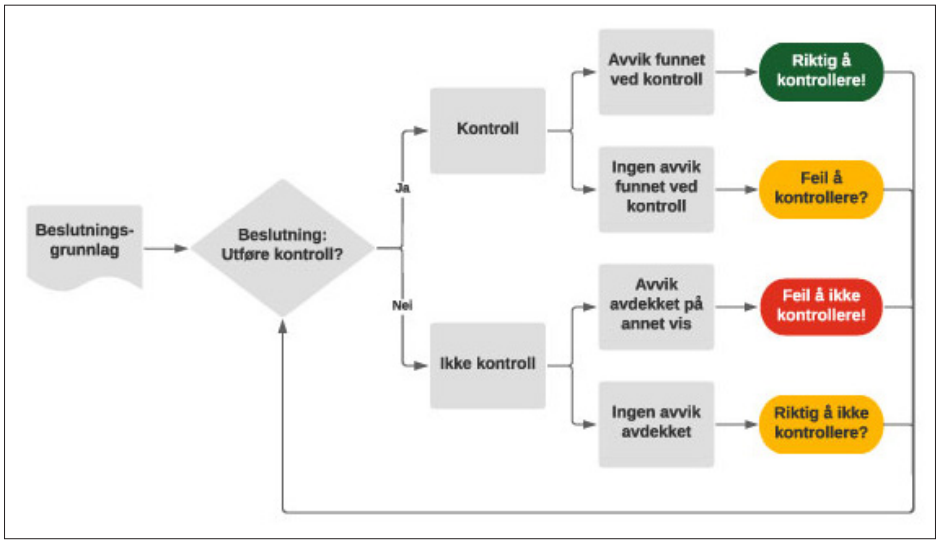
Føderert maskinlæring og kommersialisering av lovpålagte plikter

For de fleste aktører er arbeid med etterlevelse av lovpålagte plikter og andre regelverk først og fremst forbundet med kostnader, men etter hvert som etterlevelses-prosesser blir mer datadrevet, oppstår det muligheter for å gjøre arbeid med lovpålagte plikter om til nye kommersielle produkter og tjenester, gjennom bygging og bruk av matematiske beslutningsmodeller med maskinlæring (ML).

PhD
Lars Erlend Leganger
Direktør i PwC

Det meste av dagens kunstige intelligens (AI, fra engelsk «artificial intelligence») bruker såkalt overvåket[1] ML. Dette er matematiske algoritmer som lar datamaskiner automatisk finne sammenhenger og mønstre i potensielt store datasett, og fra dette bygge komplekse beslutningsmodeller som styrer AI-løsningenes (mer eller mindre) intelligente beslutninger og handlinger: Jo mer relevante data en har om beslutningene som skal tas, jo mer treffsikre og rettferdige ML-modeller kan en bygge. Skal det for eksempel bygges AI for å øke treffsikkerheten av en stikkprøvekontroll, er det viktig med data om hva slags mønstre som tidligere har kjennetegnet saker der kontroll gav funn, se figur 1.



Figur 1: Maskinlærte beslutningsmodeller bygges («trenes») ofte med historiske data om hvordan tilsvarende beslutninger har blitt gjort tidligere, og hva utfallet ble. Fra «Automatisering av revisjon», Revisjon og Regnskap nr. 3 2022.

De siste årenes teknologiske fremskritt innen maskinlæring har drastisk økt nyttepotensialet og verdien av data som er relevante for produktene og tjenestene en aktør leverer. For aktører som leverer produkter og tjenester som involverer mennesker, vil beslutningsrelevante data ofte inneholde personopplysninger, hvis bruk er beskyttet og regulert av personopplysningsloven med EUs personvernforordning (General Data Protection Regulaton – GDPR).

GDPR og regulatorisk sandkasse

Å bygge verdiskapende kunstig intelligens innenfor rammene av hva GDPR tillater kan være krevende. Mangelen på gode løsninger svekker muligheten til å jobbe datadrevet i europeisk nærings- og samfunnsliv, og på sikt kan det gjøre oss mindre konkurransedyktige sammenlignet med andre jurisdiksjoner, hvor individets rett til privatliv ikke vektes like tungt som kollektivets nytte fra utvikling og bruk av datadrevne løsninger. For å stimulere til ansvarlig innovasjon

[1] På engelsk brukes begrepet «supervised». Det norske begrepet «overvåket» henspiler ikke på personovervåkning – men på at en med denne typen ML-modell styrer/overvåker hva slags vurderinger ML-modellen lærer seg ved å definere ønsket utfall / «fasit» i treningsdataene: F. eks. kan antihvitvasking kunstig intelligens bygges ved å mate overvåkede-ML-algoritmer med data om hvilke historiske transaksjoner som var – og ikke var – knyttet til hvitvasking.

