SAMTYKKE

Sist revidert: 06.02.2017

Arbeidsgruppe: Marte Shetelig (Storebrand) og Fred Richard Elsheim (DNB)

Referansegruppe: Trond Kiplesund (Sparebank 1) og Torjus Sandvik Moe (Handelsbanken)

Formålet med dette notatet er å gi en foreløpig vurdering av hva som eventuelt blir nytt og/eller endret i forhold til gjeldende rett ved implementering av GDPR/ny norsk lov, for det ovennevnte tema. Notatet er basert på den engelske, danske og/eller svenske versjonen av GDPR, og må revideres i forbindelse med norsk oversettelse samt høring/implementering av norsk lov. Også senere uttalelser fra myndigheter, artikkel 29 gruppen mv. kan gi grunnlag for en revisjon av notatets vurderinger og konklusjoner. Notatet har ikke som formål å gi en uttømmende beskrivelse av gjeldende rett.

FORORDNINGEN

(Beskrivelse av innholdet/kravene etter forordningen med henvisninger til de aktuelle artikler.)

Direktivet artikkel 2	Personopplysningsloven § 2	Forordningens artikkel 4
(h)'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	7)samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,	(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

De sentrale artikler om samtykke i forordningen:

I all hovedsak videreføres definisjonen av samtykke nå i forordningens artikkel 4 (11), ref. direktivets artikkel 2 bokstav h og personopplysningslovens § 2 (7).

Samtykke er i artikkel 4 (11) definert som følger:
*"«consent» of the data subject means any **freely given**, **specific**, **informed** and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"*

Direktivet artikkel 2 bokstav h lyder:
"(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

Personopplysningslovens § 2 (7) lyder:
"samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,"

Personvernforordningen angir i artikkel 6 nr. 1 at samtykke i artikkel 6 nr. 1 (a) er ett av flere mulige og likestilte hjemmelsgrunnlag for lovlig behandling av personopplysninger. I finansnæringen er et av de mest praktiske hjemmelsgrunnlag *nødvendig behandling for å kunne inngå eller gjennomføre en avtale* jf. artikkel 6 nr. 1 (b), som i dag er å finne i personopplysningslovens § 8, bokstav a).

I likhet med dagens regelverk, personopplysningslovens § 8, kommer samtykke etter artikkel 6 nr. 1 (a) ikke til erstatning for avtalegrunnlaget i artikkel 6 nr. 1 (b), men som et alternativt eller ekstra hjemmelsgrunnlag der hvor den aktuelle behandling ikke kan gjennomføres med hjemmel i avtale alene. Samtykke alternativt/ekstra hjemmelsgrunnlag gjelder også i forhold til de øvrige grunnlag i artikkel 6 nr. 1 bokstavene (c) til og med (f). De konkrete betingelser for å kunne anvende samtykke presiseres i form av dokumentasjonskrav, formkrav, mulighet for tilbakekall, mv. i forordningens artikkel 7.

Sentrale punkt i forordningens fortale:

Forordningens fortale er mer informativ enn direktivets:

- "freely given" (avgitt frivillig): Samtykke er hjemmelsgrunnlag for behandling av personopplysninger ut over det som er nødvendig for å gjennomføre en «avtale» nevnt ovenfor. Samtykke skal ikke oppstilles som en betingelse for å inngå en avtale eller benytte en tjeneste, dersom det ikke er nødvendig med samtykke for å gjennomføre avtalen eller tjenesten. Det er formålet med behandlingen som er avgjørende for hva som er «nødvendig». Samtykke kan kun kreves for den behandlingen som er nødvendig for å levere tjenesten. Et eksempel på en avtale hvor det kan stilles som en betingelse at det avgis et samtykke før avtalen inngås kan være en forsikringsavtale hvor det er nødvendig med helseopplysninger for å kunne bedømme risiko, beregne premie og gjennomføre forsikringsavtalen. Et eksempel på en avtale hvor det ikke kan stilles som en betingelse at det avgis et samtykke før avtalen inngås kan være en kontoavtale hvor det som vilkår for å inngå kontoavtalen kreves at kunden avgir samtykke til deling eller salg av opplysninger for markedsføringsformål.

