PIXI om databeskyttelse

Undervisning af medarbejdere i Selvejende Institutioner

Version 10.01.2022

Om personoplysninger

Hvad er en personoplysning

Personoplysninger er alle informationer der kan knyttes til fysiske personer, og som direkte eller indirekte fortæller noget om disse personer.
Det kunne **fx være** (ikke udtømmende)

- Navn
- Adresse
- CPR-nummer
- Ægteskabelig status
- Fagforening
- Helbred
- Billeder

Det indirekte ligger i, at informationer, hvis de gennemtænkes eller sættes sammen, også kan afsløre noget om en given person. Det kunne fx være

- Fagforening – kunne fortælle noget om politisk overbevisning
- Foreningsmedlemskab – kunne fortælle noget om interesseområder
- Billede – kunne fortælle noget om personen fx helbred
- Kombinationen af ovennævnte eksempler kan der yderligere udledes mulige oplysninger om den givne person.

Hvilke typer personoplysninger er omfattet, når der tales persondata

Der er fastlagt 30 forskellige typer af personoplysninger. Se vedlagt oversigt og forklaringer (bilag 1).

Der er forskel på personoplysninger. Personoplysninger er inddelt i 3 niveauer af følsomhed (som også fremgår af bilag 1).

Jo mere følsom en personoplysning er, jo strengere krav er der til, at personoplysningen er beskyttet, når den indsamles, anvendes og opbevares.

Almindelige oplysninger – er de mindst følsomme og anvendes med en fornuftig omtanke for sikkerhed.

Fortrolige oplysninger – er almindelige oplysninger, som er mere private personoplysninger og derfor skal behandles som fortrolige oplysninger og med en vis sikkerhed.

Følsomme oplysninger – er personoplysninger, som på grund af deres karakter er særligt følsomme, og derfor skal behandles med ekstra omtanke og sikkerhed

Beskyttelse af personoplysninger

Hvorfor skal vi passe på personoplysninger

Personoplysninger er ”kun til låns”. Det vil sige, at personoplysningerne ikke er institutionens oplysninger.

Dette gælder, uanset

- om en borger selv afleverer sine personoplysninger til institutionen eller
- om institutionen modtager/indsamler oplysninger om borgerne fra andre fx en forvaltning eller
- om institutionen selv henter oplysninger om borgerne fra andre fx offentlige myndigheder eller
- om institutionen/en medarbejder selv opsamler/noterer oplysninger om borgeren på papirnoter, huskesedler, fraværslister på PC og lign. (kaldes ofte ustrukturerede data).

Hvis personoplysninger kommer i de forkerte hænder, kan de misbruges. Det kan have en stor indflydelse på den person, hvis oplysninger det drejer sig om.

Det kunne være, at personen fx oplever forskelsbehandling, identitetstyveri, skade på sit omdømme, sociale konsekvenser, indflydelse på privatliv, skade på menneskelig værdighed mm.

Hvis det sker, kaldes det: ***et brud på fysiske personers rettigheder eller frihedsrettigheder.***

Det er grundlæggende det, som vi alle arbejder på at undgå.

Hvornår skal vi passe på personoplysninger

Der skal passes på personoplysninger i alle tilfælde:

1. Når de modtages fra borgere eller andre fx via mail, systemer, dokumenter eller mundtligt
2. Når de anvendes i daglige arbejde med borgerne
3. Når de opbevares fx som dokumentation for en beslutning
4. Når de sendes videre til borgere eller andre fx via mail eller systemregistreringer eller mundtligt

Den samlede betegnelse for pkt. 1-4 er, at der sker en ”behandling” af personoplysninger.

Hvordan passer vi på personoplysninger

Helt overordnet skal niveauet af databeskyttelse passe til dagligdagen i institutionen.

Det betyder, at måden personoplysninger behandles eller beskyttes på, ikke skal være en hindring for en fornuftig daglig drift.

Omvendt må der ikke slækkes på måden personoplysninger behandles eller beskyttes på, fx fordi det kan synes besværligt i det daglige arbejde

Dette er årsagen til, at databeskyttelseslovgivningen uddyber, hvordan man skal opføre sig i arbejdet med personoplysninger. Bl.a. skal man løbende overveje, om noget kan gå galt og beskytte oplysninger derefter.

