Roskilde Gymnasium

Håndbog i behandling af personoplysninger

Roskilde Gymnasium
Juni 2025

Indhold

Indledning
I denne håndbog kan du læse de regler for behandling af personoplysninger, der gælder for alle medarbejderne på Roskilde Gymnasium (kapitel 1).

Reglerne er udmøntet i tjeklister og beskrivelser, som gælder for specifikke medarbejdergrupper. Disse finder du i kapitel 2.

I kapitel 3 finder du en FAQ om personoplysninger.

I håndbogen er der henvist til Gymnasiefællesskabets (GF's) skabeloner, som kan bruges direkte eller som inspiration for vores egne breve, notater og anden form for dokumentation. Der henvises også til GF's uddybende vejledninger om, hvordan systemer som DocuNote, HR-Databasen og GymBetaling bruges på en praktisk måde, så det understøtter fx sletning.

Ansvarlighed

Roskilde Gymnasium er forpligtet til at behandle personoplysninger om elever og medarbejdere efter reglerne[1], og eftersom alle medarbejdere på Roskilde Gymnasium i større eller mindre omfang beskæftiger sig med personoplysninger, er lovlig behandling af personoplysninger en opgave, som vi deler.

Den nærmere ansvarsfordeling er som følger:

- **Øverste ledelse (bestyrelsen):** Det er den øverste ledelse, der har det endelige ansvar for, at Roskilde Gymnasium behandler personoplysninger i overensstemmelse med gældende lovgivning.
- **Daglig ledelse (Rektor):** Rektor er ansvarlig for, at formålene med behandling af personoplysninger er i overensstemmelse med gældende lovgivning, samt at retningslinjerne til understøttelse af politikken er kommunikeret klart og tydeligt til medarbejderne.
- **Datasikkerhedstovholder:** Datasikkerhedstovholderen er den primære kontaktperson til DPO'en. PÅ Roskilde Gymnasium er datasikkerhedstovholderen Torben Geilman. Datasikkerhedstovholderens rolle er bl.a. at holde sig ajour med nyheder vedr. databeskyttelse, holde styr på databehandleraftaler og risikovurderinger, udbrede politikker og praksis beskrevet i denne håndbog til de relevante medarbejdere og sørge for hurtig handling i forbindelse med datalæk. Funktionen er nærmere beskrevet i kapitel 1.
- **Databeskyttelsesrådgiver (DPO):** DPO'ens rolle er at overvåge, at Roskilde Gymnasium overholder gældende regler for beskyttelse af personoplysninger, herunder at stå til rådighed for hele skolen i forhold til rådgivning på området. DPO'en er desuden Roskilde Gymnasiums kontaktperson udadtil – både i forhold til de registrerede og i forhold til Datatilsynet eller andre parter. DPO'en rapporterer til det øverste ledelsesniveau.
- **Medarbejdere:** Medarbejdere, der behandler personoplysninger, er ansvarlige for at gøre sig bekendt med formålene med behandlingen og de retningslinjer for databeskyttelse, der vedrører deres arbejde. Lærerne skal vide, hvilke it-systemer og it-værktøjer der må bruges som led i undervisning, herunder til fjernundervisning.

Alle Roskilde Gymnasiums medarbejdere skal kende denne håndbog og vide, hvordan indholdet i tjeklisterne praktiseres. Derfor er:

[1] Lovgivningen om behandling af personoplysninger findes i persondataloven fra den 26. maj 2018: "i den europæiske databeskyttelsesforordning og i den danske databeskyttelseslov".

- Håndbogen blevet præsenteret på et personalemøde. I den forbindelse har alle medarbejdere kvitteret for læsning af håndbogen i HR-databasen i forbindelse med samtykkeerklæring.
- Den gældende version af håndbogen er altid tilgængelig på Google-drevet under "Styredokumenter" og på skolens hjemmeside.

Roskilde Gymnasiums opgaver

For at vi på Roskilde Gymnasium kan sige, at vi behandler personoplysninger efter reglerne, skal vi kunne sige "ja" til følgende udsagn:

1. Vi sikrer, at vi kun **indsamler** de personoplysninger, der er hjemmel til i lovgivningen, i overenskomsterne eller i form af et samtykke fra den registrerede person selv.
2. Vi **orienterer** den registrerede person om, at vi behandler pågældendes personoplysninger, og vi støtter den registrerede i at udøve sin ret til indsigt, berigtigelse, sletning og klage.
3. Vi opbevarer personoplysninger i it-systemer, der yder tilstrækkelig **sikkerhed ved behandlingen af personoplysninger**.
4. Vi sikrer, at personoplysninger kun kan **ses/tilgås** af de medarbejdere eller andre personer, der aktuelt har en jobfunktion på Roskilde Gymnasium eller en rolle (fx forældre), der berettiger til det.
5. Vi sikrer, at vores it-leverandører (**databehandlere**) kun behandler personoplysningerne efter instruks fra os, hvilket kræver, at der indgås en kontrakt med tilhørende databehandleraftale, og at der sker kontraktopfølgning – samt at vi i det hele taget kun indgår aftaler med de leverandører, der ud fra en risikovurdering vurderes at have en sikkerhed og dataetik, der bidrager til at beskytte vores personoplysninger.
6. Vi sikrer, at personoplysninger **slettes**, når de ikke længere er nødvendige for vores opgave.
7. Vi har ajourførte og kendte **retningslinjer og tjeklister**, som på en klar og letforståelig måde fortæller vores medarbejderne, hvordan de skal håndtere personoplysninger korrekt.
8. Vi fører **fortegnelser** over hovedområderne for vores persondatabehandling.
9. Vi har en **databeskyttelsesrådgiver** (DPO).
10. Vi har en plan for håndtering af **brud på datasikkerheden** (fx datalæk).

Roskilde Gymnasiums samlede beskrivelse af vores gode databehandlingsskik

Her kan du se en samlet oversigt over skolens overordnede retningslinjer for behandling af personoplysninger og de underliggende tjeklister og beskrivelser, samt hvem de retter sig imod.

Kategori	Dokumenter	Findes hvor	Skal være kendt af	Årshjul – ajourføring samt ansvarlig
Skolehåndbogens kap. 1	Generel beskrivelse af skolens retningslinjer for behandling af personoplysninger inkl. konkrete ● Leveregler ● Politikker ● Andet	På Skolens hjemmeside og som en del af skolens styredokumenter på Google Drev	Alle medarbejdere på skolen	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.
Skolehåndbogens kap. 2	Konkrete tjeklister og retningslinjer for konkret håndtering af personoplysninger til: ● Administrative medarbejdere ● IT-administratorer ● Gymnasie- og læsevejledere ● Kommunikationsmedarbejdere ● Elever ● Ledelse	På Skolens hjemmeside og som en del af skolens styredokumenter på Google Drev	Den medarbejdergruppe, som tjeklisten/ retningslinjerne angår	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.
Skolehåndbogens kap. 3	FAQ med viden og beskrivelser af reglerne og hvad de betyder i et skolesammenhæng	På Skolens hjemmeside og som en del af skolens styredokumenter på Google Drev	Opslagsværk for medarbejderne Skal være kendt af ledelse og datasikkerhedstovholder	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.
Personale-håndbogen	Beskrivelse til medarbejderne om, hvordan skolen behandler deres personoplysninger som led i ansættelsen	På Skolens hjemmeside og som en del af skolens styredokumenter på Google Drev	Alle medarbejdere på skolen	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.

Elevorientering	Beskrivelse af skolens retningslinjer for elevernes brug af fx Lectio, digitale undervisningsværktøjer, adfærd ifm. online-undervisning ● Leveregler/husregler ● Kobling til skolens studie- og ordensregler	På Skolens hjemmeside	Alle elever, lærere, administrative medarbejdere samt ledelse på skolen	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.
Risikovurdering af it-systemer	● Faktaark med risikovurdering, herunder it-systemets formål og funktioner ifm. skolens benyttelse ● Evt. fuld risikovurdering af databehandlingen i systemet, hvis det vurderes nødvendigt	GF har udfyldt faktaark og risikovurderinger for en større mængde af it-systemer og it-værktøjer, der bruges i undervisning. Findes i DocuNote under "Risikovurderinger for IT-systemer" Internt hos skolens dataansvarlig	Skolens Ledelse	Datasikkerhedstovholderen er ansvarlig for ajourføring af hele håndbogen.
Positivliste over it-systemer og it-værktøjer, der bruges i administration og i undervisnings medfør	Simpel oversigt over de it-systemer, -værktøjer mv., som skolens ledelse har godkendt til brug på skolen (administration/undervisning)	Som bilag til denne håndbog "Positivliste over digitale værktøjer"	Alle elever, lærere, administrative medarbejdere samt ledelse på skolen	Dokumentet er dynamisk. Administreres af tovholder.
Oversigt over databehandlere	Simpel oversigt over de it-leverandører og databehandlere, som skolen bruger (til administration/undervisning)	På Skolens hjemmeside og som en del af skolens styredokumenter på Googledrev	Skolens ledelse	Dokumentet er dynamisk. Administreres af tovholder.
Fortegnelse over behandlingsaktiviteter	Formel oversigt over de behandlinger af personoplysninger, som skolen udfører vedr. fx HR-administration og elevadministration	På Skolens hjemmeside og som en del af skolens styredokumenter på Googledrev	Alle elever, lærere, administrative medarbejdere samt ledelse på skolen	Dokumentet er dynamisk. Administreres af tovholder.
Plan for håndtering af sikkerhedsbrud	Forretningsgang for håndtering af brud på persondatasikkerheden og	På Skolens hjemmeside og som en del af skolens	Alle elever, lærere, administrative	Dokumenterne bruges løbende, når der opstår brud eller

	skolens samarbejde med DPO'en om håndteringen	styredokumenter på Googledrev	medarbejdere samt ledelse på skolen	sikkerhedshændelser

Kapitel 1 - Retningslinjer for behandling af personoplysninger, der gælder for alle medarbejderne på Roskilde Gymnasium.

1. Roskilde Gymnasiums leveregler for datasikkerhed (alle medarbejdere)

En nem måde at komme i gang med at praktisere persondatabeskyttelse og informationssikkerhed i det daglige er ved at vænne sig til at efterleve følgende enkle leveregler i praksis:

1. Brug **passwords** på din computer, smartphone mv. og opdater med et nyt, unikt password hver gang systemet beder om det (hvilket på computeren er hver 6. måned) – eller oftere. **Memorér** dit password og undlad dermed så vidt muligt at skrive det ned. Et password må under ingen omstændigheder fremgå af fx post it's, der sidder på din computer. Tast aldrig dit password mens din computer er koblet til en storskærm eller lignende, hvor passwordet kan aflures

2. Aktivér din **pauseskærm**, når du forlader dit skrivebord.

3. Læg **fysiske dokumenter** med personoplysninger i aflåst skab, skuffe eller kontor, når du forlader dit skrivebord i længere tid, og altid før du forlader skolens lokaler.

4. Papirdokumenter med personoplysninger skal altid bortskaffes ved **makulering**.

5. **Print**, der indeholder personoplysninger, hentes i printeren straks. Overvej hvad du printer.

6. **E-mails** med fortrolige og følsomme personoplysninger sendes via Digital Post eller Sikker Mail.

7. Alle filer og dokumenter med personoplysninger oprettes, behandles og gemmes i DocuNote (ESDH).

8. Hvis personoplysningerne er modtaget eller sendt via **e-mail**, slettes mailen i Outlook, senest én måned efter sagsbehandlingen er afsluttet. Hvis personoplysningerne stadig er relevante, når den nævnte måned er forløbet, gemmes mailen fremadrettet i DocuNote – og kun dér.

9. Bidrag til løbende at **slette** sager og oplysninger, herunder personoplysninger, der ikke længere er relevante. En mail vil sjældent være relevant, når den er mere end et par måneder gammel.

10. Undlad at gemme personoplysninger på USB-nøgle, på skrivebordet på din bærbare computer eller lignende **usikre steder**. Brug VPN, hvis du arbejder på din computer ude af huset.

11. Tag ikke nye it-systemer eller digitale platforme i brug, uden at den er godkendt af ledelsen vedr. sikkerheden i systemet, og der er indgået en kontrakt og en **databehandleraftale** med leverandøren. Se bilaget "Positivliste over digitale værktøjer".

12. Følg husreglerne for digital undervisning. Se bilagene "Husregler for digital undervisning" og "K8 Tjekliste med afsæt i Datatilsynets Om brug af billeder og video i skoler"

13. Udvis **fortrolighed** om de personoplysninger, du bliver bekendt med som led i dine arbejdsopgaver – del og videregiv ikke personoplysninger uden at være sikker på, at det er i orden.

14. Åben ikke mails, der ser mistænkelige ud, eller som kommer fra afsendere, du ikke kender.

15. Ved **tyveri eller bortkomst af it-udstyr** (fx pc, tablet og/eller smartphone, som man har fået udleveret som arbejdsredskab på Roskilde Gymnasium), skal man straks kontakte skolens datasikkerhedstovholder Torben Geilman.

16. Kontakt nærmeste leder eller IT-administrator, hvis du bliver opmærksom på noget mistænkeligt.

Udover disse leveregler har vi formuleret de retningslinjer, der fremgår af dette kapitel.

2. Tavshedspligt

Som medarbejder på Roskilde Gymnasium skal man omgås personoplysninger med omtanke. Al information, der omhandler navngivne eller identificerbare fysiske personer (medarbejdere, kollegaer, elever, ansøgere, forældre og andre pårørende, bestyrelsesmedlemmer eller andre), er fortrolig og må ikke deles med nogen uden for Roskilde Gymnasium – og heller ikke med kollegaer på Roskilde Gymnasium, der har arbejdsfunktioner, som gør det unødvendigt, at de kender de pågældende oplysninger.

Alle medarbejdere på Roskilde Gymnasium er omfattet af følgende klausul om;

Tavshedspligt

Roskilde Gymnasiums medarbejdere har tavshedspligt med hensyn til alle forhold, som man erfarer som led i ansættelsen. Det betyder, at man som medarbejder hverken må bruge eller videregive personoplysninger til andre formål end de tjenstlige opgaver, man er pålagt.

Det betyder også, at medarbejderens personlige kendskab til en (person-)oplysning eller en sag ikke berettiger medarbejderen til at bruge eller søge på sådanne oplysninger i de it-systemer, som medarbejderne af tjenstlige årsager har adgang til på Roskilde Gymnasium, fx ESDH, CPR-registreret, Lectio eller andre steder.

Tavshedspligten følger af forvaltningsloven og straffelovens regler om tavshedspligt i offentlig tjeneste. Tavshedspligten gælder både under og efter ansættelsesforholdet.

Brud på tavshedspligten under ansættelsen betragtes som misligholdelse af ansættelsesforholdet og kan afhængigt af forseelsens grovhed medføre ansættelsesretlige sanktioner, herunder skriftlig advarsel, opsigelse eller øjeblikkelig bortvisning.

Tavshedspligten fremgår også i en kortere version af ansættelsesbrevet.

Hvis der opstår en situation, hvor fortrolige personoplysninger kan være havnet hos uvedkommende tilintetgjort, tabt, ændret eller utilsigtet videregivet til uvedkommende, skal man straks kontakte sin nærmeste leder, som hjælper med håndteringen, jf. næste afsnit.

3. Handlepligt i tilfælde, hvor personoplysninger kan være havnet hos uvedkommende

Hvis der opstår en situation, hvor der kan være sket et brud på datasikkerheden for personoplysninger, skal man **STRAKS** kontakte sin nærmeste leder, som hjælper med at få kontakt til DPO'en og den øvrige håndtering.

Årsagen til, at man straks skal reagere er, at Roskilde Gymnasium har pligt til at håndtere et sikkerhedsbrud og eventuelt foretage anmeldelse til Datatilsynet uden unødig forsinkelse og senest indenfor 72 timer. Derfor er det nødvendigt at komme i gang hurtigst muligt.

Det kan være i følgende (eller lignende) situationer:

	Hændelse
1	En elev overhører to læreres samtale om alvorlige helbredsproblemer hos en anden elev
2	En medarbejder har trykket på et link i sin arbejdsmail, som viser sig at indeholde en virus, der straks spreder sig til hele skolens it-netværk og filer. Dette resulterer i, at al skolens data, herunder CPR-numre, helbredsoplysninger mv. om skolens medarbejdere bliver krypteret og låst. Skolen har backup af sine systemer, men det er også lykkes bagmændene at kryptere noget af back up'en.
3	En medarbejder får stjålet eller mister sin arbejdscomputer (bærbar eller stationær). På computeren findes der fx: • MUS- eller mødereferater med personoplysninger • Økonomiske oplysninger, fx betalingskortoplysninger • Sager om it-support med skærmprint eller kopier af personoplysninger fra it-systemet • Systemadgange uden stærke passwords • Oplysninger om elevers helbred eller faglige standpunkt
4	En medarbejder sender (pr. post eller e-mail) personoplysninger til en forkert modtager.
5	En medarbejder kommer ved en fejl til at lægge fx elevers telefonnumre på hjemmesiden.

Når sikkerhedsbruddet er konstateret, og nærmeste leder og DPO'en er inddraget, får vi i fællesskab overblik over skaden.

DPO'en vurderer, om hændelsen er et sikkerhedsbrud, der skal anmeldes til Datatilsynet, og om der evt. også skal ske underretning af de berørte registrerede personer.[2]

4. Instruks om adfærd til forebyggelse og håndtering af hackerangreb (alle)

Hvis uheldet er ude, og din computer, smartphone mv. rammes af hackerangreb, skal du **STRAKS**:

- Trække computerens netværksstik ud af væggen (hvis det er en stationær computer)
- Slukke udstyret
- Kontakte skolens it-administrator og nærmeste leder. Disse kontakter DPO'en.

Du skal ikke betale den løsesum, som hackerne evt. kræver. Årsagen er, at du ikke kan være sikker på at få den fulde kontrol over computeren og filerne tilbage, selv om du betaler.

[2] Jf. GF's skabeloner, som findes på GF's Intranet under Datasikkerhed > Håndtering af muligt sikkerhedsbrist f.eks. læk af personoplysninger.

5. Medarbejderadfærd til forebyggelse af hackerangreb på Roskilde Gymnasiums it-udstyr og skolens it-systemer:

1. Du skal holde din computer (og evt. også bærbar computer, smartphone, tablet, mv.) **ajour med de seneste versioner af software og antivirus**, da det giver den bedste sikkerhed. Det er især programmer som Java, Adobe Reader og Flash Player, du selv skal sørge for opdatering af. Microsoft-programmerne opdateres automatisk af Roskilde Gymnasium.
2. Roskilde Gymnasium sørger for daglig **backup** af alt materiale på netværksdrevet og i de systemer, som Roskilde Gymnasium har godkendt til persondata. Derimod skal du selv sørge for at tage backup af data, der (undtagelsesvist) ikke ligger disse steder.
3. Vær **skeptisk over for e-mails**, som er mistænkelige i sprog, layout eller den sammenhæng, du modtager dem i. Det gælder også, selv om mailen umiddelbart kommer fra en kendt afsender, jf. beskrivelsen af ransomware og social Engineering nedenfor. Spørg din nærmeste leder eller it-administrator, hvis du er det mindste i tvivl.
4. Vær især **forsigtig med at åbne links eller vedhæftninger**, hvis mailen er mistænkelig, jf. pkt. 3.
5. Hvis du er nødt til at åbne en vedhæftet fil eller link, *selv om* mailen er mistænkelig, kan du begrænse skaden ved at **åbne filen eller linket via din smartphone i stedet for på computeren**. Årsagen er, at smartphonen ikke har adgang til netværksdrevet.
6. Hvis du er i tvivl om, hvordan instruksen skal efterleves i praksis, kan du kontakte din nærmeste leder eller it-administrator.

6. Forretningsgang vedr. overvågning af alarmer fra Heimdal

Formålet med Heimdal, som skolens antivirusprogram hedder, er blandt andet at beskytte skolens data og infrastruktur, herunder at minimere risikoen for ransomware, malware, trojanskhest, virus mv. Hvis Heimdal f.eks. detekterer trafik på usikre hjemmesider fra en pc, sender Heimdal automatisk en mail med info til IT afdelingens driftsmail DriftMail@gymadm.dk, og evt. også til skolens lokale IT-medarbejder, hvis skolens lokale IT-medarbejder er sat op til at modtage alarmer.

Alarmmailen indeholder en beskrivelse af problemet, herunder:

1. hvilken URL/fil/harddisk mv. advarslen angår,
2. oplysning om maskinnavn og brugerinfo,
3. information om navne på de tilgåede usikre hjemmesider, som har udløst alarmen

Gymnasiefællesskabets IT-afdeling tjekker løbende (dog kun sporadisk i weekender og ferielukkeperioder) alarmmails fra Heimdal, og IT-afdelingen vurderer konkret ud fra de informationer der modtages om maskinen skal sættes i isolation (dvs. hvor al nettrafik blokeres via Heimdal Dashboard), eller om det er tilstrækkeligt, at få fat på maskinen og give den et lokalt sikkerhedstjek uden først at sætte den i isolation.

Skolens ledelse og/eller lokale it-afdeling vil altid blive orienteret om de alarmer, som Gymnasiefællesskabets IT-afdeling vurderer som kritiske.

7. Disse it-systemer må du bruge som medarbejder ("Positivliste") (alle)[3]

Som ansat på Roskilde Gymnasium skal du bruge de it-systemer, som skolen stiller til rådighed, til alt der er arbejdsrelateret, herunder digital kommunikation og opbevaring. Dette gælder især, når du behandler personoplysninger.

De it-systemer, som Roskilde Gymnasium har godkendt til håndtering af personoplysninger, er følgende systemer (se særskilt om, hvad Lectio må bruges til nedenfor):

7.1 Til alle medarbejdere:

- Outlook og Outlook Web App (mail)
- Office365 (Jf. nedenstående må der ikke gemmes personlige oplysninger i OneDrive eller OneNote)

7.2 Til administrative medarbejdere og vejledere:

- Outlook og Outlook Web App (mail)
- Office365 (Jf. nedenstående må der ikke gemmes personlige oplysninger i OneDrive eller OneNote)
- Digital post
- DocuNote (ESDH)[4]
- Statens lønsystem og LDV
- Navision stat
- Indfak2
- HR-Databasen
- Gymbetaling
- CPR-Registeret
- mTid
- Biblioteksystemet Cicero
- HR-Manager
- Lectio
- Optagelse.dk
- US2000
- Netprøver.dk

Der må **ikke** håndteres og gemmes personoplysninger i andre systemer end de ovenfor nævnte (se dog nedenstående om midlertidig opbevaring).

Der må af hensyn til sikkerheden **ikke** håndteres og/eller gemmes personoplysninger i cloud-tjenester (fx Google Apps) eller på USB-nøgler, på lokalt drev eller på skrivebordet på medarbejderens egen computer.

Der må ikke gemmes personoplysninger i cloud-tjenester (fx GoogleApps, OneDrive, OneNote, DropBox), USB-nøgler, på lokalt drev eller på skrivebordet på medarbejderens egen computer mv. da disse steder af flere årsager ikke er sikre (se dog nedenstående om midlertidig opbevaring).

[3] Ang. skolens retningslinjer til elever om "Disse systemer skal du bruge som led i undervisning": GF har udarbejdet skabelon til "Guidelines for digital/virtuel undervisning på Roskilde Gymnasium", som kan bruges til orientering til eleverne. Skabelonen findes på GF's Intranet under Datasikkerhed > GDPR ved digital undervisning.

[4] ESDH er en forkortelse for Elektronisk System til Dokumenthåndtering. På Roskilde Gymnasium bruges et system, der hedder DocuNote.

På Roskilde Gymnasium er vi opmærksomme på, at mange personoplysninger i praksis opbevares midlertidigt i et it-system, der ikke fremgår af ovenstående liste over godkendte systemer. Midlertidig opbevaring må foretages på den enkelte medarbejders personlige serverdrev, eller krypterede lagermedier, som er udleveret af skolen.

