Håndbog i behandling af personoplysninger

Gefion Gymnasium

Gefionhåndbogen, 2024-2025

GEFION
GYMNASIUM

Gymnasiefællesskabet

Indhold

Indledning

I denne håndbog kan du læse de regler for behandling af personoplysninger, der gælder for alle medarbejderne på Gefion 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.

Ansvarlighed

Gefion Gymnasium er forpligtet til at behandle personoplysninger om elever og medarbejdere efter reglerne[1], og eftersom alle medarbejdere på Gefion 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 Gefion 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.
- Tovholder/GDPR-team: Rektor udpeger en tovholder/et GDPR-team blandt medarbejderne, som bidrager til og understøtter implementeringen af retningslinjerne og redskaberne til beskyttelsen af personoplysninger og datasikkerheden. Tovholder/GDPR-teamet samarbejder med DPO'en og GF's datasikkerhedsmedarbejdere.
- Databeskyttelsesrådgiver (DPO): DPO'ens rolle er at overvåge, at Gefion 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 endvidere Gefion 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 fjernundervisning).

Alle Gefion Gymnasiums medarbejdere skal kende denne håndbog og vide, hvordan indholdet i tjeklisterne praktiseres. Den gældende version af håndbogen er derfor gennemgået på awareness-møder, hvor der var mødepligt (se Awareness-dokumentation i særskilt ark, DocuNote). I den forbindelse har alle medarbejdere kvitteret for læsning af håndbogen i gymbetaling.dk. Den gældende version af håndbogen er altid tilgængelig på Gefion Gymnasiums hjemmeside samt på intranet (Google-Drev).

[1] Lovgivningen om behandling af personoplysninger findes i den europæiske databeskyttelsesforordning og i den danske databeskyttelseslov.

Gefion Gymnasiums opgaver

For at vi på Gefion 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 hans personoplysninger og vi støtter ham i at udøve retten 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 Gefion Gymnasium eller en rolle (fx forældre), der berettiger til dette
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 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**
10. Vi har en plan for håndtering af **brud på datasikkerheden** (fx datalæk)

Oversigt over Gefion Gymnasiums samlede beskrivelse af vores gode databehandlingsskik

Her kan du se en samlet oversigt over skolens overordnede retningslinjer for behandling af personoplysninger, samt de underliggende tjeklister og beskrivelser og 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	Gefion Gymnasiums hjemmeside samt kap. 1 i denne håndbog.	Alle medarbejdere på skolen	Ajourføring: Juni (jf. Årshjul) Ansvarlig: AML
Skolehåndbogens kap 2	Konkrete tjeklister og retningslinjer for konkret håndtering af personoplysninger (procedurebeskrivelser) til: • Administrative medarbejdere • IT-administratorer • Studievejledere • Kommunikationsmedarbejdere • Elever • Ledelse	Gefion Gymnasiums hjemmeside samt kap. 2 i denne håndbog.	Den medarbejdergruppe som tjeklisten/ retningslinjerne angår	Ajourføring: Juni **Ansvarlig: Adm.**
Skolehåndbogens kap. 3	FAQ med viden og beskrivelser af reglerne og hvad de betyder i en skolesammenhæng		Opslagsværk for medarbejderne Skal være kendt af ledelse og tovholder	
Personalehåndbogen	Beskrivelse til medarbejderne om, hvordan skolen behandler deres personoplysninger som led i ansættelsen	Gefion Gymnasiums hjemmeside	Alle medarbejdere på skolen	Ajourføring: Juni **Ansvarlig: Adm. og ledelse**
Elevorientering	Beskrivelse af skolens retningslinjer for elevernes brug af fx Lectio, digitale undervisningsværktøjer, adfærd ifbm. online-undervisning • Leveregler/husregler • Kobling til skolens studie- og ordensregler	Gefion Gymnasiums hjemmeside samt på ”IT på Gefion” (intranet)	Alle elever, lærere, administrative medarbejdere samt ledelse på skolen	Ajourføring: Juni Ansvarlig: AML.
Risikovurdering af it-systemer	• Faktaark om it-systemets formål og funktioner ifbm. skolens benyttelse	Findes i DocuNote under ”Risikovurderinger for IT-systemer”	Tovholder (AML) samt BHB	Dokumentet er dynamisk. Administreres af tovholder (AML)

		samt under ”Databehandlere ” (under ”Fysiske forhold” -> ”Databehandleraftaler”).		
Positivliste over it-systemer og it-værktøjer, der bruges i drift og undervisning	Simpel oversigt over de it-systemer, -værktøjer mv., som skolens ledelse har godkendt til brug på skolen (administration/undervisning)	Findes i DocuNote		Dokumentet er dynamisk. Administreres af tovholder (AML)
Oversigt over databehandlere	Simpel oversigt over de it-leverandører og databehandlere, som skolen bruger (til administration/undervisning)	Findes i DocuNote		Dokumentet er dynamisk. Administreres af tovholder (AML).
Fortegnelse over behandlingsaktiviteter	Formel oversigt over de behandlinger af personoplysninger, som skolen udfører vedr. fx HR-administration og elevadministration	GAP- ark (findes i DocuNote) samt dokumenterne Fortegnelse over behandlingsaktiviteter for hhv. elever og medarbejdere		Dokumentet er dynamisk. Administreres af tovholder (AML).
Plan for håndtering af sikkerhedsbrud	Forretningsgang for håndtering af brud på persondatasikkerheden og skolens samarbejde med DPO’en om håndteringen	GF har skabeloner til forretningsgang, indberetning til Datatilsyn, underretning til de registrerede samt intern log for skolen		Dokumenterne bruges løbende, når der opstår brud eller sikkerhedshændelser

Kapitel 1 - Retningslinjer for behandling af personoplysninger der gælder for alle medarbejderne på Gefion Gymnasium

Gefion Gymnasiums leveregler for datasikkerhed (alle)

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

1. Brug **passwords** (eller fingeraftryk som adgangskode) 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 passwords og undlad derved så vidt muligt at skrive det ned. Et password må under ingen omstændigheder fremgå af noter, der er tilgængelige for andre. Tast aldrig passwords mens computeren er koblet til projektor eller lignende, hvor passwordet kan aflures.

2. Aktivér din **pauseskærm og lås skærmen**, 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.** Kontakt kontoret.

5. **E-mails** med fortrolige og følsomme personoplysninger sendes via E-Boks, med krypteret mail eller Sikker Mail (Rmail). Mails fra xxx@gefion-gym.dk er TLS krypteret

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

7. Hvis personoplysningerne er modtaget eller sendt via **e-mail**, slettes mailen senest 1 måned efter sagsbehandlingen er afsluttet. Hvis personoplysningerne stadig er relevante, når den nævnte måned er forløbet, gemmes mailen fremadrettet i ESDH

8. 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

9. 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

10. Tag ikke nye it-systemer eller digitale platforme i brug, uden at det er godkendt af ledelsen (AML) vedr. sikkerheden i systemet og indgået en kontrakt og en **databehandleraftale** med leverandøren

11. 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

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

13. Ved **tyveri eller bortkomst af it-udstyr** (fx pc, tablet og/eller smartphone, som man har fået udleveret som arbejdsredskab på Gefion Gymnasium), skal man straks kontakte [hvem på skolen]

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

Tavshedspligt (alle)

Som medarbejder på Gefion 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 Gefion Gymnasium – og heller ikke med kollegaer på Gefion Gymnasium, der har arbejdsfunktioner, som gør det unødvendigt, at de kender de pågældende oplysninger.

Alle medarbejdere på Gefion Gymnasium er omfattet af følgende klausul om

Tavshedspligt

Gefion 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 Gefion Gymnasium, fx EDSH, 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 hændeligt eller ulovligt kan være tilintetgjort, tabt, ændret eller utilsigtet videregivet til uvedkommende, skal man straks kontakte sin leder, som hjælper med håndteringen, jf. næste afsnit.

Handlepligt i tilfælde hvor der kan være sket brud på datasikkerheden (bl.a. læk)

Hvis der opstår en situation, hvor der kan være sket et brud på datasikkerheden for personoplysninger skal man STRAKS kontakte uddannelsesleder Andreas Lange (AML) eller IT-support Mikkel Fog (MFO) som hjælper med håndteringen.

Årsagen til at man skal reagere straks er, at Gefion Gymnasium har pligt til at håndtere et sikkerhedsbrud straks og en eventuel anmeldelse til Datatilsynet skal ske uden unødig forsinkelse inden 72 timer, og derfor er det nødvendigt at komme i gang meget hurtigt.

Følgende er eksempler på brud på datasikkerheden:

	Hændelse
1	Man 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.
2	Man 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
3	Man sender (pr. post eller e-mail) personoplysninger til en forkert modtager

Når bruddet er konstateret og AML /MFO og DPO 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.

Instruks om adfærd til forebyggelse og håndtering af hackerangreb

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 Mikkel Fog (MFO) 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, selvom du betaler.

Medarbejderadfærd til forebyggelse af hackerangreb på Gefions 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 Gefion Gymnasium.

2. Skolen sørger for daglig **back up** af alt materiale på netværksdrevet og i de systemer, som skolen har godkendt til persondata, jf. afsnit [5]. Derimod skal du selv sørge for at tage back up af data, der (undtagelsesvist) ikke ligger disse steder.

3. Vær **skeptisk overfor e-mails**, som er mistænkelige i sprog, layout eller den sammenhæng, du modtager dem i. Det gælder også, selvom mailen umiddelbart kommer fra en kendt afsender. 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, *selvom* 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.

