SAF-T Regnskap:

Bruk og misbruk av personopplysninger

Målet med innføringen av Standard Audit File – Tax (SAF-T) Regnskap er å gjøre det enklere å dele, kontrollere og analysere regnskapsdata. Økt bruk og tilgjengelighet øker også risikoen for at regnskapsdata kommer på avveie eller misbrukes bevisst eller ubevisst, av interne eller eksterne parter.

PhD
Lars Erlend Leganger
Direktør i PwC

Personvernjurist
Christine Ask Ottesen
Direktør i Advokatfirmaet PwC

Selskaper er lovpålagt å fremskaffe regnskapsdata på SAF-T-format når/om Skatteetaten ber om det ved en eventuell kontroll, men regnskapsdata på SAF-T-format har også mange potensielle anvendelsesområder både internt i foretaket og ved revisjon.[1] Standardiseringen og forenklingen ved SAF-T tilrettelegger for økt bruk av regnskapsdata i verdiskapende prosesser og analyser, men økt bruk og tilgjengelighet øker også risikoen for at regnskapsdata kommer på avveie eller misbrukes bevisst eller ubevisst, av interne eller eksterne parter.

Fremskritt innen stordataanalyse både utvider mulighetene for, og reduserer kostnadene ved, å «sette data i arbeid» gjennom analyser og datadrevet automatisering. Dette gjør forretningsrelevante data om bedrifter, produkter, og enkeltindivider mer anvendelige og attraktive. I takt med at potensialet for å bruke – og misbruke – data øker, stilles det høyere krav til hvordan en jobber med (regnskaps)data: «Klassiske» risikoer knyttet til behandling av regnskapsdata – som lekkasje av børssensitiv informasjon og innsidehandel, eller avsløring av forretningshemmeligheter om priser og marginer – har fått selskap av nye risikoer og krav. Ikke minst gjelder dette hvordan en behandler og beskytter de personopplysningene[2] som direkte eller indirekte inngår i foretakets regnskapsdata.

Hva er en personopplysning?

- Personopplysninger er «enhver opplysning om en identifisert eller identifiserbar fysisk person
- En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet[1]
- Anonyme opplysninger, altså opplysninger som ikke kan identifisere fysiske personer, er ikke ansett som personopplysninger. Opplysninger kan ved første øyekast fremstå som anonyme, men likevel være personopplysninger i lovens forstand, dersom det kan være mulig å identifisere en eller flere personer ad omveier. Eksempler på dette er kontonummer, en bils registreringsnummer og opplysninger knyttet til kundenumre. Slike opplysninger kan kobles sammen med andre opplysninger, og dermed identifisere personen opplysningen er knyttet til

1 GDPR artikkel 4: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-1#KAPITTEL_gdpr-1

Personopplysningsloven

Personopplysningsloven[3] stiller strenge krav til virksomheters behandling av personopplysninger – også når behandlingen utføres for å etterleve andre lovpålagte krav, som eksempelvis tilgjengeliggjøring av regnskapsdata på SAF-T-format. Dette innebærer blant annet at den enkelte virksomhet må vurdere og dokumentere det rettslige grunnlaget for behandlingen av personopplysninger, ta stilling til kravene til dataminimering og sletting, samt gjennomføre nødvendige sikkerhetstil-

1 Se bl.a. Revisjon og Regnskap 8/2020 for en overordnet introduksjon til SAF-T Regnskap, Revisjon og Regnskap 1/2021 for en drøfting av mulighetene SAF-T Regnskap åpner for revisjon, og Revisjon og Regnskap 2/2021 for ny SAF-T i MVA-melding og fremtidige muligheter for sanntidsrapportering.

2 Se faktaboks for nærmere definisjon og eksempler på hva som kan utgjøre personopplysninger.

3 Norge innførte ny personopplysningslov i 2018. Loven består av nasjonale regler og implementerer EUs personvernforordning «General Data Protection Regulation» (GDPR) i norsk rett.

tak – som tilgangsstyring, logging, kryptering, og/eller pseudonymisering.

I denne artikkelen ser vi på noen relevante personvernutfordringer – og -muligheter – ved etterlevelse av lovpålagte SAF-T-krav, og ved bruk av SAF-T i analyser og andre verdiskapende aktiviteter.

