Datatilsynet

Finansdepartementet
Postboks 8008 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
13/3769-71	16/02038-2/AHO	20.04.2017

Høringsuttalelse - Hvitvaskingslovutvalgets utredning NOU 2016: 27

Vi viser til høring av NOU 2016:27 om tiltak mot hvitvasking og terrorfinansiering.

Datatilsynet gir her sin høringsuttalelse.

1. Generelle merknader

1.1 Tiltak mot hvitvasking og terrorfinansiering må harmoniseres med kravene til personopplysningsvern på en konkret måte

Forslaget til ny hvitvaskingslov bygger i hovedsak på et nytt hvitvaskingsdirektiv fra EU, det fjerde i rekken. Direktivet er allerede foreslått endret av Kommisjonen, men det er ikke klart hvordan direktivet endelig vil bli.

Arbeidet med å forhindre og bekjempe hvitvasking og terrorfinansiering er utpreget internasjonalt. I stor grad er reglene utviklet etter standarder satt av Financial Action Task Force (FATF), hvor kravene til personopplysningsvern ikke har særlig oppmerksomhet.

Tiltakene er rettet inn mot å skape gjennomsiktighet i det finansielle system for å forebygge og hindre at det brukes til hvitvasking og terrorfinansiering.

Tiltakene medfører strenge krav til kundekontroll, risikoanalyser og risikoprofilering, overvåking av transaksjoner, utveksling av informasjon, undersøkelser og rapportering av mistenkelige transaksjoner mv. Dette medfører behandling av store mengder personopplysninger og har innvirkning på enkeltmenneskets krav på et personopplysningsvern og privatliv.

Datatilsynsmyndighetene i Europa har flere ganger uttrykt bekymring for at personopplysningsvernet i praksis ikke blir hensyntatt i tilstrekkelig grad i utviklingen av tiltakene og reglene for å bekjempe hvitvasking og terrorfinansiering.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Vi viser her til artikkel 29 gruppens[1] «opinion on data protection issues related to the prevention of money laundering and terrorist financing».[2]

Uttalelsen inneholder omfattende kartlegging av utfordringer knyttet til personopplysningsvern og over 40 anbefalinger. Dokumentet er ment som veiledning til blant annet lovgivere, både på EU-nivå og nasjonalt nivå.

Vi viser også til uttalelse[3] fra European Data Protection Supervisor[4] (EDPS) om fjerde hvitvaskingsdirektiv og forholdet til personopplysningsvern.

Begge disse uttalelsene understreker betydningen av at det må gjennomføres systematiske personvernkonsekvensvurderinger (Data Protection Impact Assessment – DPIA) .

Videre fremheves betydningen av å omsette de generelle kravene til personopplysningsvern som er gitt i personverndirektivet til konkret og håndfast lovgivning på området for bekjempelse av hvitvasking og terrorfinansiering.

Som et eksempel kan vi vise til at personopplysningsvernet bygger på et prinsipp om proporsjonalitet og dataminimalitet. Opplysningene som behandles må være adekvate og relevante og begrenset til det som er nødvendig for formålet. Hva dette betyr i det enkelte tilfelle beror på området man er på, noe som krever konkrete vurderinger. For å etterleve dette prinsippet er det blant annet nødvendig at lovgivningen presiserer nærmere hvilke typer data (personopplysninger) som vil være relevant og nødvendig å samle inn og behandle som ledd i kundekontroll, og eventuelt hvilke typer data som vil være uproporsjonalt og følgelig ikke tillatt å behandle. For at loven skal gi beskyttelse mot at ikke det skjer uproporsjonal innsamling og behandling av personopplysninger, må den være så presis som forholdene tillater. Det er ikke tilstrekkelig å si at de rapporteringspliktige kan behandle de opplysninger som er nødvendig. Det setter også de rapporteringspliktige i en svært vanskelig situasjon, for det blir opp til dem å finne ut hvor grensene går. Lovteksten og forarbeidene gir liten veiledning.

Datatilsynet må dessverre konstatere at lovforslaget og utredningen ikke reflekterer de uttalelsene som datatilsynsmyndighetene har gitt på området.

Vi anbefaler departementet å foreta en nærmere personvernkonsekvensvurdering og kartlegge behovet for mer presis regulering og andre tiltak i lys uttalelsene vi har vist til over.

---

[1] The Article 29 Working Party er et rådgivende organ etablert i medhold av personverndirektivet (direktiv 95/46) artikkel 29. Organet består blant annet av representanter fra datatilsynsmyndighetene i EU/EØS.
[2] Opinion 14/2011. www.ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
[3] Opinion av 4. juli 2013. www.edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_en.pdf
[4] EUs uavhengige datatilsynsmyndighet. Gir blant annet råd om personopplysningsvern i tilknytning til EU-regulering.

