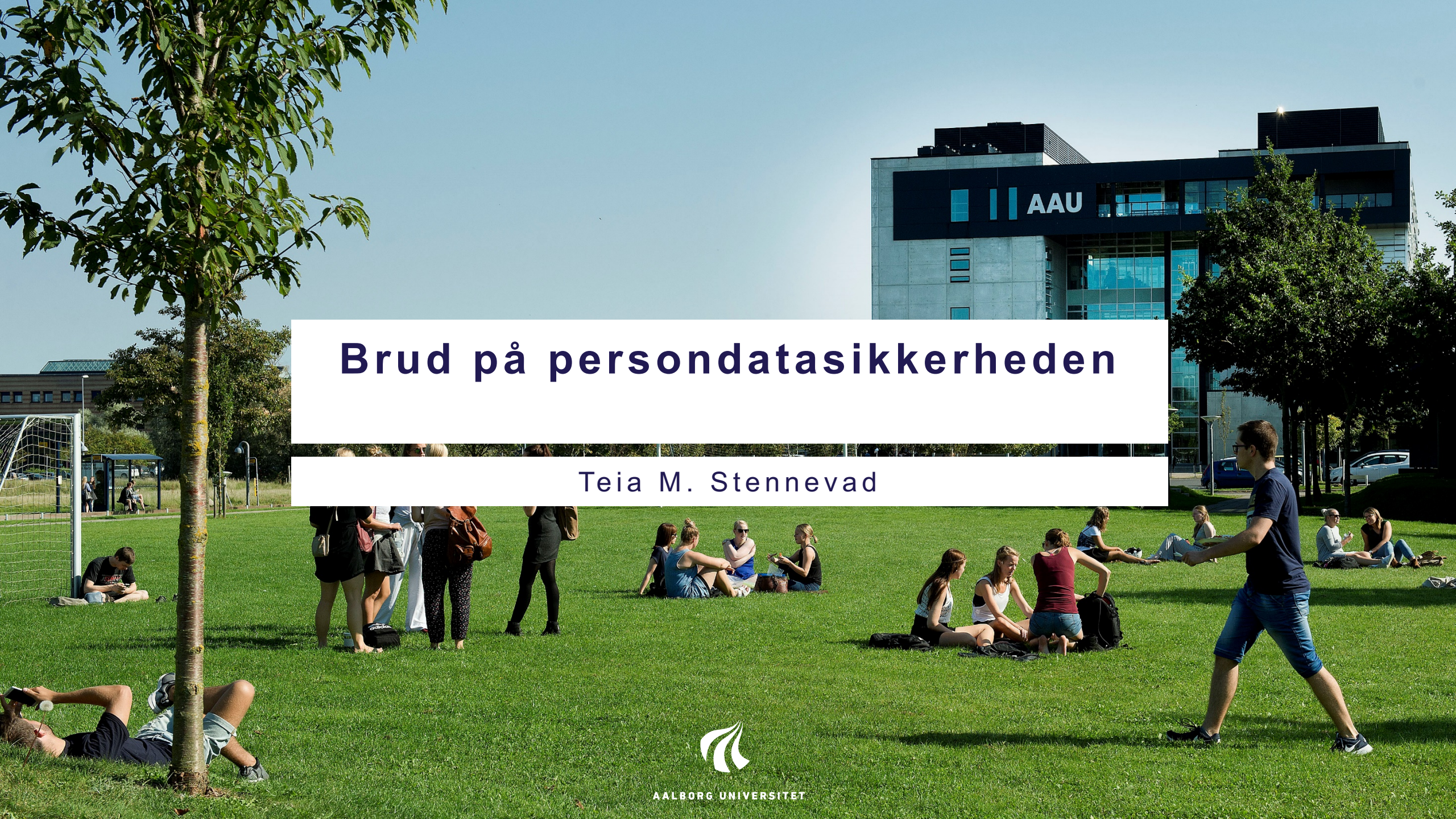


Brud på persondatasikkerheden

Teia M. Stennevad

AALBORG UNIVERSITET

Hvad er et brud på persondatasikkerheden?

