

Rutinebeskrivelse

En rutinebeskrivelse (RB) sikrer god og effektiv saksflyt ved å gi detaljerte rutiner om den konkrete fremgangsmåten ved behandlingen og avgjørelsen av UNEs saker. En RB godkjennes og revideres av avdeling for faglig støtte og analyse (fagavdelingen).

Saksnr. (360^o) : 15/00596
Dato : 18.06.2019
Versjon : 07
Ansvarlig : Seksjonssjef GJS
Saksbehandler : KSO
Nummer : RB-27

Rutiner for anonymisering av UNEs vedtak

Formål

Sørge for enhetlige rutiner for anonymisering av UNEs vedtak for de unntakstilfellene der et vedtak skal sendes andre enn parten og dennes fullmektig.

1	Innhold	
2	Innledning	3
3	Typetilfeller når vedtak skal anonymiseres	3
3.1	Fremleggelse av vedtak som belyser forvaltningspraksis i forbindelse med rettssak	3
3.2	Oversendelse av opplysninger i saker til andre forvaltningsorganer	3
3.3	Særlig om oversendelse til JD.....	4
3.4	Utlegg på åpne og offentlige sider	4
3.5	Sammendrag til Praksisbasen.....	4
4	Hvilke opplysninger skal anonymiseres?.....	4
5	Opplysninger som i utgangspunktet ikke skal sladdes:	5
6	Praktisk gjennomføring	5
7	Kryptert e-post	5

2 Innledning

UNE skal i noen få sammenhenger anonymisere egne vedtak, jf. pkt. 3 nedenfor.

Utgangspunktet for rutinebeskrivelsen er forvaltningslovens regler om taushetsplikt om personopplysninger og personopplysningslovens regler om personvern, og tilhørende krav til forsvarlig behandling av slike opplysninger (informasjonssikkerhet).

Dersom den som har krav på taushetsplikt samtykker i at personopplysninger kan utgis, er anonymisering som utgangspunkt unødvendig. Se også RB- S-31 om utlevering av personopplysninger.

Anonymisering av opplysninger innebærer at opplysningene i dokumentet ikke på noen vis kan knyttes til identifiserbare enkeltpersoner, heller ikke indirekte gjennom sammensetningen av variabler (eks. kombinasjon av aldersintervall, geografisk tilknytning mv.), koder, koblingsnøkler eller krypteringsformler. Hvilken anonymisering som kreves for at enkeltpersoner ikke vil kunne identifiseres må vurderes konkret, jf. også pkt. 3.

Aidentifisering av opplysninger innebærer at navn, fødselsdato, DUF-nr og andre personentydige kjennetegn er fjernet eller erstattet med vide kategorier eller en kode/fiktive navn eller lignende slik at enkeltpersoner ikke kan identifiseres direkte gjennom dokumentet.

Når dokumenter er anonymiserte eller aidentifiserte slik at de ikke lenger kan knyttes til en bestemt person vil de ikke lenger inneholde personopplysninger, og dokumentet omfattes ikke lenger av regelverket om taushetsplikt.

Anonymisering må ivareta disse hensynene:

- Taushetsbelagte personopplysninger skal ikke utleveres.
- Anonymiseringen bør ikke gå lenger enn det hensynet til personvernet og taushetsplikten tilsier – slik at de anonymiserte vedtak fortsatt kan kaste lys over praksis.
- Hensynet til personvernet skal ved tvilstilfeller tillegges avgjørende vekt.

3 Typetilfeller når vedtak skal anonymiseres

3.1 Fremleggelse av vedtak som belyser forvaltningspraksis i forbindelse med rettssak

UNE som forvaltningsorgan har en plikt å sørge for at vi overholder vår lovpålagte taushetsplikt og det er UNE, som behandlingsansvarlig for disse opplysningene, som vil stå ansvarlig ved brudd på denne taushetsplikten.

Dette tilsier at det som hovedregel gjelder at det er saksbehandler i UNE som skal anonymisere vedtak som belyser forvaltningspraksis for fremleggelse i retten¹.

Dersom det er behov for dialog med fullmektig om hvilke vedtak som er mest relevante å legge frem for retten, kan saksbehandler oversende vedtak som ikke er anonymisert, da e-post sendes kryptert. Se pkt 7. Saksbehandler har det endelige ansvaret for å anonymisere vedtakene som legges frem for retten.

3.2 Oversendelse av opplysninger i saker til andre forvaltningsorganer

UNE kan i enkelte tilfeller oversende opplysninger i enkeltsaker til andre forvaltningsorganer. Adgangen til slik utlevering er hjemlet i forvaltningsloven § 13b første ledd bokstav b. Vilåret for slik utlevering er at opplysningene er nødvendig for å fremme avgiverorganets (dvs. UNEs)

¹ Denne hovedregelen gjelder ovenfor alle UNEs prosessfullmektiger: overlevering til RA, Kluge eller Prosedyreseksjonen i UNE.

«oppgaver etter lov, instruks eller oppnevningsgrunnlag». Vurderes dette vilkåret som oppfylt, gir bestemmelsen UNE en forholdsvis vid adgang til å utlevere opplysninger. Det gjøres imidlertid oppmerksom på at det som en hovedregel kun er opplysninger fra enkeltsakene som kan oversendes. Unntaket gir ikke adgang til å oversende saksdokumenter i sin opprinnelige form, eksempelvis vedtak i saken. Se FV-01 Taushetsplikt i utlendingssaker.

3.3 Særlig om oversendelse til JD

Når JD ber om å få oversendt vedtak i en av departementet identifisert enkeltsak, er anonymisering unødvendig. Adgangen til slik utlevering følger av forvaltningsloven § 13b første ledd bokstav b. Utlevering av opplysninger til departementet i identifiserte enkeltsaker, eksempelvis mediasaker, faller innunder rammene for dette unntaket. Dette unntaket vil også som utgangspunkt gjelde opplysninger som angir begrunnelsen for vedtaket. E-post til JD kan sendes på ordinær måte via Outlook, da e-post mellom JD og UNE sendes kryptert. Se pkt. 7.

3.4 Utlegg på åpne og offentlige sider

Utlegg på UNETT, une.no, UDIs regelverksportal og Lovdata Pro skal anonymiseres. Dette kan eksempelvis være aktuelt ved utlegg av stornemndvedtak på disse sidene.

3.5 Sammendrag til Praksisbasen

Ved utlegg på UNEs praksisbase skal sammendragene anonymiseres før publisering. Se RB-22 UNEs praksisbase, innlegging av avgjørelser i basen.

4 Hvilke opplysninger skal anonymiseres?

I henhold til forvaltningsloven § 13 første og annet ledd er alle opplysninger som anses som personlige, direkte eller indirekte, omfattet av forvaltningens taushetsplikt. Dette innebærer at anonymiseringen må sørge for minimering av risiko for at opplysninger om en person kan bli identifisert, og at alle opplysninger som kan være egnet til å identifisere personen skal fjernes. Jo mer inngripende og sensitive opplysningene er i et vedtak, desto sterkere er kravene til hvilke opplysninger vi vurderer anonymisert.

Av hensyn til dokumentets illustrasjonsverdi om praksis kan opplysningene ved behov erstattes av generelle kategorier (eks. et aldersintervall som erstatning for konkret alder), dersom hensynet til anonymisering ivaretas. Når opplysninger erstattes av generelle kategorier, skal dette fremgå av dokumentet ved at teksten settes i klammer.

Listen med momenter i det følgende er ikke uttømmende, og er kun ment som en veiledning. Graden av anonymisering må vurderes konkret i hver enkelt sak.

Følgende opplysninger skal anonymiseres i vedtakene:

- Klagerens og andre personers (eks. slektingers);
 - Navn, herunder aliasnavn,
 - DUF- nummer.

- Konkret vurdering- dersom slike opplysninger (alene eller i kombinasjon med andre opplysninger) vil kunne bidra til å identifisere personer:
 - Opplysninger om de steder klageren bor/ har bodd/oppholdt seg i hjemlandet og i Norge, inkludert eventuelt asylmottak (f.eks. mindre landsbyer, detaljerte opplysninger om lokale forhold mv.).
 - Opplysninger om hvilket politidistrikt som har registrert klagerens søknad.
 - Detaljerte opplysninger om arbeidssted, arbeidsgiver, yrkestitler, stilling, karriere osv. i klagerens hjemland eller i Norge.