På Roskilde Gymnasium bruger vi Google som Cloudstjeneste. I Google må der ikke skrives personlige oplysninger undtagen følgende i dokumenter på Roskilde Gymnasiums GoogleDrev:

- Elevernes egne refleksioner om dem selv.
- Lærernes faglige kommentarer til elevernes refleksioner. Personlige kommentarer om fx væremåde, sygdom, ordblindhed og opførsel må altså ikke skrives i et dokument, som ligger på Google Drev.

- Elevernes personlige opgavebesvarelser.
- Lærernes faglige formative og summative evalueringer af elevernes personlige opgavebesvarelser.

- Grupper af elevers opgavebesvarelser.
- Lærernes faglige formative og summative evalueringer af grupper af elevers opgavebesvarelser.

For medarbejdere med adgang til det administrative netværk derudover også på administrationens fælles serverdrev.

Når dokumenter opbevares midlertidigt, skal dokumenterne overføres til et godkendt it-system hurtigst muligt – dog senest 1 måned efter endt brug.

7.3 Til lærere og undervisere:

Skolens ledelse har på baggrund af en konkret risikovurdering foretaget af GF godkendt følgende it-systemer til kommunikations- og undervisningsformål på Roskilde Gymnasium:

- Outlook (mail)
- Office365
- Lectio
- UNI-login

8. Midlertidig opbevaring

Der må ikke gemmes personoplysninger i cloud-tjenester (fx GoogleApps, OneDrive, OneNote, DropBox), USB-nøgler, på lokalt drev eller på skrivebordet på medarbejderens egen computer mv. da disse steder af flere årsager ikke er sikre (se dog nedenstående om midlertidig opbevaring).

På Roskilde Gymnasium er vi opmærksomme på, at mange personoplysninger i praksis opbevares midlertidigt i et it-system, der ikke fremgår af ovenstående liste over godkendte systemer. Midlertidig opbevaring må foretages på den enkelte medarbejders personlige serverdrev, eller krypterede lagermedier, som er udleveret af skolen.

På Roskilde Gymnasium bruger vi Google som Cloud tjeneste. I Google må der ikke skrives personlige oplysninger undtagen følgende i dokumenter på Roskilde Gymnasiums Google Drev:

- Elevernes egne refleksioner om dem selv.

- Lærernes faglige kommentarer til elevernes refleksioner. Personlige kommentarer om fx væremåde, sygdom, ordblindhed og opførsel må altså ikke skrives i et dokument, som ligger på Google Drev.
- Elevernes personlige opgavebesvarelser.
- Lærernes faglige, formative og summative evalueringer af elevernes personlige opgavebesvarelser.
- Grupper af elevers opgavebesvarelser.
- Lærernes faglige formative og summative evalueringer af grupper af elevers opgavebesvarelser.

For medarbejdere med adgang til det administrative netværk derudover også på administrationens fælles serverdrev.

Når dokumenter opbevares midlertidigt, skal dokumenterne overføres til et godkendt it-system hurtigst muligt – dog senest 1 måned efter endt brug.

Se i øvrigt afsnit 14 om, hvordan der slettes effektivt i diverse systemer.

9. Positivliste over digitale værktøjer

GF er ansvarlig for på vegne af skolen at risikovurdere de af skolen anvendte administrative og digitale værktøjer. Alle risikovurderede værktøjer findes i GF's Masterark. Masterarket kan anvendes af det enkelte gymnasium til at finde nye digitale værktøjer, der eventuelt ønskes taget i brug i undervisningen. Inden et nyt værktøj tages i brug er det essentielt, at skolen forholder sig til de anførte opmærksomhedspunkter samt til konklusionen, da det kan vise sig at være nødvendigt at tage eventuelle forholdsregler samt iværksætte lokale foranstaltninger inden ibrugtagning.

På GF's intranet med stien "Datasikkerhed → Skolernes data behandlere, risikovurderinger og tilsynsrapporter" er der et link til det aktuelle Masterark, der ligger i DocuNote. Det er også muligt at tilgå en dateret version af Masterarket direkte fra siden.[5]

Gymnasiefællesskabet har gjort det nemt for skolerne at vejlede eleverne ved fx at implementere Gymnasiefællesskabets skabelon til "Husregler for digital undervisning" og/eller "Guidelines ved anvendelse af digitale/virtuel undervisning", som i tillæg til "Husregler for digital undervisning" rummer et bud på en ledelsestekst til det overordnede ansvar samt anbefaling om at have en "positivliste" med alle de af ledelsen godkendte it-værktøjer.

[5] Vedr. dataminimering/risikominimering ved brug af digitale undervisningsplatforme: Dette kan ske på forskellig vis, men GF's skabelon til "Husregler for digital undervisning", som findes på GF's intranet, er en hjælp til at komme i gang.

10. Virtuel undervisning og videomøder

Til virtuel undervisning og interne videomøder bruger Roskilde Gymnasium:

- Google Meet

11. Husregler vedr. medarbejderes brug af AI-chatbots

Nedenstående retningslinjer skal efterleves, når skolens medarbejdere anvender en AI-chatbot ifm. arbejdet:

Disse husregler gælder ved brug af AI-chatbots, fx ChatGPT, Gemini og Copilot.[6] De nævnte chatbots kan tilgås både gratis og som betalingsversioner.

Før man tager en chatbot i brug, bør man altid:
- være opmærksom på muligheder for konfiguration af privatlivs- og sikkerhedsindstillinger
- have procedurer for tildeling og lukning af brugeradgange
- have sletterutine vedr. prompts
- fordele ansvar for at ovenstående procedurer og rutiner efterleves.

Al inddata til en AI-chatbot skal ske med omtanke og i overensstemmelse med nedenstående regler:

Det er ***ikke tilladt*** at:
- dele eller behandle personoplysninger
- generere tekst, der kan bruges til at identificere enkeltpersoner
- overtræde ophavsrettigheder[7] eller andre immaterielle rettigheder[8]
- behandle anden information, der kan klassificeres som fortrolig eller forretningshemmeligheder, herunder fx:
  - **Personlige data:** Identifikationsoplysninger, der kan identificere en person, såsom navne, adresser, telefonnumre, e-mailadresser, CPR-numre, sundhedsoplysninger, finansielle oplysninger etc.
  - **Medarbejderoplysninger:** Information om medarbejdere, inklusive lønoplysninger, personalefiler, performance evalueringer, og andre personlige oplysninger.
  - **Elevoplysninger:** Information om elever, inklusive oplysninger om individuelle forhold, uddannelsesparathed, fravær, klager.
  - **Interne dokumenter:** Strategiplaner, udviklingsplaner og -strategier, udviklingsprojekter samt nye initiativer.
  - **Finansielle rapporter og data**: Ikke offentliggjorte finansielle rapporter, budgetter, prognoser, investeringsanalyser, og anden finansiel information.
  - **Kontrakter og aftaler:** Detaljer om underskrevne kontrakter, aftaler med leverandører, partnere eller andre tredjeparter, inklusive betingelser, priser, og andre følsomme oplysninger.
  - **Sikkerhedsinformation:** Detaljer om sikkerhedsprotokoller, adgangskoder, krypteringsnøgler og andre oplysninger relateret til organisationens IT-sikkerhed.

[6] ChatGPT er en chatbot baseret på kunstig intelligens (AI), der er udviklet af OpenAI. Gemini er en chatbot drevet af kunstig intelligens (AI), udviklet af Google. Copilot er en AI-drevet assistent, integreret i Microsoft 365-programmer.
Det er frivilligt, om man vil gøre brug af værktøjerne.

[7] Ophavsrettigheder beskytter typisk kunstneriske og litterære værker, såsom bøger, musik, film, software, fotografier og kunstværker.

[8] Andre immaterielle rettigheder beskytter forskellige typer af intellektuel ejendom, herunder fx varemærker, patenter og design.

- **Juridiske Dokumenter:** Upublicerede juridiske dokumenter, rådgivning, retssager, og andre følsomme juridiske informationer.

Når du bruger AI-chatbots, skal du have fokus på:

- **Formål:** Overveje, om det er nødvendigt at bruge værktøjet, og hvordan det bedst bruges ansvarligt og effektivt.
- **Minimering**: Kun afgive oplysninger, som skønnes absolut nødvendige, for at opgaven kan løses.
- **Rigtighed**: Kontrollere, vurdere og evt. validere de svar, som chatbotten genererer.
- **Nødvendighed:** Rense svar for evt. personoplysninger/personhenførbare oplysninger og/eller andet indhold af fortrolig karakter. Hvis et genereret svar indeholder information, der kan karakteriseres som fortroligt eller følsomt, skal indholdet slettes eller anonymiseres.
- **Ansvarlighed:** Have klare rutiner for sletning af prompts og lukning af adgange.
- **Læk af persondata:** Sikkerhedsbrist f.eks. deling af personoplysninger skal håndteres i overensstemmelse med skolens alm. regler. Hvis du kommer til at uploade/dele personoplysninger via et AI-værktøj, skal du kontakte skolens datasikkerhedstovholder eller skolens DPO.

Du bør altid følge god skik og være gennemsigtig og ærlig, når materialet er helt eller delvist skabt med hjælp fra en AI-chatbot, fx angive kildehenvisning(er).

12. Mailpolitik (alle)

De vigtigste regler er følgende:

1. Al arbejdsrelateret brug af e-mail på Roskilde Gymnasium sker via Outlook eller Outlook Web App gennem skolens Microsoft Exchangeserver. Det betyder, at private e-mailkonti ikke må bruges til arbejdsrelateret kommunikation.
2. Roskilde Gymnasiums mailsystem er standardindstillet til automatisk at slette mails, når de er 13 mdr. gamle. Dette for at undgå, at mailsystemet bruges som arkiv.
3. Uanset denne automatiske sletning skal medarbejderen selv være opmærksom på, at mails med følgende typer af personoplysninger maksimalt må opbevares i Outlook i én måned, efter sagen er slut: fortrolige og følsomme[9] personoplysninger (fx oplysninger om trivsel, studievejledning, psykolog, diagnoser, ordblindhed, fraværsårsager, sociale problemer, gæld, kriminalitet, familiestridigheder og lignende). Når der er gået mere end en måned fra den sag, som mailen angår, er slut skal mailen enten slettes eller overføres til et sikkert it-system, som skolen stiller til rådighed (se nedenfor om sletning af mails).
4. Mails med øvrige personoplysninger slettes også, straks de har mistet deres relevans, hvilket normalt er inden for et par måneder. Skal mailen gemmes i længere tid, overføres den til DocuNote og slettes i mailsystemet. Kun administrative medarbejdere har mulighed for at gemme i DocuNote.
5. Arbejdsrelaterede mails mv. i Outlook er skolens ejendom, som skolen kan åbne og læse i særlige tilfælde. Dette sker dog kun, hvis det er strengt nødvendigt af hensyn til driften eller som led i fx it-support, som du evt. selv anmoder om. Dvs. at skolen ikke foretager fx stikprøvekontroller af indhold i e-mails mv.[10]Hvis skolen vil læse medarbejdernes e-mails, skal det varsles 6 uger på forhånd overfor medarbejderne.
6. Skolen læser ikke medarbejderes e-mails i Outlook, der er tydeligt mærket "privat". For nemheds skyld vil vi dog opfordre dig til at bruge en privat e-mailkonto til privat kommunikation.
7. Private mailkonti må ikke bruges til arbejdsrelateret kommunikation.
8. E-mails med CPR-numre eller helbredsoplysninger, der sendes til eksterne modtagere, skal sendes via Sikker Mail eller Digital Post (spørg evt. administrationen om hvordan).

Sletning af mails (kommentar til pkt. 2 og 3 ovenfor): For at sikre at mails med personoplysninger ikke opbevares for længe, skal hver medarbejder én gang månedligt gennemgå sin mailkonto (indbakke inkl. undermapper, sendt og slettet post).

Finder man ved sådan en gennemgang mails med personoplysninger, der overskrider opbevaringsgrænsen, skal mailen slettes straks.

13. Dette må du bruge Lectio til (alle)

Lectio kan bruges til:

- Elevers fraværsregistrering (under forudsætning af at man kun bruger de prædefinerede valgmuligheder)
- Helt korte beskeder om aflysninger, møder, fravær mv.
- Aflevering af skoleopgaver

[9] Følsomme personoplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske eller biometriske data - med det formål entydigt at identificere en fysisk person, helbredsoplysninger, seksuelle forhold eller seksuel orientering.

[10] Hjemlen til Roskilde Gymnasiums adgang til medarbejdernes mailkonti findes i GDPR art. 6 litra e.

- CPR-numre og karakterer, da vi pt. ikke har et alternativt opbevaringssted.

Roskilde Gymnasium bruger ikke Lectios kommunikationsfunktioner (fritekstfelter) når der indgår personoplysninger, da disse funktioner ikke er sikre nok til at fx oplysninger om elevers sygdom, trivsel og sociale forhold kan registreres der. Fremover bruger vi i stedet e-mail til at kommunikere om den slags, jf. ovenstående retningslinjer for brug af e-mails.

I Lectios kommunikationsfunktioner (fritekstfelter) skriver vi kun kortfattede, ikke-fortrolige personrelaterede oplysninger, fx "møde afholdt", "fravær drøftet", mv.

Vi opbevarer ikke egentlige elevsager i Lectio. I stedet bruges DocuNote (ESDH) og de deri oprettede elevmapper til studievejledning, sanktionssager, lægeerklæringer, SU- og SPS-ansøgninger og karakterer. Her har ledelsen, administrationen og studievejlederne adgang.

Fortrolighed omkring oplysninger i Lectio
Som medarbejder kan man evt. have adgang til oplysninger i Lectio, som er overflødige i forhold til ens funktion eller arbejdsopgaver, fx CPR-numre eller oplysninger om karakterer, fravær og opgaver for elever.

OBS: Det understreges, at man naturligvis ikke må bruge sin Lectio-adgang til at tilgå ***oplysninger, som man ikke har en tjenstlig årsag til at kende.***

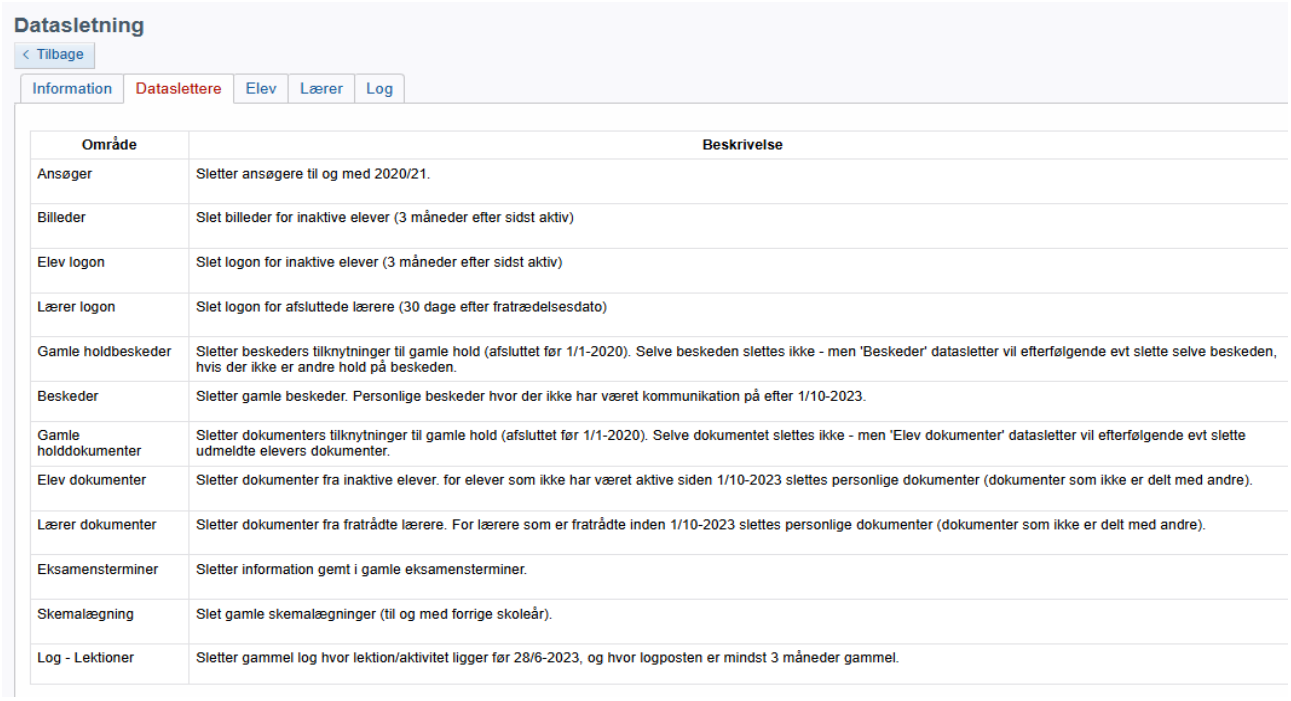
Lectio fører en systemlog, der registrerer aktivitet i systemet. Loggen viser én brugers trafik i systemet. Det kontrolleres ved stikprøvekontrol løbende fra ledelsens side, om loggen udviser aktivitet, som ikke modsvares af de opgaver, medarbejderne er pålagt som led i tjenesten.

14. Hvem står for oprydningen i de oplysninger, der allerede er registreret?

Ledelsen og administrationen står for at få slettet de gamle oplysninger om afgående elever (og fx vejleder- og administrativ note for nuværende elever) i Lectio.

Skolens Lectio-administrator sørger for sletning af afgående elever og fratrådte medarbejderes adgang til Lectio via modulet "Datasletning".

14.1 Datasletning i Lectio – Oplistning af alle de data som skolen kan slette



Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Område	Beskrivelse
Ansøger	Sletter ansøgere til og med 2020/21.
Billeder	Slet billeder for inaktive elever (3 måneder efter sidst aktiv)
Elev logon	Slet logon for inaktive elever (3 måneder efter sidst aktiv)
Lærer logon	Slet logon for afsluttede lærere (30 dage efter fratrædelsesdato)
Gamle holdbeskeder	Sletter beskeders tilknytninger til gamle hold (afsluttet før 1/1-2020). Selve beskeden slettes ikke - men 'Beskeder' datasletter vil efterfølgende evt slette selve beskeden, hvis der ikke er andre hold på beskeden.
Beskeder	Sletter gamle beskeder. Personlige beskeder hvor der ikke har været kommunikation på efter 1/10-2023.
Gamle holddokumenter	Sletter dokumenters tilknytninger til gamle hold (afsluttet før 1/1-2020). Selve dokumentet slettes ikke - men 'Elev dokumenter' datasletter vil efterfølgende evt slette udmeldte elevers dokumenter.
Elev dokumenter	Sletter dokumenter fra inaktive elever. for elever som ikke har været aktive siden 1/10-2023 slettes personlige dokumenter (dokumenter som ikke er delt med andre).
Lærer dokumenter	Sletter dokumenter fra fratrådte lærere. For lærere som er fratrådte inden 1/10-2023 slettes personlige dokumenter (dokumenter som ikke er delt med andre).
Eksamensterminer	Sletter information gemt i gamle eksamensterminer.
Skemalægning	Slet gamle skemalægninger (til og med forrige skoleår).
Log - Lektioner	Sletter gammel log hvor lektion/aktivitet ligger før 28/6-2023, og hvor logposten er mindst 3 måneder gammel.

Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Dataslet elev

Område	Generel sletteregel
Stamdata	Elevens stamdataoplysninger slettes 2 år efter elevens slutdato. Sletning omfatter kontakt- og adresseoplysninger, adminnoter samt ansøgeroplysninger, studieretningsønsker, valgfagsønsker og fagvalg.
Værger	Cpr-værger slettes 1 år efter elevslutdato eller efter 18 års fødselsdag. Andre kontakter slettes 1 år efter elevslutdato eller hvis der er sat flueben på tjekboksen "Dataslet 18 år". (kan slettes fra først kommende måned efter der er gået 1 år fra elevslutdato eller fra dagen hvor elev fylder 18 år). Sletning omfatter alle værgeoplysninger.
Elevsager	Elevens elevsager slettes efter elevens slutdato. Sletning følger de sletteregler der er opsat på den individuelle elevsag.
Fraværsårsager	For elever som er aktive: Elevens fraværsårsagsnoter slettes efter 2 skoleår (aktuelt registreringer i 2021/22 eller før). (kan slettes fra den 01/12 inde i det efterfølgende skoleår). For elever som ikker er aktive: Slettes 5 måneder efter sidste dag (aktuelt registreringer i 2023/24 eller før). Sletning omfatter elevs indtastede årsager til fravær.
Karakter- og fraværsbemærkninger	Elevens karakterbemærkninger og fraværsbemærkninger slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter alle typer fraværsbemærkninger som samtaler, advarsler mv. og tilhørende noter samt alle typer karakterbemærkninger og tilhørende noter.
Karakterer	Elevens karakterer slettes efter elevs slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter Karakterer og karakternoter givet til eleven (men IKKE protokollinjer).
Fraværsregistreringer	Elevens fraværsregistreringer slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter fraværsregistreringer på aktiviteter.
Opgaveafleveringer	Elevens opgaveafleveringer slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes opgaveafleveringer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes opgaveafleveringer 10 år efter elevens slutdato. Sletning omfatter opgavefiler, opgaveindlæg, opgavekarakterer samt opgavefravær.
Opgaveafleveringsnoter	Opgaveafleveringsnoter slettes 2 år efter elevens slutdato. Sletning omfatter karakternoter, elevnoter og lærernoter på elevs opgaveafleveringer.

Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Dataslet Lærer

Område	Generel sletteregel
Friholdelser	Lærerens friholdelser slettes efter 1 skoleår. (kan slettes fra den 5. måned inde i det efterfølgende skoleår). Sletning omfatter lærerens friholdelsesperioder og årsager dertil.
Kompetencer	Lærerens kompetencer slettes 1 år efter lærerens fratrædelsesdato Sletning omfatter lærerens XPRS-kompetencer og XPRS-prøveterminscensurkompetencer.
Tidsregistreringer	Lærerens tidsregistreringer slettes efter 5 år (kan slettes 5 finansår efter tidsregistreringens slutdato). Sletning omfatter tidsregistreringstidspunkt, -type, -timetal og -noter.
Tilskudsmærker	Lærerens tilskudsmærker slettes efter 5 år (kan slettes 5 finansårefter efter TMK slutdato). Sletning omfatter manuelle TMK-linjer på læreren.
Stamdata	Lærerens stamdataoplysninger slettes 1 år efter lærerens fratrædelsesdato. Sletning omfatter kontakt- og adresseoplysninger, bankoplysninger og trækprocent.
Cpr nummer og navn	Lærerens stamdataoplysninger som cpr, navn og initialer kan ikke slettes via generel dataslet, men man kan manuelt fjerne / omdøbe det på den enkelte lærers stamdatafaneblad, fx 5 år efter fratrædelsesdato. Forslag til rettelse: Fjern CPR, omdøb Fornavn og efternavn til Ophørt samt omdøb unikke initialer til fx op1, op2 ... osv.

15. Password-politik (alle)

Når man modtager sit password fra Roskilde Gymnasium, skal man straks ændrer det til et nyt, personligt, komplekst password.

Passwordet skal altid være unikt og må ikke anvendes andre steder, fordi det ellers risikerer at kunne opsnappes af andre i forbindelse med et datalæk i andre IT-systemer.

Det nye password skal opfylde følgende krav:

- Minimum 12 karakter (men gerne flere – jo længere, jo stærkere)
- Blandede store og små bogstaver
- Tal
- Specialtegn

Eksempel på gyldigt password kunne være 20_RoedPiste.18.

Passwordet skal skiftes senest efter 90 dage (systemet beder om det), men det må gerne skiftes oftere.