Disse it-systemer må du bruge som medarbejder ("Positivliste"):

Som ansat på Gefion Gymnasium skal du bruge de it-systemer, som skolen stiller til rådighed, til al arbejdsrelateret, digital kommunikation og opbevaring. Dette er især vigtigt, når du behandler **personoplysninger**.

De it-systemer, som Gefion Gymnasium har godkendt til **personoplysninger**, er følgende systemer (se særskilt om, *hvad Lectio samt cloud-tjenester som fx Google og apps må bruges til nedenfor*):

Til alle medarbejdere:

- Outlook (mail)
- Office365
- HRdatabasen
- Gymbetaling

Til administrative medarbejdere og studievejledere:

- Outlook (mail)
- Office365
- E-Boks
- Lectio
- Optagelse.dk
- Netprøver.dk
- Bibliotekssystemet Boss
- DocuNote ESDH
- Statens lønsystem og LDV

- Navision stat
- Indfak2
- HRdatabasen
- Gymbetaling
- CPR-Registeret

Der må ikke gemmes personoplysninger i andre systemer end de nævnte (se dog nedenstående om midlertidig opbevaring) og på medarbejderens krypterede, personlige computer.

Der må ikke gemmes følsomme personoplysninger i cloud-tjenester (fx GoogleApps) og USB-nøgler. På Gefion 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 (fx GoogleApps). På Gefion Gymnasium bruger vi Google som Cloudstjeneste, dette gælder også virtuel undervisning på GoogleMeet. Når dokumenter opbevares midlertidigt, skal dokumenterne enten slettes eller overføres til et godkendt it-system hurtigst muligt – dog senest 1 måned efter endt brug. I Google må der ikke opbevares personlige, følsomme oplysninger undtagen følgende:

● 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

1 Mailpolitik

Ansatte på Gefion Gymnasium skal bruge de systemer, som skolen stiller til rådighed, til al arbejdsrelateret kommunikation. De vigtigste regler er følgende:

1. Arbejdsrelaterede mails sendes fra og modtages i Gmail

2. Mails med fortrolige og følsomme personoplysninger skal altid sendes til e-Boks eller med krypteret mail. Mails fra Gefions Gmail- adresser er som udgangspunkt altid krypteret (TLS). Se nedenfor for yderligere kryptering (Rmail)

3. Der må ikke bruges andre mailkonti end medarbejderens officielle skolemail til skolerelateret indhold. Derfor må der aldrig laves videresendelsesregler, eller videresendes til andre mailkonti (fx hotmail og lignende)

Straks efter en medarbejders fratræden lukkes medarbejderens mailadresse ned.

Medarbejderen skal selv være opmærksom på, at mails med følgende typer af personoplysninger max må opbevares i 1 måned efter sagen er slut: fortrolige og følsomme personoplysninger (dvs. oplysninger om trivsel, studievejledning, psykolog, diagnoser, ordblindhed, fraværsårsager, sociale problemer, gæld, kriminalitet, familiestridigheder og lignende). Når der er gået mere end 1 måned fra den sag, som mailen angik, er slut, skal mailen enten slettes eller overføres til et sikkert it-system (DocuNote).

Mails med øvrige personoplysninger slettes også straks, de har mistet deres relevans, hvilket normalt er indenfor et par måneder. Skal mailen gemmes i længere tid, overføres den til DocuNote og slettes i mailsystemet

Arbejdsrelaterede e-mails 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 vi ikke foretager fx stikprøvekontroller af indhold i mails mv. [2]

Vi læser ikke medarbejderes e-mails der er tydeligt mærket ”privat”. For nemheds skyld vil vi dog opfordre dig til at bruge en privat mailkonti til privat kommunikation.

Private mailkonti må ikke bruges til arbejdsrelateret kommunikation.

E-mails med CPR-numre eller helbredsoplysninger, der sendes til eksterne modtagere, skal sendes via Sikker Mail eller E-Boks (spørg evt. administrationen om hvordan)

<u>Kryptering af mails</u>

Alle mails afsendt via skolens Gmail er som udgangspunkt krypteret (med TLS). Krypteringen sker, når mailen forlader IT-Center Fyns server, og dekrypteringen sker, når mailen når frem til modtagerens

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

mailboks. Medarbejderen skal ikke selv foretage sig noget i krypterings- og dekrypteringsfasen. Kontoret, studievejledere og ledelsen vil have en ekstra mulighed for at sætte et ekstra krypteringslag på deres mails (Rmail). Hvis man som medarbejder vurderer, at man har et ekstraordinært behov for en ekstra krypteringsmulighed ved afsendelse af mail så kontakt administrationen.

Hvordan sendes der besked til e-boks

Administrationen, ledelsen og studievejlederne har mulighed for at sende post til elever eller forældres e-boks via DocuNote.

Brugeradgange og rettigheder

Medarbejderne på Gefion Gymnasium må kun behandle personoplysninger i de systemer, som Gefion Gymnasium har godkendt til formålet.

Den enkelte medarbejder på Gefion Gymnasium gives personlige autorisationer og rettigheder til systemerne. Adgangskoder til systemerne må derfor ikke deles med andre og må kun "huskes" af systemet, hvis der er tale om en personlig computer.

Overflødiggjorte autorisationer lukkes. Har man som medarbejder en autorisation, som ikke længere svarer til, hvad man har behov for til udførelsen af sine arbejdsopgaver, men som derimod giver adgang til flere personoplysninger eller flere IT-systemer end 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, om dette er tilfældet.

Sletning af mails

For at sikre at mails med personoplysninger ikke opbevares for længe, skal hver medarbejdere 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 de slettes straks.

2 Dette må du bruge Lectio til fremover

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

Gefion Gymnasium bruger ikke Lectios kommunikationsfunktioner (fritekstfelter), da disse funktioner ikke er sikre nok til at fx oplysninger om elevers sygdom, trivsel og sociale forhold kan registreres der. Gefion bruger i stedet **e-mail** til at kommunikere om den slags.

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

Studievejleder- og administrativ note bruges heller ikke fremover. Vi opbevarer heller ikke **egentlige elevsager** i Lectio fremover.

I stedet bruges DocuNote (ESDH) og de i heri oprettede elevmapper til studievejledning, sanktionssager, lægeerklæringer, SU- og SPS-ansøgninger. Her har ledelsen, administrationen og studievejlederne adgang.

På skolens hjemmeside under fanen "sikker kommunikation med Gefion Gymnasium" kan elever, værger og medarbejdere se, at vi opfordrer til kun at kommunikere om helt få ting via Lectio, herunder at det kun er de prædefinerede fraværsmuligheder ("Andet", "Kom for sent", Skolerelaterede aktiviteter", "Private forhold", "Sygdom"), der må bruges. Eleverne og forældre opfordres til ikke at uddybe fraværet i fritekstfeltet. I stedet opfordres de til at skrive en mail via Rmail.

Fortrolighed omkring oplysninger i Lectio

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

Via Lectios systemlog kontroller administrator, at data i Lectio kun bruges til tjenstlige formål og ikke uvedkommende formål. Administrator gennemgår standardmæssigt loggen 1 gang halvårligt og efter behov ved konkret mistanke om uhensigtsmæssig brug af Lectio.

Hvem står for oprydningen i de oplysninger, der allerede ér registreret

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

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

Hvad må fælles undervisningsnetværksdrev som GoogleSuite bruges til?

På Gefion Gymnasium benytter vi os af GoogleSuite/Enterprise/Legacy[3] igennem EduLife. Edulife-tjenesten leveres af Wizkids og er en skybaseret læringsplatform (LMS) der fletter Googles produkter sammen med Gefions administrationssystem.

For ovennævnte tjenester fra Google gælder der på Gefion Gymnasium (med henvisning til de beskrevne retningslinjer for behandling af personoplysninger i denne håndbogs kapitel 1):

- Personoplysninger må kun behandles af ansatte som er beskæftigede med de opgaver som er formålet med den givne behandling/opbevaring. Personoplysninger må ikke ukritisk lægges ud på Drev.
- Man skal som altid behandle personoplysninger med omhu. Google (gennem WizKids) garanterer, at deres system (GSuite såvel som GMail) er sikkert, så der i teorien gerne må ligge følsomt data. Men vi anbefaler, at man ikke lægger følsomt data på drev. Der må heller ikke behandles ellers opbevares personfølsomme eller fortrolige oplysninger i cloud-tjenester/skyer som fx Dropbox. Dropbox må kun bruges til almindelige data som ikke er personhenførbare hverken direkte eller indirekte (gælder både almindelige og følsomme oplysninger).

Nedenfor ses en oversigt over behandlingen og opbevaringen af personoplysninger

	DocuNote	E-mail	Mobilt udstyr, PC og USB	Fælles undervisnings-netværksdrev	Studieadministrative systemer (fx Lectio)	Andre cloudtjenester
Alm. personoplysninger	Ja	Ja. Skal slettes efter senest 30 dage	Nej	Ja	Ja	Nej
Personnummer	Ja	Nej	Nej	Nej, frarådes	Ja	Nej
Følsomme og andre fortrolige personoplysninger (logning kræves)	Ja	Rmail	Nej	Nej, frarådes	Nej	Nej

[3] GSuite (*GSuite for education, Google Enterprise/Legacy*) er en samlebetegnelse for Googles tjenester som de af Gefion benyttede *Drev*, *Docs, Sheets, Sites, Slides* etc.).

