Håndbog om sikker databehandling

Denne materialesamling skal hjælpe med at overholde databeskyttelsesforordningen. Du kan få yderligere informationer ved at læse skolens retningslinjer for databehandling, som kan ses i Lectio (dokumenter/alle lærer/persondataforordningen)

Indhold

Tavshedspligt

Som ansat på Odsherreds Gymnasium er du i medfør af forvaltningslovens[1] §27 omfattet af tavshedspligt:

Tavshedspligt

§ 27. Den, der virker inden for den offentlige forvaltning, har tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til oplysninger om

1) enkeltpersoners private, herunder økonomiske, forhold og

2) tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningerne angår, at oplysningerne ikke videregives.

Stk. 2. Den, der virker inden for den offentlige forvaltning, har desuden tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, når det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Det samme gælder, når en oplysning ved lov eller anden gyldig bestemmelse er betegnet som fortrolig, herunder når fortrolighed følger af en EU-retslig eller folkeretlig forpligtelse el.lign.

Stk. 3. Den, der virker inden for den offentlige forvaltning, har herudover tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, når det er nødvendigt at hemmeligholde en oplysning til beskyttelse af væsentlige hensyn til rigets udenrigspolitiske interesser, herunder forholdet til andre lande eller internationale organisationer.

Stk. 4. Den, der virker inden for den offentlige forvaltning, har desuden tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til oplysninger, som det i øvrigt er nødvendigt at hemmeligholde for at varetage væsentlige hensyn til

1) forebyggelse, efterforskning og forfølgning af lovovertrædelser samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig eller disciplinær forfølgning,

2) gennemførelse af offentlig kontrol-, regulerings- eller planlægningsvirksomhed eller af påtænkte foranstaltninger i henhold til skatte- og afgiftslovgivningen,

3) det offentliges økonomiske interesser, herunder udførelsen af det offentliges forretningsvirksomhed,

4) forskeres og kunstneres originale ideer samt foreløbige forskningsresultater og manuskripter eller

5) private og offentlige interesser, hvor hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Stk. 5. Inden for den offentlige forvaltning kan der kun pålægges tavshedspligt med hensyn til en oplysning, når det er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til bestemte offentlige eller private interesser som nævnt i stk. 1-4.

Stk. 6. En forvaltningsmyndighed kan bestemme, at en person uden for den offentlige forvaltning har tavshedspligt med hensyn til fortrolige oplysninger, som myndigheden videregiver til den pågældende uden at være forpligtet hertil.

Stk. 7. Fastsættes der i henhold til § 1, stk. 3, regler om tavshedspligt, eller pålægges der tavshedspligt efter stk. 6, finder straffelovens § 152 og §§ 152 c-152 f tilsvarende anvendelse på overtrædelse af sådanne regler eller pålæg.

[1] Forvaltningsloven: LBK nr. 433 af 22/04/2014, gældende november 2018

Principper for god behandling

God databehandlingsskik

Som ansat på Odsherreds Gymnasium skal du medvirke til at sikre, at alle personoplysninger behandles på en lovlig, rimelig og gennemsigtig måde jf. Databeskyttelsesforordningens art. 5, stk. 1, litra a.

Lovlig henviser til, at du som ansat på Odsherreds Gymnasium sikrer, at der er et lovligt hjemmelsgrundlag til behandlingen. Lovligt hjemmelsgrundlag er indsamling og behandling af personoplysninger, der er nødvendige for at skolen kan overholde lovgivningen og kollektive overenskomster eller på baggrund af samtykke. Se for en uddybning af oplysningerne orienteringsskrivelser til elever, jobsøgende og medarbejdere i Lectio (dokumenter/alle lærer/persondataforordningen)

- Rimelig henviser til, at du som ansat på Odsherreds Gymnasium kun må behandle personoplysninger, hvis behandlingens formål med rimelighed ikke kan opfyldes på anden måde.

Gennemsigtig indebærer, at du som ansat på Odsherreds Gymnasium skal oplyse den registrerede om den behandling, vi foretager om vedkommende. Behandlingen af personoplysninger skal således ske på en åben og oplyst måde. Skolen oplyser elever, ansatte samt kommende elever og ansatte om behandlingen i orienteringsskrivelser, se skolens hjemmeside samt Lectio (dokumenter/alle lærer/persondatafor-ordningen).