Behandling av personopplysninger kan kreve risikoreduserende tiltak

Skatteforvaltningsloven gir myndighetene vide fullmakter til å hente inn og behandle data som har betydning for foretaks bokføring og skatteplikt – inkludert taushetsbelagte data – i forbindelse med kontroll.[4] Bokføringsforskriften § 7–8 stiller krav til at bokførte opplysninger kan gjengis i «standardisert form» – SAF-T Regnskap. Kravet om gjengivelse av regnskapsdata på standardisert form endrer ikke i seg selv hvilke – og hvor mye – data skattemyndighetene har lovhjemmel til å be om, men standardiseringen utvider mulighetsrommet for hvor store mengder data det er praktisk gjennomførbart å hente inn og behandle. Bokføringsforskriftens krav om standardisering oppfyller personopplysningslovens krav til behandlingsgrunnlag for arbeid med bygging og validering av SAF-T-filer.

Krav utover det rettslige grunnlaget

Personopplysningsloven angir imidlertid en rekke krav utover at det skal foreligge et rettslig grunnlag for behandlingen. En skal eksempelvis også sikre ivaretakelse av de registrertes rettigheter og gjennomføre tilfredsstillende risikoreduserende tiltak ved behandlingen av personopplysninger. Å samle regnskapsdata i SAF-T XML-fil(er) gjør det enklere å utveksle og behandle dataene, men det kan samtidig svekke ivaretakelsen av den enkeltes personvern om ikke tilstrekkelige risikoreduserende tiltak implementeres knyttet til behandlingen:

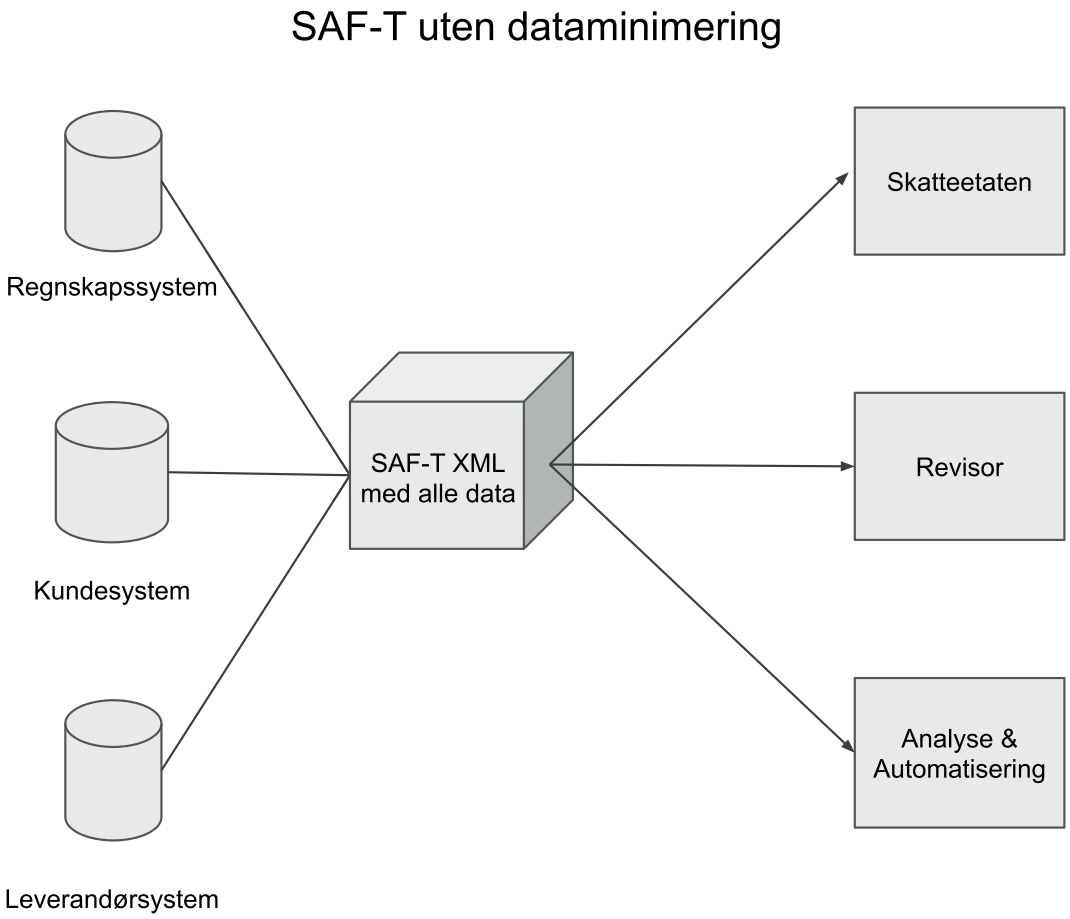
Behovsbasert tilgangsstyring er et viktig tiltak for å etterleve prinsippet om dataminimering – altså at man ikke behandler mer data enn det som er tilstrekkelig for å oppnå formålet med behandlingen. I (moderne) regnskapssystemer og datavarehus kan forskjellige brukere og systemer gis differensierte tilganger basert på roller og oppgaver – når man utfører oppgaver/analyser knyttet til en spesifikk leverandør trenger en ikke nødvendigvis tilgang til alle data om de øvrige leverandørene, kundene osv. For en SAF-T XML-fil er det ikke like enkelt – i utgangspunktet har man enten tilgang på en fil, eller ikke – mer differensiert tilgangsstyring krever spesialbygde løsninger rundt SAF-T-filen.

