolen finder anmodningen berettiget), eller efter følgende retningslinjer (åremålet regnes fra eleven har forladt skolen).

Situation	Tidsfrist	Hjemmel
Identifikationsoplysninger (navn og CPR-nr.) oplysninger om studieretning og indskrivningsperioder	Ingen slettefrist. Dog skal sletning ske ved meddelelse om den studerendes død.	
Eksamensbevis samt oplysninger der er nødvendige for at generere et eksamensbevis	30 år	§38, stk. 1 i den almene eksamensbekendtgørelse
Oplysninger, der er nødvendige for at udstede attestationer for gennemført undervisning	10 år	Gymnasiebekendtgørelsen
Oplysninger om elever af betydning for årsrapporten (fx oplysninger om elevbetalinger til fester, begivenheder og studieture (beløb, dato og elev))	5 år	Bogføringsloven §10
Oplysninger om SPS (søgning om tilskud til samt administration af midler)	5 år	§14 i SPS bekendtgørelse 4
Oplysninger om SU	5 år	SU-styrelsens udmelding
Alle andre elevoplysninger	Kan (i princippet) slettes når eleven forlader skolen (dog i praksis ved udgangen af kalenderåret)	
Logningsdata af elevers internettrafik på skolens netværk samt i it-systemer	6 måneder fra de er registreret	Sikkerhedsbekendtgørelsen
TV-overvågning	30 dage fra optagelsen	

Medarbejderoplysninger:

Oplysninger om medarbejdere slettes enten, når medarbejderen selv anmoder om det (og skolen finder anmodningen berettiget), eller efter følgende retningslinjer (åremålet regnes fra fratræden)

Situation	Tidsfrist	Hjemmel
Jobansøgere	Personoplysninger om ansøgere, der ikke blev ansat slettes 6 måneder efter rekrutteringsprocessen er afsluttet. Undtaget - Hvis samtykke til længere opbevaring	
Nuværende medarbejdere	Personoplysninger på personalesagen (og i IT-systemer) kan opbevares indtil medarbejderen er fratrukket. Undtaget - hvis medarbejderen beder om sletning af forældede personoplysninger undervejs i ansættelsesforholdet, fx en gammel tjenestelig advarsel, skal skolen forholde sig aktivt til, om fortsat opbevaring er saglig, proportionel og relevant. Skolens afgørelse om afslag på at slette en personoplysning på medarbejderens anmodning er en forvaltningsretlig afgørelse, som skal indeholde en høring, begrundelse og klagevejledning.	
Fratrådte medarbejdere	Personoplysningerne på personalesagen slettes 5 år efter fratræden. Undtaget 1 - Personalesager for ansatte, der er født den 1. i måneden og medarbejdere i chefstillinger slettes ikke, da der kan være afleveringspligt til Statens Arkiver. Undtaget 2 - Hvis der verserer arbejdsskadesag, retssag eller arbejdsretlig tvist mellem medarbejderen og arbejdsgiver slettes personalesagen først 3 år efter den pågældende sag er afsluttet.	

Orientering om læk til den registrerede person

Ved brud på reglerne om beskyttelse af personoplysning, brud på fortroligheden, læk, overbehandling og utilsigtet sletning, skal den dataansvarlige skole anmelde hændelsen til Datatilsynet inden 72 timer, efter at skolen er blevet bekendt med bruddet på persondatasikkerheden.

Overskrides fristen skal dette begrundes særskilt overfor datatilsynet.

Anmeldelsen skal mindst indeholde:

- a) En beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder hvis det er muligt kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
- b) Angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren
- c) Beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- d) Beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødigt forsinkelse også de registrerede personer om bruddet på persondatasikkerheden i et klart og forståeligt sprog.

Databeskyttelsesrådgiveren

Databeskyttelsesrådgiverens funktion er at vejlede skolen om praktiske redskaber og arbejdsformer der kan styrke beskyttelsen af personoplysningerne på institutionen, fx ved brug af it-systemer, ved brug af databeskyttende standardindstillinger samt ved formulering af retningslinjer og procedurer for, hvordan personoplysninger behandles på skolen.

Behandlingssikkerhed

Den dataansvarlige skole skal have tekniske, fysiske og organisatoriske foranstaltninger, der giver et passende sikkerhedsniveau for de personoplysninger, som skolen behandler.

Sikkerhedsniveauet fastlægges ud fra en afvejning af, hvilke og hvor mange personoplysninger, der er tale om, ressourceforbruget med etableringen af sikkerheden samt risikoen for de registrerede personer ved et læk.