3 Password-politik

Når man modtager sit password fra Gefion Gymnasium, er det meget vigtigt, at man straks ændrer det til et nyt, personligt, komplekst password.

Det nye password skal indeholde følgende:

- Mindst 8 karakter (men 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 180 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 poste it's, der sidder på computeren.

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

Tavshedspligt

Som medarbejder på Gefion 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 lignende) er fortrolig, og må ikke deles med nogen uden for Gefion Gymnasium.

Sletning af udtjente digitale arbejdsredskaber

Det sker løbende, at man som medarbejder får nye digitale arbejdsredskaber (fx pc, MAC, tablet, smartphone eller lignende). Udtjente digitale arbejdsredskaber skal i den forbindelse afleveres til IT, der sørger for effektiv og korrekt sletning af arbejdsrelateret data. Har man mulighed at købe det udtjente arbejdsredskab til privat eje, og ønsker man dette, skal udstyret inden købet forbi IT for en tilsvarende effektiv sletning af arbejdsrelateret data.

Procedure i tilfælde af utilsigtede læk af persondata

For instruks om håndtering af datalæk – se bilag til denne håndbog.

Om brugen af Apps i undervisningen

Man skal være opmærksom på, hvilke apps man bruger i undervisningen, om app'en er obligatorisk for eleven – og om det kræves at eleven logger ind (fx via Unilogin eller ved at oprette en konto, hvor der skal afgives personoplysninger). Der er IKKE tale om apps hentet fra udbydere som vi allerede har databehandleraftaler med (fx Google Apps, App Store, Google Play, Chrome webshop) men udelukkende om apps der er afgrænset fra ovenstående, og som modsvarer følgende kriterier:

· Eleverne er tvunget til at bruge dem i undervisningen

· Eleverne skal logge ind med deres Unilogin/personlige oplysninger for at få adgang (her skelnes igen mellem apps i undervisningen og undersøgelser igangsat fra skolens side som fx elevtrivselsundersøgelsen, hvor skolen laver en individuel databehandleraftale med udbyderen). Det kunne være visse quizapps (ikke Kahoot), apps om klima og vejr og/eller Youtube, hvis det kræves, at eleven har en konto og logger ind (altså ikke kun streamer noget).

Handling: Bruger man en app, som modsvarer dette, så skal man handle. Man kan man komme om det på én af følgende måde:

Lad i stedet for brugen være frivillig for eleverne og stil evt. et alternativ til rådighed. Ifølge reglerne skal man også gerne have taget stilling til, om virksomheden bag app'en har udarbejdet en privatlivspolitik, og at der i app'en sker mulighed for indhentelse af nødvendige samtykker til at bruge den (det gør stort set alle firmaer etc. nu om dage) og i den forbindelse, at det er muligt at trække samtykket tilbage og få slettet sine oplysninger i app'en.

Man skal sikre sig at der kan laves en databehandleraftale med skolen inden brugen.

Det kan være svært at lave en statisk liste over apps der bruges i undervisningen, da man jo bruger lidt forskelligt nogle gange – og fremover også vil det. Er man i tvivl om ovenstående i forhold til om den obligatoriske app man bruger i undervisningen kunne være noget, som man skal handle på, så kontakt uddannelsesleder Andreas Lange eller Gefion Gymnasiums DPO, Pernille Heiring; pfh@gfadm.dk

Generel IT- sikkerhed – hvad kan du selv gøre? Hurtig tjekliste

- Fortæl aldrig dit password til andre. Hvis du mener at nogle kender dit password, så skal du ændre det til et nyt. Brug ikke et password på skolen som du bruger privat (fx til Facebook el. lign.).
- Pas på med at bruge fremmede USB- nøgler. De kan indeholde virus, malware og lignende. Bed hellere om at få tilsendt filer på e-mail
- Brug ikke USB-nøgler som sikkerhedsbackup
- Husk at låse din skærm, når du går fra din PC.
- Lad være med at svare eller åbne e-mails med ukendt eller mistænkeligt indhold og afsender
- Behandl skolens data forsvarligt, og forhold dig kritisk til de netsteder, du besøger
- Lad være med at installere ukendte programmer på din PC
- Lån ikke din PC ud til andre
- Bruger du Smartphone ifb. med arbejdet, skal den sikres med adgangskode, pinkode el. lign.
- Det anbefales, at medarbejdere der arbejder med personfølsomt materiale (adm. personale, studievejledere o.lign.) ikke tager fysiske kopier indeholdende følsomme personoplysninger med hjem. Hvis det alligevel sker, skal man være opmærksom på, at uvedkommende ikke har adgang til

oplysningerne. Det anbefales, at de fysiske kopier (med personfølsomme oplysninger) tages med tilbage til skolen og/eller makuleres, når der ikke længere er behov for at have dem liggende i fysisk form. Almindelig opgaveretning o.lign., som underviserne foretager, kan uden problemer tages med hjem i fysisk form.

4. Instruks om beskyttelse af persondata udenfor Gefion Gymnasiums lokaler (hjemmearbejdsplads)

Når man arbejder med personoplysninger udenfor Gefion 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 arbejde med personoplysninger uden for skolens lokaler er:

1. Man tilgår de it-systemer, der er godkendt til Gefion Gymnasiums persondata via skolens VPN-løsning. 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 Google, på USB-nøgle eller i papirform, skal personoplysningerne overføres til et godkendt it-system på Gefion Gymnasium hurtigst muligt og allersenest 1 måned efter sagsbehandlingen er afsluttet. Samtidig slettes personoplysningerne fra det usikre opbevaringssted.

3. Medarbejderen skal sørge for, at familiemedlemmer og andre uvedkommende ikke får adgang til personoplysninger som led i hjemmearbejde.

4. 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.

5. Instruks om sletning af datamedier ifbm. privat køb af udtjente arbejdsredskaber

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

Inden det udtjente arbejdsredskab overgår til medarbejderens privat 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 uigenkaldelig.

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

6. Instruks om hvordan man sletter personoplysninger i usikre systemer

På Gefion 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, din 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**
Skrivebord (Filer, fx word, excel, power point, mv.)	Filen slettes 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.
USB-stick	Indholdet på USB'en slettes ved at stille musen på "ekstern disk" i skærmbilledet "denne PC", højre-klikke 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.
Hjemmesiden	Tanja (TOR) administrerer hjemmesiden og kan slette billeder og kontaktinfo om skolens medarbejdere.

Kapitel 2 Tjeklister og beskrivelser til specifikke medarbejdergrupper

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

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

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

Den enkelte medarbejder på Gefion 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.

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

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

Omsat til hverdagssprog betyder det, at vi må behandle CPR-numre som led i de opgaver, vi normalt løser som led 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 E-Boks
- Opbevares i sikre it-systemer og ikke andre steder
- Sendes via Sikker Mail eller E-Boks, hvis de indgår i en mailkorrespondance
- Makuleres, hvis de indgår i et fysisk dokument og formålet med dette dokument er udtjent,

CPR-numre fremgår ikke af skolens ansættelsesbreve.

<u>Om videregivelse af CPR-numre</u>

Gefion 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, E-Boks eller krypteret digital indberetningsformular).

9. Instruks om brug af Sikker Mail til CPR-numre og andre fortrolige og følsomme personoplysninger (TAP)

Når CPR-numre (og andre fortrolige eller følsomme personoplysninger) sendes via e-mail ud af huset, skal der bruges Sikker Mail eller E-Boks. 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 Gmail/E-Boks, men overføres[4] til ESDH indenfor en måned.

Endvidere 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, men det er 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 ér sikker, jf. ovenfor.

Sikker Mail via E-Boks

Nogle medarbejdere på Gefion Gymnasium har integreret E-Boks til deres ESDH.

Mailkorrespondance via E-Boks er sikker fra afsender til modtager (begge parter inklusive). Modtageren kan læse mailen på borger.dk, E-boks.dk eller virk.dk (sidstnævnte for skoler og virksomheder).

Forsendelse via E-Boks sker ved opslag på CPR-nummer.

Sikker Mail via certifikat (modellen aftales med ledelsen og it-administratoren)

På Gefion Gymnasiums hjemmeside er det muligt at sende sikker mail via forsiden på hjemmesiden (gå ind i "Send sikker mail" som ses nederst på forsiden).

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

- Alle **skabeloner** ligger på GF's hjemmeside: https://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/datasikkerhedintra

[4] Senest 1 måned efter sagsbehandlingen er afsluttet

- 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 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 hans 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 ifbm. 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.

11. Tjekliste – Elever, Optag (TAP)

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

ANSØGERE					
1	Hentning af ansøgere fra optagelse.dk til Lectio		Skolen	MAN (og BVE)	Februar/Marts
2	Indlæsning af ansøgere fra Lectio til DocuNote mhbp. oprettelse af ansøgningssag i DocuNote		Skolen	MAN	Februar/Marts
3	Generel orientering til elever og forældre om behandling af personoplysninger som led i optag	Region Hovedstadens fordelingsudalg laver tekst til kvitteringsbreve mm. Gefion tilføjer tekst vedr. behandling af personoplysninger mv. Dette sker i kvitteringsskrivelsen.	Skolen	MAN/BPO	Ultimo marts
4	Brug af krypteret mailforbindelse (Sikker Mail eller E-Boks) ved ekstern e-mail-kommunikation med andre gymnasier, fordelingsudvalg, UUV, hjemmet mv., hvis mailen indeholder CPR-nummer eller andre fortrolige eller følsomme personoplysninger		Skolen	MAN	
5	Optagelsesprøve: noter, vurderinger og begrundelser oprettes og gemmes i DocuNote. Afslag med begrundelse gives via E-Boks		Skolen	BPO	
6	Videregivelse af personoplysninger til modtager-skole, hvis ansøgeren ikke kan optages på Gefion Gymnasium, kan som udgangspunkt ske, hvis ansøgeren er orienteret om det via orienteringsbrevet i punkt 2 ovenfor. Ellers kræver videregivelsen muligvis elev-samtykke.		Skolen	Adm.	
7	Orientering på hjemmesiden om, hvordan man kommunikerer sikkert digitalt med skolen		Skolen	AML/TOR	
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	Adm.	

