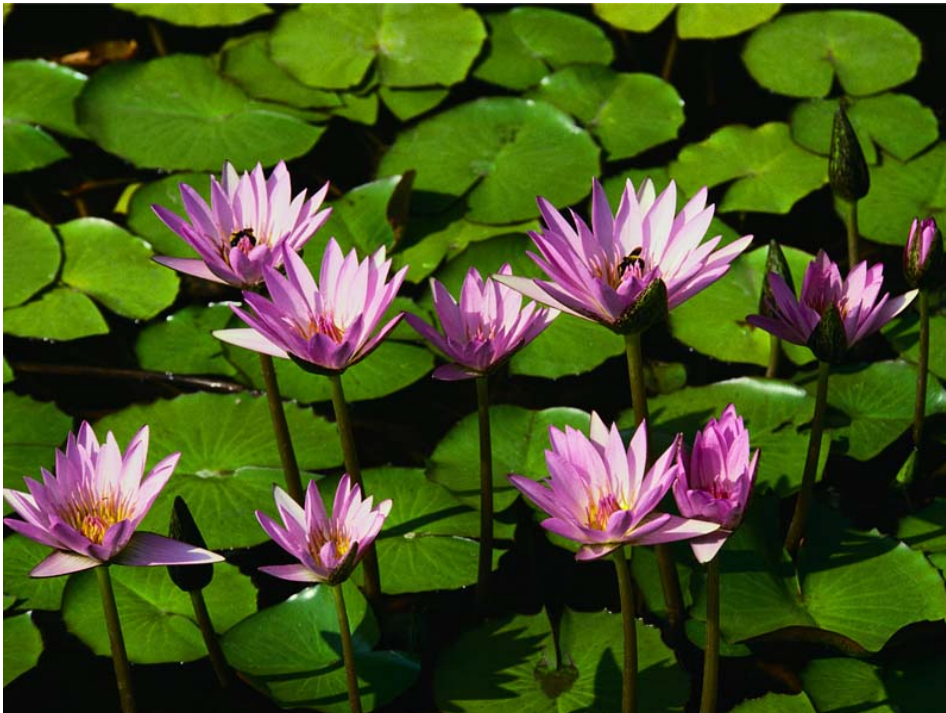


Prosjekt – Behandling av personopplysninger i finanskonsern

1.	Mandat.....	2
2.	Kartlegging av aktuelle problemstillinger.....	2
2.1	Skillet mellom vesentlig mislighold og annen behandling	3
2.2	Sletterutiner	3
2.3	Bruk av felles elektronisk kundesystem	4
2.4	Tilgangsstyring	4
2.5	Skillet markedsføring og kundepleie	5
2.6	Misligholdsregister	5
2.7	Kvalitet	6
3.	Avslutning	6



1. Mandat

I henhold til prosjektbeskrivelsen¹ skulle gruppen legge spesielt vekt på:

- kartlegging av hvordan personopplysninger flyttes eller deles mellom virksomheter i konsernet,
- kartlegging av felles elektroniske kundesystemer,
- om kundenes rettigheter etter personopplysningsloven blir ivaretatt,
- kvalitet på kundeopplysninger og
- om tilsynene gir indikasjoner på urettmessig bruk av opplysninger på tvers av virksomheter.

Deltakere:

Christine Ask Ottesen

Frode Bergland Bjørnstad (prosjektleder)

Gruppen har:

- Avholdt møte med Finansnæringens hovedorganisasjon forut for tilsynet for å få bedre kjennskap til aktuelle problemstillinger
- Gjennomført 10 stedlige tilsyn i Oslo, Bergen, Førde og Trondheim
- Rapportert ved gjennomført planlegging, ved gjennomførte tilsyn og ved utsendelse av rapport.