Særlige opmærksomhedspunkter i dagligdagen

Samtykke

Alle personoplysninger som anvendes i jeres dagligdag, vil som udgangspunkt være lovlige at behandle.

Der er dog visse tilfælde, hvor borger eller medarbejder skal give deres samtykke inden personoplysningen må indsamles og bruges af institutionen eller videregives til andre udenfor institutionen. Det kan fx være i forbindelse med offentliggørelse af billeder.

Det er vigtigt at være opmærksom på hvilken borger/medarbejder, der har givet samtykke til hvad. Det er nemlig kun for disse personer og personoplysninger, at den aftalte behandling må foretages.

Din leder skal udpege de områder i dagligdagen, hvor samtykker er nødvendige.

Derudover skal din leder informere dig om, hvordan du i praksis skal behandle oplysninger så samtykket overholdes.

Hvis du skal deltage, når selve samtykket skal indgås, eller når det evt. trækkes tilbage, skal du også informeres om, hvilke rutiner der gælder for dette arbejde.

Kommunikation & Sociale Medier

Hvis der kommunikeres med borgere på mail, er det et lovkrav at mailen sendes krypteret, hvis den indeholder følsomme eller fortrolige personoplysninger. At en mail er krypteret, betyder populært sagt, at det indhold der er i mailen, kun kan læses af afsender og modtager af mailen.

På samme måde skal der være stor opmærksomhed ved anvendelse af sociale medier (Facebook, egen hjemmesider mv), og særligt at kommunikation via sociale medier på det kraftigste frarådes (chat-funktioner og tilsvaret). Neutrale opslag og anvendelse af billeder, kan ske som det er beskrevet herunder.

Billeder & Video

Billeder & video (herefter benævnt som billeder) anvendes ofte i dagligdagen.

I må gerne behandle billeder som led i jeres arbejde, hvis I har et konkret formål med det. Det kan fx være, at I har billeder af børnene på deres garderobekasser, eller billeder hængende af jeres borgere der laver forskellige aktiviteter.

I må gerne tage billeder og bruge dem internt i institutionen, hvis de borgere der er på billedet, ikke kan føle sig udstillede eller krænkede. Man skal derfor overveje, hvilke konsekvenser billedet kan have for de borgere, der er på billedet.

I skal altid bruge samtykke fra borgeren, hvis billederne skal offentliggøres fx på jeres hjemmeside, i trykte publikationer eller på jeres sociale medier. I bør selvfølgelig stadig overveje, hvilke konsekvenser en offentliggørelse af billedet kan have for borgeren ift. at føle sig udstillet/krænket.

En borger kan afvise, at der må tages billeder af vedkommende, uanset typen af billeder. Et samtykke kan også trækkes tilbage, og det medfører at der ikke må anvendes billeder af denne borger fremover.

Vær opmærksom på, at rydde op i billedarkiver, på medier (Facebook mv.), på telefoner, kamera, tablets mv., så der er et minimum af billeder, der skal administreres. Tag og gem ikke flere billeder end nødvendigt.

Borger spørger til hvilke oplysninger institutionen har om dem

Alle medarbejdere bør være opmærksom på, at borgere (og medarbejdere) direkte eller indirekte kan spørge til, hvilke oplysninger institutionen har om dem. Det kan også være:

- spørgsmål til om personoplysninger er korrekte
- indvendinger mod at personoplysninger indsamles og behandles
- ønsker til at personoplysninger slettes

Dette er en ret som borgeren har, og henvendelser som institutionen har pligt til at besvare. Dette kaldes at opfylde registreredes rettigheder.

I alle tilfælde må medarbejderen henvise borger til leder eller anden udpeget medarbejder, som har ansvaret for at svare på borgerens spørgsmål. Desuden bør medarbejder advisere leder om henvendelsen.

Opbevaring / slettefrister

Personoplysninger må opbevares så længe, at der er et behov / et formål med dette. Når formål / behov ikke længere er til stede, skal oplysningerne slettes. Der er naturligvis forskel på, hvor lang opbevaring/slettefristen er. Det afhænger af hvilket fagområde, der er tale om. Skal du være medansvarlig for opbevaring/sletning af personoplysninger, skal de nærmere regler og rutiner oplyses af din leder.

