Personvernregler for konsern:

Binding corporate rules

Fra mai neste år må alle norske virksomheter følge EUs nye personvernforordning. Binding Corporate Rules (BCR) kan bli en gunstig løsning for konsern som operer over landegrensene og andre med et større økonomisk samarbeid.

Advokatfullmektig
Charlotte Thuesen
Deloitte Advokatfirma

Advokat
Bjørn Ofstad
Deloitte Advokatfirma

Når EUs personvernforordning (GDPR) implementeres i Norge mai neste år, må alle virksomheter behandle personopplysninger etter et strengere sett av regler – et viktig stikkord er bedre kontroll. Bedre kontroll kan være utfordrende, og særlig for konsern, eller grupper av selskaper, som operer på tvers av landegrenser. Positivt er det da at ny personvernforordning lovfester muligheten til bindende konsernregler som gjør det lettere å overføre personopplysninger, eksempelvis HR-data, internt i et konsern.

Når kravene til virksomheters behandling av personopplysninger skjerpes, kan et selskap holdes ansvarlig for valg av samarbeidsparter, rutiner for all behandling av data må kartlegges og dokumenteres og sanksjonsnivået skjerpes. Personvernutfordringen mange selskaper står overfor i dag gjelder særlig den økende overføringen av personopplysninger mellom stater, for eksempel ved outsourcing av tjenester, men også mellom samarbeidende selskaper. Med GDPR innføres eksplisitt lovhjemmel for såkalte bindende konsernregler (binding corporate rules, BCR), en praktisk etterlevelsesmekanisme for konsern og andre med økonomisk samarbeid som behandler personopplysninger over landegrenser. For å sikre at personvernet blir ivaretatt, kan konsern eller selskaper med et felles økonomisk samarbeid inngå en BCR, en intern avtale som oppfyller spesifikke krav til etterlevelse av personvernregelverket.

Hvorfor BCR?

Overføring av personopplysninger ut av EØS-området er kun tillatt dersom det kan gis tilstrekkelige garantier for forsvarlig behandling av opplysningene. Det må som regel foreligge avtaleverk, for eksempel i form av EUs standardkontrakter og databehandleravtaler, for hver overføring og med alle som skal behandle opplysninger på vegne av en behandlingsansvarlig. Avtaleforvaltningen kan bli svært omfattende, og alle overføringsavtaler må meldes til Datatilsynet.

Etter hva som har vært godtatt praksis fra europeiske tilsynsmyndigheter og nå ved ny personvernforordning, kan en slik garanti også være bruk av bindende konsernregler. BCR er et smidig avtaleverk, som forenkler flyten av personopplysninger mellom selskaper i samme konsern, eller som har et økonomisk samarbeid. En BCR-avtale må forhåndsgodkjennes av Datatilsynet eller tilsvarende tilsynsmyndighet i EU. Når virksomheter først har inngått en BCR, vil denne fungere som et rammeverk for all overføring av personopplysninger mellom stater og selskaper underlagt denne. Virksomheten slipper dermed å inngå nye avtaler hver gang personopplysninger skal overføres, og Datatilsynet behøver ikke å varsles. Det er samtidig verdt å nevne at den ikke gjelder for overføringer til selskaper utenfor konsernet eller BCR-strukturen, og i slike tilfeller må det fortsatt inngås alminnelige databehandleravtaler og/eller overføringsavtaler.

BCR som instrument pålegger avtalerettslige forpliktelser for etterlevelse av personvernregelverket mellom de samarbeidende selskapene, harmoniserer praksisen og gjør det enklere å kommunisere utad hvordan personopplysninger behandles innen konsernet. En BCR kan sees på som en etterlevelsesmekanisme for konsern, og er et konsept som har vist seg å passe godt med det faktiske behovet til slike virksomheter.

Ved å være underlagt en BCR har hvert enkelt selskap gitt en rettslig garanti for behandlingen av personopplysninger, det er derfor ikke behov for en overføringsavtale eller en omfattende databehandleravtale for hvert enkelt tilfelle.