OPTAGNE ELEVER					
9	Oprettelse af elevsager i DocuNote + oprettelse af kassationskode på ansøgningssagen		GF	Adm.	
10	Generel orientering til elever og forældre om behandling af personoplysninger som led i skolegang	Skabelon **E1a**	Skolen Orienteringen gives på skolens hjemmeside		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 [*] Gymnasium (mail og Lectio) • Brug af skolens it • Brug af apps som led i undervisning • Brug af fx billeder af kammerater	**Elevhåndbog** Eller GF's skabelon til "Husregler for digital undervisning"	Skolen	AML/IT-udvalget	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	AML via gymbetaling	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	Skabelon **E2**	Skolen	AML, DPO	Snarest og senest 1 måned efter anmodningen
IKKE-OPTAGNE ELEVER					
14	Sletning af ikke-optagne ansøgere i Lectio		Skolen	Adm.	

12. 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 Fx via link eller henvisning i det velkomstbrev, der udleveres til brobygningseleverne til sted på skolens hjemmeside om "Generel orientering om behandling af personoplysninger til gæster mv."	Skabelon G15	Skolen	Adm.	

2	Oplysninger om brobygningselever opbevares i et sikkert it-system, fx DocuNote, og slettes 5 år efter det kalenderår, hvori eleven har udløst taxametertilskud[5]		Skolen	Adm.	

13. 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	LWE	

14. 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	E5	Skolen		Kan med fordel ske forud for sidste skoledag
2					
3	Inaktivering af elever i **Lectio**. Sker manuelt. Udløser **kassationskoder i DocuNote** og **GymBetaling**. Sletning af **elevers log-on adgang til Lectio**. Se side 18 ovenfor om hvordan		Skolen	Adm.	Inden 1. august
4	Udtræk af GymBetaling fsva. 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		--	--	
5	Mail til alle **it-leverandører**, der har hentet personoplysninger om eleverne via integration til UNI-login, om at ALLE oplysninger om afgåede elever skal slettes		Skolen Orienteringen kan med fordel gives på skolens hjemmeside		Senest med udgangen af kalenderåret
6	Sletning af alle "løse" personoplysninger om afgåede elever fra diverse it-systemer (mail især). Sker som udgangspunkt manuelt.		Skolen (lærere, administrative medarbejdere,		Senest med udgangen af kalenderåret

[5] Manuelt eller via automatisk kassationsfunktion

			ledere, studievejledere)		
7	Sletning af fotos af afgåede elever		Skolen (kommunikation)	TOR	Snarest muligt
8	Hvis eleven afbryder sit stx-forløb og fortsætter på andet gymnasium: videregivelse af personoplysninger til modtager-skole, hvis der er hjemmel i uddannelses-bkg. Ellers kræver videregivelsen elev-samtykke.		Skolen	Adm.	Løbende

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

- Alle **skabeloner** ligger på GF's hjemmeside: https://www.gymnasiefaellesskabet.dk/gym/index.php/intranet/datasikkerhedintra

- GF's **arbejdsgangsbeskrivelser om brug af personaleoplysninger som led i lønsamarbejdet** ligger på GF's intranet: 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 hans 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 (mhbp. omsorgsdage), lønoplysninger, skatteoplysninger, pensionsforhold, NemKonto, foto, ansættelsesbrev

Følsomme personoplysninger:
Oplysninger om handicap, helbredsdiagnoser, fagforeningsmæssige tilhørsforhold

16. Tjekliste – rekruttering og nyansættelser (TAP)

Nr.	Opgave	Evt. 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	**M0**	Sekretær	BPO	Løbende via rekrutteringsportal	
2	Indstilling af korrekte brugeradgange til rekrutteringsplatformen for ansættelsesudvalget (tidligere medlemmer af ansættelsesudvalg nedlægges som brugere)		Sekretær/ evt. it	Primært BPO	Løbende via rekrutteringsportal	

3	Påmindelse om tavshedspligt til ansættelsesudvalg		Ledelse/ sekretær	BVE, BHB	Ved opstart	
4	Indstilling af automatiserede slette-datoer i rekrutteringsplatformen		Respektive brugere i adm. og ledelse		Ved opstart eller undervejs	Sker automatisk i rekrutteringsportal
5	Sikring af ansøgerens forudgående, skriftlige samtykke til skolens indhentning af straffeattest, referencer og helbredsoplysninger[i]	**M4**	Ledelse/ sekretær	Ledelsen	Undervejs	
6	Brug af krypteret mailforbindelse eller E-Boks til fagforening samt til handicappede ansøgere		Sekretær		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: **M1a** Lang orientering til personale-håndbog: **M1**	Sekretær/ BPO	Står på hjemmeside +ansættelsesbrev	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)	**M3**	Ledelse/ Sekretær/ BPO		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/ BPO		Senest [3 år] efter afslutning af rekrutterings-proces	

17. 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		Skolen og GF i samarbejde/BPO		Ifbm. ansættelse	
12	Generel orientering af medarbejderen om behandling af hans/hendes *egne* personoplysninger som led i ansættelsesforhold	Lang orientering til personalehåndbog: **M1**	Skolen		I ansættelsesbrevet – eller via særksilt orienteringsmail til nuværende medarbejdere	
13	Kvittering for udlån af IT-udstyr Kvittering for udlevering af nøgle/nøglekort	M7 M9	Skolen/MFO		Når udleveringen sker	
14	Udsendelse af (link) til skolens retningslinjer om fx • Sikker digital kommunikation med Gefion Gymnasium (mail og Lectio) • Brug af skolens it • Særlige retningslinjer for medarbejderens arbejdsområde	Se afsnit 1 i Skolehåndbog i behandling af personoplysninger	Skolen	AML, BHB	Ifbm. ansættelse – eller via særksilt 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	**M5** og **M5a** samt **HRdatabasen**	Skolen	Sker via gymbetaling	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	**M2**	Skolen		Senest 1 måned efter modtagelse af oplysningerne	
	Besvarelse af medarbejderens anmodning om indsigt, berigtigelse eller sletning efter reglerne i databeskyttelsesforordningen	**M6**	Skolen	Adm./ledelse	Senest 1 måned efter anmodningen	

18. 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.	Gefion orienteres mhbp. kassationskode på personalesagen GF Løn kontaktes mhbp. koordinering af andre skrivelser til medarbejderen som led i fratrædelse	Så hurtigt som muligt og **helst 14 dage inden sidste arbejdsdag**	**M10**	
2	Inddragelse af nøgle + lukning af låsebrik	Nærmeste leder Pedellen orienteres mhbp. lukning af låsebrik	Senest den sidste ansættelsesdag	Sidste halvdel af kvitteringen for udlevering af nøgler udfyldes **M9**	
3	Aflevering af it-udstyr Alternativt køb af det lånte udstyr til privat eje	Nærmeste leder MFO indgår aftalen om salg pva. skolen	Senest den sidste ansættelsesdag	Kvittering for returnering eller køb anvendes. **M7** eller **M8**	
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/MFO		Gefions forretningsgang for sletning af datamedier T4	
5	Lukning af bruger- og administratoradgange til it-systemer	IT/bruger-administrator	Senest den sidste ansættelsesdag	Gefions 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	Senest den sidste ansættelsesdag	**M11**	
7	Opsigelse af hjemmeopkobling (bredbånd) og telefonabonnement	--	--		
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, HRdatabasen 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	Senest når medarbejderen fratræder	[retningslinjer]	
9	Sletning af medarbejderens foto og kontaktoplysninger fra skolens hjemmeside (samt i googles cache-kopi af hjemmesiden)	IT/TOR	Senest den sidste ansættelsesdag	Ikke relevant	
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		Efter 5 år. Kassationskode påføres, når P-sagen inaktiveres	DocuNote vejledning om sletning i ESDH anvendes	

19. Sådan arbejder vi med personoplysninger i studievejledning på Gefion Gymnasium

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

Gymnasielovens § 59, stk. 1: For at fastholde elever i uddannelse og sikre et sundt læringsmiljø skal institutionen i samarbejde med Ungdommens Uddannelsesvejledning og eventuelt Studievalg yde bistand til de elever, der har behov herfor […].

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 […].

1. Behandling af personoplysninger som led i fastholdelsesvejledningen

På baggrund af ovenstående hjemmel kan vi behandle følgende personoplysninger i den del af studievejledningen, 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
- 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.

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 Gefion Gymnasium har vi prioriteret at kunne hjælpe eleverne med de ting, de betror studievejlederen, 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 GymBetalingen, hvor studievejlederen 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.

