Datatilsynet

Skattedirektoratet
Postboks 9200 Grønland
0134 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
2013/173983	13/00275-4/BSO	14. mai 2013

Høringsuttalelse- Forslag til lov- og forskriftsendringer som følge av a-opplysningsloven

Datatilsynet viser til høringsbrev av 4. mars 2013 om forslag til lov- og forskriftsendringer som følge av a-opplysningsloven.

Datatilsynet fremhever at en storstilt samling av personopplysninger ett sted forutsetter god styring og kontroll internt. Datatilsynet peker også på at det ikke er tilstrekkelig at lov og forskrifter gir overordnede krav. Det må i tillegg etableres systemer som faktisk kan støtte opp om de krav som følger av gjeldende rett, herunder taushetsplikten. Det er viktig at systemene sikrer at tilgangsstyringen er sammenfallende med de ulike etaters legitime behov, herunder at det kun gis tilgang på nødvendige og relevante opplysninger.

Av kapasitetshensyn har ikke Datatilsynet ikke hatt mulighet til å gå grundig gjennom høringsnotatet. Datatilsynet ber derfor på generelt grunnlag om at direktoratet ser hen til - og eventuelt vurderer kompensering for - eventuelle negative personvernkonsekvenser forslagene kan medføre.

For en nærmere beskrivelse av personvernutfordringer, vises det til Datatilsynets høringsuttalelse av 12. juni 2011 om forslaget fra arbeidsgrupperapporten. I denne høringsuttalelsen beskriver tilsynet flere personvernutfordringer med et sentralt innsamlingspunkt.

Datatilsynet ber om at direktoratet i det videre arbeidet ser hen til innspillene som er gitt i høringsuttalelse av 12. juni 2011.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Bård Soløy Ødegaard
seniorrådgiver

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

Vedlegg: Datatilsynets høringsuttalelse av 12. juni 2011

Kopi: Fornyings- administrasjons- og kirkedepartementet, Postboks 8004 Dep, 0030 OSLO

Datatilsynet

Finansdepartementet
Postboks 8008 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
10/319 SL KRJ/KR	11/00256-2	12. juni 2011

Høring - Arbeidsgrupperapport om forslag til ny ordning for arbeidsgiveres rapportering

Vi viser til Finansdepartementet sin høring av 4. mars 2011, samt til dialog vedrørende utsatt frist for vårt høringssvar.

Et slikt sentralt innsamlingspunkt som det legges opp til ved bruk av EDAG vil innebære store personvernmessige utfordringer. Datatilsynet har derfor kommentarer til noen av hovedpunktene i utredningen. Vi understreker imidlertid at tilsynet på bakgrunn av kapasitetshensyn ikke har hatt mulighet for å gå grundig gjennom hele rapporten. Datatilsynet vil imidlertid berømme Finansdepartementet og arbeidsgruppen for å ha hatt stor fokus på personvern i utredningen.

Storstilt samling av personopplysninger ett sted
Slik arbeidsgruppen viser til innebærer det en økt personvernrisiko å samle opplysninger om ansettelse, lønn og skattetrekk for alle arbeidstakere ett sted. Det er dessuten flere steder i rapporten vist til at det kan bli aktuelt å legge til rette for ytterligere rapportering gjennom EDAG. Selv om en slik sentral samling kan bedre kvaliteten på opplysningene, vil det være personvernmessige utfordringer knyttet til bl.a. krav til informasjonssikkerhet, tilgangsstyring, herunder krav til logging og innsyn i logger, innsyn for den registrerte for øvrig og sletting av opplysninger.

Behandlingsansvar og utlevering
Arbeidsgrupperapporten foreslår primært å legge behandlingsansvar for EDAG hos Skattedirektoratet. For opplysninger som blir hentet ut fra den sentrale løsningen, vil den etaten som innhenter opplysningene bli behandlingsansvarlig. NAV blir da behandlingsansvarlig for de opplysninger de henter ut fra registeret, mens Skattedirektoratet fortsatt vil være behandlingssansvarlig for de samme opplysningene i det sentrale registeret fram til disse slettes. Likeledes vil det være for andre parter som skal benytte løsningen.

En behandlingssansvarlig er etter personopplysningsloven § 2 nummer 4 definert som den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Bruk av flere behandlingsansvarlige i en og samme løsning, hvor

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

grensedragningene mellom de ansvarlige er flytende og avhengig av om informasjon er uthentet eller ikke, er etter Datatilsynets vurdering uheldig. Videre kan det virke noe underlig å gi Skattedirektoratet behandlingsansvar for opplysninger de ikke har behov for selv, noe som kan være tilfellet der de samler inn opplysninger for andre etater.

For etater der det legges opp til innsamling av overskuddsinformasjon, slik som for NAV, kan det imidlertid være uheldig å gjøre disse behandlingsansvarlige. Ved å gjøre selve innsamleren behandlingsansvarlig unngår man at NAV får behandlingsansvar for andre enn egne brukere (utover ansvaret for AA-registeret). Dette problemet oppstår som følge av at det legges opp til innsamling av overskuddsinformasjon, noe som i utgangspunktet er i strid med personopplysningsloven § 11 bokstav d.

