GDPR-håndbog

Til alle medarbejdere - vedrørende IT-sikkerhed og behandling af personoplysninger for Sct. Norberts Skole & Børnehus

Version	Dato	Ændret af	Godkendt af
1.0	03-10 2024	Jacob Bæk	
1.1	12-06-2024	Jacob Bæk	
1.2	22-09-2026	Jacob Bæk	

Indholdsfortegnelse

Formål ... 4
Organisation og ansvar ... 4
Definitioner ... 5
Medarbejderinstruks ... 6
Kommunikation (Intra og E-mail) ... 6
Behandling af personoplysninger ... 7
Lovligt grundlag ... 7
Anmodninger fra registrerede ... 8
Udlevering af personoplysninger til eksterne parter ... 8
Brug af tjenester/systemer ... 8
Elektronisk opbevaring af personoplysninger ... 9
Fysisk opbevaring af personoplysninger ... 9
Sletning af personoplysninger ... 9
Fjernarbejdspladser mv. ... 10
Transport ... 10
Gæster ... 10
Fortrolighed ... 10
Adgange ... 10
Password-sikkerhed ... 10
Brug af billeder, sociale medier og AI ... 11
Udstyr uden opsyn ... 11
Clean desk policy ... 12
Face down policy ... 12
Tyveri ... 12
Bortkommer udstyr som har tilgang til skolens data, skal dette meddeles straks! ... 12
Krav til mobile enheder ... 12
Tekniske krav ... 12
Brugskrav ... 12
Sikkerhedsbrudsvejledning ... 13
Hvad er et sikkerhedsbrud ... 13
Mistanke om brud på sikkerheden ... 14

Formål

Dette dokument har to formål:

1. Dels at tjene som et praktisk instrument på og børnehus arbejde med beskyttelsen af personoplysninger
2. Dels som en skriftlig dokumentation af vores indsats for at overholde databeskyttelsesforordningen.

Alle medarbejdere på Sct. Norberts Skole & Børnehus og Børnehus bør læse, forstå og overholde denne håndbog. Hvis retningslinjerne i denne håndbog ikke bliver overholdt, kan/vil det medføre sanktioner for Sct. Norberts Skole & Børnehus og børnehus og yderste konsekvens for den enkelte medarbejder.

Håndbogens indhold er at betragte som intern information og skal derfor behandles fortroligt.

Organisation og ansvar

Arbejdet med GDPR forudsætter, at både ledelsen og medarbejderne hos Sct. Norberts Skole & Børnehus og børnehus aktivt varetager følgende ansvarsområder:

Ledelsens ansvar

- Sætte rammerne for det overordnede sikkerhedsniveau.
- Sikre at hele Sct. Norberts Skole & Børnehus og børnehus er bevidst om sikkerheden gennem daglig adfærd og den nødvendige uddannelse.
- Sikre at sikkerhedsforanstaltninger evalueres og overholdes.
- Effektuere evt. vedtagne sanktioner i tilfælde af manglende overholdelse af denne håndbog.

Medarbejderens ansvar

- Det er medarbejderens ansvar at efterleve de instrukser og retningslinjer, der gives i denne håndbog.