Tidligere passwords må ikke genbruges – eller opdateres (til fx 20_RoedPiste.19)

Passwordet skal skiftes, hvis kollegaer eller andre kan have set eller lånt det.

Passwords må kun "huskes" af systemet, hvis der er tale om en personlig computer med unikt login fra forsiden.

Memorér dit password og undlad at skrive det ned. Et password må under ingen omstændigheder fremgå af fx post it's, der sidder på din computer.

Tast aldrig dit password mens din computer er koblet til en storskærm eller lignende, hvor passwordet kan aflures.

16. Instruks om beskyttelse af persondata udenfor Roskilde Gymnasiums fysiske lokaler (hjemmearbejdsplads) (alle)

Når man arbejder med personoplysninger uden for Roskilde Gymnasiums lokaler (fx på hjemmearbejdsplads) er sikkerheden særligt udfordret både fysisk og teknisk. Fx er risikoen for tyveri øget. Dette kræver særlig omtanke.

Sikkerhedskravene til at arbejde med personoplysninger uden for skolens lokaler er:

1. Vi tilgår de it-systemer, der er godkendt til Roskilde Gymnasiums persondata[11] via VPN-løsningen på https://vpn.gymadm.dk/. Derved kan man undgå at lagre midlertidige lokale dokumentversioner på sin egen bærbare pc. ***Problemet med den midlertidige opbevaring eller lokale dokumentversioner er nemlig især at huske at få disse versioner slettet effektivt igen***.
2. Hvis personoplysninger midlertidigt (undtagelsesvist) opbevares på en bærbar pc, i Outlook, på USB-nøgle, på udleverede krypterede lagringsmedier eller i papirform, skal personoplysningerne overføres til et

[11] Jf. side 14.

godkendt it-system på Roskilde Gymnasium hurtigst muligt og allersenest én måned efter sagsbehandlingen er afsluttet. Samtidig slettes personoplysningerne fra det usikre opbevaringssted.

3. Papirdokumenter med personoplysninger skal tages med retur til skolen med henblik på forsvarlig makulering. Det gælder også, hvis der printes uden for skolens lokaler.
4. Medarbejderen skal sørge for, at familiemedlemmer og andre uvedkommende ikke får adgang til personoplysninger som led i hjemmearbejde.
5. Den bærbare computer, tablet eller smartphone samt tilhørende passwords er medarbejderens personlige arbejdsredskab og må ikke deles med eller udlånes til andre – heller ikke familiemedlemmer.

17. Instruks om sletning af datamedier ifm. privat køb af udtjente arbejdsredskaber (alle)

Det sker, at man som medarbejder på Roskilde Gymnasium får et nyt digitalt arbejdsredskab (pc, mac, tablet, smartphone eller lignende), og at man samtidig får tilbudt at købe det udtjente arbejdsredskab af Roskilde Gymnasium til privat eje.

Inden det udtjente arbejdsredskab overgår til medarbejderens private eje, skal det forbi IT-administratoren, som gennemfører en effektiv sletning af arbejdsrelaterede data, herunder personoplysninger, på det udtjente redskab.

Det er kun IT-administratoren, der kan gøre dette, da der kræves særlige programmer. Sletning med de standardfunktioner, som er til rådighed på det udtjente redskab, giver ikke tilstrækkelig sikkerhed for, at sletning er effektiv og uigenkaldeligt.

Som led i køb af det udtjente arbejdsredskab modtager man faktura. Her kvitterer man for, at det udtjente redskab har været til sletning hos IT-administratoren.

18. Instruks om hvordan man sletter personoplysninger i systemer som fx Outlook mv. (alle)

På Roskilde Gymnasium opbevares fortrolige og følsomme personoplysninger i de godkendte it-systemer og ikke andre steder.

I denne instruks kan du læse om, hvordan du sletter personoplysningerne fra et "usikkert" system.

Det er vigtigt, at sletning af personoplysningerne fra det usikre system er det, man kalder "effektiv", dvs. at oplysningerne ikke kan gendannes i det usikre system, når du har udført sletterutinen.

Usikkert system	**Effektiv sletterutine**
Outlook (mails)	Mailen slettes (fra indbakken, sendt post eller "slettet post") ved at trykke "delete" mens "*shift*"-knappen holdes nede. Denne kommando sikrer, at mailen bliver slettet permanent fra mailserveren efter 90 dage. I den 90-dages periode vil mailen kunne gendannes med "Gendan"-funktionen i slettet post.
Stifinder/skrivebord (Filer, fx word, excel, power point, mv.)	På Windows systemer slettes Filer ved at højre-klikke på filen og vælge "slet" Vær opmærksom på, om pc'en er indstillet til at slette permanent med det samme eller blot overføre filen til papirkurven. Hvis sidstnævnte er tilfældet, skal filen også slettes fra papirkurven for at være slettet effektivt. På Mac systemer slettes filer ved at højre-klikke på filen og vælg "Flyt til papirkurv" derefter skal man holde "Command" knappen ned samtidig med højre-klikker på papirkurv. Så vælger man "Tøm papirkurv".

USB-stiks	Indholdet på USB'en slettes ved at stille musen på "ekstern disk" i skærmbilledet "denne PC", højreklikke og vælge "formater". ***BEMÆRK at denne kommando sletter ALT indhold på USB'en.***
Fysisk print	Fysiske dokumenter tilintetgøres ved makulering straks dokumentet har udtjent sit formål. Der er en makulator i kopirummet på Roskilde Gymnasium.
Hjemmesiden	Roskilde Gymnasiums kommunikationsmedarbejder administrerer hjemmesiden og kan slette billeder og kontaktinfo om medarbejdere. Cache-filer fra søgemaskiner som fx Google, slettes som beskrevet her

Vejledningen kan også hentes på GF's intranet Tips til hvordan man sletter persondata effektivt

Kapitel 2 - Tjeklister og beskrivelser til specifikke medarbejdergrupper

Som det fremgår i indledningen på side 6 og frem, om skolens opgaver vedr. beskyttelse af personoplysninger, skal vi have retningslinjer, der støtter medarbejderne i at arbejde på en måde, der i praksis beskytter personoplysninger mod bl.a. for lang opbevaring eller uvedkommendes kendskab.

Dette kapitel indeholder Roskilde Gymnasiums konkrete retningslinjer til specifikke medarbejdergrupper om praktisk beskyttelse af personoplysninger.

19. Instruks om brug af administrative systemer. Brugeradgange og rettigheder (TAP)

Administrative medarbejderne på Roskilde Gymnasium må kun behandle personoplysninger i de it-systemer, som Roskilde Gymnasium har godkendt til formålet.

Disse er:

- Outlook (mail)
- Office365
- E-Boks
- DocuNote (ESDH)
- Statens lønsystem og LDV
- Navision stat

- Indfak2
- GymBetaling
- CPR-Registeret

Der må **ikke** gemmes personoplysninger i andre systemer end de nævnte.

Den enkelte medarbejder på Roskilde Gymnasium gives autorisationer og rettigheder til it-systemerne ud fra en konkret vurdering af medarbejderens arbejdsopgaver. Overflødiggjorte autorisationer lukkes.

Har man som medarbejder en autorisation, som (ikke længere) svarer til, hvad man har behov for til udførelse af sine arbejdsopgaver, men som derimod giver adgang til flere personoplysninger eller flere it-systemer, end hvad der er nødvendigt, skal man straks give sin nærmeste leder besked herom.

Det vil sige, at man som medarbejder selv skal reagere og kontakte sin nærmeste leder, hvis man har adgang til "for meget" eller "for lidt" – eller hvis man er i tvivl, om dette er tilfældet.

Det kontrolleres også løbende og mindst hvert 2 gange årligt fra ledelsens side, at autorisationerne svarer til det saglige behov.

Fremgangsmåderne for brugeroprettelser kan ses i [Forretningsgange for brugeroprettelser].

Om passwords til systemerne gælder skolens generelle passwordpolitik i afsnit 15. Passwordpolitik.

20. Instruks om brug af CPR-numre (TAP)

På Roskilde Gymnasium må vi bruge CPR-numre til "entydig identifikation eller som journalnummer", jf. databeskyttelseslovens § 11.

Det betyder at Roskilde Gymnasium må anvende CPR-numre som identifikation eller journalnummer i de opgaver, der løses i elev- og personaleadministration, bogholderi, it-drift og -support, undervisning, mv.

CPR-numre er fortrolige personoplysninger, og derfor skal de:

- Kun ses og behandles af de medarbejdere, hvis arbejdsopgaver berettiger til det, fx som led i lønadministration eller som "adresseliste" til udsendelse af mails via Digital Post
- Opbevares i sikre it-systemer og ikke andre steder
- Sendes via Sikker Mail eller Digital Post, hvis de indgår i en mailkorrespondance
- Makuleres, hvis de indgår i et fysisk dokument, og formålet med dette dokument er udtjent.

CPR-nummer fremgår som standard af blanketten til fraværsmelding. Den medarbejder, der lægger en udfyldt blanket på sin leders forladte skrivebord, skal selv være opmærksom på, at blanketten dermed er frit tilgængelig for forbipasserende, indtil lederen er retur.

CPR-numre fremgår ikke af skolens ansættelsesbreve.

20.1 Om videregivelse af CPR-numre

Roskilde Gymnasium videregiver kun CPR-oplysninger til eksterne modtagere (fx SKAT eller UVM), hvis det er nødvendigt for, at vi kan udføre vores opgaver, og hvis videregivelsen kan ske på sikker vis (fx via Sikker Mail, Digital Post eller krypteret digital indberetningsformular). Såfremt skolen modtager EU-fondsstøttemidler til et projekt på skolen med deltagelse af elever og/eller lærere, vil skolen for at være berettiget til at modtage støtten ifølge lovgivningen skulle afrapportere en række personoplysninger om de deltagende, herunder cpr.-numre, til Erhvervsstyrelsen/tilsynsmyndigheden.

21. Instruks om brug af Sikker Mail og andre fortrolige og følsomme personoplysninger (TAP)

Når CPR-numre (og andre fortrolige eller følsomme personoplysninger) sendes via e-mail, skal der bruges Sikker Mail eller Digital Post. Herved krypteres indholdet i mailen, så uvedkommende ikke kan læse med.
Kravet om Sikker Mail gælder, uanset om CPR-oplysningerne (eller de andre fortrolige eller følsomme personoplysninger) fremgår af overskriften, teksten, vedhæftninger eller links.

Man kan slippe for at bruge Sikker Mail, hvis man sletter eller overstreger alle CPR-numre (og øvrige fortrolige eller følsomme personoplysninger) i mailen, inden den sendes. Det kan fx være en praktisk model, hvis modtageren ikke har en Sikker Mail-løsning.

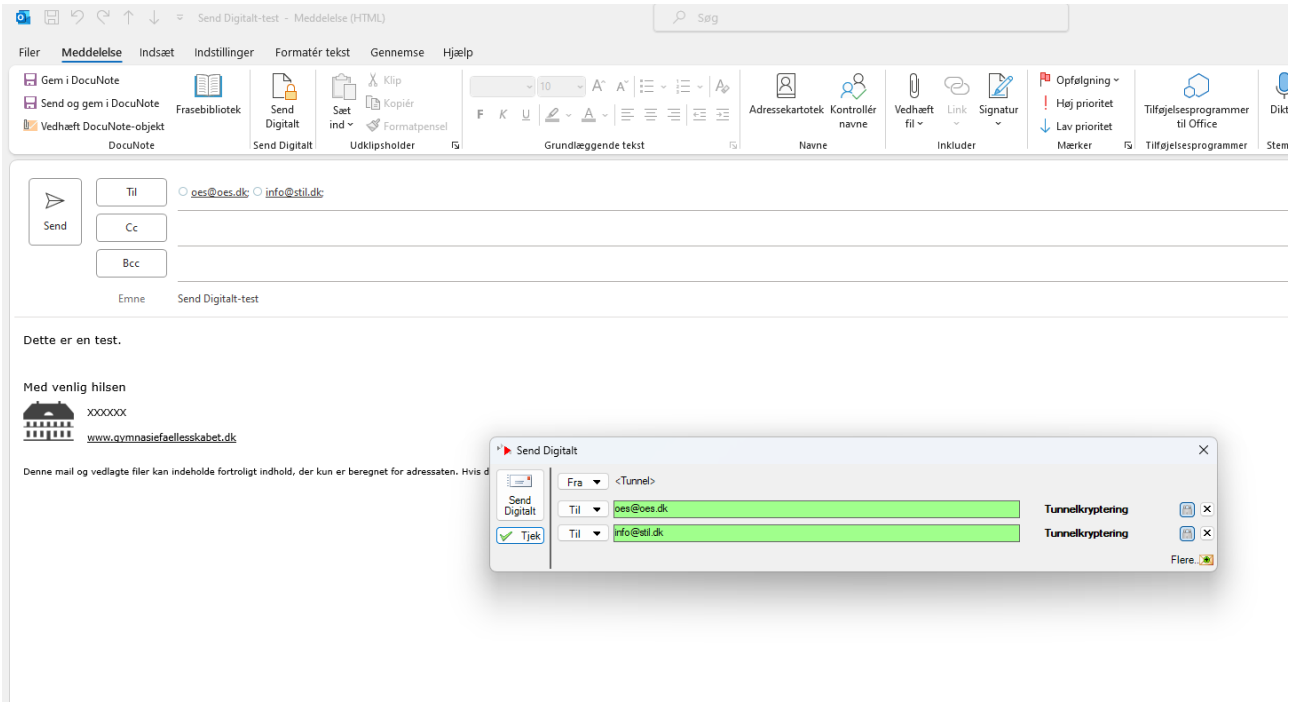
Husk at når den sikre mail er afsendt, skal den ikke blive liggende i "sendt post" i Outlook/Digital Post, men overføres[12] til DocuNote (ESDH) indenfor de tidsfrister, der er beskrevet i afsnit 1. og Roskilde Gymnasiums leveregler for datasikkerhed, på side 10.

[12] Senest 1 måned efter sagsbehandlingen er afsluttet.

21.1 Hvordan ved man, om man sender Sikker Mail?

Sikker Mail via tunnelmail

Åbn en mail og klik på "Send Digitalt":



I stedet må man ringe til modtageren og spørge om, hvordan de kan modtage sikker mail.

Følgende skoler anvender tunnelmailen via Gymnasiefællesskabet:

- Allerød Gymnasium
- Aurehøj Gymnasium
- Borupgaard Gymnasium
- Egedal Gymnasium & HF
- Espergærde Gymnasium & HF
- Frederiksværk Gymnasium
- Gefion Gymnasium
- Gentofte HF
- Gladsaxe Gymnasium **(ggadm.dk)**
- Greve Gymnasium
- Helsingør Gymnasium **(adm.hels-gym.dk)**

- Himmelev Gymnasium
- Køge Gymnasium
- Nordfyns Gymnasium
- Nyborg Gymnasium
- Nørre Gymnasium
- Roskilde Gymnasium
- Roskilde Katedralskole
- Rungsted Gymnasium
- Rysensteen Gymnasium
- Sct. Knud Gymnasium
- Solrød Gymnasium
- Tårnby Gymnasium og HF
- Virum Gymnasium
- Ørestad Gymnasium **(adm.oegnet.dk)**

Man kan også tjekke hjemmesiden hos modtageren. Her vil der typisk være oplyst en sikkermail@[domæne].dk for modtagerinstitutionen. Man skal dog være opmærksom på, at en sådan sikker mailadresse typisk er en fælles funktionspostkasse for hele institutionen, dvs. at flere administrative medarbejdere kan have adgang. Brugen af denne model kræver derfor, at man som afsender sikrer sig, at mailen (automatisk eller manuelt) bliver fordelt internt i modtagerinstitutionen til den rette person. Dette kan sikres ved at skriver "Fortroligt. Skal videresendes til [navn på person]" i mailens emnefelt, hvorved de øvrige medarbejdere, der har adgang til indbakken i den sikre fællespostkasse, bliver advaret om, at mailen skal videresendes.

Desuden kan man i særlige tilfælde (fx hvis der er tale om følsomme personoplysninger eller en hastende sag) vælge at sende en adviseringsmail (uden fortrolige og følsomme personoplysninger) til modtagerens egen (usikre) mailadresse med information om, at der nu ligger en sikker mail i den fælles postkasse og venter på at blive fordelt.

Danske Gymnasier fører en liste over gymnasiernes hovedpostkasser, som findes her. Det er dog ikke helt klart, om der for alle gymnasiers vedkommende er tale om sikre mailadresser. Brug af denne liste fritager derfor ikke afsenderen fra at tjekke, om modtagerens postkasse er sikker, jf. ovenfor.

22. Sikker Mail via Digital Post

Nogle medarbejdere på Roskilde Gymnasium har integreret Digital Post til deres Outlook og/eller DocuNote (ESDH). Hvis ikonet for "Digital Post/Send Digitalt" fremgår af ens mailsystem, har man adgang til at afsende via Digital Post fra Outlook.

Mailkorrespondance via Digital Post er sikker fra afsender til modtager (begge parter inklusive). Modtageren kan læse mailen på borger.dk og mit.dk.

Vær opmærksom på, at når man sender til en skole eller institutions Digital Post, så er der normalt tale om en fællespostkasse, hvorfor man bør følge anbefalingerne i afsnittene umiddelbart ovenfor, hvis man bruger denne model.

Forsendelse via Digital Post sker ved opslag på CPR-nummer. Om opmærksomhedspunkter ved brug af CPR-numre til fx opslag i Digital Post se "instruks" i afsnit 22. Sikker Mail via Digital Post.

23. Elevoplysninger – generel info til skolens elevadministrative medarbejdere (TAP)

- FAQ om elevoplysninger findes i kapitel 3.

- ***Alle skabeloner ligger på GF's hjemmeside: Inspirationskatalog og dokumenter elever (gymnasiefaellesskabet.dk)***
  https://www.gymnasiefaellesskabet.dk/gym/index.php/inspirationskatalog-og-dokumenter-elever

- ***GF's vejledning om brug af standardstruktur til elevsager i DocuNote ligger på GF's hjemmeside:***
  https://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/esdh

Følgende **light tjekliste** kan med fordel bruges som overblik over to-do's som led i modtagelse, håndtering, opbevaring og sletning af personoplysninger:

1. Er der tale om en personoplysning, som vi har brug for/må registrere?
2. Er den registrerede person orienteret om behandlingen og om sine rettigheder vedr. indsigt, berigtigelse, sletning mv.?
3. Hvilke it-systemer må personoplysningen gemmes i?
4. Fortrolighed, logning, brugerstyring, slettemulighed
5. Hvor længe må/skal vi opbevare personoplysningen – og hvordan får vi den slettet igen?

Typiske personoplysninger i elevforløb:

Almindelige personoplysninger
Stamoplysninger/kontaktoplysninger, oplysninger om afgiverskole, ansøgning, udtalelser fra UUV, foto, ansøgningen, notater ang. uddannelsesparathed, optagelsesprøve, optagelsesbrev, diverse erklæringer og oplysninger om særlige forhold, dispensationer, individuelle aftaler fx om udlån af iPad, bøger, tilladelser, bemyndigelser, evt. lægeerklæringer om fravær ifm. undervisning og/eller eksamen, fritagelse fra idræt, mentorordninger, særlige forhold fx hemmelig adresse, kopi af pas, kørekort, mv.

Eksamensklager og dokumenter fra sagsbehandlingen af klagesagen.

Breve ang. advarsler om for højt fravær, mødereferater, beviser vedr. snyd ved prøver, breve om sanktioner (fx fratagelse af SU, prøveaflæggelse i alle fag, ikke-indstillet til eksamen, bortvisning.

Følsomme personoplysninger:
Oplysninger om handicap, helbredsdiagnoser, studievejlederens løbende notater samt ledelsens evt. notater på baggrund af fx bekymringshenvendelser fra hjemmet og lignende.

Ansøgning om SPS, refusionsanmodninger, mentor, bemyndigelseserklæring, testresultater, udtalelser.

Ansøgning om dispensation til udeboende SU, beregning efter aktuel forældreindkomst, ligestillingssager (udlændinge), notater, øvrige sagsdokumenter.

23.1 Tjekliste – Elever, Optag (TAP)

Nr	Opgave	Evt. GF-Skabelon	Ansvarlig for udførelse	Initialer på skolens	Hvornår

				ansvarlige medarbejder	
ANSØGERE					
1	Hentning af ansøgere fra optagelse.dk til Lectio		Skolen	MKE	marts
2	Indlæsning af ansøgere fra Lectio til DocuNote mhp. oprettelse af ansøgningssag i DocuNote		GF IT	MKE	marts
3	Generel orientering til elever og forældre om behandling af personoplysninger som led i optag	Skabelon **E0**	Skolen Orienteringen kan med fordel gives på skolens hjemmeside + link i kvitteringsbrev	MKE/MES	Senest 10 dage efter ansøgningen er modtaget
4	Brug af krypteret mailforbindelse (Sikker Mail eller Digital Post) ved ekstern e-mail-kommunikation med andre gymnasier, fordelingsudvalg, UUV, hjemmet mv., hvis mailen indeholder CPR-nummer eller andre fortrolige eller følsomme personoplysninger		Skolen	MKE	løbende
5	Optagelsesprøve: noter, vurderinger begrundelser oprettes og gemmes i DocuNote. Afslag med begrundelse gives via Digital Post		Skolen		juni/juli
6	Videregivelse af personoplysninger til modtager-skole, hvis ansøgeren ikke kan optages på Roskilde Gymnasium, kan som udgangspunkt ske, hvis ansøgeren er orienteret om det via orienteringsbrevet i punkt 2 ovenfor. Ellers kræver videregivelsen muligvis elev-samtykke.		Skolen	MKE	marts/april/ maj
7	Orientering på hjemmesiden om, hvordan man kommunikerer sikkert digitalt med skolen, se afsnit 22.		Skolen	MES	
8	Sletning af oplysninger om ikke optagne ansøgere og deres forældre (på alle medier – også i Outlook), når optagelsesprocessen er slut		Udføres manuelt af skolen, da der ikke findes en funktion til automatisk sletning	MKE/GF IT	Med udgangen af kalenderåret 2018

OPTAGNE ELEVER					
9	Oprettelse af elevsager i DocuNote + oprettelse af kassationskode på ansøgningssagen		GF		
10	Generel orientering til elever og forældre om behandling af personoplysninger som led i skolegang	Skabelon **E1a**	Skolen Orienteringen ligger på skolens hjemmeside + link i velkomstbrev	MKE/MES	Senest 10 dage efter skolen har påbegyndt sin administration af skolegangen
11	Udsendelse af (link) til elevhåndbog om fx retningslinjer om ● Sikker digital kommunikation med Roskilde Gymnasium (mail og Lectio) ● Brug af skolens it ● Brug af apps som led i undervisning ● Brug af fx billeder af kammerater	**Elevhåndb og** eller GF's skabelon til "Husregler for digital undervisnin g"	Skolen	KLE/MKE	Senest samtidig med at eleven begynder at bruge it-systemerne mv.
12	Indhentning af (dokumenteret) samtykke til fx ● Offentliggørelse af elevens foto på hjemmesiden, Facebook, i trykte publikationer, mv. ● Registrering af helbredsoplysninger som i studievejledning, ansøgning om SPS og daglig kommunikation med fx lærere	Skabelon **E3a** og **E3**	Skolen	MKE/KLE	Inden skolen begynder at registrere oplysninger eller offentliggøre fotos, der kræver samtykke
13	Besvarelse af elevens eller forældrenes anmodning om indsigt efter reglerne i databeskyttelsesforordningen	**E2**	Skolen	MKE/KLE	Snarest og senest 1 måned efter anmodningen
IKKE-OPTAGNE ELEVER					
14	Sletning af ikke-optagne ansøgere i Lectio		Skolen		Med udgangen af kalenderåret

23.2 Tjekliste – Brobygningselever (TAP)

Nr	Opgave	Evt. GF-Skabelon	Ansvarlig for udførelse	Initialer på skolens ansvarlige medarbejder	Hvornår
1	Orienteringsskrivelse til brobygningseleven om, at skolen behandler personoplysninger. Dette gives	Skabelon **E5**	Skolen	MKE/MES	

	Fx via link eller henvisning i det velkomstbrev med skoleskema, der udleveres til brobygningseleverne den første dag, til sted på skolens hjemmeside om "Generel orientering om behandling af personoplysninger til gæster mv.				
2	Oplysninger om brobygningselever opbevares i et sikkert it-system, fx DocuNote, og slettes 5 år efter det kalenderår, hvori eleven har udløst taxametertilskud[13]		Skolen		

23.3 Tjekliste – Elever, skolegang (TAP)

Nr	Opgave	Evt. GF-Skabelon	Ansvarlig for udførelse	Initialer på skolens ansvarlige medarbejder	Hvornår
1	Varsling af kontrol med computer til eksamen med netadgang	Skabelon **E4**	Skolen	TG	Afventer nyt fra uvm vedr. sommer 2019
2	Når eleven fylder 18 år, skal værges kontaktoplysninger, herunder CPR-nummer slettes, medmindre eleven i særlige tilfælde har afgivet samtykke til, at skolens stadig må kontakte værgen med oplysninger om eleven.	RGE1 (udarbejdes)	Administration og studievejledning	KLE	Når eleven fylder 18 år

[13] Manuelt eller via automatisk kassationsfunktion.

