

# Datatilsynet slår hårdt ned på utilstrækkelige risikovurderinger

PUBLICERET  
6 Maj 2020

Som følge af tre anmeldte databrud har Datatilsynet netop truffet en afgørelse om utilstrækkelige risikovurderinger og behandlingssikkerhed hos virksomheden Brobizz.

Brobizz anmeldte i efteråret 2019 tre databrud, hvor der i forbindelse med besvarelser af kundehenvendelser blev videregivet personoplysninger til uvedkommende. I forbindelse med Datatilsynets behandling af sagerne blev Brobizz anmodet om at fremlægge deres risikovurdering samt oplysninger vedrørende virksomhedens specifikke procedurer og instrukser om behandling af personoplysninger. Datatilsynet udtalte **alvorlig kritik**, idet de konkluderede, at Brobizz ikke havde foretaget en tilstrækkelig vurdering af risici i virksomhedens behandling af personoplysninger.

## DE KONKRETE HÆNDELSER

Sagen udspringer af tre hændelser, som fandt sted henholdsvis den 20. september, 29. november og 12. december 2019.

De specifikke hændelser forløb som følger:

1. En kundeservicemedarbejder udleverede telefonisk lokationsdata til en anden person end den registrerede kunde. Dette drejede sig om en person (A), der fik udleveret lokationsdata om sin ekskæreste (B).
2. En anden kundeservicemedarbejder opdaterede, på anmodning af C, ved en fejl kunde D's e-mailadresse med C's e-mailadresse, og sendte efterfølgende en ny kode til den C's e-mailadresse, hvorefter C havde adgang til kunde D's konto.
3. En tredje kundeservicemedarbejder opdaterede kunde E's e-mailadresse under kunde F's kundenummer, som kunde E angiveligt troede var sit eget, hvorefter kunde E kunne tilgå kunde F's Brobizz-profil.

## AFGØRELSEN

Datatilsynet angav, at der var grundlag for at udtale **alvorlig kritik** af Brobizz' behandling af de omtalte personoplysninger. Der lagdes særligt vægt på, at Brobizz' håndtering af kundernes personoplysninger ikke skete i overensstemmelse med reglerne i

databeskyttelsesforordningens artikel 32, stk. 1 og artikel 32, stk. 2, som uddybes her.

Datatilsynet gav samtidig Brobizz et **påbud** efter databeskyttelsesforordningens art. 58, stk. 2. Herefter skal BroBizz foretage en ny vurdering af risici for de registrerede, der er forbundet med den type behandling af personoplysninger, som BroBizz foretager. BroBizz skal særligt sikre den rigtige identitet på den person, der fremsætter en anmodning, som omhandlet i forordningens artikel 15-21, jf. artikel 32, stk. 2. Datatilsynet gav BroBizz en 4-ugers frist til at efterleve påbuddet.

#### BEGRUNDELSE FOR AFGØRELSEN

Datatilsynet traf sin afgørelse, fordi Brobizz' ikke havde sikret sig – og fået bekræftet – identiteten på den person, der fremsatte anmodning om indsigt i kunders persondataoplysninger. Kundeservicemedarbejderne videregav derudover personoplysninger om bl.a. lokation om tre kunder til uvedkommende. Det følger af databeskyttelsesforordningen, at:

- den dataansvarlige kan, hvis der hersker rimelig tvivl om identiteten af en person, fremsætte en anmodning om yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet.
- den dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved den dataansvarliges behandlinger af personoplysninger.

Da medarbejderne hos BroBizz ikke handlede i overensstemmelse med de persondataretlige regler, og fordi hændelserne samtidigt skete tre gange inden for en kort tidsperiode, fandt Datatilsynet, at sagerne er udtryk for, at de interne procedurer og instrukser enten ikke er tilstrækkelige, eller at medarbejderne ikke i tilstrækkelig grad er bekendt med håndteringen af personoplysningerne. Datatilsynet fandt derfor, at Brobizz ikke havde truffet passende foranstaltninger for at sikre et passende sikkerhedsniveau svarende til BroBizz' risici ved behandlingen af personoplysninger.

#### LUND ELMER SANDAGERS KOMMENTAR

Brobizz-sagen understreger endnu en gang vigtigheden af, at virksomheder, private som offentlige, overholder et passende sikkerhedsniveau ved behandling af personoplysninger og får analyseret de risici, der måtte være ved den pågældende virksomheds behandling af persondata. Det gælder specielt ved udlevering af personoplysninger, hvor virksomheden skal sikre, at den anmodendes identitet bekræftes

Lund Elmer Sandager rådgiver løbende om, hvordan risikovurderinger udarbejdes. Se vores tidligere artikel om risikovurderinger her.

Har du brug for rådgivning om GDPR og for hjælp til at sikre, at du overholder reglerne om kravene til interne risikovurderinger, herunder i forhold til en passende behandlingssikkerhed i din virksomhed, er du altid velkommen til at kontakte Lund Elmer Sandagers specialister i GDPR advokat Anders Linde Reislev eller associeret partner, advokat Torsten Hylleberg.

#### KONTAKT



## Torsten Hylleberg

### Associeret partner, advokat

Torsten Hylleberg leder IT-retsafdelingen og er certificeret IT-advokat.

Han er højt specialiseret indenfor persondataret og IT-ret og rådgiver en lang række private virksomheder og offentlige myndigheder. Torsten...