Definitioner

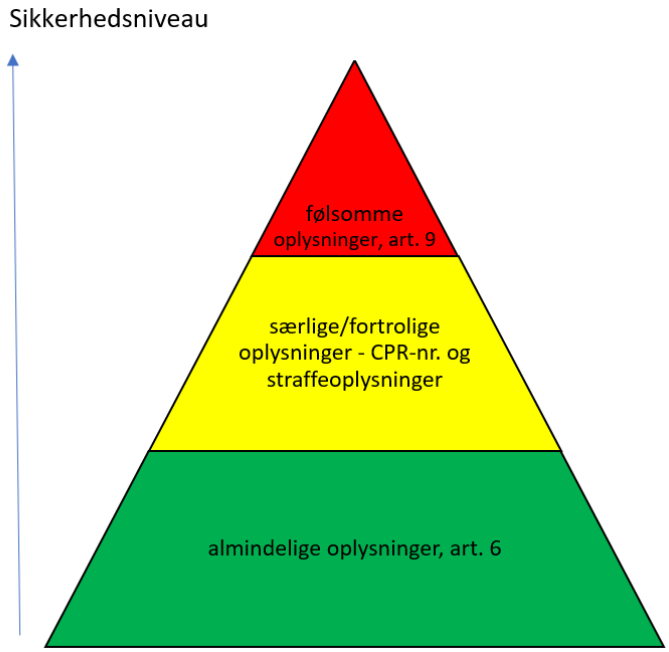
Vi behandler personoplysninger i mange forskellige aspekter af vores daglige arbejde, og det er vigtigt, at du som medarbejder hos Sct. Norberts Skole & Børnehus er opmærksom på, hvornår og hvordan de forskellige typer af personoplysninger håndteres korrekt.

Personoplysninger er alle oplysninger, der kan ledes tilbage til en fysisk person. Det kan fx være et navn, et telefonnummer eller en adresse.

Nedenfor har vi defineret nogle kernebegreber, som kan hjælpe dig med at forstå resten af håndbogens indhold.

Databeskyttelsesforordningen	Den lovgivning, som pr. 25. maj 2018 regulerer behandlingen af personoplysninger (træder sammen med danske databeskyttelseslov i stedet for persondataloven).
Almindelige personoplysninger	Enhver oplysning om en identificeret eller identificerbar fysisk person, fx navn, adresse, telefonnummer, billede, nummerplade, eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger.
Fortrolige oplysninger	Oplysninger der betragtes som værende fortrolige oplysninger, fx CPR-nummer, oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold, oplysninger om interne familieforhold, herunder oplysninger om fx ulykkestilfælde.
Følsomme personoplysninger	Oplysninger om: Race og etnisk oprindelse, politisk overbevisning, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger, og seksuelle forhold eller seksuel orientering Listen er udtømmende og bestemt af EU
Registrerede	Alle personer, hvis oplysninger er registreret hos os, fx elever, medarbejdere og leverandører.
Behandling af personoplysninger	Alt hvad Sct. Norberts Skole & Børnehus gør med personoplysninger, herunder opbevaring og sletning. Dette gælder både elektronisk og manuel behandling.
Dataansvarlig	Den, der beslutter formål, omfang og metoder til behandling af personoplysninger, fx når Sct. Norberts Skole & Børnehus behandler oplysninger om medarbejdernes data
Databehandler	Den, der behandler personoplysninger på vegne af den dataansvarlige, fx et firma, som håndterer løn eller en cloudtjeneste.

Hvis personoplysninger er følsomme, skal vi sikre et højere beskyttelsesniveau end hvis der er tale om almindelige personoplysninger. Beskyttelsesniveauet følger altså typen af personoplysninger.



Medarbejderinstruks

Det følgende er de konkrete instrukser og retningslinjer, som alle ansatte skal følge i forbindelse med IT-sikkerhed og behandling af personoplysninger. Det er vigtigt at understrege, at det er *alles* ansvar at sikre, at databeskyttelsesreglerne bliver overholdt.

Kommunikation (Intra og E-mail)

Formålet med denne retningslinje er at sikre, at der ikke opbevares gamle personoplysninger i din mailindbakke og besked, som burde være arkiveret eller slettet. Det er også vigtigt at sikre, at oplysninger, som andre skal have adgang til, opbevares i de korrekte systemer og ikke bliver liggende i din e-mail.

Som udgangspunkt skal alt kommunikation med elever og forældre foregå gennem skolens intranet. Alle beskeder der er ælder end 2 år bliver automatisk slettet i skoleintra besked system.