- Navn på sykehus, fengsler, politidistrikter, domstoler mv. i hjemlandet.
- Navn og identifiserbar informasjon om helsepersonell eller institusjoner som etter det opplyste behandler eller har behandlet klageren, og som har uttalt seg i saken.
- Detaljerte opplysninger om begåtte handlinger, idømt straff og soning i hjemlandet.

Særtilfelle for asylsaker:

- I asylsaker må UNE ta høyde for at hjemlandets myndigheter eller andre kan ha bakgrunnsinformasjon som gjør det mulig å identifisere klageren eller andre personer selv om slik identifisering ikke nødvendigvis er mulig for enhver i Norge. Samtidig vil opplysningen om at en person har søkt asyl være taushetsbelagt. Det innebærer at opplysning om at personen har adresse på et asylmottak normalt vil være taushetsbelagt og bør anonymiseres.

5 Opplysninger som i utgangspunktet ikke skal sladdes:

- Navn på klagerens advokat/fullmektig eller navn på beslutningstager i UNEs vedtak.
- Tidsangivelser som for utenforstående ikke kan tilbakeføres til klageren, så som søknadsdato, datering av klage og andre brev, og vedtaksdato.
- Hjemland/ statsborgerskap og eventuell etnisitet. Dette kan være opplysninger som har hatt stor betydning for utfallet av saken og som illustrasjon av praksis.

Dersom slike opplysninger i det konkrete tilfellet, eventuelt i kombinasjon med andre opplysninger som fremgår av vedtaket, er egnet til å identifisere klageren eller andre enkeltpersoner, skal sladding likevel foretas.

6 Praktisk gjennomføring

UNEs vedtak skal som hovedregel sladdes elektronisk. Det må påses at sladdingen (fjerningen av metadata i dokumentet) ikke senere kan reverseres av mottakere. For å sikre seg mot slik reversering skal dokumenter sladdes ved hjelp av programmene PixEdit eller Adobe Acrobat Pro.

I de tilfeller hvor sladdede opplysninger erstattes av generelle kategorier, kan «lagre som»-funksjonen i Word benyttes for å omdanne word-dokumentet til pdf- format. Alternativt må dokumentet skrives ut og skannes inn igjen i PDF-format.

7 Kryptert e-post

Reglene om personvern og taushetsplikt i personopplysningsloven og forvaltningsloven setter rammene for utlevering av personopplysninger. Dette gjelder både for utlevering av opplysninger til klageren og fullmektig, men også til andre forvaltningsorganer. Se pkt 3 over og FV-1 Taushetsplikt i utlendingssaker. Gir regelverket adgang til utlevering av personopplysninger, kan slike opplysninger sendes via ordinær e-post i Outlook til enkelte mottakere. For øvrige mottakere må ferdig utkast til e-post sendes til postmottak@une.no hvor det bes om kryptering før utsendelse.

UNEs datasystem bruker en løsning som kalles TLS (Transport Layer Security) ved oversendelse og mottak av e-post. Denne løsningen sørger for at e-post UNE står som avsender

av vil bli kryptert ved oversendelse til mottaker som også benytter denne løsningen. Tilsvarende vil e-post som UNE mottar være kryptert dersom avsenderen benytter denne løsningen. Betingelsen for slik overføring er altså at mottaker og avsender har tilsvarende løsning.

UNEs kontakter som bruker denne løsningen: (nnn i e-postadressen må endres til mottakers initialer)

- Politiet (alle e-postadresser til nnn@politiet.no)
- Regjeringsadvokaten e-post til nnn@regjeringsadvokaten.no)
- Justis- og beredskapsdepartementet (alle e-poster til nnn@jd.dep.no)
- Domstolene (e-post til nnn@domstol.no)
- Utenriksdepartementet (e-post til nnn@mfa.no)
- NID (e-post til nnn@nidsenter.no)
- IMDi (e-post til nnn@imdi.no)
- Advokatfirmaene Kluge, Riisa og Norman & Co.

E-post mellom UNE og UDI går på en lukket forbindelse og ikke ut på internett. Dette gjelder også Landinfo som er del av UDIs IT- løsning.

TU kan verifisere om andre mottakere av e-post har slik sikring. Henvend deg via Helpdesk med epostadressen det gjelder.

Jan Olav Barstad (sign.)
fungerende seksjonssjef