Formålsbegrænsning

Når der indsamles oplysninger, skal man gøre sig klart, til hvilke formål oplysningerne indsamles og det skal være saglige formål. Vi må således ikke indsamle oplysninger med den begrundelse, at det *måske* senere kan vise sig nyttigt at være i besiddelse af oplysningerne.
Efter indsamlingen må viderebehandlingen af oplysningerne ikke ske på en måde, der er uforenelig med det oprindelige formål.

Dataminimering

Når Odsherreds Gymnasium behandler personoplysninger, skal vi sikre, at behandlingen begrænses til det, der er nødvendigt for at opfylde formålet.
Vi skal således vurdere, om den konkrete behandling kan opfyldes ved at behandle færre personoplysninger.

Opbevaringsbegrænsning

Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for Odsherreds Gymnasium Fat have oplysningerne.

Rigtighed

Oplysninger, der er eller viser sig urigtige eller unøjagtige, skal snarest berigtiges eller slettes.

Integritet og fortrolighed

Du skal som ansat på Odsherreds Gymnasium beskytte oplysningerne mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt(slettes), ødelægges eller beskadiges. Dette sikrer vi ved at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger.

Man må således ikke behandle personoplysninger, før det er sikret, at der ved behandlingen foreligger en tilstrækkelig sikkerhed.

OBS: Alle ovenstående principper skal varetages i forbindelse med behandling af personoplysninger, HVER eneste gang.

E-mails

Retningslinjer for brug af e-mail

Som ansat på Odsherreds Gymnasium skal du bruge de it-systemer, som skolen stiller til rådighed, til al arbejdsrelateret, digital kommunikation. De vigtigste regler er følgende:

1. Arbejdsrelaterede e-mails sendes fra og modtages i Outlook.
2. Du skal være ekstra påpasselig med at sikre dig, at du sender til rette modtager, når du sender e-mails med personoplysninger.
3. E-mails med fortrolige og følsomme oplysninger skal altid sendes til e-Boks eller med krypteret e-mail.
4. Arbejdsrelaterede e-mails mv. i Outlook er skolens ejendom, som skolen kan åbne og læse i særlige tilfælde. Dette sker dog kun, hvis det er nødvendigt af hensyn til driften eller som led i fx it-support, som du evt. selv anmoder om.
5. Vi læser ikke medarbejderes e-mails i Outlook, der er tydeligt mærket "privat", idet dette er privat korrespondance, som er omfattet af brevhemmeligheden. For nemheds skyld vil vi dog opfordre dig til at bruge en privat e-mailkonto til privat kommunikation.
6. Private e-mailkonti må ikke bruges til arbejdsrelateret kommunikation. Der må ikke videresendes arbejdsrelaterede e-mails fra Outlook til en privat e-mailkonto.
7. Straks efter din fratræden lukkes din e-mailadresse ned. Du kan dog tilgå e-mails i 60 dage efter din fratræden.
8. Alle medarbejdere har pligt til at åbne e-mails løbende og sørge for sletning og arkivering af e-mails indeholdende personoplysninger.

Her kan du læse om de uddybende begrundelser for reglerne om brug af e-mail

Årsagen til at arbejdsrelaterede e-mails skal sendes via Outlook er, for at IT-Afdelingen kan holde styr på sikkerheden omkring domænet @odsherreds-gym.dk, fx holdes alle ansattes PC-er ajour med antivirus, spamfilter og firewall og der sørges for kryptering og back up. Dermed sikres oplysningerne i mailkorrespondancen mod utilsigtet sletning, uvedkommendes kendskab og hackerangreb.

Du skal sørge for at slette de arbejdsrelaterede e-mails i din Outlook, så snart relevansen er ophørt.

- Bemærk, at e-mails som udgangspunkt aldrig bør indeholde CPR-numre. Overvej altid om følsomme informationer om elever eller medarbejdere bør ske via e-mail.

Hvis e-mailen indeholder oplysninger om helbredsdiagnoser, cpr.nr. eller andre følsomme personoplysninger, må e-mailen ikke opbevares i Outlook længere end nødvendigt, som udgangspunkt **maksimalt 30 dage**. Hvis e-mailen sendes ud af gymnasiets domæne, @odsherreds-gym.dk skal der anvendes Sikker Mail eller e-Boks. Alle e-mails findes i Outlook indtil du selv sletter dem.

Hjemmel

Hjemlen til Odsherreds Gymnasium adgang til medarbejdernes e-mailkonti findes i EU-databeskyttelsesforordningens art. 6, stk. 1, litra e.