- Databeskyttelsesforordningens definition: brud på persondatasikkerheden er en hændelse *der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet*
  - Når får (uautoriseret) adgang til personoplysninger, de ikke har et sagligt grundlag for at have adgang til. Det kan både være personer uden for eller inden for dataansvarliges organisation.
  - Den dataansvarliges medarbejdere ændrer eller sletter personoplysninger ved et uheld.
  - Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.
  - Den dataansvarliges medarbejdere videregiver ubevidst eller bevidst personoplysninger om en person (f.eks. Kunde) til en anden person (f.eks. Kunde) – eller måske ligefrem flere andre uvedkommende personer.
  - Når manglede kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

- Som med sikkerhedshændelser generelt så kigger man i praksis på om datas *fortrolighed, integritet eller tilgængelighed* er blevet kompromitteret

Kompromitteret fortrolighed

- Hvis datas fortrolighed er blevet kompromitteret, så betyder det, at nogen, som ikke burde have adgang til data, har fået det
  - Det kan gælde for både interne og eksterne – så fortroligheden kan både bliver kompromitteret, hvis en kollega, der ikke har en saglig grund (hvilket vil sige at de ikke har arbejdsopgaver, der relaterer sig til data) til at skulle se data, har fået adgang til dem, og det gælder også, hvis en eksterne part, f.eks. en samarbejdspartner, en besøgende eller lign. får adgang til data, som de ikke har en saglig begrundelse for at have adgang til, og dermed ikke er autoriseret til.
  - Hvis man printer man en liste med personoplysninger, som går til direkte print, og man enten glemmer det eller f.eks. får det sendt til en forkert printer, og man måske i sidste ende helt mister sit print
  - Eller man lader man en kollega låne sine adgangstilladelser til en løsning (f.eks. Workzone) og de går ind i en sag og får adgang til personoplysninger, som de ikke er autoriseret til
  - Man får selv tilsendt eller på anden vis adgang til personoplysninger, man ikke er autoriseret til

Kompromitteret integritet

- Hvis datas integritet er blevet kompromitteret, så betyder det, at der er sket noget med data, som gør, at de ikke længere er rigtige/korrekte
  - Der er altså sket en ændring af data. Det gælder både uautoriserede og utilsigtede ændringer af data
  - Det kan f.eks. være at data på en personalemappe ved et uheld er blevet ændret, hvis vi overskrive data f.eks. om en studerende, eller hvis en udefra kommende har skaffet sig adgang til data og ændret dem (i det sidste tilfælde vil både integritet og fortrolighed være kompromitteret)
  - Det kan også ske at en back-up er fejlet, og man kan ikke genskabe data korrekt

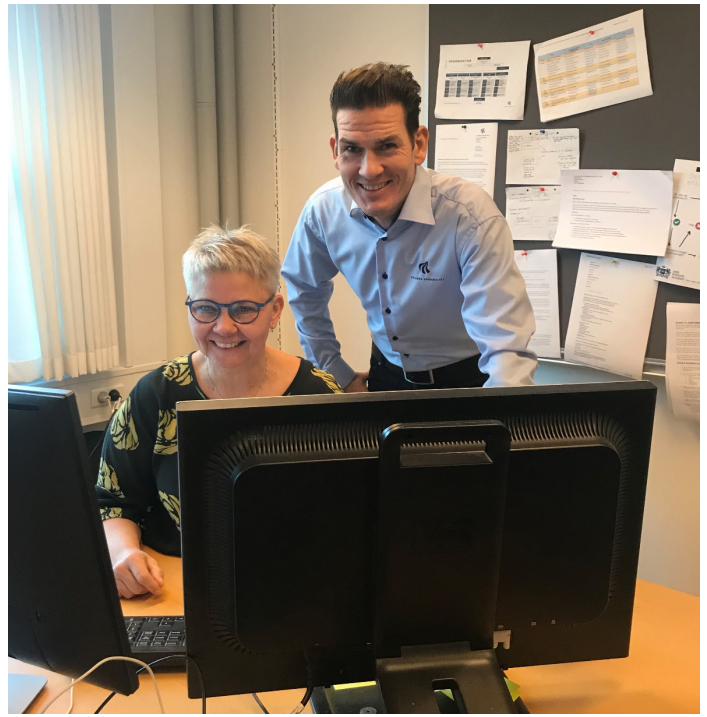
Kompromitteret tilgængelighed

- Hvis datas tilgængelighed er kompromitteret, så betyder det, at de der har brug for data (de der er autoriseret til at arbejde med data) ikke længere kan tilgå dem.
  - Der er f.eks. sket et nedbrud i et system, som gør, at data ikke kan tilgås, eller der er hackere, der har låst data på f.eks. en server, så medarbejdere ikke kan tilgå dem.
  - Det kan ske f.eks. ved nedbrug i lønsystemerne og medarbejderdata kan ikke tilgås, og dermed kan der ikke udbetales løn.
  - Særlig kritisk er dette også for hospitaler, hvis de ikke kan få adgang til digitale patientjournaler eller prøvesvar, hvis systemet er brud ned.

Processen for den interne anmeldelse

- Hvem kan anmelde?
  - Alle kan anmelde – både medarbejdere og eksterne (f.eks. studerende)
  - Anmelder kan f.eks. være den, der har forårsaget hændelsen (hvis man sender en mail til en forkert modtager), den der opdager hændelsen (hvis man opdager, at man har adgang til oplysninger i f.eks. en sag i WorkZone, som man ikke mener, man burde have adgang til, eller hvis man finde print liggende frit tilgængeligt med personoplysninger)

- Hvem tager imod anmeldelsen?
  - Det gør to af GDPR-enhedens medarbejdere: Dorthe Bach og Niels Dahl Thellufsen



Processen for den interne anmeldelse
Fortsat

- Under ‘Anmeldelse af sikkerhedshændelse’ (https://www.informationssikkerhed.aau.dk/sikkerhedshaendelser/) kan I finde det skema, der skal ske anmeldelse igennem
- Der vil ske tilrettelser i dette skema, så det vil ændre sig lidt i sin form
  - Det nye skema vil kræve lidt flere informationer end det nuværende. Det er ud fra tanken om, at de, der håndterer sikkerhedshændelse, skal vende tilbage til anmelder så lidt som muligt

Processen for den interne anmeldelse
Fortsat

- Når GDPR-enheden har modtaget anmeldelsen, går de i gang med at sagsbehandle
- Det er GDPR-enheden, der styrer processen og er ansvarlige for den
- De kontakter anmelder hvis:
  - De skal have uddybning af sagens omstændigheder
  - Hvis anmelder har en aktiv rolle i at 'stoppe ulykken'
  - Hvis anmelder har eller skal have en aktiv rolle med at forebygge at lignende hændelser sker igen

Processen for den interne anmeldelse
Fortsat

- Eksempel på sagshåndtering:
  - GDPR-enheden modtager en meddelelse om en anmeldt sikkerhedshændelse, hvor en medarbejder ved AAU har sendt en mail, der indeholder CPR-numre, til en forkert modtager.
    - Anmeldelsen oprettes som en sag (i WorkZone).
    - GDPR-enheden tager kontakt til den person, der har fejlsendt mailen for at afklare forløbet, og om der allerede er fortaget handlinger for at retten fejlen:
      - Har man forsøgt en tekniske tilbagekaldelse af mailen?
      - Er modtageren af de fejlsendte oplysninger blevet kontaktet?
      - Er modtageren af de fejlsendte oplysninger blevet bedt om at slette mailen?
    - Er der ikke blevet igangsat fejlrettende handlinger, tager GDPR-enheden initiativ til dette.
      - Ved en fejlsendt mail vil det typisk være den medarbejder, der har sendt mailen, som bliver bedt om at sende en opfølgningsmail – med støtte fra GDPR-enheden
    - Når hændelsen er håndteret og 'ulykken stoppet', så dokumenteres dette på sagen af GDPR-enheden – og sagen afsluttes
    - Er der behov for det, så laver GDPR-enheden en opfølgning – evt. i samarbejde med den medarbejder, der har sendt mailen, for at kigge på om lignende hændelser kan forebygges fremadrettet

Processen for den interne anmeldelse
Fortsat

- Det er GDPR-enheden (og DPO) der vurderer om hændelsen er af sådan en karakter, at den skal:
  1. Anmeldes til Datatilsynet, og
  2. Om der skal ske en orientering til den registrerede (den person, hvis personoplysninger er blevet kompromitteret)

- Og det er GDPR-enheden der varetager eventuel anmeldelse og orientering

Spørgsmål?

AALBORG UNIVERSITET