23.4 Tjekliste – Elever, dimission (TAP)

Nr.	Opgave	Evt. GF-Skabelon	Ansvarlig for udførelse	Initialer på skolens ansvarlige medarbejder	Hvornår
1	Generel orientering til afgående elever om nedlukning af it-adgange og sletning af data	**E9**	Skolen		Kan med fordel ske forud for sidste skoledag
2	Oprettelse af pdf-version af eksamensbevis for hver elev. Sker manuelt. Gemmes i mappen "eksamensbeviser" i DocuNote (fælles for årgangen)		Skolen		
3	Inaktivering af elever i **Lectio**. Sker manuelt eller automatisk, hvis elevens uddannelsesforløb fuldføres. Udløser **kassationskoder i DocuNote** og **GymBetaling**. Sletning af **elevers log-on adgang til Lectio**. Se side 18 ovenfor om hvordan		Skolen		Når eleven udmeldes, dog inden 1. august
4	Udtræk af GymBetaling for så vidt angår de elevoplysninger, der ikke vedrører enten skolens regnskab eller elevens samtykkeblanket (regnskabsoplysninger og samtykker gemmes i 5 hhv. 7 år fra dimission), men som skolen alligevel ønsker at gemme i en årrække			Punktet benyttes ikke pt.	
5	Mail til alle **it-leverandører**, der har hentet personoplysninger om eleverne via integration til UNI-login, om at ALLE oplysninger om afgående elever skal slettes		Skolen Orienteringen kan med fordel gives på skolens hjemmeside + link i kvitteringsbrev	TG	Senest med udgangen af kalenderåret
6	Sletning af alle "løse" personoplysninger om afgående elever fra diverse it-systemer (mail især). Sker som udgangspunkt manuelt	Se afsnit 7	Skolen (lærere, administrative medarbejdere, ledere, studievejledere)		Senest med udgangen af kalenderåret
7	Sletning af fotos af afgåede elever		Skolen (kommunikation)		Snarest muligt
8	Hvis eleven afbryder sit uddannelsesforløb på Roskilde Gymnasium og fortsætter på andet gymnasium: videregivelse af personoplysninger		Skolen		Løbende

	til modtagerskole, hvis der er hjemmel i uddannelses-bek. Ellers kræver videregivelsen elevens samtykke.				

24. Medarbejderoplysninger – generel info til skolens personaleadministrative medarbejdere (TAP)

- FAQ om elevoplysninger findes i kapitel 3

- ***Alle skabeloner ligger på GF's hjemmeside, men bliver i nærmeste fremtid placeret i DocuNote.***
  Inspirationskatalog og dokumenter medarbejdere (gymnasiefaellesskabet.dk)

- ***GF's arbejds- og forretningsgangsbeskrivelser om brug af personaleoplysninger som led i lønsamarbejdet ligger på GF's hjemmeside:***
  https://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/lon-personale/225-forretningsgangsbeskrivelser

- Følgende **light tjekliste** kan med bruges som overblik over to-do's som led i modtagelse, håndtering, opbevaring og sletning af personoplysninger:

1. Er der tale om en personoplysning, som vi har brug for/må registrere?
2. Er den registrerede person orienteret om behandlingen og om sine rettigheder vedr. indsigt, berigtigelse, sletning mv.?
3. Hvilke it-systemer må personoplysningen gemmes i?
4. Fortrolighed, logning, brugerstyring, slettemulighed
5. Hvor længe må/skal vi opbevare personoplysningen – og hvordan får vi den slettet igen?

Typiske personoplysninger i et ansættelsesforhold:

Almindelige personoplysninger
Stamoplysninger/kontaktoplysninger, oplysninger om uddannelse (og indirekte om overenskomstmæssigt tilhørsforhold), anciennitet, CV/meritter, dokumentation for erhvervserfaring og tidligere ansættelser, personlige og særlige forhold, civil status, antal børn under 7 år samt disses CPR-nummer (mhp. omsorgsdage), lønoplysninger, skatteoplysninger, pensionsforhold, NemKonto, foto, ansættelsesbrev.

Følsomme personoplysninger:
Oplysninger om handicap, helbredsdiagnoser, fagforeningsmæssige tilhørsforhold.

25. Tjekliste – rekruttering og nyansættelser (TAP)

Nr.	Opgave	GF-skabelon	Ansvarlig for udførelse	Initialer på skolens ansvarlige medarbejder	Gøres hvornår	Deadline (dato)
1	Orientering af ansøgerne om, at vi behandler personoplysninger om ham/hende som led i rekrutteringen	Skabelon **M0**	Sekretær	KLE	Ved opstart fx på hjemmesiden eller i	

					rekrutteringsportal	
2	Indstilling af korrekte brugeradgange til rekrutteringsplatformen for ansættelsesudvalget (tidligere medlemmer af ansættelsesudvalg nedlægges som brugere)		Sekretær/ evt. it	KLE	Ved opstart	
3	Påmindelse om tavshedspligt til ansættelsesudvalg		HN	HN	Ved opstart	
4	Indstilling af automatiserede slettedatoer i rekrutteringsplatformen		Sekretær	KLE	Ved opstart eller undervejs	
5	Sikring af ansøgerens forudgående, skriftlige samtykke til skolens indhentning af straffeattest, referencer og helbredsoplysninger (fodnote)	Skabelon **M4**	Ansættelsesudvalg	Ansættelsesudvalg	Undervejs	
6	Brug af krypteret mailforbindelse eller Digital Post til fagforening samt til handicappede ansøgere		Ansættelsesudvalg	Ansættelsesudvalg	Undervejs	
7	Udarbejdelse af ansættelsesformular samt valg af ordlyd til "kort" orientering om behandling af personoplysninger i ansættelsesbrev + link til "lang" orientering	Kort orientering i ansættelses-brev: Skabelon **M1a** Lang orientering til personale-håndbog: Skabelon **M1**	Sekretær	HN	Når den endelige kandidat er valgt	
IKKE-ANSATTE KANDIDATER						
8	Indhentning af samtykke til længere opbevaring af cv i "kandidatbank" (hvis opbevaring i + 6 måneder)	Skabelon **M3**	Ledelse/ sekretær		Ved opstart eller undervejs eller til slut	
9	Manuel sletning af oplysninger om ikke-ansatte ansøgere (på alle medier herunder Outlook og ESDH) når rekrutteringsproces er slut		Alle medlemmer af ansættelses-udvalg samt sekretær		Senest 6 mdr. efter afslutning af rekrutterings-proces	

10	Manuel eller automatiseret sletning af ansøgninger/cv i "kandidatbank"		Sekretær		Senest 3 år efter afslutning af rekrutterings-proces	

26. Tjekliste – Ansatte medarbejdere (nye og nuværende) (TAP)

Nr.	Opgave	Evt. GF-skabelon	Ansvarlig for udførelse	Initialer på skolens ansvarlige medarbejder	Gøres hvornår	Deadline (dato)
11	Oprettelse af personalesag i DocuNote	Ansættelse – arbejdsgangs-beskrivelse	Skolen og GF i samarbejde		Ifm. ansættelse	
12	Generel orientering af medarbejderen om behandling af hans/hendes *egne* personoplysninger som led i ansættelsesforhold	Lang orientering til personalehåndbog: Skabelon **M1**	KLE	HN	I Ansættelsesbrevet – eller via særskilt orienteringsmail til nuværende medarbejdere. kan også placeres i teamhåndbogen.	
13	Kvittering for udlån af IT-udstyr Kvittering for udlevering af nøgle/nøglekort	Skabelon **M7** Skabelon **M9**	Skolen		Når udleveringen sker	
14	Udsendelse af (link) til skolens retningslinjer om fx ● Sikker digital kommunikation med Roskilde Gymnasium (mail og Lectio) ● Brug af skolens it ● Særlige retningslinjer for medarbejderens arbejdsområde	**Skolehåndbog** i behandling af person-oplysninger	KLE	KLE	Ifm. ansættelse – eller via særskilt orienteringsmail til nuværende medarbejdere	
15	Indhentning af (dokumenteret) samtykke til fx ● Offentliggørelse af foto på hjemmesiden, Facebook, i trykte publikationer, mv. ● Registrering af helbredsoplysninger ● Andet efter skolens valg	Skabelon **M5** og Skabelon **M5a** samt **HR-databasen**	KLE	KLE	Inden den behandling, som der bedes om samtykke til, påbegyndes	

16	Orientering af medarbejderen om modtagelse af *nye* personoplysninger om ham, der rækker ud over den indledende orientering i M1, og som medarbejderen ikke kan forventes at være bekendt med, at arbejdsgiveren har modtaget	Skabelon **M2**	Skolen	HN	Senest 1 måned efter modtagelse af oplysningerne	
	Besvarelse af medarbejderens anmodning om indsigt, berigtigelse eller sletning efter reglerne i databeskyttelsesforordningen	Skabelon **M6**	Skolen	HN	Senest 1 måned efter anmodningen	

27. Tjekliste – fratrædende medarbejder (TAP)

	Handling	**Ansvarlig**	**Hvornår**	**GF-Skabelon**	**Initialer og frist**
1	Fratrædelsesbrev til medarbejderen med info om: ● Relevante punkter nedenfor ● Oplysning om, at skolen bevarer medarbejderens personalesag i 5 år fra udgangen af fratrædelsesåret, hvorefter den slettes i sin helhed. Hvis medarbejderen ønsker (dele af) personalesagen opbevaret i en længere periode, skal skolen vide det inden udløbet af de 5 år – dog helst snarest.	Roskilde Gymnasium Roskilde Gymnasium orienteres mhp. kassationskode på personalesagen GF Løn kontaktes mhp. koordinering af andre skrivelser til medarbejderen som led i fratrædelse	Så hurtigt som muligt og **helst 14 dage inden sidste arbejdsdag**	Skabelon **M10**	**HN**
2	Inddragelse af nøgle + lukning af låsebrik	Nærmeste leder Pedellen orienteres mhp. lukning af låsebrik	Senest den sidste ansættelsesdag	Sidste halvdel af kvitteringen for udlevering af nøgler udfyldes Skabelon **M9**	KLE/ERN
3	Aflevering af it-udstyr Alternativt køb af det lånte udstyr til privat eje	Nærmeste leder Roskilde Gymnasium indgår aftalen om salg på vegne af. skolen	Senest den sidste ansættelsesdag	Kvittering for returnering eller køb anvendes. Skabelon **M7** eller Skabelon **M8**	KLE/TG

4	Sletning af indhold (data og software med skole-licens) på det afleverede it-udstyr. ***Sletning sker, uanset om medarbejderen ønsker at aflevere eller købe udstyret, jf. pkt. 3***	IT-administrator	Senest en måned efter udstyret er afleveret.	Roskilde Gymnasiums forretningsgang for sletning af datamedier T4	TG
5	Lukning af bruger- og administratoradgange til it-systemer	IT/bruger-administrator	Senest den sidste ansættelsesdag	Roskilde Gymnasiums Forretningsgang for brugeroprettelse og -ændringer i administrative IT-systemer.	
6	Oprettelse af autosvar på medarbejderens e-mailadresse med info om medarbejderens fratræden og oplysning om, at mailen ikke videresendes automatisk, men skal genfremsendes til [navn på nærmeste leder]. Autosvar bevares i 30 dage. Lukning af mailkonto efter 30 dage.	Nærmeste leder/ IT-administrator	Senest den sidste ansættelsesdag	Skabelon **M11**	GF
7	Opsigelse af hjemmeopkobling (bredbånd) og telefonabonnement	TG	Senest den sidste ansættelsesdag		TG
8	Sletning (samt overflytning til ESDH, hvis relevant for P-sagen) af de forskellige "løse" oplysninger om medarbejderen, der måtte befinde sig i Outlook, e-Boks, HR-databasen og andre systemer. Det kan fx være løbende korrespondance og opfølgning, bilag fra fratrædelsessag, MUS-referater, lægeerklæringer, mv., som det ikke har relevans at gemme i de 5 år, vi bevarer P-sagen.	Nærmeste leder og administrationen	Senest når medarbejderen fratræder	Se retningslinjer	HN
9	Sletning af medarbejderens foto og kontaktoplysninger fra skolens hjemmeside (samt i googles cache-kopi af hjemmesiden)	MES	Senest den sidste ansættelsesdag		HN

10	Sletning af P-sag NB: for medarbejdere, der er chefer eller født den 1. i måneden, påføres ikke kassationskode, men overføres til særskilt mappe.	Roskilde Gymnasium	Efter 5 år. Kassationskode påføres, når P-sagen inaktiveres	DocuNote vejledning om sletning i ESDH anvendes	KLE

28. Gymnasievejledning – sådan arbejder vi med personoplysninger

De lovgivningsmæssige rammer for gymnasievejledningen lægger op til, at gymnasievejledning er **fastholdelsesvejledning**, jf. følgende:

> *Gymnasielovens § 59, stk. 1: For at fastholde elever i uddannelse og sikre et sundt læringsmiljø skal institutionen i samarbejde med kommunalbestyrelsen og eventuelt Studievalg Danmark yde bistand til de elever, der har behov herfor. […]*[14]
>
> *STX-bekendtgørelsens § 50, stk. 1: Institutionen fastlægger retningslinjer for sit arbejde med at sikre et sundt læringsmiljø, hvor eleverne trives, og med at fastholde elever i uddannelse, herunder om institutionens arbejde med at nedbringe elevernes frafald fra uddannelsen. […]*[15]

28.1 Behandling af personoplysninger som led i fastholdelsesvejledningen

På baggrund af ovenstående hjemmel kan vi behandle følgende personoplysninger i den del af gymnasievejledningen, der har karakter af fastholdelsesvejledning:

- Stamoplysninger på elev og forældre, dvs. navn, adresse, CPR-numre, telefonnummer, mailadresse
- Elevens foto
- Elevens oplysninger fra ansøgningen, fx oplysninger om tidligere skoleaktiviteter, elevens begrundelse i fritekst for at søge om optagelse hos os, elevens karakterer fra 9. eller 10. klasse, evt. bilag med udtalelser, diverse erklæringer og oplysninger om særlige forhold
- Evt. vurderinger fra Ungdommens Uddannelsesvejledning om uddannelsesparathed
- Evt. resultater fra optagelsesprøve
- Oplysninger om elevens faglige resultater og standpunkt samt om deltagelse i prøver og eksamen
- Oplysninger om fravær og fraværsgrunde (dog ikke helbredsdiagnoser)
- Oplysninger om formodet eller konstateret snyd ved prøver og eksamen, overtrædelse af skolens studie- og ordensregler, strafbare forhold og/eller misbrug af skolens it-systemer eller netværk
- Oplysninger om sanktioner for ovenstående
- Oplysninger om gæld til skolen som følge af evt. manglende bogaflevering.

Fastholdelsesvejledningen må kun omfatte registrering af såkaldt "følsomme personoplysninger", hvis eleven skriftligt har givet sit samtykke til det, og forældrene (til elever under 18 år) har bekræftet dette samtykke.

[14] LBK nr. 41 af 12/01/2024.
[15] BEK nr. 497 af 17/05/2017.

Følsomme personoplysninger er: personoplysninger 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, jf. databeskyttelsesforordningens art. 9.

På Roskilde Gymnasium har vi prioriteret at kunne hjælpe eleverne med de ting, de betror gymnasievejlederen, fx helbredsproblemer. Derfor beder vi eleven (og forældrene hvis eleven er under 18 år) om samtykke til registrering af følsomme personoplysninger som led i fastholdelsesvejledning.

Samtykket indhentes via GymBetaling, hvor studievejlederen med sin administratoradgang selv kan gå ind og se, om eleven har givet samtykke.

Den formulering, som skolen bruger i samtykkeblanketten kan findes i DocuNote.[16]

Hvis eleven har givet samtykke, kan følsomme personoplysninger registreres, forudsat dette er proportionelt, sagligt og nødvendigt for at hjælpe eleven. Registreringen sker i mappen "Studievejledning" i DocuNote, hvortil gymnasievejlederen har adgang. Se afsnit 4 nedenfor om brug af it som led i studievejledningen.

Hvis samtykke er afslået, må gymnasievejlederen ikke notere følsomme personoplysninger om eleven. Hverken elektronisk eller i hånden. Heller ikke som led i en "en god snak", gymnasievejlederens "egen" nedskrevne historik over elevens udvikling, eller hvis samtalen har mere terapeutisk karakter a la psykologsamtale. Derved vil gymnasievejlederen være afskåret fra at hjælpe de elever, der kommer til gymnasievejlederen i en svær situation pga. fx migræneanfald eller andre helbredsproblemer med fx at se lempeligt på det fravær, der skyldes disse ting.

28.2 Behandling af følsomme personoplysninger som led i vejledning om særlige vilkår eller ydelser

Hvis vejledning til eleven specifikt drejer sig om følgende emner, må gymnasievejlederen gerne registrere de følsomme personoplysninger (fx helbredsoplysninger og lægelige oplysninger), der er nødvendige for at dokumentere, at eleven er kandidat til det særlige vilkår eller ydelsen. Dvs. at her kræves der ikke samtykke fra elev (eller forældre):

Vilkår eller ydelse	Gymnasievejlederen må registrere	Hjemmel
Specialundervisning eller anden specialpædagogisk bistand (se nedenfor om SPS-ansøgning)	Oplysninger om særlige behov "på baggrund af sagkyndige oplysninger og udtalelser herom… ".	Bek. om de gymnasiale uddannelser § 51
Sygeundervisning	Oplysninger om "Elever og kursister, der midlertidigt på grund af sygdom i længere tid ikke kan følge den almindelige undervisning" må registreres med henblik på "tilbud om sygeundervisning".	Lov om gymnasiale uddannelser § 62 og Bek.om de gymnasiale uddannelser §§ 52-56
Udeboende SU	Oplysninger, der dokumenterer tilstedeværelsen af de betingelser, der er nævnt i § 20, stk. 2, nr. 4, om "ganske særlige forhold i hjemmet, f.eks. (…) langvarig	SU-bek. § 20

[16] GF-skabelon E3a.

	sygdom (...)". Skolen "kan bl.a. til brug for sin afgørelse efter stk. 2, nr. 4, indhente en udtalelse fra de sociale myndigheder ... ".	
Reeksamen	Oplysninger om "dokumenteret sygdom" = lægeerklæring	Alm. eks.bek. § 9
Eksamen på særlige vilkår	Oplysninger om eksaminandens "fysiske eller psykiske funktionsnedsættelse (...), når det er nødvendigt for at ligestille" eksaminanden med andre."	Alm. eks.bek. § 19

Studievejlederens registrering af oplysningerne sker i mappen "studievejledning", eller "SU" i DocuNote, hvortil gymnasievejlederen har adgang. Se afsnit 4 nedenfor om brug af it som led i studievejledningen.

28.3 Særligt om ansøgning om SPS

Som nævnt i skemaet oven for må gymnasievejlederen gerne registrere "Oplysninger om særlige behov på baggrund af sagkyndige oplysninger og udtalelser herom" med henblik på "specialundervisning eller anden specialpædagogisk bistand".

Hvis skolen vurderer, at eleven er kandidat til en ansøgning om SPS-støtte, skal eleven dog skriftligt give sit specifikke samtykke til, at der indgives ansøgning til Styrelsen for Undervisning og Kvalitet.

Dette sker via GymBetaling, hvor gymnasievejlederen med sin administratoradgang selv kan gå ind og se, om eleven har givet samtykke.

Den formulering, som skolen bruger i samtykkeblanketten, kan ses på sidste side.

28.4 Brug af it-systemer til gymnasievejledning

Referat af møder med gymnasievejlederen lægges fremover i "Studievejledning" i **DocuNote**.

Hvis der er tale om særlige vilkår eller ydelser, jf. afsnit 2 og 3 ovenfor, bruges de særlige DocuNote-mapper, der findes til disse formål.

DocuNote-mapperne er oprettet på forhånd for hele årgangen.

Referater, noter, mv. med fortrolige eller følsomme personoplysninger fra studievejledningen må under INGEN omstændigheder gemmes i andre systemer eller platforme, undtagen hvis dette sker absolut undtagelsesvist, og gymnasievejlederen er MEGET omhyggelig med sletningen bagefter.

Brugeradgange til studievejledningsmapperne i DocuNote gives til gymnasievejlederne på årgangen, nærmeste leder og elevsekretær.

Kun de medarbejdere, der varetager gymnasievejledning eller har administrative eller ledelsesmæssige opgaver i forhold til studievejledningen, har brugeradgang til personoplysningerne i studievejledningsmapperne. Disse medarbejdere har brugerrettigheder til at søge, inddatere, redigere, rette og slette oplysninger i studievejledningsmapperne.

Det kontrolleres hver 6. måned, at kun de relevante medarbejdere har adgang til mapperne.

DocuNote fører en systemlog, der registrerer al aktivitet (inddatering, søgning, redigering, sletning mv.) i systemet. Loggen viser ikke selve resultatet af aktivitet (dvs. ikke det inddaterede/fremsøgte/slettede i ren tekst). Den viser derimod en brugers trafik (fx "XX søgte på [cpr]", "YY inddaterede", "ZZ slettede") i systemet 6 måneder tilbage.

Det kontrolleres løbende fra ledelsens side, om loggen udviser aktivitet, som ikke modsvares af de opgaver, medarbejderne er pålagt som led i tjenesten.

Sletning af oplysninger fra studievejledningen

Studievejledningsmapperne i DocuNote slettes automatisk, når eleven er blevet student. Den automatiske sletning sker ved, at de administrative medarbejdere inaktiverer de elever, der enten er blevet studenter eller har forladt skolen af andre årsager i det forgangne skoleår i Lectio. Dette bør ske kort tid efter skoleårets afslutning. Herved aktiveres der en automatisk sletning af studievejledningsmappen.

Oprydning i tidligere systemer

28.5 Lectio

På baggrund af en risikovurdering af funktionerne i Lectio (som GF har foretaget i december 2020 og ajourført senest i 2023) ligger det fast, at vi på Roskilde Gymnasium skal have vores egne procedurer for at:

- gennemføre sletning vha. Lectios slettefunktioner. Faciliteterne til sletning findes under "Stamdata".
- tage stikprøvekontroller af om sletningen er effektiv.

De slettefunktioner, der er indført i Lectio i 2019, er ikke automatiserede funktioner, men skal aktiveres håndholdt. Lectios slettefunktion er heller ikke 100 % effektive, men efterlader data. Det virker tilfældigt, hvad der efterlades, og hvad der slettes.