En tilnærming som samsvarer med tilsynets tidligere praksis, er å gjøre Skattedirektoratet til databehandler for de andre partene. Det betyr uansett ikke, etter tilsynets oppfanting, at alt kan samles i et stort felles register. Bakgrunnen for det er en lignende situasjon påpekt i kontrollrapporten mot Altinn Sentralforvaltning tilbake i 2008. Kontrollrapporten er vedlagt for ordens skyld.

Sentral lagring og dobbeltlagring
Nevnte kontroll mot Altinn og mot Skattedirektoratet tilbake i 2008 pekte på noen sentrale punkter som etter tilsynets oppfatning vil gjøre seg gjeldende i denne sammenheng også. Dette gjelder segmentering av informasjonssystemet og unødvendig dobbeltlagring av informasjon. Førstnevnte beskrives best i et sitat fra kontrollrapporten mot Altinn:

"Personopplysninger kan behandles på vegne av andre med grunnlag i en databehandleravtale. Dette betyr i praksis at man, dersom man behandler personopplysninger på vegne av flere behandlingsansvarlige, må behandle informasjon for hver enkelt behandlingsansvarlig separat."

Vedrørende unødvendig dobbeltlagring viser tilsynet til vurderingen av Skattedirektoratet sitt servicearkiv under kontrollen tilbake i 2008. Dette er beskrevet i kontrollrapportens punkt 5.1.7, hvor det konkluderes med at dobbeltlagring ikke kan anses å være i samsvar med personopplysningslovens bestemmelser om gyldig behandlingsgrunnlag og sletting. Etter Datatilsynets vurdering bør opplysningene videreformidles til de enkelte etatene kort tid etter innsamling. Opplysningene bør deretter slettes for å unngå dobbeltlagring. Et unntak fra dette er opplysninger til NAV. Opplysninger til dette formålet må kunne lagres i en kortere periode fram til eventuell innhenting av slike opplysninger blir aktuelt.

Ulevering fra registeret til de enkelte etatene
Opplysninger til NAV (utover AA-registeret) bør kun utleveres etter begjæring; dette for å hindre at det innhentes opplysninger om andre personer enn det som er nødvendig.

Innhenting av opplysninger fra EDAG bør logges, og den registrertes innsynsrett bør omfatte innsyn i disse loggene. Loggingen bør minimum omfatte hvilke opplysninger som ble innhentet, hva som eventuelt ble gjort med opplysningene utover dette (lest, skrevet/endret), tidspunkt for innhentingen mv. og hvilken avdeling eller seksjon som initierte dette.

Kopi: Fornyings- administrasjons- og kirkedepartementet, Postboks 8004 Dep, 0030 OSLO

Vedlegg: Korrespondanse mellom Datatilsynet og Norsk Tipping (08/01389)
Brev til DIFI og Skattedirektoratet om bruk av MinID for pålogging til Folkeregisteret (11/00009-5)
Endelig kontrollrapport med vedtak mot Altinn og Skattedirektoratet (08/00291-10 og 08/00297-5)

Bruk av MinID
Datatilsynet har mottatt mange henvendelser fra arbeidstakere som reagerer kraftig på at systemer som man er avhengig av for å kunne utføre arbeidsoppgavene sine, legger opp til bruk av personlige verktøy som MinID. Dette gjelder også for EDAG-løsningen. Datatilsynet anser dette problematisk av flere årsaker:

1. *Rolleblanding* – skille mellom deg som privatperson og arbeidstaker. Ser man på informasjon gitt i forbindelse med opprettelse av bruker hos MinID står det gjerne at *MinID er din personlige elektroniske ID. Du bruker MinID for å levere selvangivelsen, bestille skattekort, få tilgang til selvbetjeningstjenester på nav.no, søke lån og stipend i Lånekassen, og til en rekke andre offentlige tjenester*. Det er altså en klar forventning om at MinID utelukkende skal brukes til private formål, ikke til å utføre dine arbeidsoppgaver.

2. *Informasjonssikkerhet* - bruk av Altinn innebærer at arbeidstakerne som skal rapportere kan sitte hvor som helst og logge seg på elektroniske tjenester gjennom Altinn. Dette kan igjen gi manglende kontroll med tilgangen til opplysningene og hva de benyttes til. Vi viser til personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.

3. *Styringsretten* - kan en arbeidsgiver i kraft av styringsretten pålegge en arbeidstaker å bruke MinID? Vi viser til at man som borger har adgang til å reservere seg mot bruk av løsningen som privatperson. Datatilsynet er derfor skeptisk til at arbeidsgiver kan pålegge slik bruk. Se http://www.difi.no/elektronisk-id/personvern-ogtryggleik.

4. *Fødselsnummer* – etter Datatilsynets vurdering av personopplysningsloven § 12 er det problematisk om arbeidsgiver krever bruk av fødselsnummer som pålogging for å rapportere på vegne av en virksomhet. Vi viser til bestemmelsens krav til saklig het og nødvendighet for å benytte denne identifikatoren

Spørsmål knyttet til rolleblanding er etter alt å dømme et økende problem. Tilsynet har hatt sammenlignbare saker med blant annet Norsk Tipping som krevde at ansatte hos tippekommisjonærene skaffet seg personlige tippekort for å utføre arbeidsoppgaver. Denne praksisen ble etter dialog med tilsynet endret. Korrespondanse i nevnte saker er vedlagt for ordens skyld.

Med hilsen

Bjørn Erik Thon
direktør

Frank U. Eriksen
seniorrådgiver