Fysisk sikkerhed

Fysisk sikkerhed dækker over den beskyttelse af personoplysninger der findes:

- i institutionens lokaler (dørlåse, aflåste skabe, valgt placering af personoplysninger i lokaler mv.),
- i og omkring teknisk udstyr (PC, printer, tablets, mobiltelefoner mv.),
- hos medarbejdere og andre personers adgange til lokaler
- gennem medarbejders adfærd i lokaler

Medarbejdere er medansvarlige for løbende at vurdere og overholde den fysiske sikring, der er vedtaget. Det gøres ved at være opmærksom på, at personoplysninger ikke håndteres eller opbevares forkert fx

- ved at tager en personalesag med følsomme oplysninger ud i et fælleslokale
- ved at PC/tablet ikke er låst, når den forlades
- ved at glemme at låse aftalte døre
- ved at samtale om personlige forhold med en borger samtidig med andre hører på osv.

Sker der noget, der minder om ovennævnte, bør der rettes op på forholdet med det samme, og det skal vurderes, om der er sket et potentielt eller faktisk persondatabrud.

Persondatabrud

Et persondatabrud er en hændelse, hvor personoplysninger er gjort tilgængelige for fremmende personer, der ikke skal have kendskab til oplysningerne. Det kunne fx være:

- En mail med personoplysninger er sendt til en forkert gruppe personer, der har åbnet mailen og læst informationerne.

- En medarbejder har adgang til personoplysninger, der ligger udenfor vedkommendes ansvarsområde, og medarbejderen har orienteret sig i oplysningerne.
- En liste med borgers private oplysninger er tabt i et indgangsparti og kan ikke genfindes.

Det kan også være en hændelse, hvor personoplysninger fx er "forsvundet/tabt/fejlformidlet" men er ikke nødvendigvis kommet til fremmede personers kendskab. Det kunne være:

- En mobiltelefon med personoplysninger, er tabt på et offentligt sted – men er returneret.
- En medarbejder har adgang til personoplysninger, der ligger udenfor vedkommendes ansvarsområde, men har IKKE orienteret sig i oplysningerne.
- Et pengeskab er stjålet og fundet, men ingen papirer med personoplysninger mangler

Som medarbejder er du medansvarlig for at opdage persondatabrud, uanset hvilken type der er tale om. I det øjeblik du opdager noget, der tyder på en fejl, der inkluderer forkerte personoplysninger til forkerte personer, **skal du omgående informere** den ansvarlige hos jer.

Persondatabrud skal håndteres indenfor 72 timer, så der er ingen tid at spilde.

BILAG 1 – Oversigt over personoplysninger

Persondatakategori	Niveau	Forklaring
Adresser generelt	Almindelig	Oplysninger om fysiske personers adresser
Anden information	Almindelig	Oplysning om en person, som ikke kan passe ind i én af nedenstående kategorier. Det kan fx være information om bolig eller bil, profilnavne på sociale medier, sko/ tøjstørrelser eller anden information om borger. Det må ikke være en følsom oplysning
Ansættelsesforhold	Almindelig	Oplysninger vedr. ansættelsesforholdet, f.eks. hvor den pågældende arbejder (tjenestested) eller om den pågældendes arbejdstid er 37 timer pr. uge
Digitale fodspor	Almindelig	Oplysninger om en persons færden i det digitale rum, f.eks. oplysninger om, hvilke hjemmesider personen har været inden på, eller hvilke wi-fi netværk personen har været logget på
Ejerforhold	Almindelig	Oplysninger om ejerforhold på f.eks. en ejendom
Foto, video	Almindelig	Fotos eller video med fysiske personer vil være personoplysninger, selv om det ikke findes andre identifikationsoplysninger på f.eks. fotos af børn i en børnehave.
Fødselsdato	Almindelig	
GPS-lokationer	Almindelig	GPS-lokationer, som kan sige noget om, hvor fysiske personer befinder sig (geografisk placering). GPS-enhed kan f.eks. sidde i en bil eller i en smartphone
Karakterudskrift	Almindelig	Karakterer
Kontaktoplysninger	Almindelig	Telefonnummer, e-mail osv.