Vigtig Information vedr. elever skal altid gemmes i klasselog

Husk at har man en besked der er vigtig at gemme klasselog så klik på "gem i klasselog" eller

Private e-mails

Du må ikke anvende din arbejdsmail til privat brug. Hvis du alligevel bruger din arbejdsmail til privat brug, skal sådanne e-mails tydeligt markeres ”Privat” og lægges i en folder/mappe, som også hedder ”Privat”.

Orden i din mailboks

Det er vigtigt, at du holder orden i din mailboks. Det betyder, at du skal flytte alle e-mails over i en undermappe, som passer på specifikke elever/projekt. På den måde kan man også nemt finde relevant korrespondance igen, og man kan slette en hel mappe, hvis der er behov for det.

Husk aktivt at sikre dig, at de e-mails, der slettes, reelt slettes fra både din *Indbakke og Sendt post*.

Du skal løbende huske også at slette mappen med Slettet post (slet i slet).

E-mails, som ikke er relevante for dig, bør slettes hurtigst muligt.

Hvis du er i tvivl om, hvor længe en e-mail må arkiveres, skal du kontakte GDPR-ansvarlige.

E-mails med følsomme eller fortrolige oplysninger

Generelt skal du forsøge at undgå at sende e-mails med følsomme eller fortrolige oplysninger.

Er der behov for at sende e-mails med følsomme eller fortrolige oplysninger internt eller eksternt, skal dette gøres krypteret. E-mail krypteres via TLS 1.2 og overførsel via internettet krypteres via https-protokollen. E-mail indeholdende personfølsomme eller fortrolige oplysninger til eksterne modtager skal altid sende af administrationen eller en leder der har adgang til at kunne sende SIKKER MAIL.

Alle e-mails (indgående såvel som udgående), som indeholder personoplysninger af følsom eller fortrolig karakter fx CPR-nummer, helbredsoplysninger og lignende, skal slettes fra mailindbakken, så snart de er behandlet. Det betyder, at hvis oplysningerne skal opbevares i længere tid, skal de flyttes over til en mappe/drev/elev system adskilt fra din mailboks og derefter slettes fra din mailboksen.

Behandling af personoplysninger

Formålet med denne retningslinje er at minimere antallet af personoplysninger, som vi behandler, samt at sikre, at oplysningerne er opdaterede og korrekte.

Du skal altid sørge for at minimere behandlingen af personoplysninger i udførelsen af dit arbejde. Det betyder, at du skal undgå at registrere flere personoplysninger end dem, der er nødvendige for at udføre dit arbejde.

Generelt arbejder vi altså med ”need to have” og ikke ”nice to have”.

Når du behandler personoplysninger, skal du også være opmærksom på, at personoplysningerne opbevares i de korrekte systemer, drev og mapper, og at der ikke opbevares urigtige eller forældede oplysninger.

Hvis du skal opdatere kreditorers, debitorers og medarbejderes kontonumre, skal du altid bekræfte oplysningerne med et opkald til den pågældende person.

Lovligt grundlag

Formålet med denne retningslinje er at sikre, at der findes det nødvendige og tilstrækkelige behandlingsgrundlag, inden vi igangsætter behandlingen af personoplysninger.

Ønsker du at indsamle personoplysninger, som vi ikke før har arbejdet med, skal du sikre dig, at der er behandlingsgrundlag til det. Du skal kontakte den GDPR-ansvarlige eller nærmeste leder for at sikre dig, at dit behandlingsgrundlag er lovligt.

Ønsker du at benytte allerede indsamlede oplysninger til et andet formål, end de tidligere er indsamlet til, skal dette godkendes af din nærmeste leder ELLER den GDPR-ansvarlige. Fx, hvis du ønsker at benytte oplysninger, som er indsamlet i forbindelse med ansættelsen af nye medarbejdere, til at lave statistikker.

Anmodninger fra registrerede

Formålet med denne retningslinje er at sikre, at alle ved, hvordan de skal håndtere en anmodning fra de registrerede.