1.2 Ny personvernforordning

Fjerde hvitvaskingsdirektiv art. 41 sier at personverndirektiv 95/46, slik det er gjennomført i nasjonal rett, skal gjelde ved behandlingen av personopplysninger.

Utvalget har derfor foretatt sine vurderinger opp mot personverndirektivet og personopplysningsloven.

Disse reglene blir imidlertid erstattet av EUs nye personvernforordning (General Data Protection Regulation – GDPR). Forordningen vil bli inntatt i EØS-avtalen og inkorporert i norsk lov. Det er forventet at reglene trer i kraft mai 2018.

Datatilsynet mener at ny hvitvaskingslov må vurderes opp mot personvernforordningen. Vi anbefaler derfor departementet å utrede dette nærmere. Arbeidet bør koordineres med justisdepartementet, som har ansvaret for innføringen av personvernforordningen i norsk rett.

Som eksempel kan vi vise til personvernforordningen art. 6 nr. 2 og 3, som uttrykkelig krever at behandling av personopplysninger som er «necessary for the performance of a task carried out in the public interest» skal fastsettes i konkret lovgivning fra EU eller medlemsstatene. I den forbindelse kan det i loven gis mer presise bestemmelser for å tilpasse anvendelsen av de generelle reglene for å «ensure lawful and fair processing». Dette inkluderer «the types of data which are subject to the processing».

Behov for, og krav til, å gi presiserende og utfyllende bestemmelser må ses i lys av de krav til lovgivningen som kan utledes av EMK art. 8. EU-domstolen har i Österreichiser Rundfunk and others (sak C-465/00 m.fl.) lagt til grunn at lovgivning som tillater behandlingen av personopplysninger må, der det foreligger inngrep i retten til respekt for privatlivet, være i samsvar med EMK art. 8.2 for å i det hele tatt kunne være i samsvar med personverndirektivet. Dette innebærer blant annet at loven må ha den kvalitet som konvensjonen krever – loven må være klar og den må inneholde de nødvendige garantier for å sikre at forstyrrelsen av privatlivet ikke går lenger enn nødvendig.

Et annet eksempel er begrensninger i innsynsretten som hvitvaskingsdirektivet forutsetter. Slike begrensninger må vurderes etter personvernforordningen art. 23, som stiller en del andre krav sammenliknet med personverndirektivet art. 13. Vi kommer nærmere tilbake til dette under.

2. Konkrete merknader til foreslåtte lovbestemmelser

2.1 Lovutkastet § 27. Forholdet til personopplysningsloven. Behandling av personopplysninger.

I bestemmelsens annet ledd er det fastsatt at «rapporteringspliktig kan behandle personopplysninger, herunder sensitive personopplysninger, for å oppfylle sine plikter etter loven her.»

Begrunnelsen for bestemmelsen er at tiltakene etter hvitvaskingsloven innebærer behandling av personopplysninger, og hensikten med bestemmelsen er å gi en hjemmel for at de rapporteringspliktige har adgang til å behandle personopplysninger.

Datatilsynet mener lovhjemmelen verken er klar nok eller gir de nødvendige garantier for å sikre at kun de personopplysninger som er nødvendige og proporsjonale blir behandlet. Vi viser her til det vi har skrevet over om behovet for blant annet å spesifisere nærmere hva slags type opplysninger som det vil være nødvendig og proporsjonalt å behandle.

Slik loven nå er formulert er det nærmest carte blanche til å behandle personopplysninger idet loven gir svært begrenset veiledning på hvor grensene skal gå.

Det er i forlengelsen av dette svært problematisk at lovteksten åpner for behandling av sensitive personopplysninger uten nærmere vurderinger av behov og forholdsmessighet, og heller ingen angivelse av eller begrensninger på typen sensitive opplysninger. Lovbestemmelsen synes også å være i strid med personverndirektivet art. 8 nr. 4 og personvernforordningen art. 9 nr. 2 bokstav g. Sistnevnte gir åpning for å begrense forbudet mot å behandle sensitive personopplysninger hvor behandlingen er:

> necessary for reasons of substansial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the data subject.

Vi viser også til ovennevnte uttalelse fra EDPS, som sier:

> Besides, the circumstances in which a CDD (Custom Due Diligence, vår merknad) must be carried out may lead to discrimination if sensitive data are processed without limitation. Leaving it to the obliged entities to decide whether they need sensitive data or not to carry out CDD involves the risk for them to take arbitrary decisions such as depriving clients of a certain ethnic origin that they consider to be suspect, or clients that have different political or religious opinions, of the right to conduct transactions.