  En konsekvens av kravet til frivillighet er at den registrerte må gis mulighet for å gi separate samtykker til forskjellige formål som samtykket omfatter. «Bundling» av samtykke til flere formål ut over det som er «nødvendig» kan derfor bli å anse som ugyldig dersom formålene er for forskjellige, jf. artikkel 7 nr. 4 og fortalens punkt (43). Frivillighet stiller krav til at det må være balanse i relasjonen mellom den registrerte og den behandlingsansvarlige. For å realisere kravet til frivillighet må det være valgfritt for den registrerte å avgi eller ikke avgi samtykke jf. «genuine or free choice» i fortalens punkt (42), og det må være like enkelt å avgi og trekke tilbake samtykket.

- "specific" (uttrykkelig/eksplisitt/aktivt): Det skal ikke være tvil om at det er avgitt samtykke. Et samtykke skal være aktivt («a clear affirmativ action»), det er ikke tilstrekkelig med forhåndsavkryssede "samtykkebokser" eller andre passive samtykker, jf. fortalens punkt (32). Dette kan medføre noe usikkerhet rundt den bruk av kollektive samtykker som Datatilsynet har åpnet for i forbindelse med tegning av kollektive forsikringsavtaler, jf. Datatilsynets merknader punkt 2 til standardkonsesjon for behandling av personopplysninger hos tilbydere av forsikringstjenester.

- "informed" (informert): Kunden må informeres i et slikt omfang at han eller hun har grunnlag for å vurdere hvilke konsekvenser det har å avgi samtykke. Dette omfatter blant annet informasjon om behandlingsansvarliges identitet og formålet med behandlingen, jf. fortalens punkt (42). Kravet til angivelse av formål i samtykket fremgår også av artikkel 6 nr. 1 (a) som krever at det skal omfatte «one or more specific purposes». Denne formuleringen må igjen fortolkes i lys forordningens artikkel 5 nr. 1 (b) som utdyper kravene til formålsbestemt behandling og krever at data skal være innhentet for «… specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…». Denne type «purpose limitation» må derfor også innfortolkes som et krav i forhold til formålsangivelse i samtykker.

Vilkårene «frivillig», «uttrykkelig/eksplisitt» og «informert» som fremgår av definisjonen i artikkel 4, utdypes nærmere i artikkel 7.

Vilkårene for samtykke i artikkel 7:

Dokumentasjonskrav (artikkel 7 nr. 1):

En virksomhet som behandler personopplysninger på bakgrunn av samtykke har alltid vært ansett å ha bevisbyrden for at samtykke foreligger. Dette kravet er presisert med ny forordning, gjennom begrepet «shall be able to demonstrate». Virksomheten må kunne dokumentere at kunden har avgitt samtykke til behandling av personopplysninger for alle behandlinger som er basert på samtykke som behandlingsgrunnlag.

Formkrav (artikkel 7 nr. 2):

- *«If the data subject's consent is given in the context of a written declaration…"*

Som i direktivet og personopplysningsloven, stilles det i forordningen ikke krav om skriftlig samtykke, noe som også klart fremgår av fortalens punkt (32) og henvisningen til "oral statement". Dette må sees i lys av det krav om skriftlighet som nå fremgår av finansforetakslovens § 9-6 (2) knyttet til utlevering av taushetsbelagte opplysninger. Basert på Departementets merknader i forarbeidene til finansforetaksloven, er imidlertid kravet til skriftlighet trolig ikke absolutt, til tross for lovens ordlyd. I Prop 125 L side 108, fremgår følgende:

