DATATILSYNET

Bankernes EDB Central A.M.B.A.
Havsteensvej 4
4000 Roskilde
Danmark

Sendt med Digital Post

26. februar 2020

J.nr. 2019-431-0044
Dok.nr. 186619
Sagsbehandler
Poul Erik Weidick

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Brud på persondatasikkerheden

Datatilsynet er blevet bekendt med, at der i perioden fra før 25. maj 2018 til den 22. august 2019, har været en række hændelser relateret til Bankernes EDB Central A.M.B.A's (herefter BEC) system. Hændelserne har medført utilsigtet videregivelse af adresseoplysninger for personer, der havde adressebeskyttelse.

1. Afgørelse

Efter en gennemgang af sagen finder Datatilsynet, at der er grundlag for at udtale **alvorlig kritik** af, at BEC's behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens[1] artikel 5, stk. 1, litra f, og databeskyttelsesforordningens artikel 32, stk. 1.

Nedenfor følger en nærmere gennemgang af sagen og en begrundelse for Datatilsynets afgørelse.

2. Sagsfremstilling

Datatilsynet har modtaget en række anmeldelser om brud på persondatasikkerheden fra dataansvarlige, jf. databeskyttelsesforordningens artikel 33.

Datatilsynet har blandt andet modtaget anmeldelser fra Maj Bank A/S, Skandinaviska Enskilda Banken, Finansiel Stabilitet, Salling bank, Hvidbjerg Bank, Frøslev-Mollerup Sparekasse, BIL Danmark, Fynske Bank, Møns Bank, Merkur Andelskasse, Coop Bank A/S, Handelsbanken, PFA Bank, Lolland Bank A/S, Swedbank, Totalbanken, Vestjyske bank, Danske Andelskasse Bank, Frørup Andelskasse, Nykredit Bank A/S, Spar Nord Bank A/S, Faster Andelskasse, Andelskassen Fælleskassen, Lægernes Bank, Den Jyske Sparekasse og Arbejdernes Landsbank.

Anmeldelserne drejer sig om videregivelse af adresseoplysninger for personer, der er registreret med beskyttet adresse i Det Centrale Personregister (CPR)
Adresseoplysningerne er utilsigtet videregivet i forbindelse med automatiserede overførsler mellem pengeinstitutter. Det skønnes, at mere end 20.000 kunder har været berørt af fejlen.

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

Det fremgår af sagen, at BEC er databehandler for en række pengeinstitutter, hvor af en del er medejere, og dermed medlemskunder, og en anden del er servicekunder.
Databehandlingen er foregået inden for rammerne af indgåede standardiserede databehandleraftaler.

En systemfejl i et system, som BEC har driftet for de dataansvarlige, har medført, at der ved en række betalingsoverførsler (clearinger) til betalingsmodtagere i et andet pengeinstitut hos BEC eller hos andre datacentraler er blevet videregivet adresseoplysninger om personer, som i CPR-registret er markeret med adressebeskyttelse.

Følgende fire forskellige forhold har været skyld i hændelsen:

1) der har været tale om en ældre løsning, hvor der ikke er implementeret adressebeskyttelse
2) i forbindelse med konvertering af oplysninger fra et ældre system til et nyt system er der sket en ukorrekt konvertering af en markering, der styrer adressebeskyttelsen
3) markeringen af adressebeskyttelse – i forbindelse med kunders ajourføring af betalinger i netbanken – er ved en fejl er blevet nulstillet.
4) kunders valg om at tilknytte en såkaldt ”særlig adresse” til sin konto, som ikke kontrolleres for adressebeskyttelse i systemet, er ved en fejl er blevet videregivet ved overførslen.

Det fremgår af sagen, at BEC har rettet fejlen ved at foretage en række programrettelser i systemet, og derudover har afskærmet de uretmæssige oplysninger for betalingsmodtagere i BEC’s onlinesystemer (netbank og mobilbank). BEC har den 3. september 2019 slettet de historiske posteringer fra danske pengeinstitutter og efterfølgende den 14. oktober 2019, slettet 2000 posteringer, fra udenlandske pengeinstitutter, det ikke var muligt at slette i første omgang.