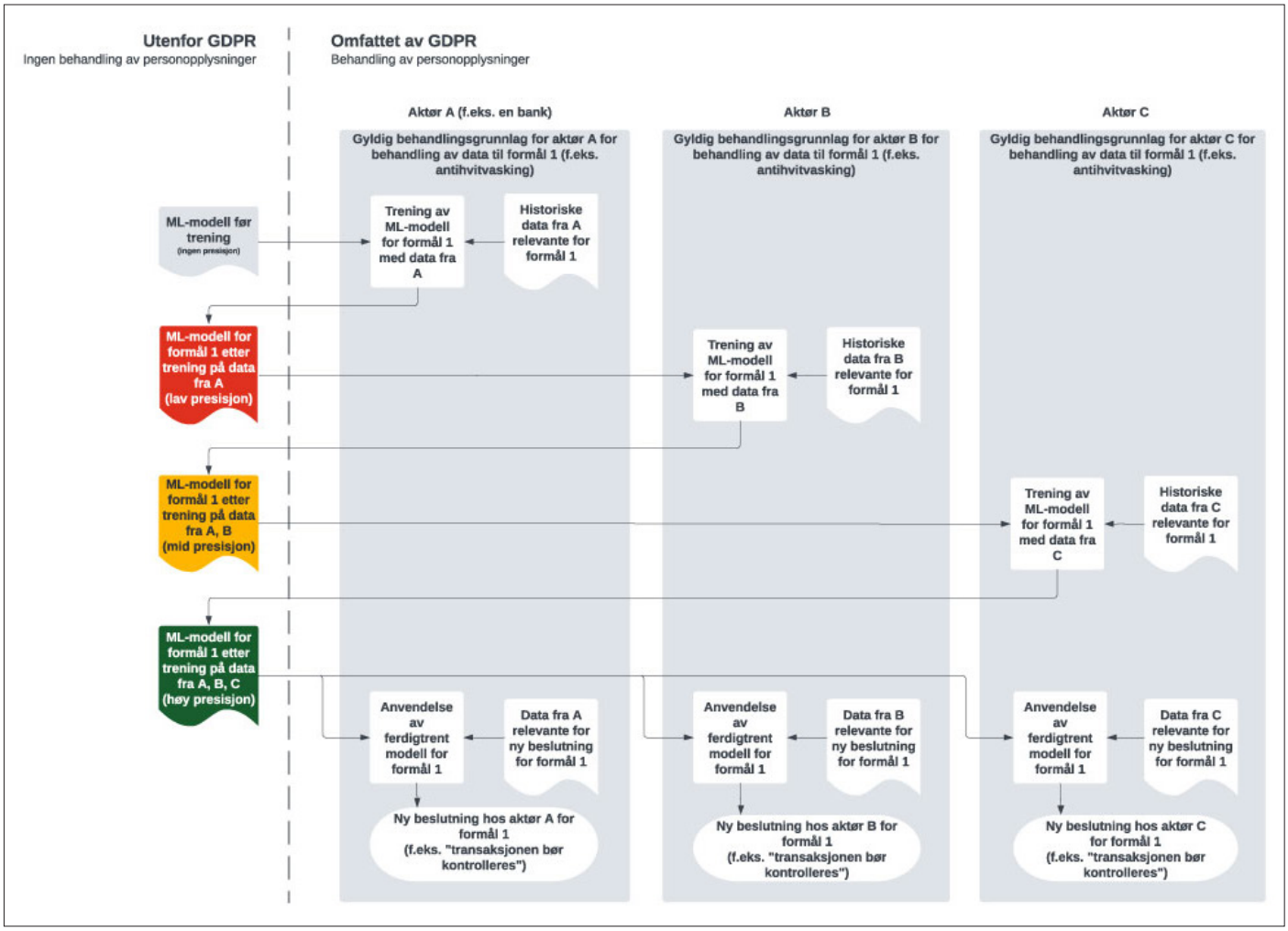
med kunstig intelligens har Datatilsynet opprettet en regulatorisk sandkasse,[2] der enkeltaktører kan få hjelp til å følge regelverket og utvikle personvernvennlig AI.