> *Adgang til å utlevere opplysninger til andre etter skriftlig samtykke fra den som har krav på taushet, bør etter departementets vurdering også omfatte samtykke gitt på annen måte, herunder elektronisk, jf. blant annet FNOs høringsmerknad. Det vises til lovforslaget § 16-2 annet ledd. Det må i så fall være en forutsetning at personvernet ikke blir materielt svekket og at samtykket er gitt i henhold til betryggende rutiner og kontroll. Departementet bemerker at det fortsatt kreves et «aktivt» samtykke, som etter gjeldende rett, jf. Finanstilsynets rundskriv nr. 11/2000.*

Før ny finansforetakslov var det ikke krav om skriftlige samtykker, annet enn etter Datatilsynets konsesjonsvilkår knyttet til behandling av sensitive opplysninger i forsikringsvirksomhet. Til tross for den klare ordlyd i finansforetakslovens § 9-6 (2) tyder forarbeidene på at bestemmelsen ikke innfører et absolutt krav om skriftlighet. Bestemmelsen må likefullt sees som et skjerpet krav til at samtykke skal avgis under betryggende forhold.

I fortalens punkt (32) fremheves det at konkludent adferd må kunne konstituere et gyldig samtykke. *«…choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data»*. Samtykke avgitt ved konkludent adferd må også innfri oven nevnte vilkår i artikkel 4, utdypet i artikkel 7. Ved konkludent adferd kan det være en utfordring både å få gitt tilstrekkelig informasjon til at det kan sies å foreligge et informert samtykke og til å kunne dokumentere dette i ettertid. Samtykke ved konkludent adferd møter også en særlig utfordring i kravet om at samtykket skal være uttrykkelig – noe som også presiseres i fortalen ved begrepet *«clearly indicates»*. Disse forhold tilsier at handlingsrommet for samtykke ved konkludent adferd er svært begrenset. Betydningen av det nye skriftlighetskravet etter finansforetakslovens § 9-6(2) vil i tillegg forhindre at samtykke avgitt ved konkludent adferd kan være hjemmelsgrunnlag for utlevering av taushetsbelagte opplysninger. På bakgrunn av beskrivelsen av konkludent adferd i fortalen vil eksempler på denne type samtykke kunne være en persons endring personverninnstillingene i en tjeneste på nett. Personens reduksjon av personverninnstillingene må, forutsatt tilstrekkelig informasjon, anses som samtykke ved konkludent adferd til at øvrig funksjonalitet forbedres på bekostning av at personvernet reduseres. Det må også trekkes en grense mot passivt samtykke ved at det faktisk må finne sted, og kunne dokumenteres, en aktiv handling som et klikk, regulering av en skyvekontroll (slider) e.l.

Etterfølgende konkludent adferd, det at en person tar i bruk en tjeneste som eksempelvis er iverksatt uten gyldig samtykke, eksempelvis passivt samtykke, kan ikke reparere det faktum at en da allerede har behandlet personopplysninger uten hjemmelsgrunnlag.

- *«clearly distinguishable from the other matters»*

Dersom kunder/registrerte blir bedt om å samtykke til en bestemt behandling av personopplysninger ved å akseptere selgers/tilbyders standardvilkår eller personvernerklæring, så skal den delen av vilkårene som gjelder samtykke til behandling av personopplysninger skilles tydelig ut fra andre forhold. Dette vil for eksempel kunne oppnås ved å innta disse vilkårene under egen overskrift/i egen "samtykkeboks" (se også punktet om *«intelligible and easily accessible form»* under), eventuelt andre visuelle virkemidler som tydelig skiller vilkårene som gjelder samtykke til behandling av personopplysninger fra de øvrige vilkår/den øvrige tekst. En felles «akseptknapp» der man aksepterer standardvilkår og samtidig samtykker, vil ikke oppfylle kravet til frivillighet jf. artikkel 7 nr. 4 og fortalens punkt (42). Ved behandling som omfatter flere formål bør det avgis samtykke til samtlige, jf. fortalens punkt (32).