Bliver du kontaktet af en registreret (fx en elever, elevers forældre/værger eller lignende) som ønsker at:

- få indsigt i sine personoplysninger
- få slettet sine personoplysninger
- få udleveret sine personoplysninger (dataportabilitet)
- få rettet sine oplysninger
- få begrænset behandlingen af sine personoplysninger
- tilbagetrække et samtykke, som han eller hun har afgivet;

skal du oplyse den registrerede om, at vi vil behandle anmodningen uden unødig forsinkelse, og at anmodningen sammen med kontaktoplysninger på den registrerede videregives til GDPR-ansvarlige, som derefter vil kontakte den registrerede. Den GDPR-ansvarlige skal sikre sig, at identiteten af den registrerede bliver bekræftet, inden anmodningen besvares.

Vi er forpligtet i loven til at håndtere de registreredes anmodninger indenfor en måned. Det er derfor vigtigt, at du kan genkende en anmodning, og at du reagerer rettidigt på den.

Udlevering af personoplysninger til eksterne parter

Formålet med denne retningslinje er at sikre, at oplysninger ikke kommer til uvedkommendes kendskab.

Udlevering af personoplysninger omfatter alle personoplysninger, også interne oplysninger om kolleger. Du skal derfor være opmærksom på, at du ikke deler følsomme eller fortrolige oplysninger om dine kolleger med andre. Dette vil sige, at hvis en kollega fx er fraværende pga. sygdom, må du ikke oplyse andre om, hvad han eller hun fejler, men blot informere om, at kollegaen er fraværende pga. sygdom.

Før personoplysninger udleveres til eksterne parter, eller før der gives adgang til personoplysningerne til en ekstern part, skal dette godkendes af GDPR-ansvarlige eller IT-ansvarlige. Eksterne parter kan både være det offentlige, samarbejdspartnere, leverandører og datter/moderselskaber.

Det skal først undersøges, om der foreligger et lovligt videresendelsesgrundlag, og om der skal etableres en databehandleraftale med den eksterne part.

Brug af tjenester/systemer

Formålet med denne retningslinje er at sikre, at vi har det korrekte aftalegrundlag med leverandører af IT-systemer.

Dette afsnit gælder særligt for alle systemer, online-tjenester, cloud-services mm.

Du må kun benytte systemer til behandling af personoplysninger, hvis de er godkendt af Sct. Norberts Skole & Børnehus. Ønsker du at benytte et nyt system til at behandle personoplysninger, skal du kontakte IT-

afdelingen, som vil afgøre, om systemet må anvendes til formålet. Anvender du et system, som du ikke tror, at IT-afdelingen har kendskab til, skal du straks stoppe anvendelsen af systemet og give IT-afdelingen besked.

Hvis du i det daglige bliver opmærksom på fejl eller mangler i et system eller en databehandlers håndtering af personoplysninger, skal du gøre din nærmeste leder ELLER den GDPR-ansvarlige opmærksom på problemet. Vedkommende skal herefter undersøge problemet og foretage den nødvendige opfølgning.

Elektronisk opbevaring af personoplysninger

Formålet med denne retningslinje er at sikre, at vi har den nødvendige sikkerhed omkring de personoplysninger, som vi behandler.

Personoplysninger skal altid opbevares på de systemer, som du har fået anvist, og må ikke gemmes lokalt på din computer, USB-nøgle eller lign. Hvis du har behov for at opbevare personoplysninger lokalt på din computer, USB eller på andre flytbare medier, kontakt da IT-afdelingen for retningslinjer.

Det er ikke tilladt at gemme personoplysninger på **egne** konti hos tjenester som fx OneDrive eller Dropbox.

Fysisk opbevaring af personoplysninger

Formålet med denne retningslinje er at sikre, at vi har den nødvendige sikkerhed omkring de personoplysninger, som vi behandler.

Fysiske dokumenter, der indeholder personoplysninger

- skal opbevares aflåst, når de ikke er i brug
- må ikke efterlades frit tilgængeligt uden opsyn
- skal makuleres, når der ikke længere er behov for at opbevare dem
- skal hentes fra printeren straks efter, de er printet.