Antihvitvasking og AI

Anti-hvitvasking er et typisk eksempel på en kontrollaktivitet der AI kan gi verdi: Mer treffsikre beslutningsmodeller for hvilke transaksjoner som bør kontrolleres for hvitvasking og terrorfinansiering (og hvilke transaksjoner som trygt kan passere) kan både føre til at flere ulovlige transaksjoner stanses (redusere «falske negative» funn), og minimere kostbar og personverninngripende kontroll av uskyldige transaksjoner (redusere «falske positive» funn). Det er imidlertid få saker som avdekkes, og vanskelig for hver enkelt bank å bygge store nok datasett-modeller der man kan lære å kjenne hvitvasking-mønstre. Siden transaksjonsdataene inneholder personopplysninger, kan ikke banker uten videre dele dataene med hverandre for å bygge en felles antihvitvask-løsning. I en fersk rapport[3] fra Datatilsynets regulatoriske sandkasse for kunstig intelligens utforskes muligheten for å bygge ML-modeller for anti-hvitvasking-transaksjonskontroll med såkalt føderert læring.

Føderert læring

Tanken bak føderert læring er enkel – i stedet for at forskjellige aktører deler data for å bygge en ML-modell på ett sentralisert sted, distribueres ML-modellen ut til de forskjellige aktørene, som hver for seg bruker sine egne data for å trene og forbedre modellen. Til slutt får alle aktørene som har bidratt tilgang på den ferdigtrente modellen, se figur 2.



Figur 2: Forenklet fremstilling av føderert læring. Forskjellige aktører kan samarbeide om å bygge/trene en ML-modell, uten at personopplysningene som benyttes i treningen behøver å deles mellom aktørene. Den forretningsmessige verdien ligger ikke i de individuelle personopplysningene hos hver enkelt aktør, men i de overordnede sammenhengene og mønstrene som en ML-algoritme gjør om til tallverdier i komplekse regnestykker gjennom overvåket læring. Den resulterende ML-modellen inneholder i seg selv ingen personopplysninger, og kan deles mellom aktørene slik at hver aktør kan bidra til modell-treningen med de personopplysningene den enkelte aktøren har behandlingsgrunnlag for.