- *«intelligible and easily accessible form»*

Samtykket skal fremstilles lettfattelig og i en tilgjengelig form. "Samtykkebokser" som krever aktive handlinger med nivåbasert informasjon, vil være en god måte å realisere dette på. Det skal legges til rette for at kunden på en enkel måte skal kunne utøve sitt eierskap til egne personopplysninger.

- *«clear and plain language»*

Det stilles krav om klart og enkelt språk i samtykketekstene - liten skrift og stammespråk må unngås. Disse formkravene følger opp noen grunnleggende prinsipper i forordningen, nemlig at informasjon om behandling av personopplysninger skal gis på en klar og tydelig måte samt at all behandling av personopplysninger skal være transparent for kunden.

«Clear and plain language» har erstattet personverndirektivets begrep «unambiguous» (utvetydig) i artikkel 7 i direktivet. Dette innebærer likevel ikke noen realitetsforskjell – et samtykke skal fortsatt være utvetydig. Dette fremgår både indirekte av den samlede ordlyd i forordningens artikkel 7 og direkte av definisjonen i artikkel 4 (11), samt av fortalens punkt (32). Her fremgår det blant annet at *«Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data…"* Tvetydighet i en samtykketekst vil dermed kunne medføre at samtykket verken fremstår som informert eller eksplisitt.

Momenter for vurdering av om samtykke er avgitt frivillig (artikkel 7 nr. 4):

Det er avgjørende at samtykker som er satt som vilkår/forutsetning for å kunne inngå avtalen eller motta tjenesten/ytelsen, er nødvendig for å oppfylle kontrakten der behandlingsgrunnlaget er artikkel 6 nr. 1 b), jf. fortalens punkt (43) siste setning. Se for øvrig eksemplene nevnt innledningsvis i notatet under omtalen av «frivillig».

Samtykker skal følgelig ikke bidra til at virksomheter setter som vilkår for sine tjenester at den registrerte gir samtykke til behandling av «overskuddsinformasjon» som ikke er nødvendig for å realisere det angitte formålet. Så lenge samtykke er frivillig og kunden er tilstrekkelig informert betyr imidlertid ikke dette at en bank eller et forsikringsselskap er avskåret fra å be om samtykke til deling av kundeopplysninger mellom selskaper i et konsern og/eller en konserngruppe, eller at det bes om samtykke til bruk av andre typer data om kunden, eksempelvis adferdsdata i tjenester/på nettsider, for å forbedre eksisterende tjenester og/eller markedsføre tilpassede produkter og tjenester til den registrerte.

Minimaliseringsprinsippet er kodifisert i artikkel 5 nr. 1 (c), jf. grunnkravet i POL § 11 b) – og innebærer at behandlingsformål skal være saklig begrunnet i virksomheten. Der et forsikringsselskap for eksempel mottar en uredigert legejournal og velger å behandle helseopplysninger som ikke er nødvendige for å gjennomføre den aktuelle forsikringsavtalen, vil det være en behandling i strid med artikkel 5. Selskapet må således avstå fra å behandle slik informasjon, eller be om samtykke fra kunden til å behandle de øvrige helseopplysningene til et annet formål saklig begrunnet i virksomheten.

Fortalens punkt (42) fremhever også momentet at samtykket ikke skal inneholde «unfair terms» noe som også vil være et vurderingstema i forhold til «frivillighet». Basert på fortalens punkt (43) vil *«a clear imbalance»* ikke bare være et moment, men en ugyldighetsgrunn. Et praktisk eksempel her er bruk av samtykkeerklæringen i et arbeidsforhold hvor arbeidstaker ikke har reell mulighet til å nekte samtykke. En mer uklar ubalanse, for eksempel i styrkeforholdet mellom partene, vil kun være et moment i en samlet vurdering av samtykkets gyldighet. Dette kan imidlertid ikke forstås dithen at det en finansinstitusjon alltid vil være i «clear imbalance» ovenfor forbruker, og derfor ikke kan benytte samtykke som behandlingsgrunnlag. Så lenge valgfriheten er reell (frivillig) og det å ikke samtykke er uten konsekvens for kundeforholdet, vil ikke dette frata avgitte samtykker sin gyldighet.