2.2 Lovutkastet § 28. Formålsbestemt behandling av personopplysninger.

Datatilsynet anbefaler at det uttrykkelig fastsettes et forbud mot å behandle personopplysningene til andre formål enn til å forebygge og avdekke hvitvasking og terrorfinansiering, herunder ethvert kommersielt formål. Selv om dette, som utvalget peker på, implisitt kan utledes av ordet «bare», så er et slikt forbud viktig for å understreke formålsbegrensningsprinsippet.

Vi vil også peke på at utvalget i sin vurdering i punkt 7.6.2 har lagt til grunn at det vil ligge innenfor formålet å behandle opplysningene som samles inn og lagres etter loven til å etterforske profittmotivert kriminalitet. Dette synes å være i samsvar med

hvitvaskingsdirektivet så langt det er tale om å bruke opplysningene for å oppklare den straffbare handlingen som utbyttet som er hvitvasket eller forsøkt hvitvasket, stammer fra. En slik forståelse synes også å respektere formålsbegrensningsprinsippet ved at en slik bruk av informasjonen er forenlig med hovedformålet.

Derimot er det ikke adgang til å bruke opplysningene for å etterforske profittbasert kriminalitet generelt. Det må foreligge hvitvasking eller mistanke om hvitvasking (evt. terrorfinansiering). Dette gjelder også i relasjon til skatteunndragelser. Bekjempelse av skattekriminalitet generelt sett ligger utenfor formålet med hvitvaskingsdirektivet. Der man står overfor hvitvasking eller forsøk på hvitvasking av midler som er unndratt fra beskatning, vil vi anta at opplysningene kan brukes for å forfølge skatteunndragelsen. Derimot kan ikke opplysningene brukes generelt for å undersøke om midler er unndratt eller forsøkt unndratt fra beskatning.

Vi anbefaler at rekkevidden av formålsbegrensningsprinsippet her avklares og presiseres nærmere.

2.3 Lovutkastet § 31. Lagringstid og sletting av opplysninger og dokumenter.

Første ledd oppstiller en lagringstid på 5 år.

Etter utløpet av 5 år skal alle personopplysninger som et utgangspunkt slettes. Etter annet ledd er det imidlertid ikke plikt til å slette dersom videre lagring er «strengt nødvendig». Samlet lagringstid må dog ikke overstige 10 år.

Datatilsynet kan ikke se at bestemmelsen er i samsvar med hvitvaskingsdirektivet art. 40 nr. 1 siste ledd. Direktivet gir adgang til utvidet lagring «after they (altså myndighetene i landet) have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.»

Vi kan ikke se at det er foretatt slike nøye overveielser. Vi kan heller ikke se at det er presisert noe nærmere om type opplysninger eller type tilfeller hvor fortsatt lagring er forsvarlig. Det foreligger heller ingen vurdering av hvor lang ekstra lagringstid det eventuelt skal være i de konkrete tilfeller. At lagringstiden ikke skal overstige 5 år er ikke det samme som at lagringstiden ikke kan være kortere, i samsvar med prinsippet om å ikke lagre lenger enn nødvendig ut fra formålet.

Regelen slik den er utformet overlater i alt for stor grad til de rapporteringspliktige å avgjøre hva som er strengt nødvendig. Skjønnsutøvelsen her kan bli både vilkårlig og uproporsjonal, og i tillegg lite gjennomsiktig. Det er heller ikke definert hva videre lagring skal være strengt nødvendig for – altså formålet.

Vi har forståelse for at det kan tenkes tilfeller hvor lengre lagringstid kan være nødvendig og proporsjonalt, men vi mener dette må defineres og angis mye tydeligere. Derfor mener vi at

det kan være bedre å gi departementet en forskriftsfullmakt til å fastsette konkrete regler for utvidet lagringstid. Disse reglene kan da fastsettes ut fra erfaring og typetilfeller hvor man kan foreta en konkret vurdering og hvor begrunnelsen for videre lagring kan gis på en overbevisende måte i samsvar med forutsetningen i hvitvaskingsdirektivet art. 40 nr. 1.

2.4 Lovutkastet § 33. Unntak fra retten til innsyn etter personopplysningsloven.

Bestemmelsen gjør unntak fra retten til innsyn etter personopplysningsregelverket ved at den forbyr rapporteringspliktige å gi innsyn i opplysninger som «*kan vanskeliggjøre*

a) *rapporteringspliktiges overholdelse av pliktene etter loven her, eller*
b) *etterforskning eller lignende undersøkelser.*»

Etter vår oppfatning har bestemmelsen fått en alt for vid og generell utforming. Det bør presiseres mye bedre i hvilke tilfeller det ikke skal gis innsyn og i hva slags type opplysninger/informasjon.

