GDPR er fem år:
Slik får du kontroll på databehandleravtalene dine

Det er fem år siden GDPR trådte i kraft og de fleste virksomhetene tilpasset seg regelverket slik det var den gangen. Utviklingen på personvernområdet har imidlertid ikke stått stille siden 2018 og for mange er det på tide med en gjennomgang av rutiner for behandling av personopplysninger og av tidligere inngåtte avtaler.

Advokat
Arnt Olav Aardal
Partner BDO Advokater

Advokatfullmektig
Nichlas Gundelach Ødegaard
BDO Advokater

Da GDPR trådte i kraft, fikk veldig mange virksomheter med stor sannsynlighet et endret perspektiv på behandling av personopplysninger. Personvernet fikk en ny vår og regelverket krevde at virksomhetene la ned en innsats. Det ble forhåpentligvis laget en behandlingsprotokoll og det ble inngått en hel del databehandleravtaler, ikke nødvendigvis fordi virksomhetene selv forstod helt hvorfor, men fordi GDPR krevde det. Kanskje hadde deres virksomhet et større internprosjekt, kanskje ble det innleid konsulenter eller advokater for å få drahjelp i veien mot etterlevelse. Siden den gang har personvernet kanskje blitt liggende i en digital skuff og ikke vært viet noe særlig oppmerksomhet?

Prinsippene for GDPR var i de fleste sammenhengene de samme som etter den gamle personopplysningsloven, men enkeltkravene virket strengere og vanskelig å få tak på for mange. Utviklingen på personvernområdet har imidlertid ikke stått stille siden 2018. Det er på høy tid at du igjen finner frem arbeidshanskene.

Foruten at Datatilsynet strammer til skruen og øker antall overtredelsesgebyrer, handler det jo i bunn og grunn om at virksomheten overlater verdier – i form av virksomhetens personopplysninger og annen bedriftskritisk informasjon – til en tredjepart. Det er derfor fornuftig å sette en fot i bakken for å vurdere om de faktisk behandler dette trygt. Ja, du bør kanskje til og med sjekke om de er kontraktsmessig forpliktet til å behandle opplysningene på måten du forventer. Under følger noen tanker om hvor virksomheter bør starte og hvorfor.

Databehandleravtalen (DBA)

Databehandleravtaler er særavtaler med en viss kompleksitet og for mange et noe uangripelig innhold. Avtalen skal regulere og sette rammer for behandlingen av personopplysningene til de registrerte, samt ansvarsfordelingen mellom databehandler og behandlingsansvarlig. Mange av avtalene som ble inngått rundt 2018 var/er umodne og hadde stort sett som formål å etterleve minimumsplikter, ikke nødvendigvis god ivaretakelse av de registrertes rettigheter. I et så dynamisk rettsområde som personvern, kan det bety at deler av avtalene hos deg, eller virksomhetene du bistår, er utdaterte og i enkelte tilfeller ugyldige.

Avtalen kan muligens oppfylle minimumskravene i GDPR artikkel 28 (3), men det fjerner på ingen måte risikoen for at databehandleravtalens innhold kan medføre eller utgjøre brudd på andre risikobaserte krav i forordningen.

16. juli 2020 kom også Schrems II-dommen og endret rettstilstanden knyttet til overføring av personopplysninger til USA. Hvis virksomheten har databehandleravtaler som er inngått før denne datoen, er det derfor stor sannsynlighet for at disse avtalene henviser til ugyldige overføringsgrunnlag – og at virksomheten overfører personopplysninger uten rettslig grunnlag for det. Gå inn i en tilfeldig databehandleravtale og gjennomfør: CTRL+F søk deretter «Privacy shield». Fikk du treff? Da foreligger det et problem med overføringer av personopplysningene. Privacy Shield er som kjent ikke lenger gyldig som overføringsgrunnlag til USA.

Mange problemer å ta tak i

Det finnes ingen smørbrødliste for å gjennomføre en kontraktgjennomgang, ei heller for databehandleravtaler.

GDPR artikkel 28 tredje ledd oppstiller minimumskravene, men gir minimalt med veiledning på risikoområder og om hvordan de registrertes rettigheter og egne forpliktelser i databehandleravtalene skal ivaretas på en god måte. I det følgende kommer noen av de risikomomentene og problemene vi ofte stilles overfor i gjennomgangen av databehandleravtaler.