Avgi og trekke tilbake samtykke (artikkel 7 nr. 3):

Det skal være like enkelt å trekke tilbake et samtykke som å avgi det. I praksis kan dette innebære at virksomheter som utvikler en digital løsning for å avgi samtykker, enten må tilby muligheten for å

trekke samtykke tilbake i samme løsning, eller via annen løsning som tilbyr like enkel – eller enklere mulighet for å trekke samtykket tilbake.

Kunden/den registrerte skal informeres om muligheten til å trekke et avgitt samtykke tilbake. Det å trekke samtykke tilbake påvirker ikke lovligheten av de behandlingene som ble utført mens samtykket var gyldig. For eksempel vil informasjon som er innhentet med hjemmel i samtykke fortsatt kunne behandles, frem til kunden ber om sletting, men behandlingsansvarlig har ikke lenger rettsliggrunnlag for å fortsette innhenting.

Dette gjelder ikke dersom samtykket omfatter mer enn behandlingen «innhenting», så som annen prosessering av dataene, herunder lagring. Alle behandlinger som omfattes av samtykket må som utgangspunkt opphøre, dersom de ikke omfattes av annet hjemmelsgrunnlag som gjør fortsatt behandling lovlig. Når et samtykke er trukket tilbake innebærer det kun at hjemmelsgrunnlaget "samtykke" ikke lenger kan påberopes som grunnlag for fortsatt behandling.

FORORDNINGEN VURDERT MOT GJELDENDE RETT

(Beskrivelse av hva som er nytt etter forordningen, hvilke endringer dette medfører etc.)

Som allerede beskrevet medfører forordningen noen nye regler, samt en del kodifisering av etablert praksis. Det vil i det følgende bli gitt et konsentrert sammendrag av dette.

Sett hen til det vi oppfatter som praksis fra norske myndigheter og finansbransjen, er konklusjonen at presiseringene i artikkel 7 og i fortalen ikke representerer en vesentlig endring av gjeldende rett i Norge, men følgende tre presiseringer vil nok påvirke norsk praksis på sikt:

(1) dokumentasjonskravet presiseres ytterligere i artikkel 7 nr. 1
(2) Informasjonskrav presiseres ytterligere i artikkel 7 nr. 2
(3) Krav til presisjonsnivå i samtykket presiseres ytterligere i artikkel 7.

Hvorvidt disse presiseringene vil påvirke eksisterende formuleringer i alminnelig brukte samtykker i bransjen som eksempelvis *"Jeg samtykker til utveksling av dybdeopplysninger som eksempelvis transaksjons- og beholdningsopplysninger", gjenstår å se seg.*

Nærmere om de enkelte tema i artikkel 7:

<u>Kravet til frivillighet:</u>
«Bundling» av samtykke til flere formål ut over det som er «nødvendig» kan bli å anse som ugyldig dersom formålene er for forskjellige. Det er som i dag ikke anledning til å sette som vilkår for avtaleinngåelse for en tjeneste at kunden samtykker til behandling som ikke er nødvendig for å levere denne tjenesten.

<u>Dokumentasjonskrav:</u>
En virksomhet som behandler personopplysninger på bakgrunn av samtykke har bevisbyrden for at samtykke foreligger. Dette kravet er nå presisert gjennom begrepet «shall be able to demonstrate». I forhold til å dokumentere at et samtykke foreligger må virksomhetene trolig forvente å møte noe strengere dokumentasjonskrav enn i dag. Ved samtykke til utlevering av taushetsbelagte personopplysninger må dette også sees i sammenheng med det dokumentasjonskravet som er et resultat av (det ikke absolutte) skriftlighetskravet som er innført i finansforetakslovens § 9-6 (2).