Opbevaringspolitik

E-mails med persondata skal som udgangspunkt slettes efter 30 dage efter behandlingen. Bemærk at e-mails i mapperne Slettet post og Uønsket post, bliver slettet permanent efter 30 dage. Hver Office 365 e-mail konto har en online arkivmappe. En arkivmappe er en mappe, der vises sammen med brugerens primære postkasse mapper i Outlook eller Outlook Web App og hedder Archive eller Arkiv. Man har adgang til arkivmapperne på samme måde som til de andre Outlook mapper. Fordelen ved arkivmappen er, at e-

mails ikke ligger lokalt på Pc'en. Der læses i stedet online fra Office 365 i skyen, så der er større sikkerhed ved at placere e-mails i arkivmappen. Man kan dog ikke tilgå e-mails i arkivmappen uden internetadgang. Det anbefales, at sendte e-mails slettes, når de er ældre end fx 180 dage eller flyttes til en arkivmappe. Sletning af e-mails i Indbakke og Sendt post bør ske manuelt.

- Er der noget der skal gemmes længere tid, bør arkivering ske via et ESDH-system, som kun administrationen og sekretærerne har adgang til. Kontakt ovenstående i tilfælde af behov for arkivering af dokumenter i IMS.
- Husk løbende at tømme computerens papirkurv

OBS: Ovenstående er særdeles vigtigt at få styr på og ikke mindst få en vane omkring, således at Skolen i tilfælde af en indsigtsanmodning mv. kan fremfinde de nødvendige oplysninger. Yderligere skal det også kunne dokumenteres over for Datatilsynet, at vi overholder ovenstående nævnte principper for behandling af personoplysninger.

Backup og re-store

Når data bliver slettet i Outlook, kan en Outlook 365-administrator genoprette e-mails 15 dage efter, at de bliver slettet af en slutbruger. Efter den tid kan e-mailen ikke genskabes. Man kan kun gendanne enkelte emner og ikke en hel mappe. Det betyder, at e-mailen vil blive genskabt til Indbakke, og ikke til den oprindelige mappe.

Afsendelse af Sikker Mail

Medarbejdere på Odsherreds Gymnasium kan afsende Sikker Mail via tunnelmail(fusemail), som er installeret i Outlook på medarbejderens computer. På denne måde sikres det at e-mails kan sendes sikkert. Fusemail kan sende sikkert til alle domæner, der benytter samme tunnel og modtager kan modtage sikkert via tunnelen. Ovenstående fremgangsmåde kan vise om modtageren er på tunnelen.

Lectio

Retningslinjer for brug af Lectio

Formålet med denne retningslinje er at sikre, at Odsherreds Gymnasium altid er i stand til at iagttage de krav der stilles til en institution, som følger af databeskyttelsesforordningen (GDPR)[2].
Som det ser ud på nuværende tidspunkt, lever Lectio som system ikke op til disse krav, hvorfor brugen heraf skal begrænses til det absolut nødvendige.

Problemer med Lectio

Et af de store problemer ved anvendelsen af Lectio, er manglende tilstrækkelig adgangsbegrænsning. Dette indebærer, at lærere via Lectio kan tilgå alle elevers oplysninger herunder elevers fravær, skema, karakterer.

Hvordan skal vi forholde os?

Dette betyder, at du som underviser/ansat kun bør tilgå oplysninger vedrørende egne elever i Lectio fx bedømmelser / fravær mv. og ingen andre elevers oplysninger[3]. Tilmed bør der så vidt muligt ikke gemmes følsomme oplysninger i Lectio jf. art. 9[4].

Dette medfører reelt set, at enhver anvendelse af Lectio trods indskrænkning i brugen heraf, er et brud på persondatasikkerheden, som skal anmeldes til Datatilsynet. Det opfordres til at begrænse og få luget ud i mængden af oplysninger, som lægges på Lectio herunder særligt de følsomme oplysninger. Det vil på sigt betyde, at man er nødt til at få ryddet op i systemet, og få slettet/ arkiveret det, som ikke skal være i Lectio.