Utviklingen på personvernområdet har ikke stått stille siden 2018 og det er på høy tid at du igjen finner frem arbeidshanskene.

Hva er det egentlig som skal behandles?

Mange databehandleravtaler legger ikke til rette for god nok informasjonsutveksling rundt den faktiske behandlingen av personopplysninger. Det kan med andre ord skli litt ut hvilke opplysninger som behandles og på hvilken måte. Det kan være store sprik mellom hva databehandleravtalen gir adgang til og hva som blir det faktiske resultatet av behandlingene av personopplysningene. Dersom det behandles personopplysninger på annen måte enn det som er forutsatt i databehandleravtalen, er ikke bare behandlingen i strid med avtalen, den er også i strid med GDPR.

Det er derfor sentralt at avtalene regulerer hva databehandleroppdraget faktisk går ut på. Generelle termer som at databehandleroppdraget går ut på å «oppfylle et oppdrag» kommer verken databehandler eller behandlingsansvarlig til gode – den setter ikke klare nok rammer for behandlingen. Behandlingsansvarlig bør derfor etterstrebe å beskrive behandlingen og sette klare rammer for behandlingen, arten og formålet med behandlingen.

Behandlingsansvarlig bør videre ta sikte på å skrive instrukser som setter klare rammer for behandlingen, men hvor detaljert dette skal gjøres, må vurderes ut fra kompleksiteten i behandlingen. Eksempelvis bør det uttømmende behandles hvilke kategorier av registrerte som omfattes og hva slags personopplysninger som behandles. Eksempler på kategorier av registrerte er kunder, ansatte, medlemmer osv. Eksempler på type personopplysninger er fødselsdato, kundenummer, navn, telefonnummer osv. Både kategoriene og typene personopplysninger som kan behandles i databehandleroppdraget, bør reguleres mest mulig uttømmende i avtalen.

Kontroll i leverandørkjeden?

Vi ser at det i flere av avtalene vi kommer over er mangel på gode mekanismer for ivaretakelsen av kontroll på underdatabehandlere og endringer i leverandørkjeden hos databehandler. Ikke sjeldent foreligger det varslingsfrister om endringer i leverandørkjeden og underdatabehandlere som ikke er holdbare og som utgjør stor risiko for behandlingsansvarlig. Fristene er ofte så korte for godkjennelse av endringer at behandlingsansvarlige ikke har tilstrekkelig tid til å undersøke den nye underdatabehandleren. Enkelte avtaler nøyer seg også med varslingsmekanismer som at det er tilstrekkelig for databehandleren å oppdatere listen over leverandører på sin hjemmeside. Det gjør det svært vanskelig for behandlingsansvarlig å følge med på. I dagens sikkerhetspolitiske situasjon er det svært uheldig dersom det plutselig skulle vise seg at din virksomhet overfører personopplysninger til eksempelvis Kina og Russland gjennom dine databehandlere. Denne manglende oversikten sammen med upresise beskrivelser av behandlingen medfører stor risiko for både de registrerte og behandlingsansvarlig.

Ivaretakelsen av de registrertes rettigheter

Den behandlingsansvarlige har etter forordningen en plikt til å legge til rette for at den registrerte får utøvd sine rettigheter. Sentrale rettigheter som gjerne kan settes på spissen i en databehandlerrelasjon, er retten til innsyn, retting, sletting og innsigelsesretten (forordningens kapittel 3). I mange tilfeller vil det imidlertid være mer naturlig for den registrerte å henvende seg til databehandleren i stedet for behandlingsansvarlige. Siden det er den behandlingsansvarlige som er ansvarlig for ivaretakelse av de registrertes rettigheter, er det viktig at databehandleren ikke tar egne avgjørelser når de mottar henvendelser fra de registrerte. Dette kan føre til at det ikke blir gitt innsyn der hvor dette er pålagt, eller at det blir gitt innsyn i flere opplysninger enn den registrerte har krav på å få innsyn i. Det kan også medføre at databehandleren sletter personopplysninger som ikke skulle vært slettet, eller at henvendelsen fra den registrerte ikke blir besvart innen den lovpålagte fristen. I noen tilfeller kan databehandlers arbeid med henvendelser fra den registrerte også medføre uventede kostnader for den behandlingsansvarlige, eksempelvis hvis databehandleren har brukt mye tid/ressurser på sletting av personopplysninger

og fakturerer behandlingsansvarlig for dette arbeidet.