Persondatakategori	Niveau	Forklaring
MAC-adresser / IP-adresser	Almindelig	MAC-adresser på fysisk udstyr (f.eks. mobiltelefoner, tablets, PC'ere og andet elektronisk udstyr), som anvendes til forbindelse til internettet. IP-adresse unikt nummer på enheder (f.eks. computere), som anvendes til kommunikation via internettet. MAC- hhv. IP-adressen kan anvendes til identifikation af den fysiske person, som anvender enheden (f.eks. en smartphone)
Matrikelnummer	Almindelig	Entydig identifikation af et arealstykke, som også kan kobles til den fysiske person, som f.eks. ejer det pågældende arealstykke
Personlig information	Almindelig	Information om en person, f.eks. navn, køn, alder
Registreringsnummer	Almindelig	Registreringsnummer på et indregistreret køretøj, som også kan identificere ejeren eller brugeren af køretøjet, f.eks. i forbindelse med nummerpladegenkendelse ved parkering
Uddannelse og CV	Almindelig	Oplysning om, hvilken uddannelse/uddannelser en person, har samt oplysninger om en persons ansættelse/kvalifikationer. Bemærk at oplysninger om karakterer er fortrolige oplysninger.
Forbrugsoplysninger	Almindelig	Oplysninger om el, vand og varmeforbrug
Børneattester	Fortrolig	Oplysninger om børneattester
Cpr-nummer	Fortrolig	Cpr-nummer
Familieforhold	Fortrolig	Oplysninger om en persons familiemæssige relationer, f.eks. at personen er gift eller skilt eller har fire børn med tre forskellige partnere
Indkomstforhold	Fortrolig	Oplysninger om en persons økonomiske indkomst
Kontooplysninger	Fortrolig	Fysiske personers kontooplysninger, f.eks. kontonummer og pengeinstitut
Sociale forhold	Fortrolig	Fysiske personers sociale forhold, f.eks. voldelige forældre
Socioøkonomisk data	Fortrolig	Oplysninger om fysiske personers sociale status, f.eks. uddannelse, indkomst, bolig- og arbejdsforhold
Straffedomme og lovovertrædelser	Fortrolig	Oplysninger om at en person er dømt (f.eks. for vold) eller har overtrådt loven (f.eks. fordi personen er blevet taget i at køre for stærkt og har fået et klip i kørekortet, samt en bøde)
Straffeattester	Fortrolig	Oplysninger om en fysisk persons domme, bøder og tiltalefrafald med vilkår for lovovertrædelser på baggrund af oplysninger registreret i Det Centrale Kriminalregister
Biometri	Følsom	Oplysninger, som stammer fra det enkelte menneske, f.eks. fingeraftryk, og som kan bruges til at identificere den pågældende
Etnicitet	Følsom	Oplysninger om, at den pågældende f.eks. stammer fra Somalien. Oplysningen er ikke følsom, hvis formålet med behandlingen ikke er behandling af oplysninger om etnicitet. Det vil den f.eks. ikke være, hvis etniciteten alene kan udledes af den pågældendes navn eller foto
Fagforening	Følsom	En oplysning om, at den pågældende er organiseret i en fagforening. En oplysning om, at en person ikke er organiseret, er en almindelig oplysning.

Persondatakategori	Niveau	Forklaring
Filosofiske overbevisninger	Følsom	Oplysninger om, at den pågældende f.eks. er buddhist (anses ikke som en religion)
Helbred	Følsom	Alle oplysninger, som siger noget om en persons helbred, f.eks. at en person har ADHD eller får en bestemt medicin. En oplysning om at en person er syg uden nærmere angivelse af, hvad den pågældende fejler, er en almindelig oplysning
Genetik	Følsom	Genetiske oplysninger, som kan henføres til en fysisk person, f.eks. ud fra en blodprøve
Politisk overbevisning	Følsom	Oplysning om, hvilken politisk overbevisning en person har. Kan både være medlemskab af et politisk parti og angivelser af, eller at en person har de samme holdninger som et givet politisk parti
Religiøs overbevisning	Følsom	Oplysning om, at en person f.eks. er kristen, muslim eller katolik
Seksuelle forhold	Følsom	Oplysninger om en persons seksualliv, f.eks. at en person har mange seksuelle partnere
Seksuel orientering	Følsom	Oplysninger om at en person f.eks. er heteroseksuel, biseksuel eller homoseksuel