Disse retningslinjer skal skærpe opmærksomheden på enhver anvendelse af Lectio med særlig fokus på at minimere arkiveringen af særligt følsomme oplysninger. Derfor er opfordringen til alle undervisere at tænke en ekstra gang over, hvilke oplysninger du lægger ind i Lectio. På baggrund af ovenstående, er det derfor nødvendigt og ikke mindst vigtigt at få indarbejdet nogle sunde og bevidste data-rutiner hos dig som bruger af Lectio.
Et spørgsmål man med fordel kan stille sig selv er, om de oplysninger du lægger på Lectio, ikke kunne arkiveres et andet mere sikkert og forsvarligt sted. Du bør sikre dig, at oplysninger af betydning arkiveres på Odsherreds Gymnasium OneDrive, som er det alternativ der pt. forefindes, og ikke i Lectio.
Mulige opbevaringsmuligheder:

- Et elektronisk arkiv
  - Fx IMS arkiv (elevsager, hvori der ligger eks. optagelsespapirer, helbredsoplysninger)
- OneDrive (mere tænkt i forbindelse med forberedelse, karakterlister mv.)

Hvis der er oplysninger, som af en eller anden årsag bør gemmes henvises der til at alle følsomme oplysninger om eleverne som udgangspunkt arkiveres i IMS og slettes fra Lectio. Således at der i Lectio findes så få følsomme personoplysninger som muligt.

---

[2] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 (Databeskyttelsesforordningen)

[3] **Almindelige oplysninger er:**
Væsentlige sociale problemer, andre rent private forhold, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, navn, adresse, fødselsdato (identifikationsoplysning)

[4] **Følsomme oplysninger er:**
Racemæssig eller etnisk baggrund, Politisk overbevisning, Religiøs overbevisning, Filosofisk overbevisning, Fagforeningsmæssige tilhørsforhold, Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol, sindssygdom, ordblindhed m.v., seksuelle forhold eller orientering.

Beskeder i Lectio
Lectio er i øvrigt ikke den rette kanal at sende personoplysninger herunder særligt følsomme oplysninger i, med henvisning til ovenstående. Der skal derfor helst ikke ske udveksling af personoplysninger om eleverne via Lectio. Måtte der være behov for at udveksle oplysninger om eleverne, lærerne imellem, skal denne korrespondance foregå via Outlook (@odsherreds-gym.dk).

Hvordan løses problemet fremadrettet?
Denne retningslinje skal sikre, at Odsherreds Gymnasium fremadrettet bliver *compliant*[5] databeskyttelsesmæssigt, og dermed lovmedholdelig, hvilket systemet jf. ovenfor ikke kan garantere. Desværre er der pt. Ikke mange muligheder for andet valg af studieadministrativt system, som kan håndtere disse oplysninger på forsvarlig og sikker vis. Odsherreds Gymnasium er pt. i færd med at undersøge om der er andre muligheder.

På baggrund af ovenstående utilstrækkelighed i forhold til blandt andet adgangsbegrænsning indebærer det, at enhver anvendelse af Lectio i sin nuværende form reelt set medfører en overtrædelse af forordningen. Der henstilles derfor til en begrænsning i brugen af Lectio, indtil der forhåbentligt er fundet en anden og bedre løsning.

[5] At vi som Dataansvarlig sikrer os at vi overholder forordningen

Håndtering af persondata

Brug af OneDrive til dokumenter med persondata

Filer med persondata må hverken gemmes på computerens c-drev, på netværksdrevet på computeren, på en USB-pen, i Google eller Dropbox. Hvis man vil gemme filer med persondata, må man gemme på OneDrive. Hvis man benytter OneDrive, gælder følgende:

Man må ikke synkronisere OneDrive til andre enheder end den PC, som man har fået udleveret som arbejdsredskab af skolen. Man må således ikke synkronisere og gemme kopier af indholdet fra OneDrive på private PC'er. Man kan selvfølgelig tilgå OneDrive filerne fra en browser. Man skal dog være påpasselig med ikke at downloade dokumenter til den PC, man arbejder på.

Man må ikke dele følsomme persondata i OneDrive med eksterne brugere uden for Odsherreds Gymnasium.

Ved egentlig sagsbehandling i forhold til en elev eller en medarbejder, skal man anvende skolens ESDH system (IMS). Derfor har skolens administration adgang til IMS.

Det gælder også ved anvendelse af OneDrive, at der skal være et formål for behandling af personoplysningerne. Der skal være en hjemmel og oplysningerne skal være nødvendige for opfyldelse af formålet. Oplysningerne skal slettes, når de ikke længere er nødvendige for formålet, jf. databeskyttelsesforordningens art. 5.

OBS: Det er meget vigtigt ved installering af Office 365 på egen private PC, at der efter login og adgang til programmerne bliver logget ud med det samme efter endt arbejde.