Generelt anbefales det, at du begrænser udskrivning af dokumenter med personoplysninger.

Sletning af personoplysninger

Databeskyttelsesforordningen indeholder ikke konkrete frister for, hvornår vi skal slette personoplysninger. Vi har derfor vores egne sletteregler for at sikre, at vi ikke opbevarer personoplysninger, når vi ikke længere har behov for dem.

På Sct. Norberts Skole & Børnehus har vi følgende regler for sletning:

- Data på medarbejder (Løndata/ansættelse aftaler) slettes efter 5 år
  Job ansøgninger slettes 6 måneder
  Relevante person får notifikation herom
- Elev data slettes i takt med at elever forlader skolen, dette sker automatisk i Skoleintra og elevadministrations system

Hvis du er i tvivl om, hvor længe du må opbevare en specifik oplysning eller et specifikt dokument, skal du kontakte virksomhedens GDPR-ansvarlige ELLER nærmeste leder, så det sikres, at alle slettefrister er baseret på en korrekt vurdering, og at slettefristerne overholdes. Hvis du bliver opmærksom på, at der mangler en slettepolitik i et system, skal du kontakte den GDPR-ansvarlige eller nærmeste leder.

Fjernarbejdspladser mv.

Alle retningslinjer og instrukser indeholdt i denne håndbog finder anvendelse uanset, hvorfra du arbejder.

Det vil sige, at du skal overholde alle retningslinjerne i dette dokument, uanset om du arbejder hjemmefra eller fra en anden lokation end Sct. Norberts Skole & Børnehus .

Du skal være opmærksom på, at du ikke arbejder med personoplysninger på steder, hvor andre kan se din skærm og dermed kan få adgang til oplysningerne.

Derudover er det vigtigt, at du har særligt fokus på ikke at afholde digitale møder eller at have telefonsamtaler i andres påhør, så de dermed kan overhøre personoplysninger.

Transport

Alle retningslinjer og instrukser indeholdt i denne håndbog finder også anvendelse ved brug af firmabiler og anden transport, fx når du kører med din computer i din bil eller i den offentlige transport.

Vær derfor opmærksom på følgende:

- Efterlad ikke din telefon og computer i bilen. Hvis det er strengt nødvendigt, så sørg for, at de er gemt væk under bagsæderne, i handskerummet, bagagerummet osv.
- Du må ikke efterlade kundekartoteker eller lign. i bilen.
- Du må ikke efterlade fysiske papirer, arbejdssedler eller leveringssedler med personoplysninger frit synligt, så de kan ses af personer, der kigger ind i bilen. Sørg for, at oplysningerne er gemt væk i handskerummet eller andre ikke-synlige steder.

Gæster

Under et gæstebesøg må gæsten ikke have adgang til Sct. Norberts Skole & Børnehus og børnehus arbejdsdokumenter.

Fortrolighed

Du er i forbindelse med din ansættelse hos os underlagt tavshedspligt, hvilket betyder, at du ikke må videregive oplysninger til andre uden for organisationen eller benytte arbejdsrelaterede oplysninger til private formål. Fortrolige oplysninger eller andre personoplysninger må ikke deles på de sociale medier eller drøftes i det offentlige rum eller andre steder, hvor uautoriserede personer kan få adgang til dem.

Adgange

Formålet med denne retningslinje er at sikre, at sikkerhedsforanstaltningerne vedrørende adgangsbegrænsning efterleves i praksis.

Du skal kun have adgang til oplysninger, som du har behov for, for at kunne udføre dine daglige arbejdsopgaver. Opdager du, at du har adgang til oplysninger, som du ikke har behov for, skal du kontakte virksomhedens GDPR-ansvarlige ELLER nærmeste leder.

Password-sikkerhed

Du må ikke udlevere dit bruger-ID eller password til andre.

Du må ikke nedskrive dit ID eller password på papir, i software-filer, på din telefon eller andre steder, som ikke er godkendte password vaults.

Du skal ændre dit password, hvis du har mistanke om, at det er blevet set af andre.

Du skal undgå at anvende samme password til private og arbejdsmæssige formål.

Du må ikke benytte det samme password til flere forskellige mobile enheder eller systemer.

Næsten alt bruger Unilogin/MitId til ind logning i skolens systemer og deres password krav.
Er det behov for at lave adgangskode til systemer der ikke bruger Unilogin/MitId
Så skal dit password skal:

- Min 12 Bogstaver, tegn og symboler
- Være nemt for dig at huske
- Ikke kunne gættes eller udledes ved hjælp af personoplysninger, fx navne, telefonnumre, fødselsdatoer
- Ikke være forudsigelige, fx Sommer2017, Password1234, Jens2017
- Ikke indeholder flere på hinanden følgende ens karakterer, som kun består af enten tal eller bogstaver]

Brug af billeder, sociale medier og AI

- Sct. Norberts Skole & Børnehus anvender billeder som en del af den daglige dokumentation og formidling af børnenes læring, trivsel og aktiviteter. Billeder kan deles internt på institutionens godkendte kommunikationsplatforme samt i begrænset omfang på institutionens officielle hjemmeside og sociale medier.

- Forældre, der ikke ønsker, at deres barn optræder på institutionens sociale medier, kan henvende sig til ledelsen. Institutionen registrerer herefter ønsket og sikrer, at barnet ikke fremgår af fremtidige opslag.

- Institutionen anvender ikke billeder af børn i AI-systemer til analyse, billedgenerering, maskinlæring, træning af kunstig intelligens eller anden AI-baseret behandling.
  Medarbejdere må ikke uploade billeder af børn til offentligt tilgængelige AI-tjenester eller anvende AI-værktøjer til behandling af billeder af børn uden forudgående godkendelse fra ledelsen og den GDPR-ansvarlige.

- Hvis institutionen på et senere tidspunkt ønsker at anvende AI-baserede løsninger, som indebærer behandling af billeder eller personoplysninger, skal dette vurderes særskilt i forhold til databeskyttelsesreglerne.
-

Udstyr uden opsyn

Du må ikke forlade din arbejdsstation - heller ikke selvom det er kortvarigt – uden at aktivere passwordbeskyttet pauseskærm på din computer og andet udstyr. Gøres nemt med Windows tast + L

Papir og elektroniske lagringsmidler USB-nøgler, harddiske osv. skal låses inde eller på anden vis opbevares forsvarligt, når de ikke benyttes.

Clean desk policy

Før du forlader arbejdspladsen, skal du rydde dit bord for alle dokumenter, der indeholder personoplysninger.

Face down policy

Når du forlader din arbejdsstation, skal du vende dokumenter med personoplysninger med den blanke side opad eller dække dokumentet på anden vis.

Tyveri

Bortkommer udstyr som har tilgang til skolens data, skal dette meddeles straks!

Krav til mobile enheder

Mobile enheder defineres her som enhver teknisk enhed med adgang til vores netværk, data og/eller informationsaktiver, som er mobil/flytbar i sit design, dvs. det omfatter laptops, tablets og smartphones mv.

Tekniske krav

Alle mobile enheder skal leve op til følgende:

- Alle enheder skal efterleve vores generelle krav til IT-sikkerhed.
- Alle enheder skal være beskyttet af passwords, der efterlever Sct. Norberts Skole & Børnehus generelle krav til passwordsikkerhed. Se mere herom under ”Password-sikkerhed”
- Til alle funktioner, hvor Sct. Norberts Skole & Børnehus anvender kryptering, skal dette også anvendes på mobile enheder.
- Enheder der udleveret af Sct. Norberts Skole & Børnehus IT-afdeling skal benytte WiFi netværk ”Ansatte”
  Kun enheder, der administreres af Sct. Norberts Skole & Børnehus IT-afdeling, må forbindes til Sct. Norberts Skole & Børnehus netværk ”Ansatte”.
- Øvrige enheder, som ejes af udefrakommende brugere eller gæster, henvises til at anvende Bamsenet.