Detaljert logging av hvilke data som behandles av forskjellige brukere/systemer, er viktig bl.a. for å overvåke og dokumentere at databehandling skjer i henhold til personvernregelverket, og for å gjøre det mulig å avdekke og rette opp eventuell feilbehandling eller

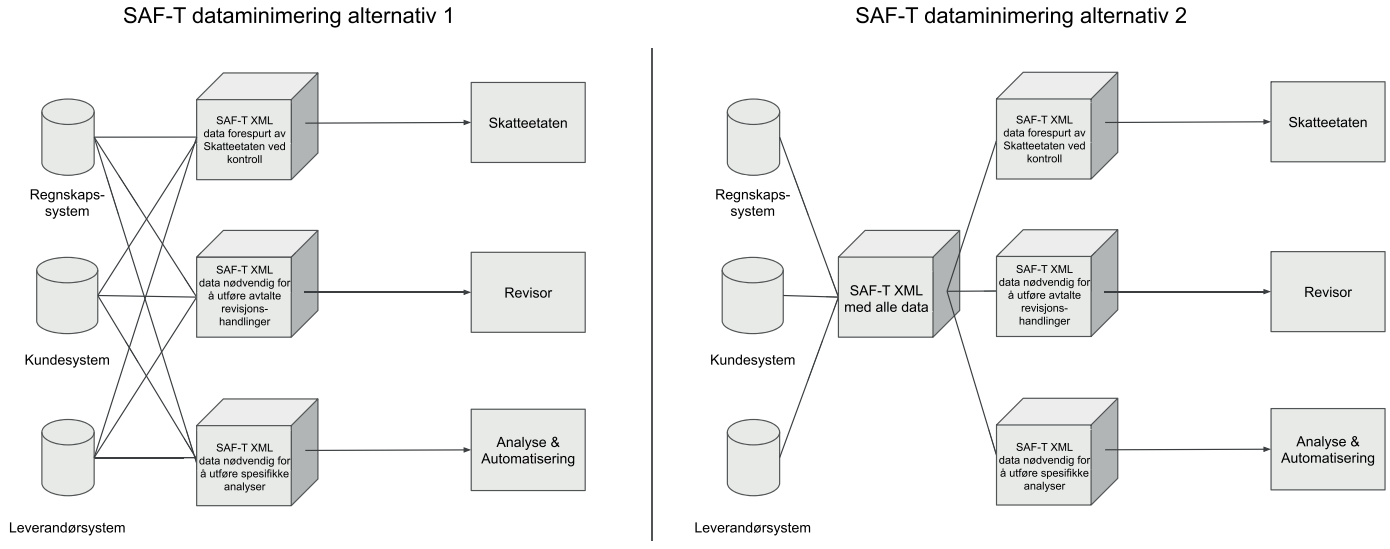
Utvalgte krav og begrep i GDPR

- **Behandlingsgrunnlag:** all behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig. Virksomheter som behandler personopplysninger, må identifisere et behandlingsgrunnlag for personopplysningene som behandles for hvert enkelt formål. Dersom en ikke kan identifisere et behandlingsgrunnlag, vil behandlingen ikke være lovlig. Typiske eksempler på rettslige grunnlag vil være samtykke, behandlingen er nødvendig for å gjennomføre en avtale, virksomhetens legitime interesse eller hvor behandlingen er nødvendig for å oppfylle en rettslig forpliktelse.
- **Behandlingsansvarlig:** er det primære pliktsubjektet etter personvernregelverket og som er overordnet ansvarlig for å overholde personvernprinsippene og regelverkets øvrige bestemmelser. Den behandlingsansvarlige er ansvarlig for å behandle personopplysninger på en lovlig, rettferdig og gjennomsiktig måte, sikre at det foreligger et behandlingsgrunnlag, behandle personopplysningene på en tilfredsstillende sikker måte, påse at de registrerte får utøvd sine rettigheter og en rekke øvrige plikter.
- **Databehandler:** en ekstern aktør som behandler personopplysninger på vegne av den behandlingsansvarlige. Databehandler opptrer på instruks fra den behandlingsansvarlige og kan derfor ikke selv bestemme formål og andre avgjørende elementer ved behandlingen. Databehandlerens adgang til å behandle personopplysninger på vegne av den behandlingsansvarlige reguleres gjennom en databehandleravtale.
- **Dataminimering:** prinsippet om dataminimering innebærer en forpliktelse til å begrense mengden personopplysninger som behandles. Dette innebærer at en bare kan behandle de personopplysningene som er nødvendige og relevante for å oppnå formålet personopplysningene behandles for.