3. BEC’s bemærkninger

BEC har ved skrivelse af den 27. december 2019 bekræftet de anførte faktiske omstændigheder.

BEC bemærker i sin redegørelse, at det fremgår af sektoraftaler (Håndbog for Sumclearingen, Håndbog for Intradagclearingen og Håndbog for Straksclearingen), at betalingsoverførsler mellem to parter normalt ledsages af adresseoplysninger, så betalingsmodtageren kan identificere betalingsafsenderen. I sektoraftalerne behandles begrebet adressebeskyttelse ikke.
Sektoraftalerne er udarbejdet med udgangspunkt i regler for videregivelse af oplysninger i betalinger, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler. Denne forordning behandler ikke adressebeskyttelse.
Regler for behandling af beskyttede adresser fremgår af LBK nr. 646 af 02/06/2017 (CPR-Loven), bl.a. § 28 om etablering af adressebeskyttelse og § 44 om videregivelse til andre private. CPR-loven nævner fx kreditoplysningsbureauer men udtrykker sig ikke klart om betalingstransaktioner og clearing.
BEC har dog lagt til grund, at det vil være i overensstemmelse med CPR-lovens hensigt, at adresseoplysninger om personer med (navne- og) adressebeskyttelse ikke videregives til betalingsmodtagere i forbindelse med betalinger, hvilket utilsigtet er sket i denne sag.

BEC anfører videre, at adresser, herunder også beskyttede adresser, fortsat sendes til udenlandske betalingsformidlere, idet disse ellers vil blive afvist i modtagende pengeinstitut på grund af anti-hvidvask- og anti-terrorfinansieringskontroller.

BEC har foretaget en systematisk gennemgang af sine systemer og den anledning udført en række programrettelser. En intern systemtest i BEC viste den 22. oktober 2019, at der i visse tilfælde ved udtræk af posteringer via netbank under visse betingelser og forudsætninger var mulighed for at inkludere adresser for 3. mandsoverførsler inden for samme pengeinstitut – herunder også beskyttede adresser – i filudtræk. Der er tale om filudtræk, som typisk anvendes af erhvervskunder til brug for disses interne økonomisystemer.
BEC har håndteret denne konstaterede risiko i forhold til de konkrete berørte dataansvarlige som en tilføjelse til den oprindelige hændelse og udsendt data til de dataansvarlige til brug for disses konkrete risikovurdering og yderligere behandling af sagen.

BEC har oplyst, at deres systemer har kørt i mange år. Betalingstransaktionerne kører i lukkede systemer, og der er ikke nogen manuel håndtering eller kontrol af transaktionerne, fra de initieres af en bankkunde eller en bankrådgiver, til de modtages hos betalingsmodtager. En konstatering af fejlen har således beroet på, at en bankkunde har henvendt sig til sin bank, fordi vedkommende har haft mistanke om eller konstateret, at en betalingsmodtager har modtaget en beskyttet adresse.

Generelt har BEC's systemer håndteret adressebeskyttelse siden 18. september 2015. Analyser har dog vist, at funktionaliteten i en række systemer ikke har været implementeret eller ikke har fungeret efter hensigten.

De håndbøger, der ligger til grund for betalingstransaktioner, udfærdiges af Finans Danmark, og håndbøgerne har hidtil ikke nævnt problematikken omkring adressebeskyttelse.
Udvikling og test af systemer har derfor hidtil fokuseret på kravspecifikationer, som udspringer af sektoraftalerne samt Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015, hvor det af artikel 4, stk. 1, fremgår at betalerens adresse, officielle personlige dokumentnummer, kunde-id-nummer eller fødselsdato og -sted skal medsendes ved pengeoverførsler. Dermed har hovedfokus været på transaktionsflow. Da adressebeskyttelse ikke nævnes specifikt i nævne direktiv og sektoraftaler, er forhold omkring adressebeskyttelse beklageligvis ikke blevet behandlet i nødvendigt omfang.
Dette kan være en medvirkende årsag til, at der ikke har været tilstrækkelig opmærksomhed og eksplicit kravstilling vedrørende adressebeskyttelse i betalingstransaktioner.

