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
- Får stjålet en computer mv.
- 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 kontrol med sikkerhedsforanstaltninger truffet hos 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 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.