En del af de underretninger om brud på persondatasikkerheden, som Datatilsynet får, vedrører oplysninger sendt med mail til den forkerte person. Nogle af disse kan undgås, hvis man slår funktionen auto-complete fra i sit mailprogram[1].

I mange mailprogrammer hos både private virksomheder og offentlige myndigheder er det en standardindstilling, at systemet foreslår en modtager, man har skrevet til før, så snart man begynder at taste i modtagerfeltet.

Det er belejligt, fordi det sparer lidt tid. Men i nogle tilfælde resulterer det i, at man kommer til at sende mailen til den forkerte modtager - fx en anden kunde eller en borger med det samme fornavn som den, man egentlig ville have skrevet til. Det kan være et brud på persondatasikkerheden, hvis mailen indeholder personoplysninger, og i de tilfælde har den dataansvarlige pligt til at underrette Datatilsynet.

Denne type sikkerhedsbrud udgør en god del af alle de underretninger om sikkerhedsbrud, som vi modtager i Datatilsynet. Derfor anbefaler Datatilsynet, at man lader det indgå i sin risikovurdering - også selv om det går ud over funktionaliteten at slå auto-complete fra.

Ansvaret for vurderingen og indførelsen af, hvad der skønnes som passende foranstaltninger, påhviler altid den enkelte dataansvarlige.

Menneskelige og tekniske fejl

Groft sagt kan man dele sikkerhedsbruddene op i to kategorier - alt efter om de skyldes menneskelige fejl eller tekniske årsager.

Hyppigst ser vi **menneskelige fejl**, fx fejlindtastninger, klippe-klistre-fejl, manglende fjernelse af personoplysninger ved "anonymisering", flettebreve og - som nævnt ovenfor - auto-complete og lignende, der medfører, at modtageren bliver indtastet forkert eller ikke verificeret inden afsendelsen af mailen.

Af **tekniske årsager** til sikkerhedsbrud er typetilfældene: dårlig kode, URL'er hvor personoplysninger (telefonnumer, cpr-nummer e.l.) er en del af en offentliggjort URL, manglende kryptering, manglende validering af brugere, manglende patchning, ingen eller kun dårligt konfigureret firewall, manglende hærdning af eksponerede komponenter, "test"-systemer med livedata, og manglende segmentering af netværk / krydscontaminering.

[1] Link: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/dec/et-raad-til-at-undgaa-simple-sikkerhedsbrud/