Brug af PC

Alle skolens PC'er er certificerede af IT-Afdelingen, hvilket blandt andet indebærer, at du ved modtagelse af PC'en skrev under på og har forstået vilkårene for lån af Odsherreds Gymnasium udstyr samt retningslinjer for god databehandlingsskik. Dokumentet (*Udlevering af bærbar GDPR)* findes også på Lectio (dokumenter/alle lærer/persondataforordningen).

Nedenstående gælder som supplement til certificeringen

- Brug adgangskode (eller fingeraftryk som adgangskode) på din computer, smartphone m.v.
- Aktivér din pauseskærm, hver gang du forlader din PC. Hvis du forlader din PC i undervisningslokalet, skal du altid lukke den ned eller slukke for den, så adgang er beskyttet med kode. Hvis du skal vise film eller andet materiale fra din PC i undervisningen henstilles til, at du kontakter IT-Afdelingen og får en låne-PC til formålet.
- Gem aldrig filer på din PC's c-drev.
    - Hvis den bliver stjålet, er der tale om et alvorligt sikkerhedsbrud, som skal indberettes til Datatilsynet.
    - Brug dit OneDrive drev til at gemme filer.
    - Ved tyveri af udstyr udleveret af skolen som arbejdsredskab skal IT-afdelingen straks kontaktes med henblik på at få slettet fortroligt eller følsomt indhold, i det omfang det er muligt.
- Elev- og personalesager oprettes, behandles og gemmes i ESDH (IMS).

- Sluk for din e-mail, inden du går ind i et undervisningslokale og tilslutter din PC til projektoren. Der kunne komme en e-mail, der som emne har en personoplysning, som ikke skal ses af andre end modtageren af e-mailen.
- Platforme og programmer som Google, Facebook og Dropbox kan udgøre en sikkerhedsrisiko i forhold til beskyttelse af personoplysninger. Begræns derfor brugen af disse platforme og programmer i undervisningen, og brug dem aldrig til deling af personoplysninger.
- Undlad at gemme personoplysninger på USB-nøgle, på skrivebordet på din bærbare computer eller lignende usikre steder. Brug VPN, hvis du arbejder med persondata på din computer ude af huset (det er kun administrativt personale, der har adgang til VPN).
    - Hvis personoplysninger opbevares på USB-nøgle, skal Odsherreds Gymnasium USB-nøgler benyttes. Som en ekstra sikkerhed kan USB-nøglen krypteres, hvilket let gøres ved at højreklikke på USB-nøglen og vælge "slå bit-locker til". Herefter vælges en personlig adgangskode, som medarbejderen selv kan huske.
- 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.
- Der skal udvises den fornødne 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.

Brug af papirdokumenter

- Læg papirdokumenter med personoplysninger i aflåst skab, skuffe eller kontor, når du forlader dit skrivebord i længere tid og altid, før du forlader arbejdspladsen.
- På skolens kontor skal papirdokumenter med personoplysninger altid opbevares i et aflåst skab.
- Dokumenter som opbevares flere steder skal når de ikke bruges lægges med de fortrolige oplysninger nedad, ellers anvendes et særligt chartek til netop dette formål.
- Papirdokumenter med personoplysninger skal altid bortskaffes ved makulering.

Hvis uheldet er ude - databrud

Når persondata bliver tilgængelige for andre end de personer der har lov til at arbejde med dem, er det et brud på sikkerheden. ***Et databrud:*** Er brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret opbevaret eller på anden måde behandlet, jf. databeskyttelsesforordningen art. 32, stk. 2.

Typiske eksempler på brud på persondatasikkerheden

Menneskelige fejl

- Sender e-mails uden kryptering med personoplysninger
- Oplysninger sendes til en eller flere forkert(e) modtager(e)
  - Fx videregivelse af oplysninger om en ansat eller studerende til uvedkommende
  - Åben ikke e-mails der ser mistænkelige ud eller som kommer fra afsendere du ikke kender
  - Vær varsom med links i e-mails fra afsendere
- Glemmer USB-sticks hvorpå gemmer sig ukrypterede personoplysninger
- Lader papirer med personoplysninger flyde i printerrummet
- Lader nøgler flyde / låner nøgler ud
- Glemmer en ulåst PC eller glemmer at låse skærm når du forlader den
- Manglende aflåsning af kontor når sidste mand går
  - Fx kan uvedkommende få uautoriseret adgang til fysiske oplysninger mv. (Fx skrivebord, ulåste skabe mv.)
- Offentliggørelse af fortrolige eller følsomme oplysninger på Internettet
  - baggrund af en fejl eller uvidenhed, om hvad der må offentliggøres
  - utilstrækkelig anonymisering.
- Ved et uheld kommer til at ændre eller slette personoplysninger
- Sammenblanding af dokumenter
  - fx i forbindelse med udskrivning eller afsendelse af post (både elektronisk og manuel post).