Brugskrav

Al brug af mobile enheder skal efterleve følgende krav:

- Du må kun behandle data på mobile enheder i den udstrækning, det er nødvendigt for udførelsen af dit arbejde.
- Du skal uden unødigt ophold melde alle tabte eller stjålne enheder til din nærmeste leder ELLER den GDPR-ansvarlige, når du bliver bekendt med tabet/tyveriet.
- Hvis du mistænker, at der er sket uretmæssig adgang til Sct. Norberts Skole & Børnehus data/systemer via en mobil enhed, skal dette uden unødigt ophold rapporteres til din nærmeste leder ELLER den GDPR-ansvarlige.
- Mobile enheder må ikke være ”jailbroken” eller ”rooted” eller have software/firmware installeret, som kan give adgang til funktionalitet, der ikke er tiltænkt at være tilgængelig for brugeren. (Spørgsmål herom rettes til din nærmeste leder ELLER den GDPR-ansvarlige)
- Du må ikke synkronisere noget af enhedens indhold til dine egne cloud-services.
- Du må ikke have piratversioner af software eller andet ulovligt materiale på enhederne.

- Applikationer må kun installeres fra officielle kilder, som er godkendt af platform-ejeren, fx Appstore eller Google Play Butik. Kode eller applikationer fra ukendt eller usikker kilde må ikke installeres uden forudgående godkendelse fra din nærmeste leder ELLER den GDPR-ansvarlige.
- Enheder skal holdes ajourført med opdateringer fra producenten.
- Sker der tilkobling til internetforbindelse udenfor Sct. Norberts Skole & Børnehus , skal forbindelsen være beskyttet med adgangskode.

Sikkerhedsbrudsvejledning

Hvad er et sikkerhedsbrud

Et sikkerhedsbrud er en hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der bliver behandlet.

Som eksempler på et sikkerhedsbrud kan nævnes:

- Andre får adgang til personoplysninger, uden at vi har givet adgang/autorisation
    - Fx ved hackerangreb eller indbrud

- En medarbejder opdager, at vedkommende uberettiget har adgang til personoplysninger.
    - Fx ved modtagelsen af en intern mail med personoplysninger, som man ikke er berettiget til at modtage.

- Du kommer til at sende personoplysninger til en forkert modtager

Bliver du opmærksom på et potentielt sikkerhedsbrud, kontaktes den GDPR-ansvarlige eller ledelsen *øjeblikkeligt.*

Ved et potentielt sikkerhedsbrud skal vi lave en risikovurdering. Risikovurderingen skal klarlægge, om der foreligger en risiko for en fysisk persons rettigheder eller frihedsrettigheder.

Konstateres det, at der foreligger et sikkerhedsbrud, som indebærer en sandsynlig risiko for den registreredes rettigheder, skal sikkerhedsbruddet anmeldes til Datatilsynet indenfor 72 timer.

Anmeldelsen skal som minimum beskrive

- typen af sikkerhedsbruddet
- oplysningernes omfang
- hvornår bruddet skete og blev opdaget
- konsekvenserne af bruddet
- hvorvidt bruddet omhandler særlige kategorier af registrerede (børn eller særligt udsatte)
- antallet af berørte personer.

Hvis vi konkluderer, at sikkerhedsbruddet sandsynligvis vil medføre en høj risiko for de registreredes rettigheder, så skal vi også give de registrerede, som er berørt af sikkerhedsbruddet, besked.

Alle sikkerhedsbrud skal dokumenteres. Dette gøres i GapPortalen under ”Dokumentation” à ”Sikkerhedsbrudslog”.