- **Tekniske og organisatoriske tiltak:** den behandlingsansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å sikre at behandlingen utføres i samsvar med personvernprinsippene. Det betyr blant annet at behandlingsansvarlige skal innføre interne rammeverk og retningslinjer som sikrer denne gjennomføringen og implementere egnede tekniske og organisatoriske tiltak, inkludert gjennomføre risikovurderinger og ev. vurdering av personvernkonsekvenser ved behov. Tiltakene skal stå i forhold til risikoen forbundet med brudd på fysiske personers rettigheter og friheter som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysningene.

4 Skatteforvaltningsloven § 10-1: (1) Skattepliktig og andre skal etter krav fra skattemyndighetene gi opplysninger som kan ha betydning for vedkommendes bokføring eller skatteplikt og kontrollen av denne. Skattemyndighetene kan kreve at den skattepliktige dokumenterer opplysningene ved for eksempel å gi innsyn i, legge frem, sammenstille, utlevere eller sende inn regnskapsmateriale med bilag, kontrakter, korrespondanse, styreprotokoller, elektroniske programmer og programsystemer. Bestemmelsene her gjelder tilsvarende for trekkpliktig som nevnt i § 8-8.
(2) Den som kan pålegges å gi opplysninger etter første ledd, har plikt til å gi opplysningene uten hensyn til den taushetsplikten vedkommende er pålagt ved lov eller på annen måte. Opplysninger som angår rikets sikkerhet, kan likevel bare kreves fremlagt etter samtykke fra Kongen.
https://lovdata.no/lov/2016-05-27-14/§10-1



Figur 1: Behandling av SAF-T-data uten hensyn til dataminimering er det teknisk enkleste, men gir økt risiko. For behandling av personopplysninger er dataminimering et krav.



Figur 2: Ved å bygge SAF-T-filer som kun inneholder de data som er nødvendige for hvert enkelt behandlingsformål, kan prinsippet om dataminimering etterleves. Avhengig av kapabilitetene til systemene/løsningene som bygger SAF-T-filene, kan slike avgrensninger gjøres enten direkte ved eksport fra kildesystemene (alternativ 1), eller ved å bearbeide SAF-T-filene etter eksport, men før videre distribusjon og behandling (alternativ 2).

misbruk. Logging er derfor et sentralt hjelpemiddel i både preventivt og reaktivt datasikkerhetsarbeid. Det er enkelt å logge når brukere/systemer åpner og/eller endrer en SAF-T-fil, men langt vanskeligere å logge *hvilke* data i SAF-T-filen som behandles når den først er åpnet – og eventuell feilbehandling eller misbruk blir vanskeligere å avdekke. Ved datalekkasjer eller uregelmessige endringer i en SAF-T-fil, blir alle som har jobbet med filen potensielle «mistenkte».