2. Kartlegging av aktuelle problemstillinger

Gruppen har på bakgrunn av prosjektets mandat og tilsynene, valgt å ta opp følgende problemstillinger i hovedrapporten:

- 1) Skillet mellom vesentlig mislighold og annen behandling
- 2) Sletterutiner
- 3) Bruk av felles elektronisk  desystem
- 4) Indikasjoner på urettmessig bruk
- 5) Kvalitet
- 6) Tilgangsstyring
- 7) Misligholdsregister
- 8) Skillet mellom markedsføring og kundepleie

¹ Vedlegg 1

2.1 Skillet mellom vesentlig mislighold og annen behandling

Bankkonsesjonen oppstiller, i tillegg til regelen om sletting når det ikke lenger er et saklig behov for oppbevaring av opplysningene jf personopplysningslovens § 28, to særskilte slettefrister. Opplysninger om kundens betalingshistorikk skal slettes senest innen 4 år fra registrering, Opplysninger om vesentlig mislighold av kontraktsforpliktelser kan likevel oppbevares i inntil 10 år.

Gruppen stilte under samtlige tilsyn spørsmål om konsernets syn på skillet mellom vesentlig mislighold og annen behandling. Få eller ingen av konsernene hadde definert dette skillet konkret. Noen antok at man skulle forholde seg til inkassoreglene, men også her var vurderingene forskjellige med hensyn til om 30, 60 eller 90 dager forsinket betaling ville utgjøre et vesentlig mislighold.

Hva som legges i begrepene vesentlig mislighold og annen behandling er, slik konsesjonen er utformet per i dag, avgjørende for når opplysningene skal slettes. Det er derfor viktig at man kommer frem til en felles forståelse av begrepenes innhold. Datatilsynet har heller ingen klar oppfatning eller praksis i forhold til hva som ligger i begrepene. Se også nærmere under punkt 2.2.

Konklusjon oppfølging:

Gruppen er av den oppfatning at det bør vurderes hvorvidt skillet vesentlig mislighold og annen behandling bør endres i konsesjonen. Per i dag har de ingen særlig betydning for finanskonsernenes oppbevaring av personopplysninger, og begrepene virker for vage i forhold til de mange behov virksomheten kan ha for oppbevaring av opplysninger.

Etter gruppens vurdering bør det utarbeides klarere sletteregler, se pkt 2.2, hvor skillet for fortsatt oppbevaring defineres nærmere enn i dag. En slik endring bør baseres på en dialog med virksomhetene og interesseorganisasjonen.

2.2 Sletterutiner

De fleste bankene hadde for dårlige rutiner knyttet til sletting av kundeopplysninger. Mange banker var ikke kjent med konsesjonens regler for sletting. I bankkonsesjonen fremgår det at opplysninger om kundens betalingshistorikk skal slettes senest innen 4 år fra registreringen. Opplysninger om vesentlig mislighold av kontraktsforpliktelser kan likevel oppbevares i inntil 10 år.

Kravet om sletting må ses på bakgrunn av formålet i samsvar med personopplysningsloven § 28. Dette medfører at kundeopplysninger ikke nødvendigvis må slettes fra aller registre. I konsesjonens punkt 5 heter det at opplysninger om kunders betalingshistorikk skal slettes senest 4 år fra registrering. Det er for bankene uklart hva som ligger i dette. I praksis blir kravet sjelden fulgt. Ofte vil andre formål tilsi en behandling av opplysningene utover de 4 årene. Da dette ikke fremkommer klart, kan bestemmelsene misforstås².

² Det fremgår av konsesjonen at slettefristene bare gjelder for kundeadministrasjon, fakturering og gjennomføring av bank- og finansieringstjenester.

Konklusjon/oppfølging :

Gruppen foreslår at konsesjonen, på sikt, tydeliggjøres slik at det klarere kommer frem at andre formål innenfor vanlig bankvirksomhet kan tilsi lagring utover slettefristene i punkt 5.

2.3 Bruk av felles elektronisk kundesystem

Med felles elektroniske kundesystem forstår gruppen alle system hvor det behandles kundeopplysninger og hvor opplysningene er tilgjengelige for flere virksomheter i samme finanskonsern. Ut fra tilsynene er gruppen av den oppfatning at det ikke nødvendigvis bør tillegges avgjørende betydning hvorvidt registeret ligger hos morselskapet eller et datterselskap. Det bør i stedet tillegges betydning hvorvidt registeret brukes av flere selskap i samme konsern.

Ut fra gjennomførte tilsyn er det få konsern som har sentrale registre for hele virksomheten. Mange har likevel et samarbeid mellom ulike virksomheter. Samarbeidet varierer fra at bankene har ansvar for hele salget av forsikring, til at bankene formidler kontakt til andre selskap.

Innenfor bankvirksomheten er det for alle et felles system for alle filialene. Systemet er bygget opp slik ut i fra den tanken at kunden skal kunne henvende seg i en hvilken som helst filial og få tilfredsstillende behandling. Det ble også opplyst at banken var av den oppfatning at kunden forventet at banken hadde tilsvarende informasjon som det kunden selv kunne se i sin nettbank. For bankene er det noen variasjoner ut fra selskapsstruktur. I to av bankene hadde bankene som eide konsernet egne kunder, mens kundene til selskapene i selve konsernet ble delt.

2.4 Tilgangsstyring

Gruppen har ved flere tilsyn sett at tilgangen til kundesystemene er svært vide. Kundebehandlerne kan ofte gå inn på alle bankens kunder. Kundeopplysningene kan gi til dels følsom informasjon om den enkelte. Slik systemene er i dag føres det svært lite kontroll med hvorvidt kundebehandlerens innsyn er rettmessig eller uretmessig. Bankene uttrykker ofte at de må ha tillit til sine egne ansatte. Det er et paradoks at bankene gir sine egne ansatte vesentlig større tillit når det gjelder beskyttelsen av andres interesser, her personvern, i motsetning til bankens egne, for eksempel fullmakter til å innvilge lån. Gruppen er fra andre områder kjent med at fristelsen til å lese andres opplysninger kan bli for stor. Tilsynet er av den oppfatning at det kan forekomme tilfeller hvor ansatte foretar innsyn hos naboer, familie eller personer som omtales i media.

Dette kan også ses som et spørsmål om informasjonssikkerhet. Når bankene gir vide tilgangsrettigheter, må de på annen måte sikre at egne ansatte ikke uretmessig misbruker disse tilgangene. Dette kan for eksempel gjøres ved å lage systemer som aktiverer tilgang ved kontakt fra kunden, mislighold av lån osv. Dersom bankene i tillegg foretar stikkprøver av hvorvidt tilgangen misbrukes vil dette gi bedre beskyttelse.

Personopplysningsloven § 11 d) oppstiller et krav om at opplysningene skal være relevante. I dette ligger det også at det ikke skal behandles flere opplysninger enn det som er nødvendig. I forhold til den enkelte ansatte får dette betydning i forhold til hvilke opplysninger det faktisk skal gis tilgang til, ut i fra en vurdering av den ansattes saklige behov for opplysninger. Dette gjelder

særlig når opplysningene er følsomme og av sensitiv karakter. Informasjonen eller tilgangen til disse opplysningene må derfor begrenses.

Konklusjon/ oppfølging: Datatilsynet bør gjennom dialog med interesseorganisasjonene, samt gjennom nye tilsyn, fortsette dette arbeidet.

2.5 Skillet markedsføring og kundepleie

Svært få banker brukte begrepet markedsføring. Markedsføring defineres i konsesjonen som aktivitet som har til hensikt å overtale nye eller eksisterende kunder til å inngå avtale om produkt i en ny produktkategori. I stedet ble det brukt begrep som skulle indikere at dette var kundeoppfølging. Det er i seg selv ikke noe galt med å drive verken kundeoppfølging eller markedsføring.

Problemet var imidlertid at flere banker ikke hadde et klart skille mellom når de behandlet personopplysninger til markedsføring og kundepleie. Skillet vil ha betydning for hjemmelsgrunnlag for behandlingen (eventuell innhenting av samtykke), bankenes adgang til å bruke opplysninger og eventuell vask mot reservasjonsregisteret i Brønnøysund.

I Datatilsynets konsesjon skilles det mellom hvorvidt kunden kontaktes i forbindelse med produkter man allerede har, eller om kontakten gjelder nye produkter. Dette skillet er avgjørende for hvorvidt en rekke plikter vil gjøre seg gjeldende for den behandlingsansvarlige virksomhet, se avsnittet over.

Konklusjon/oppfølging

Gruppen er av den oppfatning at virksomhetene ikke har en helt klart vurdering av skillet markedsføring og kundepleie. Gruppen har imidlertid ingen indikasjoner på at det markedsføres på tvers av disse grensene i strid med personopplysningsloven.