Organisatoriske fejl

- Glemmer at fastsætte eller opdatere interne retningslinjer
  - Utilstrækkelig beskrivelse af sikkerhedsprocedure
  - Manglende undervisning i sikkerhedsprocedure i forbindelse med persondatabehandling
    - Fx brug og deling af personoplysninger
- Manglende kontrol med databehandlere
- Manglende undervisning eller instruktion af medarbejdere (awareness-træning)
  - Certificering af dem som arbejder med personoplysninger
- Manglende adgangsbegrænsning
  - Fx oplysninger kan tilgås udover, hvad der er nødvendigt for rolle eller funktion
- Manglende kontrol med sikkerhedsforanstaltninger truffet hos databehandlere
- Manglende halvårlige kontroller af medarbejdernes autorisationer
- Manglende kontroller, audit og godkendelser Fx ISO27001 m.fl.

Systemtekniske fejl

- Utilstrækkelig sikkerhed i IT-systemer
  - Manglende mulighed for at slette effektivt

    - Utilstrækkelig adgangskontrol
    - For bred adgang til oplysninger mv.
- Manglende kryptering af formularer på hjemmesider til brug for fremsendelse af fortrolige eller følsomme oplysninger
- Utilstrækkelig adgangsløsning i forbindelse med adgang via internettet til at se eller indtaste bl.a. følsomme oplysninger
- Manglende logning eller problemer med om de loggede oplysninger kan anvendes til at spore hvilke oplysninger en medarbejder har tilgået
    - Manglende kontrol med afviste adgangsforsøg
- Brugeren har adgang til uvedkommende oplysninger som følge af fejl i IT-systemet.
- Uhensigtsmæssig brug af administratorrolle i forbindelse med IT-systemer.
- CMS-systemer, der designes således, at der automatisk foretages en scanning i materiale, der uploades til en hjemmeside (data discovery)
- Manglende sletningsmekanisme for behandlinger med hjemmel i samtykke, hvorved systemet automatisk sletter de personoplysninger, forordningen kræver, når den registrerede trækker sit samtykke tilbage
- Manglende design af systemer, der automatisk sletter data efter et vist tidsrum eller andre objektivt fastsatte regler.
    - Fx et økonomisystem der designes således, at det sletter eller anonymiserer alle bogførte data 5 år efter registreringstidspunktet

NB: Ovenstående er kun mulige forslag, der kan være langt flere tilfælde.

I tilfælde af et databrud

Ved brud på persondatasikkerheden skal gymnasiet, uden unødig forsinkelse og om muligt senest 72 timer efter bruddet på persondatasikkerheden, anmelde det til Datatilsynet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. I så tilfælde kan anmeldelse udelades.

Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Anmeldelsen skal indeholde

- Beskrivelse af karakteren af bruddet, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
- Angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- Beskrive de sandsynlige konsekvenser af bruddet
- Beskrive de foranstaltninger, som gymnasiet har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Dokumentation over databrud

Alle brud på persondatasikkerheden skal kunne dokumenteres, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger. Gymnasiet skal kunne fremvise en samlet liste over alle brud på persondatasikkerheden. Dette skal sikre at tilsynsmyndigheden, i denne sammenhæng Datatilsynet, er i stand til at kontrollere, at databeskyttelsesforordningens artikel 33 reelt set overholdes. Denne skal på anmodning kunne forevises for Datatilsynet.

Kontakt

Ansvaret for datasikkerheden og databeskyttelsen ligger hos den Dataansvarlige (Odsherreds Gymnasium) Derfor skal du ved brud på datasikkerheden kontakte nærmeste leder eller IT-chefen, hvis du bliver opmærksom på noget, du mener kan udgøre en risiko for sikkerheden af personoplysninger.

Kravet om dokumentation kræver at skolens DPO skal informeres om alle brud på sikkerheden og Datatilsynet skal underrettes indenfor 72 timer.

Databeskyttelsesrådgiver (DPO):
Merete Munch Scheelhardt
dpo@stenhus-gym.dk
Tlf.: 20 69 80 86