For det første finner vi grunn til å peke på at hvitvaskingsdirektivet art. 41 nr. 4, som bestemmelsen er ment å gjennomføre, knytter unntak fra retten til innsyn i personopplysninger til «In applying the prohibition of disclosure laid down in Article 39 (1)...».

Poenget er at det er i tilknytning til gjennomføringen av forbudet mot å avsløre rapportering til Økokrim mv[5]. at statene skal begrense retten til innsyn etter personopplysningsregelverket. Dette er forklart i direktivets fortalepunkt nr. 46:

> *The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspiscious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 13 of Directive 95/46 EC (...) may therefore be justified.*

Slik vi ser det, er poenget at i tilfeller hvor mistenkelige transaksjoner og annen informasjon er rapportert til Økokrim eller kan bli det, er det behov for at de rapporteringspliktige ikke gir innsyn i personopplysninger som indirekte avslører dette. Et eksempel kan være at rapporteringspliktig har undersøkt en mistenkelig transaksjon og deretter rapportert forholdet til Økokrim. Da kan det tenkes at rapporteringspliktig ikke bør gi innsyn i opplysninger som er innhentet og behandlet i tilknytning til undersøkelsen av transaksjonen fordi dette indirekte kan avsløre at det er fattet mistanke mot akkurat den transaksjonen. Selv om rapporteringspliktig ikke sier noe om at man har funnet transaksjonen mistenkelig og at den er rapportert til Økokrim, vil kunden indirekte kunne forstå at dette har skjedd. Her vil begrensningen i innsynsretten kunne ha en naturlig og forsvarlig sammenheng med avsløringsforbudet.

---

[5] Se lovforslaget § 25 (1) som gjennomfører avsløringsforbudet.

For det andre viser vi til at unntak fra retten til innsyn på nåværende tidspunkt også bør vurderes i lys av personvernforordningen art. 23. Denne bestemmelsen gir, som personverndirektivet art. 13, anledning til å begrense blant annet innsynsretten ut fra nærmere bestemte grunner. Imidlertid stiller art. 23 annet ledd spesifikke krav til hva lovgivningen som begrenser rettighetene skal inneholde, for eksempel «the categories of personal data» som er omfattet av begrensningen og «the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction».

2.5 Lovutkastet § 35. Økokrims behandling av personopplysninger.

Bestemmelsen fastsetter i første ledd at personopplysninger som mottas av Økokrim i forbindelse med rapportering mv. skal slettes etter 5 år.

I annet ledd er det imidlertid åpnet for lagring i inntil 15 år dersom det er «strengt nødvendig».

Vi mener en slik bestemmelse er alt for vag og skjønnsmessig, og ikke fremstår godt nok begrunnet. Vi viser her til merknadene under punkt 2.3 over ettersom de samme betraktninger gjør seg gjeldende her.

2.6 Lovutkastet § 40. Gjennomføring av rutiner på konsernnivå, rapporteringspliktigs virksomhet utlandet mv.

Bestemmelsen gjennomfører hvitvaskingsdirektivet art. 45.

Etter vårt syn er det viktige sider ved art. 45 som ikke gjenspeiles i lovutkastet eller utredningen.

Art. 45 første ledd sier at «*Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CTF purposes*».

Krav til å etablere felles policy og prosedyre for utveksling og behandling av data, må her ses i lys av at overføring av personopplysninger til land utenfor EØS (tredjeland) i utgangspunktet er forbudt etter personverndirektivet, med mindre det skjer til land som sikrer adekvat beskyttelse av personopplysninger. Tilsvarende gjelder etter den nye personvernforordningen.

Dersom tredjelandet ikke er anerkjent som et trygt tredjeland, kan overføring likevel skje hvis det gis tilstrekkelig garantier. En slik garanti kan være såkalte Binding Corporate Rules, som er en form for internt avtaleverk i et konsern som etablerer felles prosedyrer og regler som skal sikre et effektiv personopplysningsvern. En annen garanti kan være bruk av EUs såkalte standardavtaler (model clauses).

Slik vi forstår det er det altså et sentralt poeng med art. 45 å sikre at de rapporteringspliktige gjør det de kan for at utveksling av informasjon innad i et konsern, herunder til tredjeland, kan skje med de nødvendige garantier, og følgelig på en måte som er i samsvar med reglene for personopplysningsvern. I motsatt fall vil nemlig reglene for personopplysningsvern kunne begrense muligheten for å utveksle informasjon med virksomheter i tredjeland.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Andreas Hobæk
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO