Løbende retningslinjer for behandling af personoplysninger

Indhold

Skolen skal sikre tekniske, fysiske og organisatoriske foranstaltninger, der giver et passende sikkerhedsniveau for de personoplysninger, som behandles. Dette kapitel indeholder Gefion Gymnasiums retningslinjer til medarbejderne om persondatabeskyttelse og informationssikkerhed.

Retningslinjerne er væsentlige at kende og efterleve, fordi lovgivningen stiller krav om, at vi på Gefion Gymnasium kan redegøre for vores persondatabeskyttelse og informationssikkerhed, og fordi den digitale forvaltning, det øgede antal adgangsmuligheder, nye platforme og funktionaliteter for både elever, forældre og medarbejdere ikke udelukkende er en positiv ressource, men også indebærer en risiko for, at personoplysninger spredes, lækkes, bruges til uvedkommende formål, ikke bliver slettet, når deres formål er udtjent mv.

Retningslinjerne udarbejdes, ajourføres, implementeres og kontrolleres overholdt af ledelsen på Gefion Gymnasium.

Risikovurdering
Ledelsen på Gefion Gymnasium foretager en overordnet vurdering af sikkerheden i de IT-systemer, som er væsentlige for skolens drift.

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
- Eventuelle tidligere sikkerhedsrelaterede 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 at forholde sig tilfredsstillende til disse, hvormed et tilstrækkeligt sikkerhedsniveau etableres. Sikkerhedsniveauet fastlægges ud fra en afvejning af, hvilke og hvor mange personoplysninger der er tale om, ressourceforbruget ved etableringen af sikkerheden samt konsekvenserne af uønskede hændelser, herunder risikoen for de registrerede personer ved et evt. datalæk.

Retningslinjer for datasikkerhed
Nedenstående retningslinjer skal efterleves af alle ansatte.

1. Brug **passwords** (eller fingeraftryk som adgangskode) på computer, smartphone mv. og opdater med et nyt, unikt password, når systemet beder om det (hvilket på computeren er efter max 90 dage). **Memorér** password, 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 password, mens computeren er koblet til en storskærm eller lignende, hvor passwordet kan aflures.

2. **Lås altid skærmen,** når computeren forlades

3. **Fysiske dokumenter,** der indeholder fortrolige eller følsomme personoplysninger, skal opbevares sikkert, fx i aflåst skuffe/skab, eller på administrations-/studievejledningskontoret, hvor der kun er adgang for en begrænset personkreds. Dokumenter, der opbevares på de to kontorer, skal desuden som minimum lægges med de fortrolige oplysninger nedad, når de ikke bruges.

4. Fysiske dokumenter med fortrolige eller følsomme personoplysninger skal altid bortskaffes ved **makulering**. Kontakt kontoret.

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

6. **Mails** med fortrolige og følsomme personoplysninger skal altid sendes til e-Boks eller med krypteret mail. *Mails fra xxx@gefion-gym.dk-adresser er som udgangspunkt altid krypteret (TLS).*

7. Der må ikke bruges andre mailkonti end medarbejderens officielle skolemail til skolerelateret indhold. *Derfor må der aldrig laves videresendelsesregler eller videresende til andre personlige mailkonti (fx hotmail og lignende).*

8. Det anbefales at filer eller mails med fortrolige eller følsomme personoplysninger **arkiveres** i DocuNote. I praksis opbevares og behandles mange fortrolige og følsomme oplysninger midlertidigt i andre (ikke godkendte) systemer. Når dette er tilfældet, skal oplysningerne hurtigst muligt slettes eller overføres til et godkendt system. Som udgangspunkt bør oplysningerne ikke opbevares i ikke- godkendte systemer mere end én måned efter,

sagsbehandlingen er afsluttet. Alle medarbejdere har pligt til løbende at sikre, at dette overholdes. Husk også løbende at tømme computerens papirkurv.

9. **Slet** sager og oplysninger, herunder personoplysninger, der ikke længere er relevante (se sletteregler for forskellige typer af oplysninger i håndbogens kapitel 1).

10. Tag ikke nye IT-systemer eller digitale platforme i brug, uden at der først er sket en vurdering af sikkerheden i systemet og indgået en kontrakt/**databehandleraftale** med leverandøren.

11. Ved **tyveri af udstyr** (fx pc eller smartphone, som man har fået udleveret som arbejdsredskab på skolen), skal man straks kontakte IT med henblik på at få slettet fortroligt eller følsomt indhold, i det omfang det er muligt. Da der er tale om arbejdsredskaber, har skolen ret til at slette alt indhold på det udlånte udstyr.

12. Der skal udvises **fortrolighed** med de personoplysninger, man som led i sit arbejde bliver bekendt med. Del og videregiv ikke oplysninger uden at være sikker på, at det er i orden. Del ikke dine arbejdsredskaber (fx pc) med andre, hvis de på den måde får adgang til fortrolige eller følsomme oplysninger.

13. Åbn ikke mails, der ser mistænkelige ud.

14. Kontakt IT-support eller ledelse, hvis du bliver opmærksom på noget mistænkeligt.

Enkelte af ovenstående retningslinjer er uddybet i de følgende afsnit. Er man i tvivl om, hvordan man skal forhold sig i konkrete tilfælde, skal ledelsen kontaktes.

Google Meet
Både medarbejdere og elever skal undgå inddatering af unødvendige personoplysninger i systemet (dvs. personoplysninger der ikke er nødvendige for anvendelsen af systemet). Det gælder særligt personfølsomme personoplysninger, det især skal undgås at inddatere.

Der skal endvidere indskærpes, at elever og lærere skal benytte Google Meet via en pc/bærbar således at det undgås, at der deles fx lokationsdata, kontaktoplysninger mv. fra medarbejderens/elevens telefon.

Ved brugen af Google Meet er det muligt, at der overføres data til 3 parts lande (USA). DPO ved på nuværende tidspunkt ikke, om det rent faktisk er tilfælde (og i givet fald i hvor høj/lav grad) at Google overfører data. Overførselsgrundlaget for USA er på plads i kraft af US Privacy Shield, men der mangler stadig transparens som overvåges fra vores side.

Mailpolitik
Når der modtages en e-mail er der ikke sikkerhed for, hvem afsender reelt er, og derfor bør man ikke åbne eller svare på e-mails med ukendt eller mistænkeligt indhold og afsender. Skal der transmitteres følsomme eller fortrolige personoplysninger over det åbne net, skal e-mail'en sendes krypteret og det anbefales, at oplysningerne slettes senest 30 dage efter behandling.

Almindelige arbejdsdokumenter uden personoplysninger må gerne gemmes på PC'ens eget drev eller USB. På det personlige netværksdrev må man gemme almindelige personoplysninger og CPR-numre. Følsomme og fortrolige personoplysninger anbefales det ikke at man gemmer her pga. manglende sikkerhed (bl.a. fordi der ikke foretages logning).

Om mails

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).

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)*

4. Straks efter en medarbejders fratræden lukkes medarbejderens mailadresse ned, hvorefter der i en kort periode sendes autosvar om vedkommendes fratrædelse til de mailafsendere, der fortsat bruger mailadressen.

Kryptering af mails

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 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.

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.

Outsourcing af IT-drift til eksterne IT-leverandører (databehandlere)
Gefion Gymnasium bruger eksterne IT-leverandører til at levere, drive og/eller vedligeholde IT-systemer og/eller IT-infrastruktur. 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 fra Gefion Gymnasium. Derfor skal alt samarbejde med eksterne 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 ledelsen og IT, der sørger for, at der kun indgås kontrakt og opstartes (og forlænges) samarbejder med eksterne IT-leverandører, der vil overholde vores krav (se krav til databehandleraftaler i bilag).

Hvad må Lectio bruges til

Lectio må bruges til:

- Skemalægning og eksamensplanlægning
- Fraværsregistrering på de enkelte moduler

- Korte beskeder om aflysninger, møder, fravær mv. (følgende må ikke fremgå: mødereferater, mødenoter, helbredsdiagnoser eller oplysninger, hvoraf man kan udlede en helbredsdiagnose)
- Aflevering af skoleopgaver

Beskedfunktionen i Lectio må **ikke** anvendes til beskeder. Brug i stedet Gmail.

Lectio må ikke indeholde fortrolige eller følsomme oplysninger
CPR-numre og karakterer er fortrolige oplysninger. Disse oplysninger er vi indtil videre nødt til at opbevare i Lectio, da vi ikke har et alternativ. Derfor er det afgørende, at kun de medarbejdere, der har et tjenstligt formål med at kende personoplysninger om eleverne, fx i form af karakterer eller CPR-numre, bruger deres Lectio-adgang til dette. Underviser man ikke en elev, eller er elev gået ud, må man derfor fx ikke tilgå elevens oplysninger.

På skolens hjemmeside under [sikker kommunikation med Gefion Gymnasium] kan elever, værger og medarbejdere se, at vi opfordrer til IKKE at kommunikere om fortrolige og følsomme personoplysninger via Lectio. Kommunikationen bør i stedet ske via mail. Den interne, løbende kommunikation om elevers private forhold sker heller ikke i Lectio.
For at beskytte tidligere elevers personoplysninger mod uvedkommendes adgang, er det vigtigt, at man som medarbejder IKKE tilgår oplysninger, selv om det er muligt.

Det er ledelsen i samarbejde med administrationen på Gefion Gymnasium der tildeler brugeradgange til Lectio. Vi tilstræber, at man kun får adgang til de oplysninger, som er relevante for at kunne udføre den funktion på Gefion man har som medarbejder.

Hvad må fælles undervisningsnetværksdrev som GoogleSuite bruges til?
På Gefion Gymnasium benytter vi os af GoogleSuite[1] 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

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

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	Ja (krypteres)	Nej	Ja	Ja	Nej
Følsomme og andre fortrolige personoplysninger (logning kræves)	Ja	Ja (krypteres)	Nej	Nej, frarådes	Frarådes	Nej

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 relateret til sociale medier (fx Facebook, Twitter, Snapchat, Instagram etc.) eller 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:

a) 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.

b) 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, Anne Schultz (ansc@itcfyn.dk).

Generel IT- sikkerhed – hvad kan du selv gøre?

- 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.