Det er medarbejdere med det absolut højeste sikkerhedsniveau, der kan bruge slettefunktionerne (dvs. de medarbejdere, der kan ændre passwords). Faciliteterne til sletning findes under "Stamdata".

Sletning af "administrative noter", "elevfravær" samt "varsler" kan Lectios sletterobot ikke hjælpe med. I disse felter vil der ofte optræde følsomme personoplysninger. Disse felter kan slettes vha. GF's sletterobot, som aktiveres, hvis skolen beder GF's IT-driftschef om det.

Skolens Lectio-administrator sørger for sletning af afgåede elever og fratrådte medarbejderes **log on**-adgang til Lectio via modulet "Datasletning":

Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Område	Beskrivelse
Ansøger	Sletter ansøgere til og med 2020/21.
Billeder	Slet billeder for inaktive elever (3 måneder efter sidst aktiv)
Elev logon	Slet logon for inaktive elever (3 måneder efter sidst aktiv)
Lærer logon	Slet logon for afsluttede lærere (30 dage efter fratrædelsesdato)
Gamle holdbeskeder	Sletter beskeders tilknytninger til gamle hold (afsluttet før 1/1-2020). Selve beskeden slettes ikke - men 'Beskeder' datasletter vil efterfølgende evt slette selve beskeden, hvis der ikke er andre hold på beskeden.
Beskeder	Sletter gamle beskeder. Personlige beskeder hvor der ikke har været kommunikation på efter 1/10-2023.
Gamle holddokumenter	Sletter dokumenters tilknytninger til gamle hold (afsluttet før 1/1-2020). Selve dokumentet slettes ikke - men 'Elev dokumenter' datasletter vil efterfølgende evt slette udmeldte elevers dokumenter.
Elev dokumenter	Sletter dokumenter fra inaktive elever. for elever som ikke har været aktive siden 1/10-2023 slettes personlige dokumenter (dokumenter som ikke er delt med andre).
Lærer dokumenter	Sletter dokumenter fra fratrådte lærere. For lærere som er fratrådte inden 1/10-2023 slettes personlige dokumenter (dokumenter som ikke er delt med andre).
Eksamensterminer	Sletter information gemt i gamle eksamensterminer.
Skemalægning	Slet gamle skemalægninger (til og med forrige skoleår).
Log - Lektioner	Sletter gammel log hvor lektion/aktivitet ligger før 28/6-2023, og hvor logposten er mindst 3 måneder gammel.

Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Dataslet elev

Område	Generel sletteregel
Stamdata	Elevens stamdataoplysninger slettes 2 år efter elevens slutdato. Sletning omfatter kontakt- og adresseoplysninger, adminnoter samt ansøgeroplysninger, studieretningsønsker, valgfagsønsker og fagvalg.
Værger	Cpr-værger slettes 1 år efter elevslutdato eller efter 18 års fødselsdag. Andre kontakter slettes 1 år efter elevslutdato eller hvis der er sat flueben på tjekboksen "Dataslet 18 år". (kan slettes fra først kommende måned efter der er gået 1 år fra elevslutdato eller fra dagen hvor elev fylder 18 år). Sletning omfatter alle værgeoplysninger.
Elevsager	Elevens elevsager slettes efter elevens slutdato. Sletning følger de sletteregler der er opsat på den individuelle elevsag.
Fraværsårsager	For elever som er aktive: Elevens fraværsårsagsnoter slettes efter 2 skoleår (aktuelt registreringer i 2021/22 eller før). (kan slettes fra den 01/12 inde i det efterfølgende skoleår). For elever som ikker er aktive: Slettes 5 måneder efter sidste dag (aktuelt registreringer i 2023/24 eller før). Sletning omfatter elevs indtastede årsager til fravær.
Karakter- og fraværsbemærkninger	Elevens karakterbemærkninger og fraværsbemærkninger slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter alle typer fraværsbemærkninger som samtaler, advarsler mv. og tilhørende noter samt alle typer karakterbemærkninger og tilhørende noter.
Karakterer	Elevens karakterer slettes efter elevs slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter Karakterer og karakternoter givet til eleven (men IKKE protokollinjer).
Fraværsregistreringer	Elevens fraværsregistreringer slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes karakterer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes karakterer 10 år efter elevens slutdato. Sletning omfatter fraværsregistreringer på aktiviteter.
Opgaveafleveringer	Elevens opgaveafleveringer slettes efter elevens slutdato. For elever med slutdato efter 17/5 2017 slettes opgaveafleveringer 5 år efter elevens slutdato. For elever med slutdato før eller på 17/5 2017 slettes opgaveafleveringer 10 år efter elevens slutdato. Sletning omfatter opgavefiler, opgaveindlæg, opgavekarakterer samt opgavefravær.
Opgaveafleveringsnoter	Opgaveafleveringsnoter slettes 2 år efter elevens slutdato. Sletning omfatter karakternoter, elevnoter og lærernoter på elevs opgaveafleveringer.

Datasletning

< Tilbage

Information | Dataslettere | Elev | Lærer | Log

Dataslet Lærer

Område	Generel sletteregel
Friholdelser	Lærerens friholdelser slettes efter 1 skoleår. (kan slettes fra den 5. måned inde i det efterfølgende skoleår). Sletning omfatter lærerens friholdelsesperioder og årsager dertil.
Kompetencer	Lærerens kompetencer slettes 1 år efter lærerens fratrædelsesdato Sletning omfatter lærerens XPRS-kompetencer og XPRS-prøveterminscensurkompetencer.
Tidsregistreringer	Lærerens tidsregistreringer slettes efter 5 år (kan slettes 5 finansår efter tidsregistreringens slutdato). Sletning omfatter tidsregistreringstidspunkt, -type, -timetal og -noter.
Tilskudsmærker	Lærerens tilskudsmærker slettes efter 5 år (kan slettes 5 finansårefter efter TMK slutdato). Sletning omfatter manuelle TMK-linjer på læreren.
Stamdata	Lærerens stamdataoplysninger slettes 1 år efter lærerens fratrædelsesdato. Sletning omfatter kontakt- og adresseoplysninger, bankoplysninger og trækprocent.
Cpr nummer og navn	Lærerens stamdataoplysninger som cpr, navn og initialer kan ikke slettes via generel dataslet, men man kan manuelt fjerne / omdøbe det på den enkelte lærers stamdatafaneblad, fx 5 år efter fratrædelsesdato. Forslag til rettelse: Fjern CPR, omdøb Fornavn og efternavn til Ophørt samt omdøb unikke initialer til fx op1, op2 ... osv.

28.6 Brug af e-mail som led i gymnasievejledning

Hvis gymnasievejleder på digital vis har brug for at kommunikere om fortrolige personoplysninger (cpr-numre) eller følsomme personoplysninger (helbredsdiagnoser), sker det via e-mail på skolens mail-server, og ikke i Lectio.

Mails med fortrolige personoplysninger (cpr-numre) eller følsomme personoplysninger (helbredsdiagnoser) må opbevares i mail-systemet i 1 måned. ***Hvis de skal bruges i længere tid, skal de flyttes over i DocuNote***.

Afsender er ansvarlig for, at mails flyttes over i DocuNote i (i mappen "Generelle elevoplysninger").

Derefter skal mailen slettes i mailsystemet. Både hos afsender og modtager(e).

Mails med fortrolige eller følsomme personoplysninger må under INGEN omstændigheder sendes videre til egen, privat mailkonto.

Hvis dokumentet har foreligget i fysisk version, makuleres den fysiske version, når dokumentet er indscannet og lagret i DocuNote.

29. Kommunikation og sociale medier – sådan arbejder vi med personoplysninger

Som led i kommunikationsopgaven på Roskilde Gymnasium offentliggør vi fotos og evt. også video og/eller tekst om elever og medarbejdere via følgende medier og platforme:

a. På hjemmesiden
b. På skolens profil sociale medier: Facebook, Instagram
c. I trykte publikation, på plakater, reklamer, bannere
d. På skolens info-skærme
e. I artikler eller indslag i dagblade, aviser og på tv.

Formålet med offentliggørelsen er at formidle skolens hverdag, traditioner, rejser, begivenheder, nyheder mv. i ord og billeder og markedsføre skolens uddannelsestilbud.

Skolens offentliggørelse af fotos på internettet forudsætter, at der er hjemmel til offentliggørelsen i form af et samtykke fra de personer, der er afbilledet. Den eneste undtagelse til samtykkekravet er at skolens udførelse af en opgave i samfundets interesse eller skolens opgaver som led i offentlig myndighedsudøvelse", jf. GDPR art. 6, litra e. Dette er en bred – men konkret – vurdering.

For at forebygge tvivl om, hvorvidt der er hjemmel til den enkelte offentliggørelse, indhenter vi på Roskilde Gymnasium elevers og medarbejderes samtykke til at vi må vise billeder på hjemmesiden, i trykte publikationer mv.

Den tidligere sondring mellem "portrætfotos og situationsbilleder" er ophævet. Derfor skal vi konkret vurdere, om hvert enkelt billede – og evt. offentliggørelse heraf – falder ind under hjemlen i art. 6, litra e, jf. ovenfor, eller om der skal indhentes samtykke jf. art. 6, litra a.

"Panoramaagtige" billeder fra fx dimission, gallafest, idrætsdag, mv., dvs. et billede fra en situation, hvor man som elev/medarbejder/gæst må kunne forudse og forvente, at der fotograferes og formidles billeder fra via forskellige medier, kan således konkret behandles – vises/offentliggøres – uden de enkelte personers samtykke.

Hvis en person, der er afbildet på et sådant billede senere, gør indsigelse mod visningen af billedet på fx hjemmesiden, skal det som altovervejende hovedregel fjernes fra hjemmesiden igen, medmindre den begrundelse,

som personen giver for sin indsigelse, ud fra en objektiv betragtning er af absolut uvæsentlig karakter. Dette er altid en konkret vurdering.

Det er skolens ansvar at sørge for, at eleverne og medarbejderne på billedet/videoen har givet deres forudgående, **frivillige, oplyste samtykke** til netop den offentliggørelse, der er er tale om. Samtykket skal endvidere kunne tilbagekaldes af eleven/medarbejderen.

> *Ex.: et elev-samtykke til, at skolen må vise elevens foto på hjemmesiden i "neutral" undervisningssammenhæng, er ikke nødvendigvis ensbetydende med, at eleven også samtykker til, at elevens foto må bruges som illustration i fx en digital avisartikel om seksuelle krænkelser, idet dette kan tolkes, som om det er netop dén elev, der har været involveret i en sag om seksuelle krænkelser.*

Samtykket skal desuden kunne **tilbagekaldes** af eleven/medarbejderen.

> *Ex.: skolens offentliggørelse af foto på Facebook (og afhængigt af det konkrete mediums brugervilkår formentlig også Instagram, YouTube, Snap Chat og andre sociale medier) kan indebære, at billedet ikke kan fjernes fra Facebooks database igen. Dvs. at elevens tilbagekaldelse af samtykket i praksis bliver umulig.*
>
> *Denne konsekvens ved at give sit samtykke til offentliggørelse på Facebook mv. bør fremgå tydeligt og udtrykkeligt af den tekst, som eleven præsenteres for, når han bliver bedt om at give samtykke. Derved bliver eleven gjort opmærksom på konsekvenserne af et samtykke til offentliggørelse på Facebook el.lign.*

Praksis

Elevernes samtykke til visning af fotos/videoer gives på blanket eller i GymBetaling. Herved sikres at samtykket er gyldigt. I GymBetaling er de spørgsmål, som eleverne skal besvare, formuleret som i punkt 1-5 nedenfor.

Økonomi- og administrationschef Katja Elm er ansvarlig for formuleringen af spørgsmålene, så de passer til skolens behov.

Bemærk, at teksten med kursiv er pligtmæssige oplysningskrav, dvs. at dem kan der ikke ændres på. Det er kun selve indholdet af spørgsmålet, som der bedes om samtykke til, der kan ændres på (eller helt fjernes).
En sekretær udpeget af økonomi- og administrationschef Katja Elm er ansvarlig for at lave negativ-liste over de elever og medarbejdere, der har sagt "nej" til offentliggørelse af deres foto.
En sekretær udpeget af økonomi- og administrationschef Katja Elm formidler listen til kommunikationsmedarbejdere og administratorer af de platforme, der er nævnt i litra a-e ovenfor. De pågældende medarbejderne er herefter medansvarlige for at tjekke, at der er givet samtykke fra alle på billedet eller videoen til offentliggørelse på netop dét medie eller i dén kontekst, der er tale om, jf. ovenfor.

Sletning

Hvis elever ønsker billeder slettet fra hjemmesiden eller andre steder, står skolens kommunikationsmedarbejder Mette Schønberg for sletning af fotos fra hjemmesiden.

Når et billede slettes fra hjemmesiden, skal skolen desuden gøre et forsøg på også at få slettet Googles visning af billedet i Googles cache-resultater. Googles egen vejledning i, hvordan dette kan gøres, findes her. Vejledningen er desværre ikke let, og det kan derfor anbefales evt. at drøfte med skolens hjemmesideleverandør, hvordan hjemmesiden kan kodes, så sletning af billeder fra hjemmesiden slår igennem på Google straks.

Sletning af indhold fra Facebook og andre sociale medier står kommunikationsmedarbejder Mette Schønberg for. Billedalbums og andre billeder på Facebook, der er +3 år gamle, slettes af kommunikationsmedarbejder Mette Schønberg.

NB: Red Barnets vejledning til sletning af billeder fra diverse sociale medier findes her

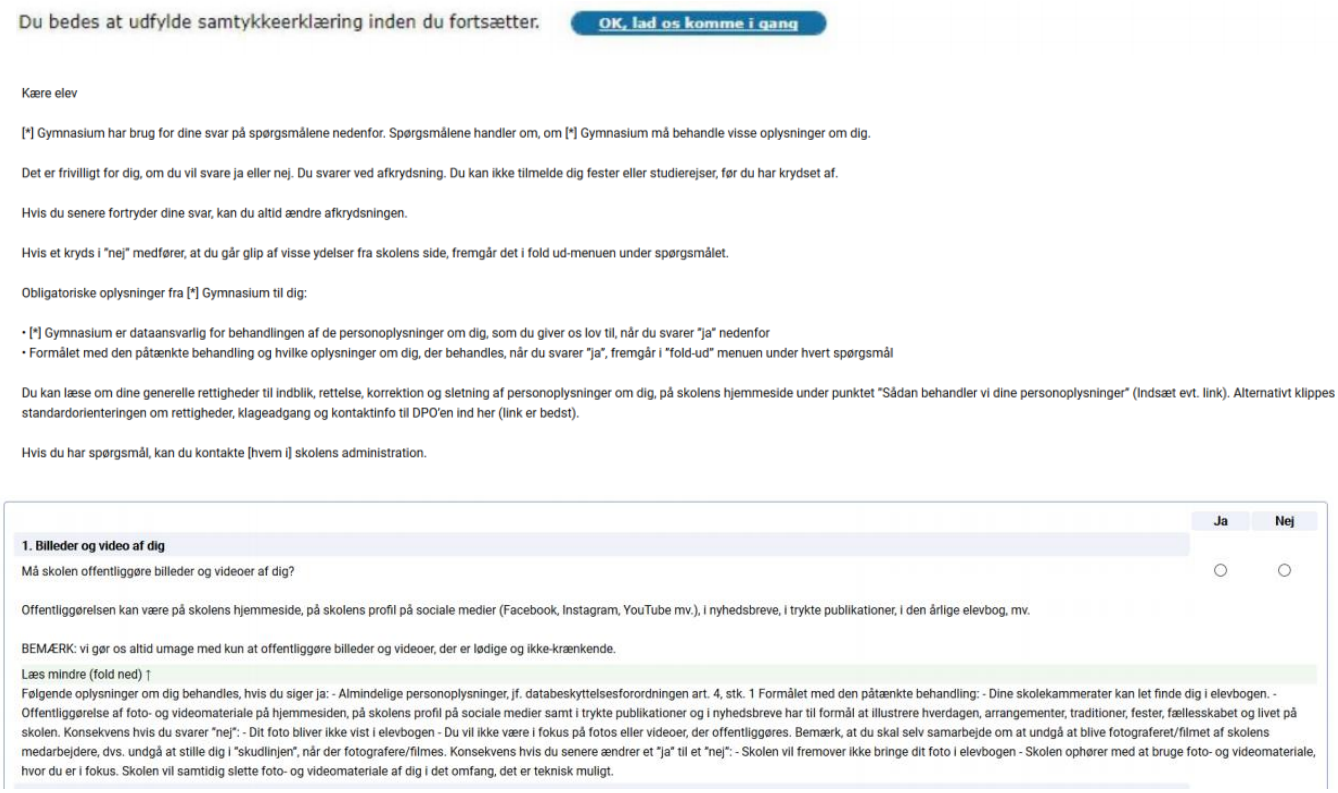
Andet

På hjemmesiden skal skolen have en "privatlivspolitik".

Hvordan er de spørgsmål, som eleverne skal besvare (give samtykke til) formuleret i GymBetaling?

Som nævnt ovenfor skal de enkelte spørgsmål tilpasses skolens behov, så man ikke spørger om mere eller mindre, end man har behov for.

Her er de spørgsmål fra GymBetaling (2020), der handler om samtykke til offentliggørelse af fotos og video, gengivet. Der findes også andre spørgsmål, men de er ikke medtaget her.



Du bedes at udfylde samtykkeerklæring inden du fortsætter. OK, lad os komme i gang

Kære elev

[*] Gymnasium har brug for dine svar på spørgsmålene nedenfor. Spørgsmålene handler om, om [*] Gymnasium må behandle visse oplysninger om dig.

Det er frivilligt for dig, om du vil svare ja eller nej. Du svarer ved afkrydsning. Du kan ikke tilmelde dig fester eller studierejser, før du har krydset af.

Hvis du senere fortryder dine svar, kan du altid ændre afkrydsningen.

Hvis et kryds i "nej" medfører, at du går glip af visse ydelser fra skolens side, fremgår det i fold ud-menuen under spørgsmålet.

Obligatoriske oplysninger fra [*] Gymnasium til dig:

- [*] Gymnasium er dataansvarlig for behandlingen af de personoplysninger om dig, som du giver os lov til, når du svarer "ja" nedenfor
- Formålet med den påtænkte behandling og hvilke oplysninger om dig, der behandles, når du svarer "ja", fremgår i "fold-ud" menuen under hvert spørgsmål

Du kan læse om dine generelle rettigheder til indblik, rettelse, korrektion og sletning af personoplysninger om dig, på skolens hjemmeside under punktet "Sådan behandler vi dine personoplysninger" (Indsæt evt. link). Alternativt klippes standardorienteringen om rettigheder, klageadgang og kontaktinfo til DPO'en ind her (link er bedst).

Hvis du har spørgsmål, kan du kontakte [hvem i] skolens administration.

	Ja	Nej
1. Billeder og video af dig		
Må skolen offentliggøre billeder og videoer af dig?	○	○

Offentliggørelsen kan være på skolens hjemmeside, på skolens profil på sociale medier (Facebook, Instagram, YouTube mv.), i nyhedsbreve, i trykte publikationer, i den årlige elevbog, mv.

BEMÆRK: vi gør os altid umage med kun at offentliggøre billeder og videoer, der er lødige og ikke-krænkende.

Læs mindre (fold ned) ↑

Følgende oplysninger om dig behandles, hvis du siger ja: - Almindelige personoplysninger, jf. databeskyttelsesforordningen art. 4, stk. 1 Formålet med den påtænkte behandling: - Dine skolekammerater kan let finde dig i elevbogen. - Offentliggørelse af foto- og videomateriale på hjemmesiden, på skolens profil på sociale medier samt i trykte publikationer og i nyhedsbreve har til formål at illustrere hverdagen, arrangementer, traditioner, fester, fællesskabet og livet på skolen. Konsekvens hvis du svarer "nej": - Dit foto bliver ikke vist i elevbogen - Du vil ikke være i fokus på fotos eller videoer, der offentliggøres. Bemærk, at du skal selv samarbejde om at undgå at blive fotograferet/filmet af skolens medarbejdere, dvs. undgå at stille dig i "skudlinjen", når der fotografere/filmes. Konsekvens hvis du senere ændrer et "ja" til et "nej": - Skolen vil fremover ikke bringe dit foto i elevbogen - Skolen ophører med at bruge foto- og videomateriale, hvor du er i fokus. Skolen vil samtidig slette foto- og videomateriale af dig i det omfang, det er teknisk muligt.

30. Studierejser – sådan behandler vi personoplysninger (TAP og rejselærer)

Elever u/18 år

Når man som rejseansvarlig lærer planlægger en studierejse til udlandet med elever under 18 år, skal man i god tid inden afrejsen kontakte det pågældende lands ambassade/konsulat i Danmark for at afklare, om der er krav om

skriftligt forældresamtykke og evt. yderligere dokumentation for at tillade mindreårige elevers ind- og udrejse af det pågældende land.

Da det er det enkelte land, der selv fastlægger og evt. justerer kravene til ind- og udrejse, findes der igen liste over hvilke lande, det handler om, eller hvilke konkrete krav der stilles. P.t. ved vi positivt, at Irland og USA stiller samtykke- og dokumentationskrav.

Kontakten til ambassaden for det pågældende land er derfor væsentlig. Kontaktoplysninger til udenlandske ambassader i Danmark findes her.

Ifølge Udenrigsministeriet er de oplysninger, der *kan* blive krævet for mindreårige elevers ind- og udrejse fx:

- En samlet liste over alle rejsende
- Et skriftligt samtykke fra forældrene (én eller evt. begge) til mindreårige elevers ind- og udrejse til landet
- Der kan være krav om, at samtykkeblanketten suppleres af oplysninger om
    - Barnets navn, fødselsdato, pasnummer, rejseformål
    - Kopi af barnets fødselsattest med navne på de samtykkende forældre
    - De samtykkende forældres navne, fødselsdato, pasnummer (inkl. navn, fødselsdato og underskrift) samt kontaktoplysninger (telefonnummer og e-mailadresse)
    - Evt. dokumentation for eneforældremyndighed
- Der kan være krav om, at dokumenterne oversættes til det pågældende lands hovedsprog og evt. underskrives for en notar (i Byretten), evt. efterfølgende legaliseres af Udenrigsministeriet og/eller evt. stemples af det pågældende lands ambassade i Danmark.

Det kan altså være en møjsommelig og tidskrævende opgave at overholde kravene.

På Roskilde Gymnasium er **den rejseansvarlige lærer** ansvarlig for, at eleverne og forældrene orienteres om de pågældende krav i god tid og senest [fx 3 måneder] før afrejsen.

Den rejseansvarlige lærer kan bistå de mindreårige elever og deres forældre med at sikre dokumentationen, herunder at dokumentationen bliver ensartet for alle de mindreårige elever.

Både op til og under hele rejsen er det dog elevens opgave selv at opbevare dokumentationen, idet skolen og den rejseansvarlige lærer ikke kan tage ansvar for at beskytte de fortrolige oplysninger om forældres pasnumre, forældremyndighed mv. under rejsen.

Medicin og allergier

Eleven medbringer selv oversigt over evt. medicin og allergier (i fysisk print) på rejsen. Hvis læreren får en kopi, er det lærerens ansvar at makulere oversigten efter hjemkomst.

Kvittering for læsning af skolens ordensregler som led i udlandsrejse

Sker i GymBetaling forud for rejsen.

Overførsel af personoplysninger visse lande uden for EU

Går studierejsen ud af EU eller EØS [17, 18] indebærer rejsen, at der sker såkaldt "overførsel af personoplysninger om rejsedeltagerne til et – i persondatabeskyttelsessammenhæng – usikkert land".

Roskilde Gymnasium tilstræber derfor at minimere de personoplysninger, der medbringes til lande uden for EU eller EØS.