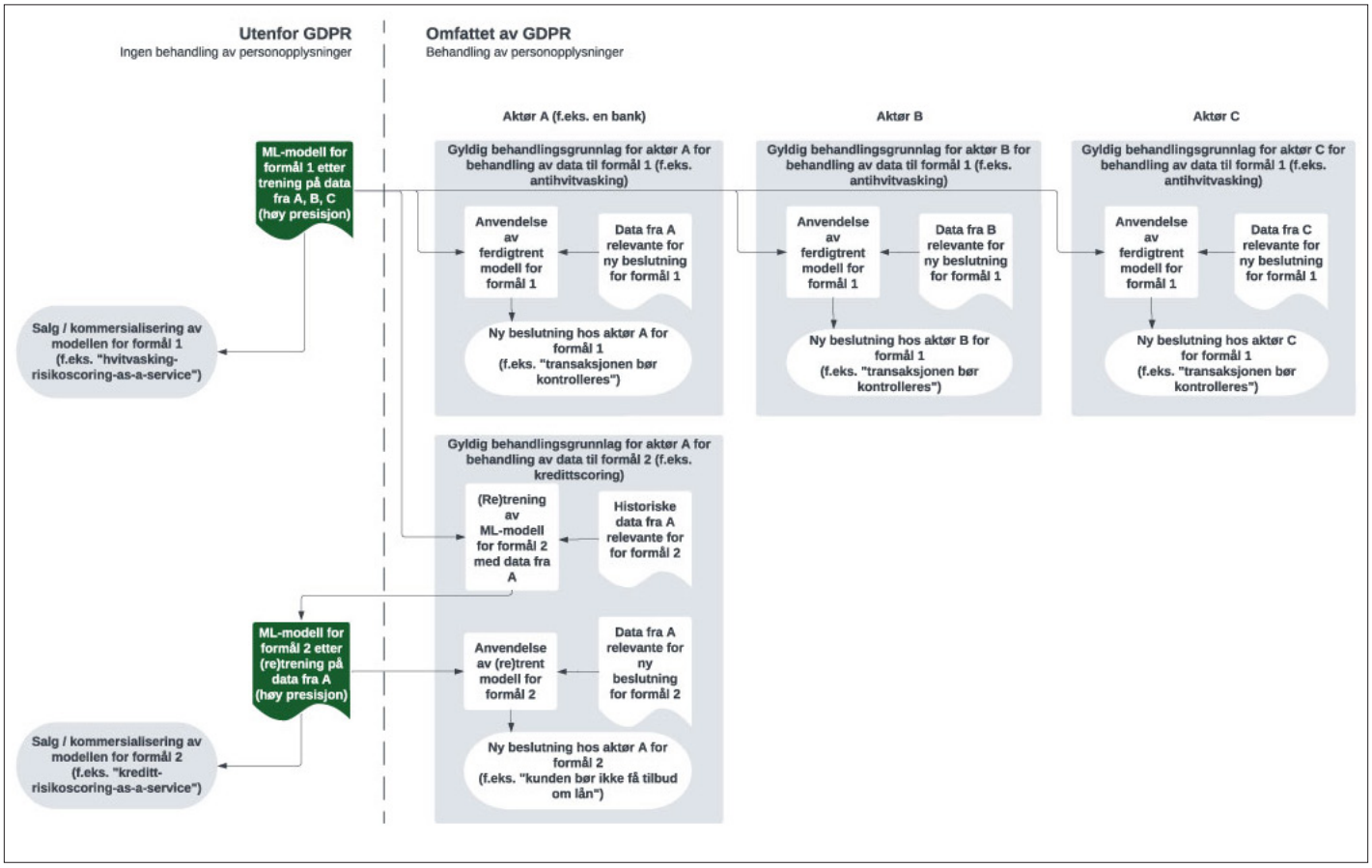
[2] https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/
[3] https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/finterai-sluttrapport/

ML-modeller

En ML-modell er i sin fundamentale form kun et sett tallverdier i et (ofte komplekst) regnestykke. ML-algoritmer behandler personopplysninger for å regne seg frem til hva de forskjellige tallverdiene skal være («trening» av ML-modellen), men sluttresultatet – den ferdigtrente modellen – inneholder ingen personopplysninger i seg selv, kun en matematisk beskrivelse av mønstre og sammenhenger ML-algoritmen har lært fra dataene.[4] Da er ikke modellen omfattet av GDPR, og sandkasse prosjektet finner da også – med noen forbehold – at føderert læring er en lovende teknologi for ansvarlig utvikling og anvendelse av AI.

Formål kan begrense bruken

At ML-modeller trent på personopplysninger fritt kan deles i føderert læring belyser en beslektet problemstilling: Data samlet inn for ett formål kan også inneholde verdifull innsikt for andre formål, men GDPR forbyr slik gjenbruk av innsamlede persondata med mindre en har gyldig behandlingsgrunnlag også for det nye formålet. Personopplysninger innhentet for å vurdere hvitvasking-risiko kan ikke uten videre gjenbrukes til å beregne kredittrisiko, ei heller kan opplysningene selges til andre aktører. Bygger man en ML-modell fra opplysningene, forholder det seg annerledes: Modellen i seg selv kan både gjenbrukes til andre formål, og selges/produktifiseres, uten å bryte med GDPR: Se figur 3.



Figur 3: En ML-modell trent opp for ett formål (f.eks. antihvitvasking), kan potensielt beskrive mønstre og sammenhenger som også er relevante for beslutninger knyttet til andre formål (f.eks. kredittrisiko). Siden modellen i seg selv ikke inneholder personopplysninger, står den utenfor GDPR, og kan kommersialiseres (f.eks. som hvitvasking-risikoscoring-as-a-service) eller re-trenes til andre formål (f.eks. kredittscoring) uten at det i seg selv bryter med personvernforordningen.