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

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

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 studievejlederen 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:

Vilkår eller ydelse	Studievejlederen 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"	STX-bkg. § 51
Sygeundervisning	"Oplysninger om sygdom, der medfører at eleven i længere tid ikke kan følge den almindelige undervisning" må registreres med henblik på "tilpasning af sygeundervisningen med elevens helbredstilstand"	STX-lovens § 62 og STX-bkg. § 52 - 56
Udeboende SU	Oplysninger der dokumenterer, at de betingelser, der er nævnt i § 19 om "ganske særlige forhold i hjemmet, fx sygdom, mv. er til stede. Skolen kan bl.a. til brug for sin afgørelse indhente en udtalelse fra de sociale myndigheder	SU-bkg § 19
Re-eksamen	Oplysninger om "dokumenteret sygdom" = lægeerklæring	Alm.eks.bkg § 9
Eksamen på særlige vilkår	Oplysninger om eksaminandens "fysiske eller psykiske funktionsnedsættelse, når det er nødvendigt for at ligestille eksaminanden med andre"	Alm.eks.bkg § 19

3. Særligt om ansøgning om SPS

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

4. Brug af it-systemer til studievejledning

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.

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 studievejlederen er MEGET omhyggelig med sletningen bagefter.

Brugeradgange til studievejledningsmapperne i DocuNote gives til studievejlederne på årgangen af nærmeste leder og/eller kontoret (BPO).

Kun de medarbejdere, der varetager studievejledning 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. Dette gøres af kontorleder, BPO og/eller uddannelsesleder AML.

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 ledelsen og kontorlederens side, om loggen udviser aktivitet, som ikke modsvares af de opgaver, medarbejderne er pålagt som led i tjenesten.

<u>Sletning af oplysninger fra studievejledningen</u>

Studievejledningsmapperne i DocuNote slettes automatisk, når eleven er blevet student eller har forladt skolen som konsekvens af elevens inaktivering i systemet.

<u>Brug af e-mail som led i studievejledning</u>

Hvis studievejleder på digital vis har brug for at kommunikere om fortrolige personoplysninger (cpr-numre) eller følsomme personoplysninger (helbredsdiagnoser), **sker det fortrinsvist via krypteret Rmail på skolens mail-server.**

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.

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

For at få sikre sletning af mailen gøres følgende:

- Mailen gives en autotekst, der hedder "denne mail indeholder fortrolige eller følsomme personoplysninger og derfor skal du slette den, når du har læst den"

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.

5. Øvrige retningslinjer for medarbejderes behandling af personoplysninger på Gefion Gymnasium

Som medarbejder på Gefion Gymnasium har du pligt til at omgås oplysninger, viden og information er med omtanke. Al information, der relaterer sig til personer (medarbejdere, elever, ansøgere, pårørende, bestyrelsesmedlemmer eller andre) er fortrolig og må ikke deles med nogen udenfor Gefion Gymnasium. Dette fremgår af alle medarbejderes ansættelseskontrakt med Gefion Gymnasium og følger også af forvaltningsloven og straffeloven.

Alle medarbejdere på Gefion Gymnasium er således omfattet af følgende tavshedsklausul:

Tavshedspligt

Medarbejderen har tavshedspligt med hensyn til alle forhold, som denne erfarer om Gefion Gymnasium og skolens ledelse, medarbejdere, elever, ansøgere, pårørende, bestyrelsesmedlemmer eller andre personer. Dette betyder, at medarbejderen hverken må anvende eller viderebringe oplysninger til andet end de tjenstlige opgaver, som medarbejderen er pålagt, og at medarbejderens personlige interesse i en sags behandling eller resultat ikke berettiger medarbejderen til at gøre sig bekendt med sådanne oplysninger, fx via EDSH, som medarbejderen af tjenstlige årsager i forvejen har adgang til.

Tavshedspligten følger af forvaltningsloven og straffelovens regler om tavshedspligt i offentlig tjeneste og gælder såvel under ansættelsesforholdet som efter dettes ophør.

Brud på tavshedspligten under ansættelsen betragtes som grov misligholdelse af ansættelsesforholdet og kan medføre ophør af ansættelsen (herunder ved øjeblikkelig bortvisning).

6. Ordlyden af det samtykke til studievejledning, som Gefion Gymnasium beder eleverne (og forældre til elever under 18 år) om

Registrering af personoplysninger af følsom karakter som led i studievejledning

Spørgsmål: Må skolen registrere og behandle de følsomme personoplysninger om trivsel og helbred, som du selv giver skolen som led i studievejledningen?

Følgende oplysninger om dig behandles, hvis du siger ja: - Almindelige og følsomme personoplysninger, jf. databeskyttelsesforordningen art. 4, stk. 1 og art. 9.

Formålet med den påtænkte behandling: - Studievejlederen kan tale med dig om de ting, der kan true din skolegang og fastholdelse, fx dine fraværsårsager, årsager til dårlig trivsel, sociale problemer, helbredsproblemer, mv., hvis du selv ønsker det - På den baggrund kan studievejlederen støtte og begrunde, at du evt. har behov for fx godskrivning af fravær i en periode, pædagogiske hjælpemidler eller lignende. På den måde kan studievejlederen hjælpe med til at øge dine muligheder for at gennemføre fag og uddannelse i svære situationer

Konsekvens hvis du svarer "nej": - Studievejledningen vil ikke omfatte følsomme personoplysninger og vil derfor blive givet på et mere overordnet niveau - Dette kan fx betyde, at skolen ikke kan støtte dig lige så godt, som hvis vi måtte behandle følsomme personoplysninger om fx trivselsproblemer og helbredsdiagnoser om dig Konsekvens hvis du senere ændrer et "ja" til et "nej": - De følsomme personoplysninger om dig, som skolen evt. allerede har registreret som led i studievejledningen, vil blive slettet. Dog slettes de ikke, hvis skolen ifølge særskilt hjemmel har opbevaringspligt for at kunne dokumentere dine forhold overfor tilsynsmyndigheden eller overfor de sociale myndigheder. I så fald slettes oplysningerne, når denne dokumentationspligt er ophørt.

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

Som led i kommunikationsopgaven på Gefion 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: FB, Instagram og YouTube
c) I trykte publikationer og på plakater ifb. med vores Orienteringsaften
d) På skolens info-skærme
e) I artikler eller indslag i dagblade, aviser og på tv

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

Skolens offentliggørelse af fotos på internettet forudsætter, at der er hjemmel til offentliggørelsen. Som offentlig institution kan skolen behandle (vise/offentliggøre) de billeder, der er "nødvendige af hensyn til 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 Gefion 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 a, jf. ovenfor – eller om der skal indhentes samtykke.

"Panorama-agtigte" 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 afbilledet på sådan et billede senere gør indsigelser mod visningen af billedet på fx hjemmesiden, skal det som altovervejende hovedregel fjernes fra hjemmesiden igen med mindre 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 kan altid **tilbagekaldes** af eleven/medarbejderen.

Praktik

Elevernes samtykke til visning af fotos/videoer gives i Gymbetaling.

I Gymbetaling er de spørgsmål, som eleverne skal besvare, formuleret som nedenfor.

Leder af IT er ansvarlig for formuleringen af spørgsmålene, så de passer til skolens behov og sende dem ud.

Skolens kommunikationsmedarbejder er ansvarlig for at tjekke Gymbetaling og være opmærksom på negativ-listen i forhold elever der ikke har givet samtykke når der skal publiceres ift. kommunikationsafdelingen.

Sletning

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

Sletning af indhold fra Facebook og andre sociale medier står **skolens kommunikationsmedarbejder** for. Billedalbums og andre billeder på Facebook, der er + 3 år gamle, slettes. **Skolens kommunikationsmedarbejder** gør det.

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

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.

Kære elev

Gefion Gymnasium har brug for dine svar på spørgsmålet nedenfor. Spørgsmålet handler om, om Gefion 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.

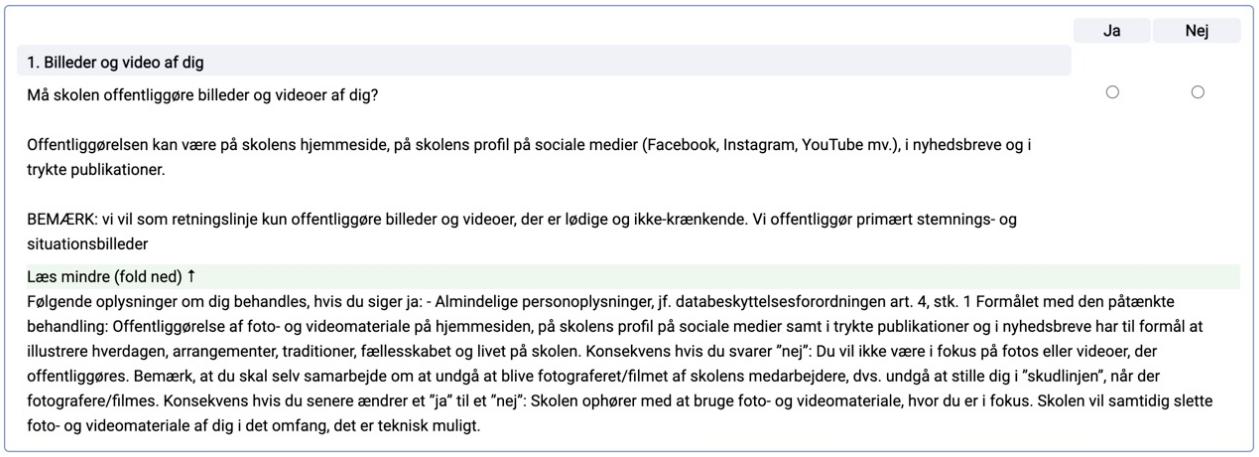
Hvis et kryds i "nej" medfører, at du går glip af visse ydelser fra skolens side, fremgår det i fold ud-menuen under spørgsmålet.