<u>Formkrav:</u>

Forordningen legger stor vekt på at informasjon skal gis på klar og tydelig måte - i en lettfattelig og tilgjengelig form. Dette kodifiserer blant annet praksis om at samtykke skal være klart og konsist og at det skal skilles ut av standardklausuler. Det vises blant annet til Forbrukerombudets veileder for samtykke, som ifølge forarbeidene til markedsføringsloven (ot.prp 62 1999-2000, punkt 3.3.10.3), bygger på kravene til et gyldig samtykke etter personvernlovgivningen. Forordningen oppfattes likevel å være klart tydeligere på kravet til enkelt språk og hvor lettfattelig og enkelt et samtykke skal være. Dette sammenliknet med både forarbeidene til personopplysningsloven (ot.prp. 92 1998-1999 s. 103-104) og forbrukerombudets veileder. Forordningens ordlyd *«intelligible», «easy accessible form»* og *«clear and plain language»* er imidlertid sammenfallende med det som de senere år oppfattes å ha vært Datatilsynets krav til, og signaler om, samtykkets ordlyd og innhold.

Krav knyttet til det å avgi og trekke tilbake samtykke:
Det skal være like enkelt å trekke tilbake samtykke som å avgi det. Kunden/den registrerte skal også informeres om at et samtykke kan trekkes tilbake.

Momenter knyttet til vurderingen av gyldig samtykke:
Presiseringen av minimaliseringsprinsippet i artikkel 5 nr.1 (c) gjør det tydelig at behandlingsgrunnlag i form av samtykke ikke kan reparere et formål som ikke er saklig begrunnet i den behandlingsansvarliges virksomhet.

TILTAK FORETAKENE MÅ GJENNOMFØRE

(Beskrivelse av hva foretakene må gjøre for å oppfylle kravene i forordningen).

Arbeidsgruppens anbefaling er at virksomhetene vurderer følgende:

Medlemmene bør vurdere sine samtykker i forhold til presiseringen i forordningen artikkel 7 nr 1 og nr 4, og for øvrig ta en gjennomgang av:

- Tilfredsstiller etablerte samtykker nye krav?
    - Særlig kravene til informasjon, jf. Kontraktsutvalgets vedlikehold av «Bankenes personvernregler»
    - Brukes samtykker som en del av etablerte standardvilkår jf. Kontraktsutvalgets mønsteravtaler og de enkelte virksomheters egne avtaler på produkter/tjenester som ikke er basert på mønsteravtaler.
- Har virksomhetene mulighet til å dokumentere avgitte samtykker, og er det gitt informasjon som er lett tilgjengelig for kunden?
- Løsninger for å trekke tilbake samtykke og informasjon om dette og konsekvensene. Dette er et sentralt punkt, som også har en side mot Data Protection by Design (innebygget personvern) og IKT utviklingskrav.
- Vurdere eksisterende behandlinger opp mot angitte formål i benyttede samtykker - er de presise nok?

VURDERING AV TILTAK FOR ARBEIDSGRUPPEN/FINANS NORGE

(Kan arbeidsgruppen lette gjennomføringen av tiltakene foretakene må gjøre? I så fall hvordan? Skal notatet følges opp gjennom bransjestandard, veileder, eller andre hensiktsmessige tiltak?)

- Forsikring – bransjefelles mal for samtykker (revideres/utvides)?
- Bank – hvordan videreutvikle/fornye Kontraktsutvalgets maler?
- Utvikle andre typer standardtekster som for eksempel personvernerklæringer?
- Generell veileder om bruk og utvikling av samtykker som behandlingsgrunnlag (med utgangspunkt i Forbrukerombudets veileder og justert for forordningens krav og de særlige hensyn som måtte gjøre seg gjeldende for enkelte deler av næringen)?