ML-modeller og revisjon

Ikke minst er dette aktuelt for revisjon: En del av revisors plikter er å opparbeide seg en forståelse av virksomheten som revideres, herunder bransjemessige faktorer og andre eksterne forhold, jf. revisorloven § 9-4 tredje ledd bokstav a. Det er stort potensial for å bruke ML-modeller i opparbeidelsen av slik forståelse. På samme måte som for anti-hvitvasking kan revisjons-ML-modeller sendes fra det ene revisjonsteamet til det neste, og trenes føderert uten at kundedata deles mellom team-

[4] En ML-modell vil i utgangspunktet ikke inneholder personopplysninger, men det kan oppstå situasjoner der enkelte deler av personopplysninger kan rekonstrueres fra modellen. Den vanligste årsaken er såkalt «overtilpasning» av modellen – istedenfor å beskrive mønstre og sammenhenger i treningsdataene, er en overtilpasset modell nær å beskrive treningsdataene i seg selv. Å kjenne og håndtere risikoen for modell-overtilpasning er en viktig del av ansvarlig AI-utvikling – ikke bare av personvernhensyn, men også fordi overtilpasning av modeller gir dårligere treffsikkerhet i bruk.

ene – både internt i et revisjonshus, og i eventuelle revisjonsbransjesamarbeid rundt utvalgte revisjonshandlinger og modeller. På samme måte som for antihvitvasking er det ikke umulig at revisjons-ML-modeller finner dype mønstre og sammenhenger i bransjemessige forhold som også kan ha anvendelsesområder utenfor revisjonsformålet modellene opprinnelig blir bygget for.

ML-modeller og underliggende motivasjon

Etterlevelse av lovpålagte plikter og andre regelverk kan gi aktører rettslig behandlingsgrunnlag etter GDPR for innsamling og bruk av personopplysninger i et omfang de ellers ikke ville hatt. Eventuelle ML-modeller som bygges og anvendes for å etterleve lovpålagte plikter, inneholder i seg selv ikke personopplysninger, og kan også anvendes til andre, gjerne kommersielle, formål. Det vil være vanskelig å etterprøve den underliggende motivasjonen for å bygge modellene: Hva skal til for å slå fast at en aktørs hovedmotivasjon for å investere i datafangst og modellering ikke er etterlevelse av en lovpålagt plikt, men en senere kommersiell anvendelse av modellene som bygges? I Regjeringens forslag til statsbudsjett for 2023 skal Datatilsynets sandkasse bli en permanent ordning – det er ingen fare for at den vil gå tom for problemstillinger med det første.

Partner i advokatfirmaet Ræder

Skjerpet skatt på havbruk, vann- og vindkraft

Advokat
Ida Heldal
Advokatfirmaet Ræder

Advokat
Tone Kaarbø

Regjeringen foreslår å innføre grunnrenteskatt på havbruk og vindkraft fra 1. januar 2023. I tillegg foreslås økt grunnrenteskatt på vannkraft og en ekstra avgift, i form av et høyprisbidrag, på vind- og vannkraft, med virkning fra 28. september 2022.

I statsbudsjettet for 2023 foreslår regjeringen skjerpet skatt på oppdrettsnæringen og kraftbransjen. Dette skjer ved innføring av grunnrenteskatt på havbruk og på landbasert vindkraft og økning i den allerede eksisterende grunnrenteskatten på vannkraft.[1]

Grunnrente er en betegnelse på avkastning av naturressurser. Skattlegging av grunnrente er begrunnet i at noen aktører (med særskilt tillatelse fra staten) tjener penger på bruk av fellesskapets ressurser og at fellesskapet derfor bør få en andel av denne avkastningen.

Bakgrunnen for forslagene om skjerpet skatt på havbruk, vind- og vannkraft kan tilskrives økte utgifter for staten og økte strømpriser. Forslagene forventes å gi staten økte skatteinntekter på ca. 33 milliarder kroner. Noen av forslagene har allerede møtt sterk motstand fra enkelte miljøer.

Artikkelen er basert på forslag fremlagt i statsbudsjettet. Det ble fremlagt en tilleggsproposisjon Prop 1 S tillegg (2022-2023) 10. november som bl.a. omhandler presiseringer knyttet til kontraktsunntak og høyprisbidrag. Stortingets budsjettforslag behandles frem mot desember. I løpet av oktober og november gjennomgås regjeringens budsjettforslag i finanskomiteen, som legger frem forslag om totale utgifter og inntekter. Normalt er partiene enige om endringer før finansdebatten som finner sted 13. desember. Vedtakene kommer ventelig 21. desember.

1 Se Prop 1 LS (2022-2023) pkt 5.2-5.4.