Det sker i praksis ved, at personoplysninger om fx pasnummer, cpr-nummer, helbredsdiagnoser mv. kun medbringes i fysisk form, dvs. ikke digitalt. Herved kan de tages med retur til Danmark og makuleres efter brug.

Af samme årsag bør personoplysninger så vidt muligt ikke sendes via fx e-mail i usikre netværk i det pågældende land.

31. TV-overvågning – interne retningslinjer (TAP)

På Roskilde Gymnasium er der opsat tv-overvågning. Nedenfor kan du læse hvorfor. Du kan også læse hvordan vi bruger de personoplysninger, vi får via tv-optagelserne og hvad dine rettigheder er, hvis du har opholdt dig i et tv-overvåget område.

Hvilke personoplysninger registrerer vi og hvad er formålet?

Vi følger procedure for opbevaring, sletning og evt. med overvågningen er kriminalitetsbekæmpelse og –forebyggelse.

Tv-overvågningen sker hele døgnet.

Hvis du opholder dig i et område, hvor der er tv-overvågning, kan du blive filmet.

Det er tydeligt markeret med skiltning, at der foretages tv-overvågning. Skiltene er opsat i umiddelbar nærhed af de opsatte kameraer. Skiltene viser et billede af et kamera.

Optagelserne bliver gennemgået ved stikprøvekontrol eller ved konkret konstateret eller konkret mistænkt kriminalitet (fx tyveri, indbrud, hærværk eller personrettet kriminalitet) eller anden ureglementeret adfærd. Optagelserne bruges kun til ovennævnte formål. Optagelserne vil blive videregivet til politiet, hvis det skønnes relevant.

Hjemlen til at foretage tv-overvågning findes i databeskyttelsesforordningens art. 6, stk. 1, litra c og e, samt i databeskyttelseslovens § 8. Hjemlen til videregivelse til politiet findes i databeskyttelseslovens § 8, stk. 2 herunder af optagelser fra skolens tv-overvågning.

[17] Norge, Island og Liechtenstein.

[18] Følgende lande er "sikre" lande uden for EU/EØS: Andorra, Argentina, Australien (passageroplysninger som led i flyrejser), Canada, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Storbritannien, Sydkorea, Uruguay.

Tv-optagelser er personoplysninger

De personoplysninger, som om de personer, der kan ses på optagelserne. Roskilde Gymnasium skal behandle personoplysninger i overensstemmelse med **god databehandlingsskik**. Det betyder, at vi skal overholde reglerne i databeskyttelsesforordningen (GDPR) og i den danske databeskyttelseslov, når tv-optagelserne optages, opbevares, gennemses, gøres til genstand for indsigt, videregives og slettes.

Pr. 1. september 2021 skal Roskilde Gymnasiums tv-overvågningskameraer registreres i POLCAM. Det sker via Politiets hjemmeside. **Nyetablerede kameraer, som er opsat efter den 1. juli 2021, skal registreres i Politiets Kameraregister senest 14 dage efter opsætning.**

Orientering om tv-overvågning

Skolen skal på eget initiativ give **meddelelse** til de personer, om hvem oplysninger indsamles, jf. GDPR art. 13 om oplysningspligt. Roskilde Gymnasiums orientering af de forskellige persongrupper, der evt. bliver tv-overvåget, sker på følgende måde:

1) elever samt forældre, besøgende, håndværkere, eksterne rengøringsfolk og andre, der opholder sig på skolens område. Orienteringen sker via skolens **hjemmeside**.
2) skolens egne medarbejdere. Orienteringen sker via skolens **personalehåndbog** samt i særskilt **varslingsbrev** (*Bemærk*: der består en særlig pligt for arbejdsgiver til at varsle indførelse af tv-overvågning 6 uger forud for iværksættelse, jf. Cirkulære om aftale om kontrolforanstaltninger)
3) medarbejdere fra eksterne firmaer, fx **rengøringsfirmaer**, kræver særlig opmærksomhed, idet det eksterne firma skal have særskilt og udtrykkelig besked om, at leverandøren SKAL videreformidle orienteringen om tv-overvågning til de medarbejdere, som leverandøren sender ud på skolen.

De oplysninger, som skolen har givet, er:

- Den dataansvarliges eller dennes repræsentants identitet
- Formålene med og hjemlen til den behandling, hvortil oplysningerne er bestemt. Kravet indebærer, at der skal gives den registrerede person tilstrækkelig information til, at han/hun bliver klar over, hvad der er baggrunden for, at der indsamles oplysninger om ham/hende
- Oplysning om, at optagelserne vil blive videregivet til politiet ved mistanke eller viden om kriminelle aktiviteter el.lign.
- Information om, at optagelser vil blive gennemgået i form af stikprøvekontrol
- Hvor længe oplysningerne bliver opbevaret
- Hvor overvågningen foregår.

God databehandlingsskik

Datatilsynet har udtalt, at indsamling af personoplysninger via tv-overvågning, der sker med henblik på at forebygge kriminalitet, sikre tryghed og støtte politiets efterforskning er et **sagligt formål**.

Gennemsyn og lagring af billeder fra en tv-overvågning må også kun ske, når formålet er sagligt. En tilsidesættelse af dette krav om saglighed kan give den person, hvis personoplysninger derved behandles ulovligt, krav på erstatning, jf. GDPR art. 82.

Roskilde Gymnasium har besluttet, at det er skolens tekniske personale samt skolens ledelse, der har brugeradgang til at gennemse tv-overvågningen. Brugeradgangene ajourføres ifm. stillingsændringer og fratræden.

Skolen har overvejet, at tv-overvågningen er proportionel, og har det ønskede formål at forebygge kriminalitet og højne trygheden hvilket ikke kan opnås med mindre indgribende midler end tv-overvågning. Skolen vurderer, at andre mindre midler ikke er tilstrækkelige og ikke har haft den fornødne effekt.

Skolen sørger for, at overvågningen gennemføres på en sådan måde, at den virker mindst muligt integritetskrænkende for elever og medarbejdere på skolen.

Videregivelse af tv-overvågning til politiet kan ske uden samtykke fra de afbildede personer, hvis formålet er kriminalitetsopklaring.

Videregivelse kræver ikke særskilt orientering om selve videregivelsen til den afbildede person, når blot skolen har givet en generel forudgående orientering om den behandling af personoplysninger, som tv-overvågningen indebærer.

Anden videregivelse, fx til forsikringsselskab, kræver samtykke fra de afbildede personer.

Sletning af tv-optagelser

For tv-overvågning gælder der en udtrykkelig sletteregel på 30 dage. På Roskilde Gymnasium slettes tv-optagelserne løbende efter 30 dage og sker derfor automatisk. Sletningen omfatter også back up'en.

Kontakt til politiet ved mistanke eller viden om kriminelle forhold

Hvis det viser sig, at der er mistanke eller viden om kriminelle eller ureglementerede forhold, og optagelserne dermed indeholder oplysninger om strafbare forhold, må der alene være tale om en **kortvarig opbevaring** med henblik på politianmeldelse, og politianmeldelse skal foretages **snarest muligt**, ligesom optagelserne skal afleveres til politiet i forbindelse med anmeldelsen og slettes fra Roskilde Gymnasiums eget system umiddelbart derefter.

Skolens videregivelse af optagelserne til politiet udløser ikke krav om særskilt orientering om selve videregivelsen til den afbildede person, når blot skolen har givet en generel forudgående orientering om den behandling af personoplysninger, som tv-overvågningen indebærer, fx på hjemmesiden, jf. ovenfor [samt teksteksemplet i dette dokuments afsnit 1.]

Datasikkerhed

Det er skolens tekniske personale og ledelse, som har adgang til at se tv-overvågningen. Det er ligeledes deres ansvar at kontakte politiet i forbindelse med mistanke om kriminalitet, sørge for relevant videregivelse af tv-optagelserne (via et sikkert medium) og sørge for, at data efterfølgende bliver slettet. Skolens ledelse og tekniske personale aftaler indbyrdes, hvordan arbejdsfordelingen foregår i denne forbindelse.

Alle tv-optagelser findes i systemet Aviglion, som hostes hos Roskilde Gymnasium og leveres/supporteres af EL:CON, og som der er indgået databehandleraftale med.

Teknisk servicechef Erik Nellerup sørger for løbende opfølgning på kontrakt og databehandleraftale med EL:CON.

Kontrakt og databehandleraftale

Udover at have indgået en databehandleaftale har Roskilde Gymnasium yderligere foretaget en risikovurdering og yderligere har skolen løbende indhentet og gennemlæst en revisionserklæring, der dokumenterer, at sikkerheden hos leverandøren fortsat er i orden.

Skiltning

Når Roskilde Gymnasium foretager tv-overvågning af steder og lokaler, der er almindelig adgang til, samt af arbejdspladser, skal skolen ved skiltning eller på anden tydelig måde oplyse om overvågningen. **Skiltningen fritager ikke skolen fra oplysningspligten på hjemmesiden/i personalehåndbogen, mv.**

32. Outsourcing af it-drift til eksterne it-leverandører (databehandlere) (IT-administrator)

Roskilde Gymnasium bruger eksterne it-leverandører til at levere, drive og/eller vedligeholde it-systemer og/eller it-infrastruktur.[19]

For en oversigt over Roskilde Gymnasiums it-leverandører og deres leverance til Roskilde Gymnasium se GF's Masterark i DocuNote med typiske databehandlere og GF's gennemgang af databehandleraftaler, som skolen kan kopiere og arbejde videre med og derved gøre til sit eget.

Hvis skolen selv ønsker at forestå indgåelse af databehandleraftalerne bør Datatilsynets skabelon til databehandleraftale bruges.

De eksterne it-leverandører, som vi samarbejder med, har adgang til at se og evt. også behandle vores data i det it-system/-infrastruktur, der leveres. Dermed bliver it-leverandøren samtidig databehandler af data og personoplysninger om Roskilde Gymnasium.

Derfor skal alt samarbejde med eksterne it-leverandører af it-systemer, der skal indeholde personoplysninger, begynde med, at Roskilde Gymnasium vurderer, om den påtænkte nye it-leverandør har et niveau af it-sikkerhed og dataetik, som Roskilde Gymnasium er tryg ved.
På Roskilde Gymnasium er det datasikkerhedstovholderen, der sørger for, at der kun indgås kontrakt og opstartes[20] (og forlænges) samarbejder med eksterne it-leverandører, der vil overholde vores krav.

Dette kræver for det første at leverandøren vil indgå en skriftlig kontrakt med Roskilde Gymnasium, hvori it-leverancen er beskrevet nøje ifht. funktionaliteter, services og sikkerhed.

Dernæst kræver det, at it-leverandøren vil indgå en såkaldt databehandleraftale om beskyttelse af de personoplysninger om Roskilde Gymnasiums medarbejdere og elever, som it-leverandøren får adgang til. For en oversigt over, hvad der bør fremgå af en databehandleraftale, se GF's skema til tjek af databehandleraftale.

Via Roskilde Gymnasiums deltagelse i **Gymnasiefællesskabets datasikkerhedssamarbejde** kan vi få hjælp til at få overblik over datasikkerheden i de it-systemer og it-værktøjer, vi bruger – eller overvejer at tage i brug – til administrative eller undervisningsmæssige formål. GF har risikovurderet og gennemset databehandleraftaler for en stor mængde it-leverandører og kan hjælpe med dokumentation (faktaark, udvidet risikovurdering, gennemgang af databehandleraftaler, kontraktvilkår samt efterfølgende kontrol af leverandøren).

Kontakt sker til Susanne (sab@gfadm.dk) eller Lotte (llt@gfadm.dk) i Gymnasiefællesskabet.

På Roskilde Gymnasium er det datatovholderen Torben Geilman der sørger for, at der holdes styr på, hvilke it-leverandører, vi bruger[21] – og at de overholder kravene. datatovholder] fører en elektronisk liste (evt. en

[19] Eksempler på eksterne it-leverandører er Gymnasiefællesskabet, Økonomistyrelsen for så vidt angår bl.a. SLS og Navision, samt leverandørerne af Lectio, Gyldendal, Gymnasiejob, Reindex biblioteksystem, leverandøren af netforbindelse, back up, mv.

[21] Fx via åbning af adgang i UNI-login. Når skolen overlader behandling af sine medarbejdere og elevers personoplysninger til en databehandler via UNI-login, skal der samtidig som krævet standard indgås en databehandleraftale. Via de forskellige

"positivliste") over it-systemer og it-værktøjer, der har gennemgået risikovurdering, og som kan bruges på Roskilde Gymnasium.

I de tilfælde, hvor der benyttes eksterne konsulenter, som på mere enkeltstående basis får adgang til Roskilde Gymnasiums data og personoplysninger, indgås der er en fortrolighedsaftale.

Bemærk, at vores administrative it-fællesskab [Gymnasiefællesskabet eller andet it-fællesskab] årligt leverer en såkaldt ISAE 3402 type 2-erklæring om sikkerheden i de it-leverancer, som fællesskabet leverer til os.[22]

Tilsvarende skal leverandører af studieadministrative it-systemer (Lectio og Ludus) hvert andet år afgive en anmærkningsfri systemrevisionserklæring (ISAE 3402) samt (fra primo 2021) tillige en erklæring om leverandørens overholdelse af kravene i databehandleraftalen (ISAE 3000), som betingelse for, at Roskilde Gymnasium kan anvende systemet.[23] Erklæringen kan findes på Oversigt over studieadministrative it-systemer omfattet af systemrevisionserklæring uden forbehold - Styrelsen for It og Læring (stil.dk)

For de statslige systemer Navision Stat, IndFak og Statens Lønsystem SLS, som Økonomistyrelsen stiller til rådighed for Roskilde Gymnasium, skal Roskilde Gymnasium til brug for revisionen indhente ledelseserklæringer fra styrelsen om styrelsens udviklings-, drifts- og vedligeholdelsesydelser vedrørende systemerne. Ledelseserklæringerne sendes elektronisk til Roskilde Gymnasium af Økonomistyrelsen.[24]

Roskilde Gymnasiums revisor har pligt til at påse, at de nævnte revisionserklæringer er indhentet af Roskilde Gymnasium, og at Roskilde Gymnasium har forholdt sig til indholdet i erklæringerne.[25]

På Roskilde Gymnasium er det datasikkerhedstovholderens opgave, at:

- Føre listen over Roskilde Gymnasiums it-systemer og it-infrastruktur, der leveres, drives eller vedligeholdes af en ekstern leverandør/it-fællesskab/databehandler/konsulent. GF's oversigtsark (link på forrige side) kan benyttes
- Arkivere kontrakten og databehandleraftalen (eller fortrolighedsaftalen) med leverandøren i [DocuNote]
- Indhente, gennemgå og følge op på de revisionserklæringer, som it-leverandøren ifølge kontrakten skal afgive til Roskilde Gymnasium
- Følge op på, at den eksterne it-leverandør (og konsulenter) sletter Roskilde Gymnasiums forældede personoplysninger.

Medarbejderens opgaver kan med fordel fremgå af et årshjul.

---

datapakker i UNI-logins administrationsmodul vælger Roskilde Gymnasium, hvilke personoplysninger it-leverandøren må få om elever og medarbejdere til brug for brugeroprettelse. Bemærk, at vi kun åbner for den "lille pakke", idet de større pakker indeholder CPR-nummer og idet det har formodningen mod sig, at CPR-nummer er nødvendigt for databehandleren.

[22] IT-fællesskabernes pligt til at levere erklæringen følger af bilag 1 i bekendtgørelse nr. 2110 af 24/11/2021 om revision og tilskudskontrol m.m. ved institutioner for erhvervsrettet uddannelse, almengymnasiale uddannelser og almen voksenuddannelse m.v. Erklæringen skal foreligge senest den 15. januar og skal dække det forudgående kalenderår.

[23] Jf. § 6, stk. 1, i bekendtgørelse om krav til studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, gymnasiale uddannelser m.fl.

[24] Moderniseringsstyrelsens pligt til at levere erklæringen følger af bilag 1 i BEK nr. 2110 af 24/11/2021 om revision og tilskudskontrol m.m. ved institutioner for erhvervsrettet uddannelse, almengymnasiale uddannelser og almen voksenuddannelse m.v. Erklæringen skal foreligge senest den 15. januar og skal dække det forudgående kalenderår.

[25] Jf. bilag 1, afsnit 2.6 i bilag 1 i BEK nr. 2110 af 24/11/2021 om revision og tilskudskontrol m.m. ved institutioner for erhvervsrettet uddannelse, almengymnasiale uddannelser og almen voksenuddannelse m.v.

Ang. de fællesstatslige systemer (SLS, HRløn, HR-databasen, GymBetaling, Navision Stat, IndFak samt HR-databasen, GymBetaling og DocuNote) sørger GF's datasikkerhedssamarbejde for at gennemgå og følge op på datasikkerheden. Dokumentationen for dette findes på GF's Intra her.

33. Roskilde Gymnasiums netværk og brugen heraf (IT-administrator)

Skolens net er opdelt i et administrativt netværk og et undervisningsnetværk, som er fysisk adskilte på hver sin server. Det er ikke muligt at tilgå et af disse netværk, uden at man er oprettet som individuel bruger på netværket.

Der findes ikke brugerkonti, der giver adgang til begge netværk via samme login. Visse medarbejdere på Roskilde Gymnasium har brugeradgang til begge netværk: Gymnasievejledere, læsevejledere, SJ, LP, SØ, KAS, bibliotekspersonalet, servicechef og pedeller, kontorpersonale, it-medarbejderen og ledelsen.

Brugeradgange og rettigheder administreres og vedligeholdes af IT-medarbejderen som kontaktes ved ønske om ændringer i adgange og rettigheder.

Når man som medarbejder får tildelt en brugeradgang (eller nulstillet sit password, fordi man har glemt det), er der tale om et standardpassword, som man straks skal ændre til et unikt, personligt password.

Der er etableret trådløst netværk på skolens geografiske område. Herfra kan der kun opnås adgang til undervisningsnetværket.

Skolens netværk består af en række drev og it-systemer, hvor det er forskelligt hvilke drev, den enkelte medarbejder har adgang til:

- På undervisningsnetværket har Roskilde Gymnasiums undervisere adgang til H-drevet som ligger på GU-FS121 og indeholder de enkelte lærernes personlige undervisningsmateriale. Dette er et personligt drev og der tages backup af det hver nat. M-drevet ligger på GU-FS121 og er beregnet til deling af lærernes faggruppe undervisningsmateriale. Dette er et fælles drev som der bliver taget backup af hver nat. N-drevet ligger på GU-FS121 og er beregnet til forskellige fagprogrammer. Dette er et fælles drev som der bliver taget backup af hver nat. P-drevet ligger på GU-FS121 og bliver brugt til materialedeling for lærerne for de enkelte klasser. T-drevet ligger på GU-FS121 og bliver brugt til generel vidensdeling for lektorerne. Dette er et fælles drev som der bliver taget backup af hver nat. V-drevet ligger på RG-Video der ligger forskellige videoer til brug i undervisningen. Dette er et fælles drev. På administrativt netværk har medarbejderne adgang til følgende netværks drev. N-drevet ligger på GA-FS121 er et fælles drev hvor bl.a. Ledelses mappen ligger og hvor kun dem der er en del af ledelsen, har adgang til. Der bliver taget backup hver nat. P-drevet som ligger på GA-FS121 og indeholder de enkelte medarbejders personlige filer. Der tages backup af det hver nat.

Roskilde Gymnasium bruger nedenstående it-systemer til følsomme og/eller fortrolige oplysninger, (jf. instruks om opbevaring af personoplysninger oven for i kapitel 3):

- Roskilde Gymnasium bruger Docunote som ESDH-system til at håndtere følsomme og fortrolige oplysninger.

Alle elever har tilsvarende adgang til at gemme på følgende af skolens drev/systemer:

- På undervisningsnetværket har Roskilde Gymnasiums elever adgang til H-drevet, som ligger på GU-FS121 og indeholder de enkelte elevers personlige opgaver og filer. Dette er et personligt drev, og der tages backup

af det hver nat. N-drevet ligger på GU-FS121 og er beregnet til forskellige fagprogrammer. Dette er et fællesdrev som der bliver taget backup af hver nat. P-drevet ligger på GU-FS121 og bliver brugt til materialedeling for lærerne for de enkelte klasser.

34. IT-systemer og it-services som Roskilde Gymnasium selv ejer, hoster og/eller vedligeholder

Roskilde Gymnasium driver ikke egne it-systemer, som indeholder personoplysninger.

35. Ansvar og plan for implementering og ajourføring af databeskyttelse (Ledelse)

Det er den øverste ledelse (bestyrelsen), der har det endelige ansvar for, at Roskilde Gymnasium behandler personoplysninger i overensstemmelse med gældende lovgivning.

Rektor er ansvarlig for, at formålene med behandling af personoplysninger er i overensstemmelse med gældende lovgivning, samt at retningslinjerne til understøttelse af politikken er kommunikeret klart og tydeligt til medarbejderne, jf. ovenstående afsnit til alle medarbejdere og specifikke medarbejder-grupper.[26]

Ledelsen rådfører sig med skolens databeskyttelsesrådgiver (DPO) vedrørende forståelse og praktisering af gældende regler for beskyttelse af personoplysninger.

Ledelsen beslutter og udruller retningslinjer og tjeklister til medarbejderne med henblik på at gøre dem bekendt med formålene med behandlingen og de retningslinjer, der er relevante for udførelsen af deres arbejde.

Ledelsen sørger endvidere for følgende, at:

- skolen har skriftlige, elektroniske **fortegnelser** over sine behandlingsaktiviteter (formelt krav i databeskyttelsesforordningen).[27] Se beskrivelse af indholdskravet til fortegnelser i FAQ'ens afsnit
- der samarbejdes aktivt med skolens **DPO**[28]
- skolen via medarbejderopmærksomhed og samarbejde med DPO'en har et beredskab til håndtering af **brud på datasikkerheden** (fx læk) og evt. rapportering om sådanne brud til Datatilsynet samt evt. også de registrerede personer inden for 3 døgn, fra bruddet er opdaget
- der foretages en **risikovurdering** i forbindelse med behandling af personoplysninger.
    - Risikovurderingen tager udgangspunkt i behandlingens karakter, omfang, sammenhæng og formål samt de anvendte systemer
    - Formålet er at sikre, at skolens behandling af personoplysninger yder tilstrækkelig sikkerhed
- de fastlagte sikkerhedsforanstaltninger revurderes løbende

35.1 Forretningsgang for håndtering af datalæk

Skolens forretningsgang for håndtering af datalæk er beskrevet i skabelon G10.

- der foreligger skriftlige **databehandleraftaler** med it-leverandører

[26] Ledelsen kan støtte sig til GF's "Ledelses Top 8" som tjekliste
[27] GF's skabeloner findes her
[28] GF's ydelseskatalog for DPO-funktionen findes her

- organisationen er orienteret om **retningslinjer for databeskyttelse**, herunder om hvilke it-systemer og værktøjer der må bruges
- der sker **orientering af de registrerede** om deres rettigheder.

36. Risikovurdering (Ledelse)

Skolens datasikkerhedstovholder har ansvaret for, at Roskilde Gymnasium foretager løbende en overordnet vurdering af databeskyttelsen og it-sikkerheden i følgende systemer:

1) De it-systemer, som er væsentlige for skolens administrative drift og gennemførelse af undervisningen, og som skolen har licens til
2) De mindre it-værktøjer, digitale læremidler, gratis apps, der på ad hoc-basis bruges i undervisningen, og som rummer behandling af personoplysninger.

Det er målet, at sikkerheden har et niveau, der beskytter dataenes (herunder personoplysningers) fortrolighed og ægthed samt sikrer dataenes tilgængelighed for de autoriserede brugere og skolens kontrol over egne data.

For de i punkt 2) nævnte systemer er målet især dataminimering.

Vurderingen tager udgangspunkt i:

- De mest almindelige og kendte sårbarheder og trusler, herunder det generelle trusselsbillede, som det beskrives af sikkerhedseksperter i fx medier og fagblade
- Lovgivning, der medfører krav om sikkerhedsforanstaltninger
- Skolens særlige karakter som arbejdsgiver og uddannelsesinstitution samt det styrkeforhold, der ligger heri
- Eventuelle tidligere sikkerhedsmæssige hændelser
- Risikoen for destruktion af data og faciliteter
- Forvanskning eller ændring af data
- Tyveri eller tab af data
- Uautoriseret offentliggørelse
- Afbrydelse af driftsafvikling, netværk og kommunikation
- Skolens adgang til at redigere i, berigtige, udtrække og slette data systematisk og kontrolleret
- STIL's tjekliste vedr. anvendelse af gratis applikationer anvendt i undervisningssektoren.

Roskilde Gymnasium ønsker ikke at sikre sig for enhver pris, men ønsker at være bevidst om enhver risiko, og forholde sig tilfredsstillende hertil, iværksætte de nødvendige foranstaltninger til minimering af risici og derigennem søge at opnå et tilstrækkeligt sikkerhedsniveau.
De nødvendige foranstaltninger fastlægges ud fra en afvejning af, hvilke og hvor mange personoplysninger der er tale om, ressourceforbruget med etableringen af foranstaltningerne samt konsekvenserne af uønskede hændelser, herunder risikoen for de registrerede personer ved et læk.

De nødvendige foranstaltninger, der er fastlagt på baggrund af risikovurderingerne, kommunikeres til skolens medarbejdere i form af instrukser til administrative medarbejderes om brugen af de administrative systemer og mere overordnede "færdselsregler" til lærerne for så vidt angår brugen af digitale læremidler.

Eleverne orienteres endvidere i en for digital undervisning[29] om skolens arbejde med risikonedbringende foranstaltninger, samt hvad eleverne selv skal være opmærksomme på, når de bruger digitale læremidler. Endelig

[29] GF har skabeloner, der findes på hjemmesiden under "Datasikkerhed".

oplyses eleverne om, hvor de kan henvende sig [til fx en it-vejleder], hvis de støder på konkrete problemer med fx apps, der beder om persondata fra elevens it-udstyr (fx adgang til kontakter, fotos, mv.).

Kapitel 3 – FAQ

Dette er et opslagsværk over grundlæggende regler og begreber om behandling af personoplysninger, og hvad de betyder i skolesammenhæng.

37. Hvilke personoplysninger kommer en skole i kontakt med

PERSONOPLYSNINGER, SOM SKOLER TYPISK KOMMER I KONTAKT MED

Stigende grad af følsomhed og strengere betingelser for behandling

Kategori	Elev	Forældre	Medarbejdere
Følsomme personoplysninger (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, foreningsmæssig tilknytning, politisk, religigøs eller filosofisk overbevisning, oplysninger om race, etnicitet, oplysninger om seksuel orientering	do	do
Semifølsomme personoplysninger	Straffedomme og lovovertrædelser	do	do
Fortrolige oplysninger *(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, portrætbillede (offentliggørelse på internet kræver samtykke), karakterer, studievejledning, oplysninger om væsentlige sociale problemer, sanktioner, eksamensbeviser, karakterer, 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,
Almindelige personoplysninger	Ansøgning, stamdata/kontaktdata, optagelse, indskrivning, udlån af bøger/Ipad, valg af studieretning, hold/fag, skema, lektiegivning, situationsbilleder fra skolens hverdag, logning af internettrafik/korrespondance på Lectio, deltagelse i arrangementer, rejser, fremmøde/fravær, udskrivning, jubilæer,	Stamdata/kontaktdata, civilstand, forældremyndighed	Stamdata/kontaktdata, rekruttering, cv, ansættelse, løn, kontooplysninger, beskatning, fri telefon og pc, hjemmeopkobling, arbejdsopgaver, kurser, meritter, fremmøde og fravær, referat af MUS-samtaler, sletning af oplysninger,

38. Hvad er "personoplysninger?"

Personoplysninger er enhver form for information om en fysisk person (fx ansatte, elever, forældre og fysiske samarbejdspartnere). Selve personoplysningerne kan være navn, adresse, fremmøde, meritter, karakterer, løn, foto, sanktionssager eller online-identifikationer såsom IP-adresser. Personoplysningerne kategoriseres i forskellige

grader af fortrolighed og følsomhed, jf. figuren ovenfor. Jo mere fortrolig eller følsom en personoplysning er, jo bedre skal skolen passe på den.

39. Hvad vil det sige, at "behandle" personoplysninger?

Begrebet "behandling af personoplysninger" dækker efter databeskyttelsesforordningen over alt, hvad man kan udsætte en personoplysning for (med digitale redskaber), herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

40. Hvad er "almindelige personoplysninger", og hvornår må en skole behandle dem?

Almindelige personoplysninger er de personoplysninger, der fremgår nederst i tabellen ovenfor.

De "almindelige personoplysninger" må behandles af skolen, hvis mindst en af følgende betingelser er opfyldt[30]:

a) Den registrerede elev eller medarbejder har givet sit *samtykke* til det
b) Behandling er *nødvendig* for indgåelse eller opfyldelse af en **ansættelseskontrakt**
c) Behandling er *nødvendig* for overholdelse af en retlig forpligtelse, som påhviler skolen, fx indgåelse af en **kontrakt**
d) Behandling er *nødvendig* for beskyttelse af vitale interesser (i en situation, hvor den pågældende person selv er ude af stand til dette)
e) 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 altovervejende hovedregel kan de almindelige personoplysninger om medarbejdere, jobansøgere, elever og forældre behandles med hjemmel i punkt b) og e) ovenfor. Det vil sige, at behandlingen kan ske uden den registrerede persons udtrykkelige samtykke.

Et eksempel på behandling af en personoplysning, der er nødvendig for skolens varetagelse af sin kerneopgave, er § 9 i bekendtgørelsen om studie- og ordensregler: *"§ 9. Institutionen registrerer digitalt og i overensstemmelse med persondatalovgivningen elevens deltagelse i undervisningen, herunder aflevering af skriftlige opgaver*".

Heri ligger hjemlen til en digital registrering af det daglige fremmøde. At formuleringen nævner, at registreringen skal ske "*i overensstemmelse med persondatalovgivningen*" indebærer, at eleven skal orienteres om behandlingen, og at oplysningerne skal opbevares i et it-system med mulighed for brugerstyring, adgangskontrol og sletning.

I et ansættelsesforhold har arbejdsgiveren ifølge skattelovgivningen indberetningspligt til SKAT om lønoplysninger. Dermed er det nødvendigt at videregive oplysninger til SKAT om medarbejderens identitet (herunder CPR-nr.), bopælskommunen og lønnens sammensætning og størrelse. Dette kan dermed ske uden samtykke.

41. Er nogen typer af data i relation til medarbejderne, som arbejdsgiveren ikke må gemme?

Arbejdsgiver må kun opbevare de personoplysninger, der er "nødvendige" for at foretage løn- og personaleadministration.

Fx må arbejdsgiver ikke opbevare oplysninger om X medarbejders hustrus gigtdiagnose for at kunne spørge interesseret ind til "hvordan det går?" – medmindre der er givet samtykke (fra hustruen vel at mærke). Ligeledes må

[30] Jf. Forordningens art. 6 og databeskyttelseslovens § 6.

der ikke opbevares personoplysninger om fx en medarbejders religiøse tilhørsforhold for fx at kunne ønske "glædelig højtid". Hvis medarbejderen har samtykket til det, er det i orden.

42. Hvilke behandlinger af almindelige personoplysninger kræver samtykke?

Følgende behandlinger af almindelige personoplysninger kræver det ovennævnte 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 og "Blå Bog")
- Registrering og opbevaring af visse helbredsdiagnoser om medarbejdere og elever
- Videregivelse af oplysninger om elev til modtager-gymnasium, hvis eleven forlader skolen
- Videregivelse af oplysninger om medarbejdere og elever til ekstern part til fx markedsføring
- Opbevaring af jobansøgeres 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.

43. Hvad er " følsomme personoplysninger", og hvornår må en skole behandle dem?

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 én 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 et retskrav kan fastlægges, gøres gældende eller forsvares
f. Behandlingen har udtrykkelig hjemmel i *speciallovgivning*, fx SU-bekendtgørelsen.

Hvad der er "nødvendigt", jf. litra b, c og f, skal fremgå udtrykkeligt af stx-lovgivningen. Fx fremgår det af optagelsesbekendtgørelsens § 28, stk. 4, at der skal tages hensyn til "*foreliggende oplysninger om en ansøgers **handicap** og i den forbindelse give ansøgerens optagelse på en institution, der er hensigtsmæssig i forhold til det pågældende handicap*." I denne situation er det nødvendigt for at fastslå ansøgernes retskrav på optagelse, at skolen modtager og behandler den følsomme personoplysning om ansøgernes handicap. I den situation skal der således ikke indhentes et samtykke til behandlingen.

44. Hvor i STX-lovgivningen er der hjemmel til behandling af følsomme personoplysninger uden samtykke?

For en oversigt over, hvor i stx-lovgivningen der findes hjemmel til behandling af følsomme personoplysninger som led i elevadministration, se Bilag 1.

45. Hvilke følsomme medarbejderoplysninger må behandles uden samtykke?

I ansættelsesforhold kan der uden samtykke behandles følsomme personoplysninger om overenskomstmæssige (fagforeningsmæssige) tilhørsforhold, hvis overenskomsten pålægger arbejdsgiveren en pligt til behandlingen. Dette er fx 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 fagretlig konfliktløsning mv.[31] 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 uden samtykke også behandles følsomme personoplysninger om helbredsdiagnoser, hvor det er nødvendigt for at administrere en § 56-ordning eller et flexjob, jf. litra b ovenfor.

46. Hvilke særlige it-sikkerhedskrav er der ved behandling af følsomme personoplysninger?

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

Hvis følsomme personoplysninger opbevares i mere end 1 måned efter en sags afslutning, skal oplysningen slettes fra fx mailsystemer og overføres til et it-system (DocuNote), der, i modsætning til mailsystemet, er egnet til at samle oplysninger samt bevare fortroligheden omkring dem, herunder via adgangs- og brugerstyring, systemlogningsfunktion og slettefunktion.

47. Hvilke personoplysninger er "fortrolige"?

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 videooptagelser af medarbejderes og elevers trafik ind- og ud af skolens bygninger i situationer, hvor der fx har været tyveri fra skolen.

Oplysninger om løn-, arbejds-, uddannelses- og ansættelsesmæssige forhold *kan* også være fortrolige, men eftersom disse oplysninger normalt kan kræves udleveret som led i aktindsigt, jf. offentlighedslovens § 21, er det udgangspunktet, at oplysningerne ikke er af fortrolig karakter.

48. Hvilke særlige it-sikkerhedskrav er der ved behandling af fortrolige personoplysninger?

Hvis fortrolige personoplysninger skal sendes via e-mail, skal det ske via en krypteret mailforbindelse, fx Sikker Mail eller Digital Post.

Hvis fortrolige oplysninger (undtagen CPR-numre) opbevares i mere end 1 måned efter en sags afslutning, skal oplysningen slettes fra fx mailsystemer og overføres til et it-system (ESDH), der er egnet til at bevare fortroligheden omkring oplysningen, herunder via adgangs- og brugerstyring, systemlogningsfunktion og slettefunktion.

[31] Jf. Forslag til databeskyttelseslov § 12 og forarbejdernes side 138 (L 68 2017-2018).

49. Må skolen offentliggøre fotos af elever på sin hjemmeside, på sociale medier, i en årbog m.m.?

Den tidligere sondring mellem "portrætfotos og situationsbilleder" er ophævet i 2019.

Situationen er derfor nu den, at skolen som dataansvarlig for behandlingen af billeder/fotos (som er personoplysninger) konkret skal vurdere, om behandlingen af hvert enkelt billede (fx offentliggørelse heraf) falder ind under hjemlen i art 6, litra e, om "nødvendig som led i udførelse af opgaver, som skolen er pålagt eller som led i skolens myndighedsudøvelse".

Hvis svaret er ja, kan billedet fx vises på hjemmesiden.

Hvis svaret hertil er nej, skal der indhentes samtykke.

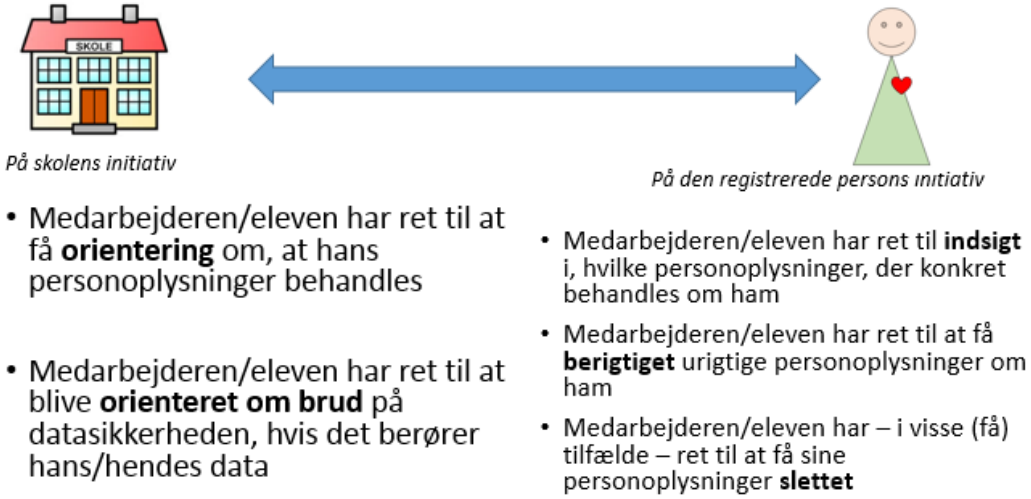
"Panoramaagtige" billeder fra fx dimission, gallafest, idrætsdag, mv., dvs. et billede fra en situation, hvor man som elev/medarbejder/gæst må kunne forudse og forvente, at der fotograferes og formidles billeder fra via forskellige medier, kan formentlig konkret behandles (vises/offentliggøres) uden de enkelte personers samtykke.

Bemærk, at en afbildet persons indsigelse mod et offentliggjort billede vil medføre, at billedet skal fjernes igen fra fx hjemmesiden. Dette uanset om der tidligere er givet samtykke eller ej. Personen har altså ret til at fortryde.

Bemærk også, at der skal ske orientering af den afbildede person om behandlingen af dennes personoplysninger, fx ved offentliggørelse på hjemmesiden. Skolen kan gennemføre denne orientering på sin hjemmeside under punktet "Sådan behandler vi personoplysninger om …".

50. Hvad er "den registreredes rettigheder"?

Den registreredes rettigheder kan illustreres på følgende måde:



Den dataansvarlige skole skal tilrettelægge sin administration på en måde, så det er *enkelt, gennemsigtigt, letforståeligt og lettilgængeligt* 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.

50.1 Hvad betyder det at "orientere om, at personoplysninger behandles"?

Den dataansvarlige skole/arbejdsgiver skal på eget initiativ orientere den registrerede person (som kan være en jobansøger, medarbejder, brobygningselev, ansøger om optagelse på gymnasiet, elev eller værge) om følgende[32]:

- At Roskilde Gymnasium er dataansvarlig
- Kontaktoplysninger på databeskyttelsesrådgiveren
- Formålet med behandlingen af den personoplysningerne og det retlige grundlag for behandlingen (lovhenvisning eller samtykke)
- Eventuelle modtagere af personoplysningerne (ikke databehandlere – kun nye dataansvarlige)
- Om personoplysningerne overføres til et tredjeland
- Tidsrummet (eller kriterierne for fastlæggelse af tidsrummet) for opbevaringen
- Den registrerede 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 ifølge en kontrakt, indgået mellem dataansvarlige og registrerede. Yderligere skal 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 kan fx gives i ansættelsesbrevet, på hjemmesiden eller i personalehåndbogen.

50.2 Hvornår skal orienteringen gives?

Orienteringen gives, senest 10 dage efter 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 det oplysningerne oprindeligt var indsamlet til, skal den registrerede person orienteres herom forud for viderebehandlingen-[33]

51. Hvad betyder det, at den registrerede person har "indsigtsret"?

Ved indsigtsret opnår den registrerede person (som kan være en jobansøger, medarbejder, brobygningselev, ansøger om optagelse på gymnasiet, elev samt værge) indsigt i behandlingen af dennes personoplysninger gennem en forespørgsel til skolen. [34]

[32] GF-skabelon M1, M1a (Ansættelsesbrev – bud på formuleringer) og M2 (Personalehåndbog – bud på formuleringer) samt E1a (Velkomstbrev elev – bud på formuleringer) kan bruges som led i den standardmæssige orientering om behandling af personoplysninger.

[33] Art. 13, stk. 3.

[34] GF's skabelon M6 (indsigt i egne oplysninger – medarbejder) og E2 (besvarelse af anmodning om indsigt – elev) kan bruges.

Den registrerede person har ret til at få skolens bekræftelse på, om personoplysninger om ham/hende behandles, få kopi af eller adgang til oplysningerne og få 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 den registrerede person selv.

Bemærk, at skolens efterlevelse af en anmodning om indsigt helt grundlæggende forudsætter, at man som skole kan finde oplysningerne frem. Dette lægger op til, at skolen over for sine medarbejdere kommunikerer klart om, i hvilke systemer og på hvilke medier personoplysninger må/skal gemmes.[35]
Inden der udleveres oplysninger til den elev eller medarbejder, der har bedt om indsigt i egne oplysninger, skal skolen sikre sig den pågældendes identitet. Hvis anmodningen fx sendes fra en mailadresse, som tilhører den pågældende elev eller medarbejder, må dette være tilstrækkelig sikkerhed.

51.1 Hvem kan bede om indsigt?
Det kan for det første den person, som oplysningerne angår.

Derudover kan den forælder, der har forældremyndighed, bede om indsigt i sit barns oplysninger samt sine egne oplysninger. Der kan ikke bedes om indsigt i den anden forælders oplysninger uden samtykke fra den pågældende. Bonusforældre, 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.

51.2 Hvordan gives indsigten rent praktisk?
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 Digital Post.

51.3 Hvor finder man de oplysninger, der skal indsigt i?
De oplysninger, der skal gives indsigt i, befinder sig fx følgende steder:

Medarbejderoplysninger:

- Personalesagen i ESDH (udleveres som kopi af dokumenter eller skærmprint)
- HR-databasen: medarbejderen logger sig selv ind, hvorefter medarbejderen selv kan se alt om sig selv (undtagen "Ledelsesnote", der har intern karakter)
- GymBetaling: her ligger der ingen medarbejderoplysninger
- Løndata: alt fremgå af lønsedler, dvs. at der ikke er nogen saglig grund til at give yderligere indsigt
- Lectio: udskrift af personoplysninger, som medarbejderen evt. ikke selv kan se

[35] Se hertil afsnittet i kapitel 7 om "Godkendte it-systemer til personoplysninger på Roskilde Gymnasium.

- Tidsregistrering: medarbejderne kan selv se denne i Excel
- Trafik ind og ud af bygningen: print af loggen fås hos pedellerne
- Brugeradgange: print af liste, som ligger hos IT-administratoren
- Loggen i ESDH, HR-databasen og GymBetaling: indsigt gives via udskrift af den konkrete medarbejders trafik i systemerne
- Log af netværkstrafik: der gives udskrift heraf, hvis en sådan log føres
- TV-overvågning: der gives adgang til se overvågningsbilleder.
- Mailkorrespondance med skolen, hvori medarbejderens oplysninger indgår: der gives print heraf
- Diverse interne kommunikationssystemer, hvori skolens lærere kommunikerer om elevers trivsel og resultater: print gives eller personens egen adgang anvendes (hvis der er 100 % indsigt i egne oplysninger i systemet for brugeren)
- Diverse læringsplatforme (for så vidt angår oplysninger om brugertrafik og indhold): print gives eller personens egen adgang anvendes (hvis der er 100 % indsigt i egne oplysninger i systemet for brugeren).

Elevoplysninger:

- Elevsagen i ESDH (udleveres som kopi af dokumenter eller skærmprint. Der gives indsigt i referater, breve, lægelige oplysninger, karakterblade, udtalelser fra sociale myndigheder til fx SPS eller SU-dispensationer, tests fx for ordblindhed, mv.)
- GymBetaling: eleven logger sig selv ind, hvorefter eleven selv kan se alt om sig selv. Dog kan eleven ikke selv se loggen over sin egen trafik i GymBetaling, hvilket administrator derfor skal hjælpe med
- Lectio: udskrift af personoplysninger, som eleven evt. ikke selv kan se
- US2000: hvis eleven har anmodet om dispensation til udeboende SU eller SPS-midler gives der print af elevens oplysninger i systemet
- Bogdepot og biblioteksystem: udskrift af oversigt over udlånt materiale
- Trafik ind og ud af bygningen, hvis elever har adgangschip: print af loggen fås hos pedellerne
- Registrering af fremmøde, jf. § 9 i studie- og ordensbekendtgørelsen
- Brugeradgange: print af liste, som ligger hos IT-administratoren
- Loggen i ESDH, HR-databasen og GymBetaling: indsigt gives via udskrift af den konkrete medarbejders trafik i systemerne
- Log af netværkstrafik: der gives udskrift heraf, hvis en sådan log føres
- TV-overvågning: der gives adgang til se overvågningsbilleder
- Mailkorrespondance med skolen, hvori elevens oplysninger indgår: der gives print heraf til eleven
- Diverse interne kommunikationssystemer, hvori skolens lærere kommunikerer om elevers trivsel og resultater: der gives print heraf til eleven
- Diverse læringsplatforme (for så vidt angår oplysninger om brugertrafik og indhold): print gives eller personens egen adgang anvendes (hvis der er 100 % indsigt i egne oplysninger i systemet for brugeren).

52. Hvad ligger der i, at "Retten til berigtigelse"?

Retten til berigtigelse er, at den registrerede person har ret til at få rettet oplysninger om sig selv, som 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 anmodning om berigtigelse af dennes personoplysninger som udgangspunkt er en forvaltningsafgørelse, der kræver høring, begrundelse og klagevejledning.

53. Hvad ligger der i "Retten til sletning"?

Den registrerede person har ret til at få personoplysninger om sig selv slettet af skolen, hvis oplysningerne ikke længere er nødvendige for at opfylde det formål, som oplysningerne er indsamlet til, 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 den baggrund har modtaget og administreret midler. Årsagen er, at fortsat opbevaring i den situation er nødvendig, for at skolen kan dokumentere sin lovlige administration af SPS-midlerne (forsvare et retskrav) over for tilsynsmyndigheden, jf. art. 17, stk. 3, litra e.

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" mhp. at underrette de eksterne parter, som behandler personoplysningerne (fx Google), om at slette alle link til eller kopier eller gengivelser af de pågældende personoplysninger.[36] [37]

En skematisk oversigt over slettefristerne kan findes i afsnit 61.

54. Hvad ligger der i "Retten til begrænsning af behandling"?

Retten til begrænsning er, at den registrerede person har ret til i visse tilfælde at få begrænset behandlingen af sine personoplysninger således, at oplysningerne som udgangspunkt ikke må underlægges andre behandlinger end opbevaring.

Den registrerede person kan anmode om begrænsning, hvis:

- Rigtigheden af personoplysningerne bestrides,
- Behandlingen af oplysningerne er ulovlig, og den registrerede person modsætter sig sletning af oplysningerne, men anmoder om begrænsning af anvendelsen
- Der ikke længere er brug for personoplysningerne, men de er nødvendige for, at et retskrav kan fastlægges, gøres gældende eller forsvares
- Den registrerede har gjort indsigelse mod behandlingen.

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.