Mistanke om brud på sikkerheden

Følgende situationer skal anmeldes til din nærmeste leder ELLER den GDPR-ansvarlige, hvorefter vedkommende igangsætter foranstaltninger og afgør, om der skal ske anmeldelse til Datatilsynet:

Har du:

- modtaget e-mails, SMS'er eller opkald, som virker mistænkelige (læs "Hvad er mistænkeligt?" nedenfor)
- sendt personoplysninger til en forkert modtager eller ved en fejl delt personoplysninger
- ved en fejl slettet personoplysninger
- opdaget, at personoplysninger har været tilgængelige for uautoriserede personer
- mistanke om, at der er sket uautoriserede ændringer i filer
- opdaget, at systemer ikke virker, som de plejer, og har mistanke om fx hacking
- mistet din computer, telefon, lagringsmedier eller andre medier eller print indeholdende fortrolige eller følsomme personoplysninger
- mistanke om, at andre kan have fået kendskab til din/dine adgangskoder.

Hvis du har mistanke om, at du har trykket på et "farligt" link eller åbnet en ukendt fil, skal du med det samme fjerne computeren fra netværket og kontakte din nærmeste leder ELLER den GDPR-ansvarlige.

Modtager du en e-mail eller SMS fra en kollega eller samarbejdspartner om fx at overføre penge, sende fortrolige oplysninger eller give adgang til fortrolige oplysninger, bør du få en bekræftelse fra afsenderen via en anden kontaktform – eks. en mundtlig bekræftelse over telefon.

Hvad er mistænkeligt?

Svindlere kan prøve at kopiere e-mails og sms-beskeder fra legitime virksomheder eller kolleger for at lokke dig til at dele oplysninger eller foretage transaktioner. Det kan også være at de lokker dig til dele data via telefonen. Begge dele kaldes phishing. Undlad at åbne bilag og klikke på links i mistænkelige og uopfordrede beskeder og videresend aldrig mistænkelige beskeder til en kollega.

Følgende er tegn på phishing-forsøg:

- afsenderens e-mailadresse eller telefonnummer stemmer ikke overens med navnet på den virksomhed, som afsenderen påstår at være fra
- beskeden er sendt til en e-mailadresse eller et telefonnummer, som du ikke har givet til afsenderen
- beskeden starter med en anonym hilsen, fx "Kære kunde". De fleste legitime virksomheder bruger dit navn, når de kontakter dig
- beskeden opfordrer dig til at følge et link eller indeholder en vedhæftet fil
- et link lader til at være legitimt, men det fører til et websted, som ikke stemmer overens med adressen på virksomhedens websted
- beskeden ser meget anderledes ud end dem, du ellers har fået fra virksomheden
- i beskeden bliver du bedt om at angive personlige oplysninger som fx et kreditkortnummer eller adgangskoden til en konto
- beskeden er sendt uopfordret til dig, og der er et bilag vedhæftet
- nogle phishing-henvendelser er skrevet i et dårligt dansk sprog eller bruger ikke æ, ø og å
- beskeden prøver at skræmme dig til at gøre noget. Det kan fx være, at dit MitId, NemID, betalingskort eller konto lukkes, hvis du ikke følger instruktionerne inden for en given periode, eller at en vigtig forretningsaftale kan gå i vasken, hvis du ikke overfører penge med det samme

- det er forsøgt at få afsenderen til at se troværdig ud ved at vise mailadressen for en ledende medarbejder eller kendt service, hvor enkelte elementer er ændret. Fx kan den stå til at være nem@MitID.nu, MIT@mitId.nu eller Support@MITID.nu.
- telefonisk kan en person udgive sig for at være en anden og forsøge at overtale dig til at afgive passwords eller lignende.
- det kan også ske via mail eller telefonisk, at nogen oplyser at have fået en ny mailadresse eller telefonnummer og dermed overtaler dig til at ændre kontaktoplysninger i vedkommendes kundeoplysninger for derved fremover at kunne logge sig ind på andre elevers medlemssider mv.

Phishing-forsøg skal rapporteres uden unødigt ophold til din nærmeste leder ELLER den GDPR-ansvarlige.