2.6 Misligholdsregister

De fleste bankene hadde i en eller annen form opplysninger om mislighold. Noen virksomheter har dette i form av egne system, andre har det lagret i det normale kunderegisteret og andre igjen utarbeider enkle filer som sendes til de ansvarlige for å følge opp slike forhold.

At finanskonsern har et behov for å føre en viss kontroll med mislighold, og hvilke kunder som eventuelt påfører slike tap, er klart. Spørsmålene i forhold til hvor lenge opplysningene kan lagres, hvem som har et saklig behov for tilgang til opplysningene og hvordan opplysningene eventuelt bør lagres er imidlertid ikke avklart.

Retten til rehabilitering er et viktig personvernprinsipp som vil ha stor betydning for hvor lenge finanskonsern kan lagre misligholdsopplysningene. Dette må særlig ses i sammenheng med pkt 2.1, hvor det fremgår at bevisstheten rundt hva som antas å være et vesentlig mislighold virker noe uavklart.

Finansnæringens hovedorganisasjon har konsesjon for opprettelse av et sentralt misligholdsregister. Dette misligholdsregisteret virker å være lite i bruk. Få konsern melder inn opplysninger hit, og tilsvarende gjelder også for sjekk mot registeret. Ettersom det enkelte

konsern har en eller annen form for misligholdsregister, stiller gruppen spørsmål ved behovet for den sentrale misbruksregisteret.

Konklusjon/oppfølging

Etter gruppens oppfatning kan brevkontroll med konkrete spørsmål være aktuelt. Det vil uansett være nødvendig at det utarbeides klare retningslinjer for lagring og bruk av disse opplysningene.

I tillegg er det nødvendig å vurdere FNHs konsesjon for et sentralt register på dette området.

2.7 Kvalitet

Gruppen har hovedsakelig ført tilsyn med store finanskonsern. Det har således ikke blitt foretatt grundige kontroller av de enkelte bankenes registre. Likevel vurderer gruppen det slik at bankene, i all hovedsak, har god kvalitet på personopplysningene. Bankenes opplysninger består hovedsakelig av faktalignende opplysninger, for eksempel at en har søkt om utvidelse av et lån i tillegg til rene kontaktopplysninger og hvilke produkter kunden har avtale om. Kundene har også en egeninteresse i å holde kontaktopplysninger og andre opplysninger oppdatert.

Konklusjon/oppfølging:

Dersom det er ønskelig med en grundigere kontroll, anbefaler gruppen målrettede tilsyn mot enkelte deler av virksomhetene. Ut i fra inntrykk på tilsynene virker dette imidlertid ikke nødvendig, med mindre tilsynet skulle være av mer konkret karakter, for eksempel basert på tips fra publikum.

2.8 Indikasjoner på urettmessig bruk

Datatilsynet har ingen klare indikasjoner på urettmessig bruk. Tilsynet har imidlertid ved enkelte banker oppdaget at samtykkeklausulen er ferdigutfylt. Dette kan indikere at samtykket ikke vil være uttrykkelig. Kravene til samtykke, jf. personopplysningsloven § 2 nummer 7 vil da ikke være oppfylt. Gruppen har bedt om redegjørelse for bankenes praksis med å innehente samtykke. For øvrig vises det til at tilsynene er gjennomført på overordnet nivå, se pkt. 2.7 Kvalitet. Gruppen viser også til at de fleste banker ikke har tilstrekkelige sletterrutiner, se pkt 2.2.

Konklusjon/oppfølging:

Dersom det er ønskelig med grundigere kontroll, anbefaler gruppen målrettede tilsyn mot enkelte deler av virksomheten.

3. Avslutning

Formålet med prosjektet er etter prosjektgruppens vurdering oppnådd. Rapporten besvarer i hovedsak oppgavene som ble gitt i mandatet.

På enkelte områder har det likevel ikke vært mulig å få ønsket oversikt over praksis. Det vises eksempelvis til punktet om kvalitet. Videre har det dukket opp spørsmål underveis som best kan

avklares ved videre kartlegging eller stedlige tilsyn. Eksempel på slike, er spørsmålet om kundebehandlernes tilgang, spørsmålet om et sentralt misligholdsregister er nødvendig, det enkelte konserns misligholdsregister, samt sletterutiner. Gruppen mener det er grunn til å følge opp prosjektet videre.