Krav til konserninterne rutiner

Artikkel 29-gruppen, EUs ekspertgruppe og rådgivende organ for personvern, har tidligere utarbeidet retningslinjer for hva en BCR må inneholde. Reglene om BCR som nå er kodifisert, er enklere enn den prosessen og de vilkårene som Artikkel 29-gruppen opprinnelig la opp til. Noen forskjeller fra tidligere regime omfatter forenkling av rapporteringsrutiner, og prosessen med tilsynsmyndighetene. Noen av kravene er utvidet, det gjelder først og fremst omfanget av de sentrale personvernprinsippene, hvor virksomhetene aktivt må beskrive hvordan disse prinsippene etterleves. Dette er dog prinsipper som må oppfylles uansett, all den tid virksomheten behandler personopplysninger og ikke er betinget av BCR. Dette gjelder

eksempelvis «privacy by design» (innebygget personvern).

Ny personvernforordning viser til tre nødvendige vilkår som må være oppfylt i BCR-avtalen:

- For det første må BCR-en være rettslig bindende for alle som omfattes av avtalen.
- For det andre må den gi registrerte rettigheter som kan håndheves.
- Som et tredje vilkår oppstilles krav om at en rekke forhold inntas i BCR, for felles etterlevelse og håndheving av alle parter. Det inkluderer blant annet en oversikt over struktur i selskapene (gruppen), overføringer mellom partene, ansvarsplasseringer, klageprosedyrer, og interne rutiner som krav til opplæring av ansatte.

Listen over forhold som må med er omfattende, noe som også er viktig for å gi et godt personvern innenfor gruppen som omfattes av ordningen.

En BCR må dermed skreddersys til det enkelte konsernet. Å starte prosessen med en BCR innebærer at selskapene må gjøre en full kartleggingsprosess over dataene som er samlet inn, hvordan de behandles og hva som er behandlingsgrunnlaget. Videre må selskapene ha både tekniske og organisatoriske tiltak på plass, og BCR er ment å gjøre slike tiltak og rutiner rettslig bindende.

Forenkler en tung prosess

Å få godkjent en BCR har vært en tidkrevende prosess. Etter som flere og flere konsern i Europa – og Norge – har søkt og fått godkjent slike konserninterne rutiner for virksomheten, har dette endret seg. Tilsynsmyndighetene i Europa har fått mer erfaring og kompetanse på området, og godkjenning av BCR skal gå raskere.

Virksomheter som har implementert BCR under et tidligere regime, behøver ikke å få ny godkjennelse av eksisterende BCR. Eksisterende konserninterne regler fortsetter å gjelde frem til de endres, oppdateres eller oppheves. Virksomheter må for øvrig tilpasse sin organisasjon til de oppdaterte kravene som følger av GDPR, slik at en allerede inngått BCR ikke blir en hvilepute for virksomheter i møte med nytt regelverk.

Behandlingsansvarlig får ved nytt personvernregelverk et større ansvar for databehandlere som benyttes og for de som behandler virksomhetens personopplysninger. I henhold til ansvarsreglene i forordningen vil behandlingsansvarlig enklere kunne holdes ansvarlig også for brudd på personvernregelverket hos en databehandler. Det vil naturlig nok også gjelde mellom selskaper i samme konsern. Ved implementering av BCR vil virksomheten bedre kunne sikre seg, ved at også samarbeidsparter behandler personopplysninger på en tilfredsstillende måte og at personvernregelverket følges.

BCR vil imidlertid først og fremst forenkle flyten av personopplysninger innenfor gruppen. Det eliminerer behovet for en-til-en avtaler, som trengs ved overføring av personopplysninger innenfor samme konsern.

Konseptet med bindende konsernregler er en praktisk ordning for større aktører. For selskaper i et konsern eller som regelmessig overfører personopplysninger til andre virksomheter, mener vi BCR er det eneste reelle alternativet.