Reduserte muligheter for differensiert tilgangsstyring og detaljert logging gjør at det kan være nødvendig å implementere andre risikoreduserende tiltak for å ivareta personvernet og holde eventuell omdømmerisiko på et akseptabelt nivå. Dette gjelder spesielt dersom en ønsker å bruke SAF-T-filer for andre behandlingsformål enn å oversende regnskapsdata til Skatteetaten i forbindelse med kontroll, se figur 1 og 2.

Et (relativt) enkelt risikoreduserende tiltak ved behandling av SAF-T-filer er å bygge forskjellige SAF-T-filer for forskjellige formål. Mange av datafeltene i SAF-T er «optional» – hvis «optional» data finnes i systemene, og ikke annet er avtalt, må de inkluderes i SAF-T-fil(ene) som tilgjengeliggjøres for skattemyndighetene ved kontroll – men samtidig er det fullt mulig å bygge en teknisk valid SAF-T-fil uten slike «optional» data. På samme måte som det er mulig å lage separate SAF-T-filer for forskjellige perioder, kan man i stedet for, eller i tillegg til å bygge og behandle én stor SAF-T-fil, lage flere separate formålsspesifikke SAF-T-filer hvor personopplysningene utelates eller anonymiseres, eller filer som bare inneholder data om de transaksjoner/kunder/leverandører som er relevante for hvert enkelt formål.

Utkontraktering av SAF-T-bygging og -validering

Enkelte foretak vil – i kortere eller lengre perioder – være avhengige av spesialbygde løsninger for fullt ut å etterleve bokføringslovens SAF-T-krav. Eksempelvis kan dette skyldes komplekse systemlandskap etter oppkjøp og fusjoner, gamle regnskapssystemer uten støtte for SAF-T som snart skal erstattes, og/eller bruk av manuelle justeringer og korreksjoner i systemene for å få totalene i regnskapet til å stemme. I slike situasjoner kan det være aktuelt å benytte seg av tredjeparter for utkontraktering av hele- eller deler av arbeidet med bygging av foretakets SAF-T-filer. Mange foretak benytter også tredjeparter til å gjennomføre uavhengige tekniske og innholdsmessige valideringer av SAF-T-filer før overlevering til Skatteetaten, for å avdekke og rette opp eventuelle feil og mangler som ville ført til at innsendelsen ikke blir godkjent.

Uansett om arbeidet med SAF-T gjøres internt eller utkontrakteres, er det foretaket selv som er behandlingsansvarlig for personopplysninger som inngår i bygging og validering av SAF-T-filene. Ved bruk av tredjeparter er det nødvendig at foretaket som behandlingsansvarlig gir sine instrukser til tredjepartene («databehandlerne») om hvordan personopplysningene skal behandles. Dette skal reguleres i en databehandleravtale. Her er det også viktig å være oppmerksom på de særlige kravene som gjelder for overføring av personopplysninger (at personopplysningene sendes eller overføres til et annet land, eller at noen i et annet land får fjerntilgang til opplysningene), dersom databehandleren ikke kan garantere at personopplysningene kun vil behandles i EU/EØS-området.[5]

SAF-T-standardisering – nye muligheter, men større ansvar

SAF-T Regnskap gjør det enklere å dele og bruke regnskapsdata. I revisjon åpner det for mer effektiv datafangst, forenkler bygging av automatiske kontroller, og gjør det enklere å gjøre datadrevne utvalg for mer treffsikker testing. Økonomifunksjonen i konsern kan bruke SAF-T-filer som felles standardisert datakilde for konsernrapportering og analyser. Finansiell og skattemessig due diligence kan gjennomføres mer effektivt. På sikt er SAF-T et viktig steg på veien mot sanntidsrapportering.

Misbruk

Men det som blir enklere å bruke, blir også enklere å misbruke. SAF-T-filer kan inneholde potensielt store mengder personopplysninger, og GDPR stiller strenge krav til behandlingen av personopplysninger – uansett om behandlingen kun utføres for å etterleve (bokførings)lovpålagte krav, eller om SAF-T-filene også brukes i andre verdiskapende analyser og prosesser. For å realisere det store analyse- og automatisering-potensialet som ligger i SAF-T Regnskap på en ansvarlig måte, er det er viktig å ha et bevisst forhold til – og tekniske kapabiliteter for – differensiering av hvilke data som inkluderes i SAF-T XML-filer bygget for forskjellige behandlingsformål og å ivareta tekniske og organisatoriske risikoreduserende tiltak ved behandling.

5 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/