Obligatoriske oplysninger fra Gefion Gymnasium til dig:

• Gefion 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".

Hvis du har spørgsmål, kan du kontakte uddannelsesleder Andreas Lange i skolens administration (aml@gefion-gym.dk).



	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 og i trykte publikationer.

BEMÆRK: vi vil som retningslinje kun offentliggøre billeder og videoer, der er lødige og ikke-krænkende. Vi offentliggør primært stemnings- og situationsbilleder

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: 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, fællesskabet og livet på skolen. Konsekvens hvis du svarer "nej": 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 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.

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

Elever u/ 18 år

Når man som rejseansvarlig lærer planlægger en studierejse til udlandet med elever u/ 18 år, undersøges der, om der er krav til skriftligt samtykke. 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. Pt. ved vi positivt, at Irland og USA stiller samtykke- og dokumentationskrav.

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

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

Både op til og under hele rejsen er det dog elevens opgave selv at opbevare dokumentationen i det omfang, *det er påkrævet*, 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 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 i visse lande udenfor EU

Går studierejsen ud af EU eller EØS [6, 7] indebærer rejsen, at der sker såkaldt "overførsel af personoplysninger om rejsedeltagerne til et – i persondatabeskyttelsessammenhæng – usikkert land".

Gefion 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.

[6] Norge, Island og Liechtenstein.

[7] Følgende lande er "sikre" lande udenfor EU/EØS: Andorra, Argentina, Australien (passageroplysninger som led i flyrejser), Canada, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz, Urugua.

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

22. TV-overvågning – interne retningslinjer (TAP)

På Gefion 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?
Formålet 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, nr. 2.

Hvor behandles dine personoplysninger?
De personoplysninger, som Gefion Gymnasium behandler, vil blive behandlet og opbevaret i skolens it-systemer som kun få af skolens medarbejdere har adgang til. Optagelser fra tv-overvågning opbevares i løbende 30 dage, hvorefter de slettes.

Dine rettigheder
Retten til at få orientering om behandling af dine personoplysninger: Du har ret til at få oplyst, at vi behandler personoplysninger om dig og hvorfor, jf. artikel 13 og 14 i databeskyttelsesforordningen. Disse oplysninger får du her. Hvis du ønsker mere udførlige oplysninger, er du altid velkommen til at kontakte skolen på info@gefion-gym.dk eller skolens databeskyttelsesrådgiver (se kontaktoplysninger nedenfor).

Retten til indsigt
Du kan få indsigt i, hvilke personoplysninger vi behandler om dig, hvad formålet med behandlingen er, hvor længe vi opbevarer personoplysningerne om dig, hvor vi har oplysningerne fra (hvis vi ikke har modtaget dem fra dig) samt hvem vi evt. videregiver dine oplysninger til, jf. art. 15 i databeskyttelsesforordningen.
Din ret til indsigt kan dog være begrænset, hvis hensynet til private interesser, fortrolighed om tredjemands oplysninger eller tavshedspligt i den offentlige forvaltning kræver det, jf. databeskyttelseslovens § 22.

Retten til indsigelse
Du kan gøre indsigelse mod vores behandling af dine personoplysninger og eventuelt kræve,
at oplysningerne bliver slettet, berigtiget eller begrænset, jf. artikel 21 i databeskyttelsesforordningen.

Retten til berigtigelse
Du kan få rettet eller suppleret personoplysninger om dig, som er forkerte eller ufuldstændige, jf. artikel 16 i databeskyttelsesforordningen.

Retten til begrænsning af behandlingen
Du har ret til at få begrænset vores behandling af dine personoplysninger,
hvis der er særlige grunde til det, jf. artikel 18 i databeskyttelsesforordningen.
Retten til sletning
Vi opbevarer tv-optagelserne i 30 dage, hvorefter de slettes automatisk. Vi har fastsat dette

tidsrum ud fra hensynet til selve formålet med tv-overvågningen. Du kan ikke umiddelbart få slettet optagelse af dig efter kortere tid, end de 30 dage.

Sådan gør du brug af dine rettigheder
Du skal kontakte skolen ved at skrive til skolen på info@gefion-gym.dk
eller skrive til skolens databeskyttelsesrådgiver på pfh@GFadm.dk. og oplyse, hvilken ret, du ønsker at gøre brug af og hvorfor. Vi vil herefter undersøge, om vi er enige med dig i dit ønske. Hvis vi ikke umiddelbart er enige, hører du fra os med en begrundelse for, hvorfor dit ønsker ikke kan imødekommes. Du vil i så fald få lejlighed til at udtale dig, før vi træffer endelig afgørelse om, hvorvidt dit ønske vil blive imødekommet. Vores afgørelse herom skal følge forvaltningslovens regler om høring, begrundelse og klagevejledning, jf. forvaltningslovens §§ 19–25.

Formalia
Gefion Gymnasium er dataansvarlig for de behandlinger af personoplysninger, vi har beskrevet ovenfor. Hvis du har spørgsmål eller ønsker at gøre brug af dine rettigheder, som er beskrevet ovenfor, kan du kontakte skolens ved at skrive til info@gefion-gym.dk eller ved at skrive til skolens databeskyttelsesrådgiver på ansc@itcfyn.dk.

Klageadgang
Du kan klage over Gefion Gymnasiums behandling af dine personoplysninger til Datatilsynet.

Orientering om tv-overvågning

Skolen skal på eget initiativ give **meddelelse** til de personer, om hvem oplysninger indsamles, jf. GDPR art. 13. Gefion 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** (OBS på 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

Gefion Gymnasium har besluttet, at det er skolens tekniske personale samt skolens ledelse, der har brugeradgang til at gennemse tv-overvågningen. Brugeradgangene ajourføres 1. gang årligt og/eller ifbm. stillingsændringer og fratræden.

Skolen har overvejet, om tv-overvågningen er **proportionel** eller om det ønskede formål (at forebygge kriminalitet, understøtte bygningsdriften og højne trygheden) kan nås 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 afbillede personer, hvis formålet er kriminalitetsopklaring.

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 at sørge for, at data efterfølgende bliver slettet. Skolens ledelse og tekniske personale aftaler indbyrdes, hvordan arbejdsfordelingen foregår i denne forbindelse.

Alle tv-optagelser hostes, ejer og supporteres selv af skolen (Gefion).

Skolens system er registreret i politiets database.

Der er tydeligt skiltet, hvor der er overvågning.

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

Gefion Gymnasium bruger eksterne it-leverandører til at levere, drive og/eller vedligeholde it-systemer og/eller it-infrastruktur.[8]

Gefion Gymnasium har en oversigt over it-leverandører og deres leverance til Gefion Gymnasium. Oversigtsarket er placeret i DocuNote.

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 Gefion Gymnasium.

Derfor skal alt samarbejde med eksterne it-leverandører af it-systemer, der skal indeholde personoplysninger, begynde med, at Gefion Gymnasium vurderer, om den påtænkte nye it-leverandør har et niveau af it-sikkerhed og dataetik, som Gefion Gymnasium er tryg ved.

På Gefion Gymnasium er det datasikkerhedstovholderen der sørger for, at der holdes styr på, hvilke it-leverandører, vi bruger[9] – og at de overholder kravene.

Bemærk, at vores administrative it-fællesskab IT Center Fyn årligt leverer en såkaldt ISAE 3402 type 2-erklæring om sikkerheden i de it-leverancer, som fællesskabet leverer til os.[10]

Tilsvarende skal leverandører af studieadministrative it-systemer (Lectio) 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 Gefion Gymnasium kan anvende systemet.[11] Erklæringen kan findes på https://www.stil.dk/administration-og-infrastruktur/systemrevision-af-studieadministrative-systemer/oversigt-over-systemer-omfattet-af-erklaeringer.

For de statslige systemer Navision Stat, IndFak og Statens Lønsystem SLS, som Moderniseringsstyrelsen stiller til rådighed for Gefion Gymnasium, skal Gefion Gymnasium til brug for revisionen indhente ledelseserklæringer fra Moderniseringsstyrelsen om styrelsens udviklings-, drifts- og

---

[8] Eksempler på eksterne it-leverandører er Gymnasiefællesskabet, Moderniseringsstyrelsen fsva. bl.a. SLS og Navision, samt leverandørerne af Lectio, Gyldendals Røde Ordbøger, Gymnasiejob, leverandøren af netforbindelse, back up, mv.

9 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 datapakker i UNI-logins administrationsmodul vælger [*] Gymnasium, hvilke personoplysninger, It-leverandøren må få om vores 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.

[10] IT-fællesskabernes pligt til at levere erklæringen følger af bilag 1 i bekendtgørelse nr. 956 af 06/07/2017 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.

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

vedligeholdelsesydelser vedrørende systemerne. Ledelseserklæringerne sendes elektronisk til Gefion Gymnasium af Moderniseringsstyrelsen. [12]

Gefion Gymnasiums revisor har pligt til at påse at de nævnte revisionserklæringer er indhentet af Gefion Gymnasium og at Gefion Gymnasium har forholdt sig til indholdet i erklæringerne[13].

På Gefion Gymnasium er det datasikkerhedstovholderens opgaver, at

- Føre listen i over Gefion Gymnasiums it-systemer og it-infrastruktur, der leveres, drives eller vedligeholdes af en ekstern leverandør/it-fællesskab/databehandler/konsulent.
- 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 Gefion Gymnasium, jf. punkt 8 ovenfor*
- Følge op på, at den eksterne it-leverandør (og konsulenter) sletter Gefion Gymnasiums forældede personoplysninger

[12] Moderniseringsstyrelsens pligt til at levere erklæringen følger af bilag 1 i bekendtgørelse nr. 956 af 06/07/2017 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.

[13] Jf. bilag 1, afsnit 2.6 i bilag 1 i bekendtgørelse nr. 956 af 06/07/2017 om revision og tilskudskontrol m.m. ved institutioner for erhvervsrettet uddannelse, almengymnasiale uddannelser og almen voksenuddannelse m.v

24. Gefion 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.

Brugeradgange og rettigheder hvilket administreres og vedligeholdes af datasikkerhedstovholderen, 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:

- **[beskrivelse af drev og systemer] SE ROSKILDE GYMNASIUMS BOG!**

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

- DocuNote

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

- GoogleSuite
- Lectio

25. IT-systemer og it-services som Gefion Gymnasium selv ejer, hoster og/eller vedligeholder (IT-administrator)

[Hvis skolen selv og driver egne it-systemer, som indeholder personoplysninger, skal skolen have en beskrivelse af systemet samt de opgaver, der knytter sig til at vedligeholde og håndhæve sikkerheden i systemet.

Der bør således foreligge en skriftlig beskrivelse af systemets opbygning, funktioner, administratorkonti- og rettigheder, tildeling af brugerautorisationer og -rettigheder, funktionsadskillelser mellem forskellige brugerkonti, alarmer i systemet ved forsøg på ikke-autoriseret brug, hvordan oplysninger i systemet slettes igen, systemlogning (hvis systemet fx indeholder CPR-numre og/eller helbredsdiagnoser eller har fritekstfelter), sikkerheden omkring systemet herunder hvilken server systemet ligger på, om der tages back up af denne server, mv.]

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

Det er den øverste ledelse (bestyrelsen), der har det endelige ansvar for at Gefion 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 medarbejdergrupper[14]

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 medarbejdere 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)[15]. Se beskrivelse af indholdskravet til fortegnelser i FAQ'ens afsnit
- At der samarbejdes aktivt med skolens **DPO**[16]
- At 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 og evt. også de registrerede personer indenfor 3 døgn fra bruddet er opdaget
- At 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.
- At der foreligger skriftlige **databehandleraftaler** med it-leverandører
- At organisationen er orienteret om **retningslinjer for databeskyttelse**, herunder om, hvilke it-systemer og værktøjer der må bruges
- At der sker **orientering af de registrerede** om deres rettigheder

27. Risikovurdering (Ledelse)

Datasikkerhedstovholder på Gefion 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

[14] Ledelsen kan støtte sig til GF's "Ledelsens Top 8" som tjekliste
[15] GF's skabeloner findes her
[16] GF's ydelseskatalog for DPO-funktionen findes her

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 datas (herunder personoplysningers) fortrolighed og ægthed samt sikrer datas tilgængelighed for de autoriserede brugere og skolens kontrol over egne data.

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
-

Gefion Gymnasium ønsker ikke at sikre sig for enhver pris, men ønsker at være bevidst om enhver risiko, og forholde sig tilfredsstillende til disse, 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 fsva. brugen af digitale læremidler.

Eleverne orienteres endvidere i en Elevhåndbog[17] om skolens arbejde med risikonedbringende foranstaltninger samt hvad eleverne selv skal være opmærksomme på når de bruger digitale læremidler. Endelig oplyses eleverne om, hvor de kan henvende sig, hvis de støder på konkrete problemer med fx apps, der beder om persondata fra elevens it-udstyr (fx adgang til kontakter, fotos, mv.)

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

Kapitel 3 – FAQ

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

28. Hvilke personoplysninger kommer en skole typisk i kontakt med og hvad er de vigtigste opmærksomhedspunkter?

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,

29. 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. figur ovenfor. Jo mere fortrolig eller følsom en personoplysning er, jo bedre skal skolen passe på den.

30. Hvad vil det sige, at "behandle" personoplysninger?
Begrebet "behandling af personoplysninger" dækker over alt, hvad man kan udsætte en personoplysning for med digitale redskaber, dvs. indsamling, registrering, systematisering, læsning, søgning, redigering, kopiering, kryptering og sletning.

31. Hvad er "almindelige personoplysninger" og hvornår må en skole behandle dem?
Almindelige personoplysninger er de personoplysninger, der fremgår af bunden af tabellen ovenfor.

De "almindelige personoplysninger" må behandles af skolen, hvis mindst en af følgende betingelser er opfyldt[18]:

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, jf. afsnit [*] 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.

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

32. Er nogen typer af data i relation til medarbejderne, som arbejdsgiveren ikke må gemme på?
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 gigt-diagnose for at kunne spørge interesseret ind til "hvordan det går" – med mindre der er givet samtykke (fra hustruen vel at mærke). Ligeledes må 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.

33. Hvilke behandling 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 "kødkataloget"/"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

34. 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 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

35. 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.

36. 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 f.eks. 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. [19] Dette gælder anset 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 flex-job, jf. litra f) ovenfor.

37. 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 E-Boks.

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 (ESDH), der (i modsætning til mailsystemet) er egnet til at samle (ikke sprede) oplysninger samt bevare fortroligheden omkring dem, herunder via adgangs- og brugerstyring, systemlogningsfunktion og slettefunktion.

38. 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 § 23, er det udgangspunktet, at oplysningerne ikke er af fortrolig karakter.

39. 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 E-Boks.

[19] Jf. Forslag til databeskyttelseslov § 12 og forarbejdernes side 138

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.

40. Må et skolen offentliggøre fotos af sine elever på sin hjemmeside, på sociale medier, i en årbog eller på en plakat?

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.

"Panorama-agtigte" 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 afbilledet 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 afbillede person om behandlingen af dennes personoplysninger, fx ved offentliggørelse på hjemmesiden. Skolen har denne orientering på sin hjemmeside under punktet "Sådan behandler vi personoplysninger om …".

41. Hvad er "den registreredes rettigheder"?

Den registreredes rettigheder kan illustreres på følgende måde:

- Medarbejderen/eleven har ret til at få **orientering** om, at hans personoplysninger behandles
- Medarbejderen/eleven har ret til at blive **orienteret om brud** på datasikkerheden, hvis det berører hans/hendes data

- Medarbejderen/eleven har ret til **indsigt** i, hvilke personoplysninger, der konkret behandles om ham
- Medarbejderen/eleven har ret til at få **berigtiget** urigtige personoplysninger om ham
- Medarbejderen/eleven har – i visse (få) tilfælde – ret til at få sine personoplysninger **slettet**

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.

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 samt værge) om følgende:

- At Gefion 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 mht. 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.

3.1 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 oplysningerne oprindeligt var tiltænkt, skal den registrerede person orienteres herom forud for viderebehandlingen[20].

[20] Art. 10.

42. 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.

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 anmode om berigtigelse, sletning, begrænsning og indsigelse, muligheden for at klage over behandlingen til Datatilsynet samt kilden til oplysningerne, hvis de ikke kommer fra den registrerede person selv.

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

Inden der udleveres oplysninger til 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.

3.2 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 egen 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.

3.3 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 E-Boks.

3.4 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
- 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 (fsva. 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 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 (fsva. oplysninger om brugertrafik og indhold): print gives eller personens egen adgang anvendes (hvis der er 100 % indsigt i egne oplysninger i systemet for brugeren)

43. 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 persons anmodning om berigtigelse af dennes personoplysninger er en forvaltningsafgørelse, der kræver høring, begrundelse og klagevejledning.

44. 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 en 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.

45. 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 opnå det oprindelige formål, hvis den registrerede person kalder et samtykke tilbage (og der herefter ikke er et andet grundlag for behandlingen), hvis den registrerede gør berettiget indsigelse mod behandlingen eller hvis behandlingen i det hele taget er ulovlig.

Bemærk, at der dog ikke skal ske sletning, hvis skolen har fx administreret følsomme personoplysninger på baggrund af et gyldigt samtykke til fx SPS-ansøgning og på den baggrund 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) overfor 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" for at underrette de eksterne parter, som behandler personoplysningerne (fx Google), om at slette alle link til eller kopier eller gengivelser af de pågældende personoplysninger.

46. 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 HRDatabasen (medarbejdere).

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

47. 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.

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

48. Hvad er en "databehandler" og hvad betyder det for dataansvaret at bruge en databehandler?
Den dataansvarlige skole kan outsource behandlingen af persondata til en databehandler, hvilket er en it-leverandør, der ejer, driver eller vedligeholder de it-systemer, som skolen har valgt at tage i brug.

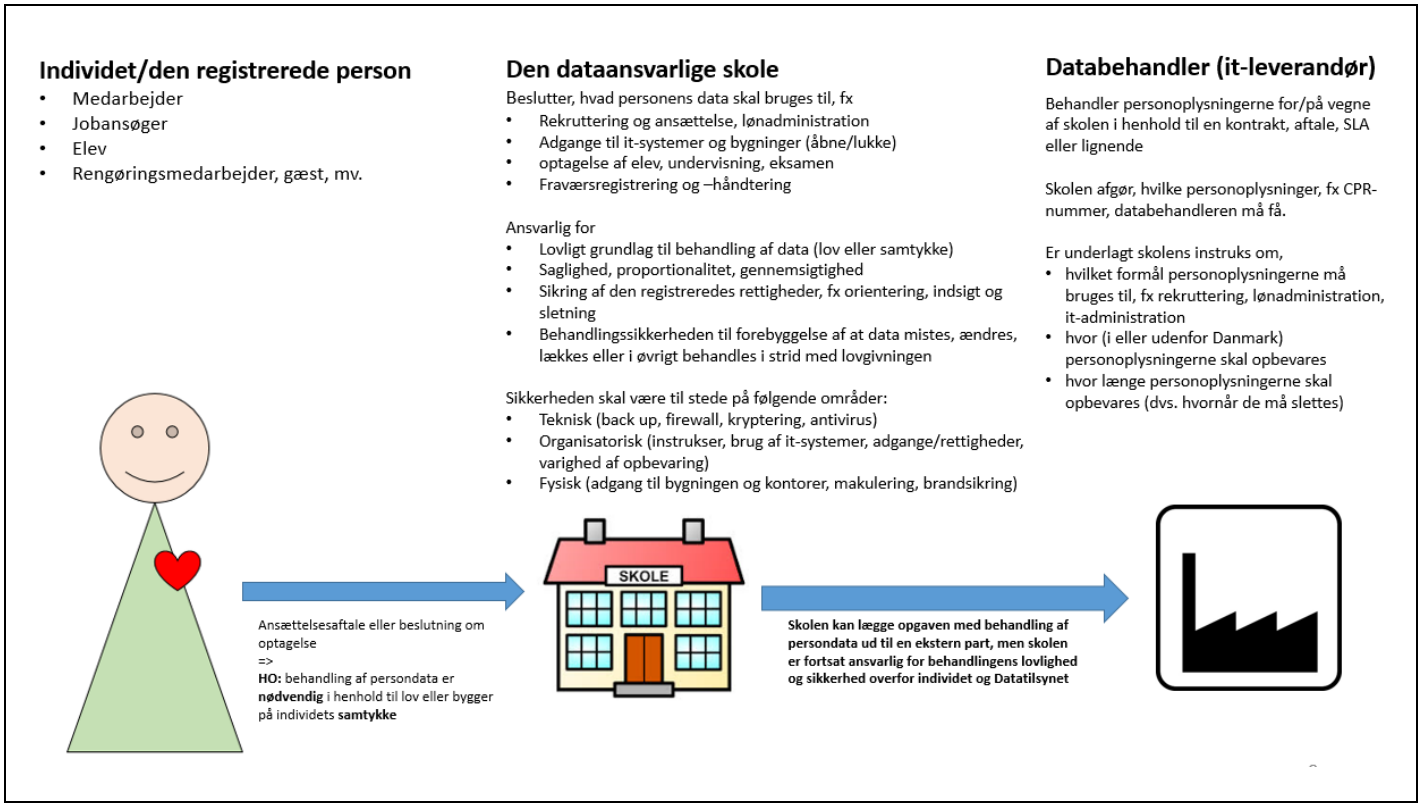
Herved lægges opgaven med behandling af data (fx administration af oplysninger som led i medarbejderrekruttering) ud til en ekstern part (fx Gymnasiejob). Ansvaret for at personoplysninger om ansøgerne behandles lovligt og kun til det tiltænkte rekrutteringsformålet er imidlertid stadig den dataansvarlige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

Databehandleren behandler altså blot personoplysningerne på vegne af skolen. 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 man som skole gør sig klart

- At den dataansvarlige skole har ejerskabet til personoplysninger om elever og medarbejdere og suverænt afgør, hvad oplysningerne skal bruges til og hvor længe
- At skolen stå til ansvar for behandlingens lovlighed overfor den registrerede medarbejder eller elev uanset om behandlingen af dennes personoplysningerne sker på skolen eller ude hos en databehandler
- At ejerskabet derfor skal kunne håndhæves og behandlingen af personoplysningerne skal kunne kontrolleres – selvom behandlingen sker hos en databehandler
- At skolen derfor skal overveje nøje, 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

Rolle- og ansvarsfordelingen, når skolen vælger at lægge opgaver med it-drift, vedligeholdelse og administration ud en til ekstern leverandør, kan illustreres med følgende model:



49. 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.

Databehandleraftalen er en del af den samlede kontrakt med it-leverandøren[21]. 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 indenfor 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. 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

[21] I stedet for en it-leverandør kan der være tale om en ad hoc konsulent. I så fald skal denne afgive fortrolighedserklæring.

den lille pakke, idet de større pakker indeholder CPR-nummer og idet det har formodningen mod sig, at CPR-nummer er nødvendigt for databehandleren.

Skolen skal løbende følge op på, om databehandleren efterlever kontrakten. Dette kan ske ved at indhente en ledelses- eller en revisionserklæring (fx en ISAE 3000[22] eller 3402[23]). Kravet om en sådan erklæring skal fremgå af kontakten 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 slettes 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.

Sletteplig ten er særligt svær i systemer, der har deling af dokumenter og oplysninger som funktionalitet, fx google docs mv.

50. Skolens sletning af personoplysninger – hvordan og hvornår?
Den dataansvarlige skole skal være i stand til at slette de personoplysninger, som ikke længere må behandles.[24]

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

Det er afgørende vigtigt, at sletning også sker hos databehandlere, 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.

3.5 Elevoplysninger

Oplysninger om elever slettes *enten*, når eleven anmoder (og skolen finder anmodningen berettiget), *eller* efter følgende retningslinjer (åremålet regnes fra eleven har forladt skolen)[25]:

---

[22] 3000-erklæringen afdækker om den databehandlende virksomhed 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.

[23] 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.

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

[25] 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-

Identifikationsoplysninger (navn og CPR-nr.), oplysninger om studieretning og indskrivningsperioder	Ingen slettefrist. Dog skal sletning ske ved meddelelse om den studerendes død	
Eksamensbevis samt oplysninger der er nødvendige for at generere et eksamensbevis	30 år	§ 38, stk. 1, i den almene eksamensbekendtgørelse
Oplysninger, der er nødvendige for at udstede attestationer for gennemført undervisning (merit)	5 år	
Oplysninger om elever af betydning for årsrapporten (fx oplysninger om elevbetalinger til fester, begivenheder og studieture (beløb, dato og elev)	5 år	Bogføringslovens § 10
Oplysninger om SPS (søgning om tilskud til samt administration af midler)	5 år	§ 14 i SPS-bkg.26
Oplysninger om SU	5 år	SU-Styrelsens udmelding
Alle andre elevoplysninger	Kan (i princippet) slettes når eleven forlader skolen (dog i praksis ved udgangen af kalenderåret)	
Logningsdata af elevers internettrafik på skolens netværk samt i it-systemer	6 måneder fra de er registreret	Sikkerhedsbekendtgørelsens § [*]
TV-overvågning	Max 30 dage fra optagelsen	

47.2 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	

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.

[26] Bekendtgørelse om særlige tilskud til specialpædagogisk bistand ved ungdomsuddannelser m.v. nr. 1377 af 09/12/2013

	U: hvis samtykke til længere opbevaring[27]	
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 er en forvaltningsretlig afgørelse, som skal indeholde en høring, begrundelse og klagevejledning.	
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[28] slettes ikke, da der kan være afleveringspligt til Statens Arkiver[29] U2: hvis der verserer arbejdsskadesag, retssag eller arbejdsretlig tvist mellem medarbejderen og arbejdsgiver, slettes personalesagen først 3 år efter den pågældende sag er afsluttet.	

[27] Hertil benyttes GF's blanket M3

[28] 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

[29] 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.

51. 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.

Fortegnelsen erstatter den nuværende anmeldelsesordning af visse behandlingsaktiviteter til Datatilsynet, som udfases. Skolens tidligere anmeldelse til Datatilsynet kan i vidt omfang kan danne udgangspunkt for fortegnelsen.

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 dokumentere, 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.

<u>Indholdskrav til skolens fortegnelse:</u>

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
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.

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

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

a. 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.

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

53. 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.

54. 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.

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

Fra den 25. maj 2018 skal alle statsligt selvejende gymnasieskoler have en databeskyttelsesrådgiver.

DPO'en i ITC FYn kan kontaktes på pfh@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 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 og ved gennemgang og udarbejdelse af databehandleraftaler, risikovurderinger og løbende kontrol med databehandlere.

56. Hvad ligger der i at sikre skolens "behandlingssikkerhed vedr. personoplysninger"?
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 ifht. overholdelsen af de beskrevne retningslinjer
- Instruktion fra den dataansvarlige til de medarbejdere, som behandler personoplysningerne om, hvordan systemerne bruges korrekt
- Medarbejdernes systematisk 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 mindst hver 6. måned opdateres til et nyt personligt unikt password bestående af mindst 8 tegn, hvori bør indgå både store/små bogstaver samt tal.
- Tydelige, skriftlige vilkår for udlån, brug og returnering af digitale arbejdsredskaber, som underskrives af den medarbejder, der låner udstyret, samtidig med udlevering af udstyret.
- Lås på de steder, hvor der foretages behandling af personoplysninger med henblik på at forhindre uvedkommendes adgang
- Kryptering af personoplysninger der sendes via e-mail (sikker mail eller E-boks)
- 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