[36] Når et billede slettes fra hjemmesiden, skal skolen desuden gøre et forsøg på også at få slettet Googles visning af billedet i Googles cache-resultater. Googles egen vejledning i, hvordan dette kan gøres findes her.

[37] Red Barnets vejledning til sletning af billeder fra diverse sociale medier findes her

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

55. Hvad ligger der i "Retten til dataportabilitet"?

Retten til dataportabilitet indebærer, at den registrerede person som udgangspunkt har ret til at modtage personoplysninger om sig selv, som den registrerede har givet, i et struktureret, almindeligt anvendt og maskinlæsbart format.

Desuden indebærer dataportabilitet en ret for den registrerede til at få overført disse personoplysninger fra én dataansvarlig til en anden. Personoplysningerne skal kunne flyttes, kopieres og overføres fra ét IT-miljø til et andet uden hindring, hvis det er teknisk muligt.

Bemærk at retten til dataportabilitet finder ikke anvendelse, når behandlingen er nødvendig for udførelse af en opgave i samfundets interesse eller henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Derfor er anvendelsesområdet for dataportabilitet meget begrænset på vores område.

56. Hvad ligger der i "Retten til indsigelse"?

Retten til indsigelse er, at den registrerede person har ret til at gøre indsigelse mod behandling af sine personoplysninger til det, der kaldes "faktisk forvaltningsvirksomhed". I skolesammenhæng er faktisk forvaltningsvirksomhed fx holdsætning, undervisning, prøvetilrettelæggelse, karaktergivning, studievejledning.

Hvis eleven eller medarbejderen gør brug af sin indsigelsesret, må skolen ikke længere behandle de oplysninger, som indsigelsen retter sig imod, medmindre den dataansvarlige kan fremføre legitime grunde til behandlingen.

57. Hvad er betingelserne for et gyldigt samtykke (til fx behandling af følsomme personoplysninger)?

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 (u: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 kan indhentes via det medium, som skolen vælger. Det kan være på en fysisk blanket eller via GymBetaling (elever og forældre) eller HR-databasen (medarbejdere).

Hvis samtykket tilbagekaldes, skal de personoplysninger, hvis behandling samtykket gav hjemmel til, slettes, medmindre der foreligger et andet behandlingsgrundlag.

58. Hvornår er man "dataansvarlig", og hvad ligger der i ansvaret?

Når en skole behandler oplysninger om sine elever og medarbejdere til undervisnings- eller HR-formål, er det normalt skolen, der er dataansvarlig. Se evt. GF's oversigtsark for info om, hvornår skolen er dataansvarlig, og hvornår fx UVM er det.

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

59. Hvad er en "databehandler", og hvad betyder det for dataansvaret at bruge en databehandler?

Roskilde Gymnasium 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 tage i brug.

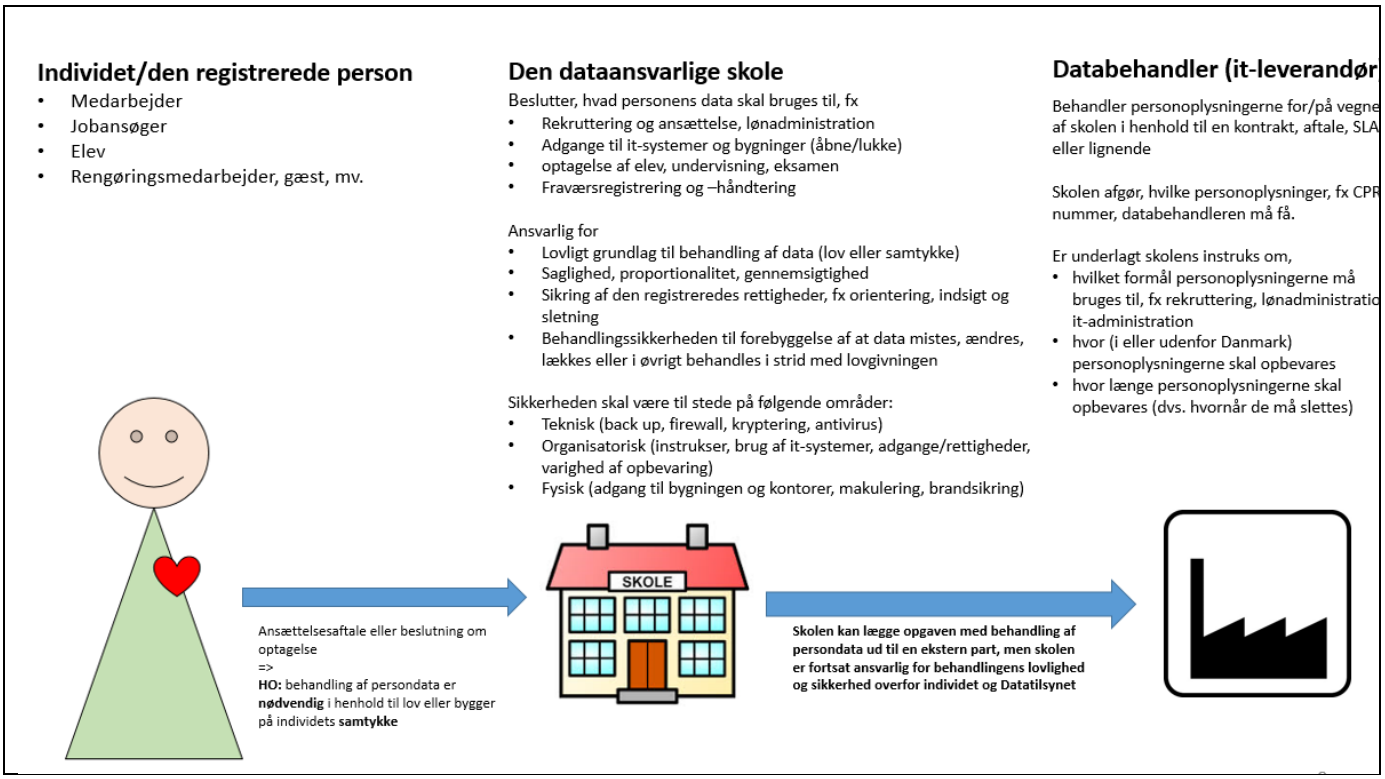
Herved lægges opgaven med behandling af data (fx administration af oplysninger som led i medarbejderrekruttering) ud til en ekstern part (fx HR. Manager). Ansvaret for, at personoplysninger om ansøgerne behandles lovligt og kun til det tiltænkte rekrutteringsformål, er imidlertid stadig den dataansvarlige skoles.

Databehandleren behandler altså blot personoplysningerne på vegne af Roskilde Gymnasium. Databehandleren må ikke behandle oplysningerne til sit 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 databehandleraftale mellem skolen og it-leverandøren.

Det er afgørende væsentligt, at skolen gør det klart, at:

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

Skolens udlicitering af rolle- og ansvarsfordelingen vedrørende opgaver med it-drift, vedligeholdelse og administration til ekstern leverandør, kan illustreres med følgende model:



60. Hvad er en "databehandleraftale", og hvad er dens formål?

En databehandleraftale indgås mellem den dataansvarlige skole og den databehandlende it-leverandør. Databehandleraftalen skal være skriftlig, herunder elektronisk, jf. GDPR art. 28, stk. 9.

Databehandleraftalen er en del af den samlede kontrakt med it-leverandøren.[38] 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 kontakten, fx skolens personalerekruttering, ***at*** personoplysningerne opbevares inden for EU (og 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 UNI-login, skal der samtidig indgås en databehandleraftale.[39] Skolen har i den forbindelse mulighed for selv at påvirke, hvilke personoplysninger databehandleren skal modtage som led i samarbejdet. Dettes vælges via forskellige datapakker i UNI-logins administrationsmodul. Det anbefales, at skolen kun åbner for den lille pakke, idet de større

[38] I stedet for en it-leverandør kan der være tale om en ad hoc-konsulent. I så fald skal denne afgive fortrolighedserklæring. En sådan findes på GF's hjemmeside (skabelon G7).

[39] GF har lagt en skabelon til databehandleraftaler på sin hjemmeside (Datatilsynets skabelon F5). I praksis involverer Roskilde Gymnasium DPO'en, når der skal indgås databehandleraftaler).

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 (fx en ISAE 3000[40] eller 3402[41]). 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 student eller medarbejderen har forladt skolen, så skal data ikke alene slettes hos skolen, men også hos databehandleren.

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

Sletteplikten er særligt svær i systemer, der har deling af dokumenter og oplysninger som funktionalitet, fx Google docs mv.

61. Skolens sletning af personoplysninger – hvordan og hvornår?

Den dataansvarlige skole skal være i stand til at slette de personoplysninger, som ikke længere må behandles.[42]

Når skolens sletteplikt indtræder, skal sletning kunne ske effektivt[43] (dvs. for bestandigt) og i alle de systemer og platforme[44], som medarbejderens/elevens personoplysninger er gemt i, fx Outlook og ESDH.

Det er afgørende vigtigt, at sletning også sker hos databehandleren, 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 sletning sker effektivt og ressourcebesparende, fx ved automatiserede sletteregler.

---

[40] ISAE 3000-erklæringen omfatter en gennemgang af de procedurer og kontroller, databehandleren har implementeret for at overholde databeskyttelsesforordningen og leve op til de krav, som følger af den indgåede databehandleraftale, herunder afdækkes bl.a. om databehandleren overholder persondataloven, herunder om databehandleren gennemfører logning af behandlingen af personoplysninger, har adgangs- og brugerstyring, har instrueret sine medarbejderne om håndtering og behandling af persondata, har styr på ind- og uddatamateriale, har rutiner for effektiv sletning.

[41] ISAE 3402-erklæringen afdækker de forretningsgange omkring en it-funktion, som har betydning for, at en finansiel rapportering er retvisende herunder forhold vedr. driften, beredskabet og dokumentationen samt den meget konkrete fysiske sikkerhed, fx hvor servere er placeret.

[42] Data slettes via automatiserede arbejdsgange i DocuNote ESDH, GymBetaling og HR-databasen, men ikke i systemer som fx Outlook, Lectio, rekrutteringsplatforme, Windows stifinder, lokale drev og formentlig heller ikke i cloud-tjenester.

[43] Se GF's vejledning Tips til hvordan man sletter persondata effektivt

[44] For en oversigt over, hvilke systemer der kan være tale om, se pkt. 4 oven for s. 14.

61.1 Elevoplysninger

Oplysninger om elever slettes, *enten* efter anmodning fra eleven (og skolen finder anmodningen berettiget), *eller* efter følgende retningslinjer (åremålet regnes fra eleven har forladt skolen):[45]

Identifikationsoplysninger (navn og CPR-nr.), oplysninger om studieretning og indskrivningsperioder	Ingen slettefrist. Dog skal sletning ske ved meddelelse om den studerendes død	
Eksamensbevis, prøvebevis, kompetencebevis mv. samt oplysninger der er nødvendige for at generere et eksamensbevis. Afsluttende standpunktskarakterer og prøvekarakterer	30 år efter uddannelsens afslutning	§ 38, stk. 1, i den almene eksamensbekendtgørelse §§ 34-38 i den almene eksamensbekendtgørelse
Andre standpunktskarakterer samt årskarakterer i ikke-afsluttede fag. Til brug for anmodninger fra (tidligere) elever om attestation af modtaget undervisning (merit) i ikke-afsluttet uddannelsesforløb eller afsluttede fag i et ikke-afsluttet uddannelsesforløb.	5 år efter undervisningens afslutning, hvis afslutningsdato er senere end 17/5-2017 – ellers 10 år efter undervisningens afslutning.	§ 72 i Bek. om de gymnasiale uddannelser
Oplysninger om elever af betydning for årsrapporten (fx oplysninger om elevbetalinger til fester, begivenheder og studieture (beløb, dato og elev)	5 år fra udgangen af det regnskabsår, materialet vedrører.	§ 12 i bogføringsloven/§ 44 i Bek. om statens regnskabsvæsen
Oplysninger om SPS (søgning om tilskud til samt administration af midler)	5 år fra udgangen af det kalenderår, hvori eleven afsluttede eller afbrød uddannelsen/undervisningen	§ 9 i Bek. om særlige tilskud til specialpædagogisk bistand m.v. til elever, kursister og deltagere med funktionsnedsættelser eller tilsvarende svære vanskeligheder
Elevregistreringer som grundlag for aktivitetsindberetning til taxametertilskud	5 år efter regnskabsårets afslutning	§ 44 i Bek.om statens regnskabsvæsen

[45] Bemærk at ved brug af den standardmappestruktur i DocuNote EDSH, som GF foreslår i Vejledningen om elevsager i ESDH, vil sletning som beskrevet ovenfor ske ved automatisk kassation, hvorved de personoplysninger, der befinder sig i en konkret mappe slettes ved automatiserede arbejdsgange, når det relevante åremål er gået. Fx slettes SU-oplysninger 5 år efter udgangen af det kalenderår, hvor eleven har forladt skolen. Det betyder, at skolens administration ikke behøver at vedligeholde den del af skolens datasamling manuelt.

Uddannelsesoplysninger til håndtering af SU-udbetaling Bek. Oplysninger til Uddannelses- og Forskningsstyrelsen vedr. indskrivninger, om afbrud og gennemførelse for SU-modtagere	30 år efter uddannelsens afslutning	SU-lovens § 13, stk. 2, nr. 2, samt udmelding fra STIL i oversigt over opbevaringskrav for uddannelsesrelaterede oplysninger på ungdoms- og voksenuddannelsesområdet ver. 3.4 af 17/5-2023
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	Jævnligt og på baggrund af risici og relevans - tidligere var der fastsat en regel om, at logningsdata skulle slettes senest efter 180 dage (den nu ophævede sikkerhedsbekendtgørelse)	Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger fra Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen, juni 2018
TV-overvågning	Maks. 30 dage fra optagelsen	§ 4 c, stk. 4, i TV-overvågningsloven

61.2 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):

Jobansøgere	Personoplysninger om ansøgere, der ikke blev ansat slettes 6 måneder efter rekrutteringsprocessen er afsluttet U: hvis samtykke til længere opbevaring[46]
Nuværende medarbejdere	Personoplysninger på personalesagen (og i it-systemer) kan opbevares indtil medarbejderen er fratrådt U: hvis medarbejderen beder om sletning af forældede personoplysninger undervejs i ansættelsesforholdet, fx en gammel tjenstlig 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

[46] Hertil benyttes blanket M3.

	er en forvaltningsretlig afgørelse, som skal indeholde en høring, begrundelse og klagevejledning. Tv-optagelser slettes efter Maks 30. dage
Fratrådte medarbejdere	Personoplysningerne på personalesagen slettes 5 år efter fratræden. U1: personalesager for ansatte, der er født den 1. i måneden og medarbejdere i chefstillinger[47] slettes ikke, da der kan være afleveringspligt til Statens Arkiver[48] U2: hvis der verserer arbejdsskadesag, retssag eller arbejdsretlig tvist mellem medarbejderen og arbejdsgiver, slettes personalesagen først 3 år efter den pågældende sag er afsluttet. Tv-optagelser slettes efter Maks 30. dage

62. Hvad skal den såkaldte "Fortegnelse over skolens behandlingsaktiviteter" indeholde?

Fra den 25. maj 2018 indføres der et krav om, at den dataansvarlige skole skal føre en intern fortegnelse over sine behandlinger af personoplysninger.

Fortegnelser skal være skriftlige, elektroniske og skal kun efter anmodning udleveres til Datatilsynet.

Formålet med fortegnelsen er at dokumentere, at den behandling af personoplysninger, der finder sted, overholder lovgivningens regler. Derfor er det nødvendigt, at man som skole får et overblik over og dokumenterer hvilke personoplysninger, man som organisationen behandler, hvor oplysningerne kommer fra, hvem man deler dem med, hvor længe man gemmer dem m.v.

Fortegnelsen vil være et hjælpeværktøj og give et overblik til brug for skolens udarbejdelse af orienteringsskrivelser til elever og medarbejderne om behandlingen af deres personoplysninger, besvarelse af indsigtsanmodninger, mv.

GF's skabelon til fortegnelse kan anvendes.

Indholdskrav til skolens fortegnelse:

a) Navn på og kontaktoplysninger for den dataansvarlige, en evt. fælles dataansvarlig, den dataansvarliges repræsentant og databeskyttelsesrådgiveren, hvis I er forpligtet til at udpege en sådan.
b) Formålene med behandlingen
c) En beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger – samt hvilke kategorier af personer, der behandles hvilke personoplysninger om
d) De kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til

[47] Ved chefstilling forstås en kontorchef (lønramme 36) og derover, og aldrig fuldmægtige og kontorpersonale, og heller ikke kontorledere. For at være omfattet af chefbegrebet skal en stilling kunne sidestilles med en chefstilling i henseende til bl.a. ledelsesbeføjelser, lønforhold og stilling i det administrative hierarki. En skoleinspektør anses for omfattet af chefbegrebet, jf. FOB 2001 549.

[48] I tilfælde af U1 eller U2: oplysningerne overføres til et arkiv i ESDH efter 5 år, hvortil kun meget få medarbejdere har adgang – herfra kan de så hentes frem, hvis det bliver nødvendigt.

e) Hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland eller denne internationale organisation og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier
f) Hvis det er muligt de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger
g) Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i art. 32, stk. 1.

Tilsvarende skal databehandlere føre en fortegnelse. Dette skal man som skole kræve af sin databehandler i kontrakten eller databehandleraftalen.

63. Hvad betyder det, at man skal "håndtere brud på datasikkerheden for personoplysninger"?

Hvis der er opstået en hændelse på skolen, hvorved uvedkommende kan have eller har fået adgang til personoplysninger, eller hvor data kan være gået tab eller have været utilgængelige i en periode, skal skolen vurdere, om hændelsen skal anmeldes til Datatilsynet.

Det skal de fleste hændelser, hvor uvedkommende kan have fået adgang, men hvis en konkret vurdering af hændelsens alvor og betydning for de registrerede personers rettigheder falder ud til, at det er usandsynligt, at uvedkommende i praksis har set personoplysningerne, da kan anmeldelsen undlades. I sidstnævnte tilfælde skal hændelse blot registreres i skolens interne log.

I praksis foretages denne vurdering af skolens ledelse, it-administrator og DPO i samarbejde.

Anmeldelse til Datatilsynet skal hurtigst muligt og om muligt inden for 72 timer fra hændelsen er konstateret.

Det skal samtidig vurderes, om der skal ske underretning af de registrerede, hvis oplysninger er berørt af bruddet.

64. Hvordan får skolen kendskab til brud på datasikkerheden (fx læk)?

Skolens medarbejdere er via retningslinjerne (i afsnit 1 ovenfor) orienteret om, at de straks skal kontakte nærmeste leder eller it-administrator, hvis der opstår en situation, hvor personoplysninger kan være havnet hos uvedkommende.

Retningslinjerne har konkrete eksempler på situationer, hvor medarbejderne skal reagere.

Den samme orientering om pligten til at reagere ved læk er også et bilag til kvitteringen (M7), som medarbejderne skal skrive under på, når de bliver ansat eller får udleveret it-udstyr eller systemadgange fra GF.

Nærmeste leder og it-administrator ved, at de skal underrette DPO'en ved henvendelser fra medarbejderne om sikkerhedshændelser.

Medarbejderne i GF's IT-afdeling er via Beredskabsplanen bekendt med, at de skal orientere DPO'en ved sikkerhedshændelser, herunder brud på datas tilgængelighed (skade på hardware, software, tjeneste og netværk samt hackerangreb), fortrolighed (hackerangreb og adgang mellem skolers data) og integritet (hackerangreb)].

65. Hvad skal anmeldelsen til Datatilsynet indeholde?

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.

Anmeldelse sker via virk.dk, hvor der skal udfyldes en formular.

66. Hvornår skal de berørte registrerede personer underrettes om læk af deres personoplysninger?

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal skolen også underrette de registrerede personer om bruddet på persondatasikkerheden.

Dette sker i samarbejde med DPO'en.

GF's skabelon G10 kan anvendes.

67. Hvordan ser loggen over sikkerhedshændelser ud og hvem fører den?

Roskilde Gymnasium ledelesansvarlige for IT fører en log over datalæk på Roskilde Gymnasium. Loggens opbygning kan ses i skabelon G9. Se også afsnit 67, G8 og G10

68. Hvad er en DPO/databeskyttelsesrådgiver – og hvordan bruger vi ham/hende?

Fra den 25. maj 2018 skal alle statsligt selvejende gymnasieskoler have en databeskyttelsesrådgiver. Gymnasiefællesskabet er DPO for samtlige partnerskoler.

DPO'en i GF kan kontaktes på dpo@gfadm.dk.

DPO'ens funktion er at rådgive skolen om dens forpligtelser efter databeskyttelsesreglerne og overvåge, hvordan personoplysninger behandles på skolen.

Samtidig er DPO'en kontaktperson til Datatilsynet og bistår skolen med at håndtere konkrete klagesager, som indbringes for Datatilsynet. På skolens konkrete anmodning bistår DPO'en skolen med at håndtere sager om brud på datasikkerheden (fx læk), fx anmeldelse af hændelsen til Datatilsynet og evt. også til de berørte registrerede personer.

DPO'en har samtidig et tæt samarbejde med GF's GDPR-team, som vejleder skolen om praktiske redskaber og arbejdsformer, der kan styrke beskyttelsen af personoplysninger 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 samt ved gennemgang og udarbejdelse af databehandleraftaler, risikovurderinger og løbende kontrol med databehandlere.

For DPO'en i GF gælder ydelseskataloget, der findes her.

69. Hvad ligger der i at sikre skolens "behandlingssikkerhed vedr. personoplysninger"?

I kapitel 1 og 2 står de retningslinjer som gælder for medarbejderne om behandling af personoplysninger på Roskilde Gymnasium.

Ved udarbejdelsen af retningslinjerne for Roskilde Gymnasium er nedenstående, som gælder generelt for et gymnasium, taget i betragtning.

Behandlingssikkerheden er de tekniske, fysiske og organisatoriske foranstaltninger på skolen, der giver et passende sikkerhedsniveau for de personoplysninger, som skolen behandler.

Sikkerhedsniveauet fastlægges af ledelsen 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.

Følgende punkter kan overvejes og udmøntes i tiltag hos den dataansvarlige skole:

- Brug af ESDH-system til den langvarige opbevaring af fortrolige og følsomme personoplysninger, idet ESDH via systemlogning gør det muligt efterfølgende at undersøge og fastslå, om og af hvem der er behandlet personoplysninger
- Udarbejdelse og brug af interne regler om organisatoriske forhold og fysisk sikring, fx administration af adgangskontrol til it-systemer (fx ESDH)
- Opfølgning ift. overholdelsen af de beskrevne retningslinjer
- Instruktion fra den dataansvarlige til de medarbejdere, som behandler personoplysningerne om, hvordan systemerne bruges korrekt
- Medarbejdernes systematiske brug og opdatering af unikke, personlige passwords, herunder opmærksomhed på, at det standard-password, som tildeles ved oprettelse i et it-system skal ændres straks og minimum hver 6. måned opdateres til et nyt personligt unikt password bestående af mindst 12 tegn, hvori bør indgå både store/små bogstaver samt tal og specialtegn.
- Tydelige, skriftlige vilkår for udlån, brug og returnering af digitale arbejdsredskaber, som underskrives af den medarbejder, der låner udstyret, samtidig med udlevering af udstyret. [49]
- Lås på de steder, hvor der foretages behandling af personoplysninger mhp. at forhindre uvedkommendes adgang
- Kryptering af personoplysninger, der sendes via e-mail (Sikker Mail eller Digital Post)
- Registrering af afviste adgangsforsøg og tekniske foranstaltninger, der kan sikre blokering for yderligere forsøg, hvis det er nødvendigt
- Back up af systemer med kritiske data, fx Lectio
- Styr på databehandlere.

[49] GF's skabeloner M7 og M8 kan benyttes.