BEC har anført, at adressebeskyttelse aktiveres af borgeren i CPR-registeret via bopælskommunen for en vis periode ad gangen eller permanent efter en myndighedsvurdering.
BEC har derfor alene adgang til oplysninger fra CPR om aktuelt beskyttede adresser, og tidspunktet for adressebeskyttelsens etablering. Det er derfor ikke muligt at opgøre antallet af historisk berørte registrerede præcist.
Den 10. september 2019 har BEC efter forespørgsel til CPR-Kontoret fået afslag på en anmodning om at modtage historiske CPR-data omkring adressebeskyttelse fra Social og Indenrigsministeriet med henvisning til CPR Lovens § 38.

4. Begrundelse for Datatilsynets afgørelse

Datatilsynet lægger – ud fra BEC's egen forklaring – til grund, at BEC i denne sag uberettiget har videregivet adresseoplysninger for personer til uvedkommende, selv om personerne var registreret i CPR med beskyttet adresse, der derfor ikke måtte videregives.
BEC derved ikke i tilstrækkelig grad har levet op til reglerne i databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Idet BEC's systemer siden 2015 har indeholdt fejl, der har resulteret i at kunders beskyttede adresseoplysninger, er blevet videregivet til uvedkommende, har BEC ikke under hensynta-

gen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, foretaget tilstrækkelige og passende tekniske eller organisatoriske foranstaltninger for at sikre tilstrækkelig sikkerhed for de pågældende oplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling, ligesom der ikke har været en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af disse foranstaltninger.

Datatilsynet finder, at BEC ved at anvende en ældre IT-løsning, hvor der ikke var implementeret adressebeskyttelse og at konverteringen af personoplysninger fra et ældre system til et nyt system ikke skete korrekt og uden at der var etableret kontrolforanstaltninger, der kunne opdage dette, ligesom markeringen af adressebeskyttelse – i forbindelse med kunders ajourføring af betalinger i netbanken – ved en fejl blev nulstillet og en række kunders tilknytning af en selvvalgt adresse til deres konti ikke blev kontrolleret for adressebeskyttelse og derfor blev videregivet, ikke har levet op til reglerne i databeskyttelsesforordningens artikel 32, stk. 1.

Det er Datatilsynets opfattelse, at der i forbindelse med behandling af personoplysninger, skal ske test og løbende opfølgning, der sikrer, at personoplysningerne behandles med vedvarende fortrolighed, integritet, tilgængelighed og robusthed.

Datatilsynet anser det for skærpende omstændigheder, at et meget stort antal kunders adresseoplysninger har været videregivet, selvom disse var registreret som beskyttede i CPR og at fejlene i BEC's systemer har været tilstede siden 18. september 2015, uden at dette er blevet opdaget.

I formildende retning har Datatilsynet lagt vægt på, at de modstridende regler i Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger – herunder adresseoplysninger – der skal medsendes ved pengeoverførsler og reglerne om beskyttede adresser i LBK nr. 646 af 02/06/2017 (CPR-Loven), kan være en medvirkende årsag til, at BEC ikke entydigt har kunnet afgøre, om adresseoplysninger skulle medsendes i betalingstransaktioner eller ej.
Datatilsynet lægger også vægt på, at BEC hurtigt og effektivt – efter bruddets konstatering – har bragt bruddet til ophør og foranlediget alle de videregivne adresser slettet.

Samlet set skal Datatilsynet udtale **alvorlig kritik** af Bankernes EDB Central A.M.B.A.
for de skete overtrædelser.

Det bemærkes, at Datatilsynet forventer at offentliggøre afgørelsen på Datatilsynets hjemmeside.

Datatilsynet anser hermed sagen for afsluttet og foretager sig herefter ikke yderligere i sagen.

Med venlig hilsen

Poul Erik Weidick

Bilag: Retsgrundlag.

Uddrag af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

Artikel 5. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)
b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)
c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)
d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)
e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)
f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Stk. 2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

Artikel 32. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.