Databehandleren kan altså ikke på eget initiativ ta avgjørelsen på vegne av behandlingsansvarlig ved krav om retting, sletting, innsyn etc. Databehandleravtalen bør derfor regulere klare ansvarsfordelinger og krav til fremgangsmåte ved mottakelse av henvendelser fra de registrerte. Det er lurt at dette spesifiseres i avtaleverket. Dette kan eksempelvis være krav til antall ressurser, hvilke ressurser, hvilke kostnadsrammer, og til hvilke frister.

Krav til sikkerhetsinnstillinger – lavthengende frukt

Like viktig som at du må ha adgang og mulighet til å kontrollere at databehandleren oppfyller sine forpliktelser, bør du også sørge for at sikkerhetsinnstillingene ivaretar informasjonssikkerheten både hos deg og hos databehandler. I den forbindelse er det greit å bite seg merke i at det ikke nødvendigvis alltid er slik at standardkonfigurering er sikkert.

Vi har gang på gang sett eksempler på at organisasjoner lar sikkerhetsinnstillingene stå på systemenes standardinnstillinger med forventning om at bruk av standardinnstillinger er synonymt med god sikkerhet, noe som ofte ikke er tilfellet. Det kan eksempelvis gjelde overgang fra lokal filserver til Microsoft OneDrive, eller overgang fra lokal Active Directory-instans til Microsoft Azure Active Directory.

SharePoint Online er en skybasert tjeneste som stadig flere organisasjoner tar i bruk. Et konkret eksempel på en standardinnstilling som kan gå på bekostning av sikkerheten, er muligheten for ekstern deling av dokumenter. Standardinnstillingen er satt til at informasjon kan deles med alle, også til mottakere som ikke krever innlogging. En slik innstilling vil ofte kunne medføre at en organisasjon blir unødvendig sårbar for uautorisert tilgang til sensitiv informasjon, herunder personopplysninger.

Et annet eksempel er muligheten for gjestebrukere i Microsoft 365 til å invitere nye gjestebrukere, uten krav om godkjennelse fra virksomheten først, som gjør en virksomhet unødvendig sårbar overfor mangelfull tilgangsstyring. Dette er bare noen problematiske eksempler som kan gå hardt utover personvernet til de registrerte.

Inneholder databehandleravtalene dine krav til sikkerheten hos databehandler?

What to do?

Nedenfor følger fem praktiske tips til deg som kjente det knyte seg litt i magen når du innså at ovennevnte virket litt gresk, eller kom på at din virksomhet har en del databehandleravtaler som du ikke har sett på siden 2018. Særlig før man går løs på punktene 2-5 er det viktig å gjøre en reell vurdering av om det faktisk foreligger en databehandlerrelasjon som krever en databehandleravtale. Det er nemlig ikke automatikk i at enhver form for behandling av personopplysninger mellom to virksomheter utgjør en databehandlerrelasjon som krever databehandleravtale. Eksempelvis vil en revisor stort sett alltid opptre som behandlingsansvarlig, selv om vedkommende betales av en annen virksomhet og behandler personopplysninger «på vegne av» virksomheten. Da kreves det ikke databehandleravtale.

1. Få oversikt.

Dersom virksomheten ikke har på plass et avtaleregister som gir fullstendig oversikt over databehandleravtalene i virksomheten, er det vanskelig å ivareta de registrertes rettigheter. Dersom det finnes et ordinært avtaleregister, kan dette brukes som utgangspunkt når det skal lages register over databehandleravtalene. Virksomheten bør også bruke behandlingsprotokollen som utgangspunkt, for her skal strengt tatt all behandling av personopplysninger komme frem. Dersom hovedavtalen innebærer at en av partene behandler personopplysninger på vegne av den andre – må det som hovedregel foreligge en databehandleravtale, jf. GDPR art. 28 tredje ledd. Dersom du ikke får treff på en databehandleravtale i dette tilfellet, må det altså inngås en avtale.

Når man først er i gang med å skaffe oversikt over hvilke databehandleravtaler og behandlingsrelasjoner som foreligger i virksomheten, anbefaler vi å bruke anledningen til å oppdatere behandlingsprotokollen. Behandlingsprotokollen og deler av databehandleravtalens innhold skal på lang vei samsvare, slik at en slik søken etter oversikt vil kunne gjøre underverker for virksomhetens kontroll med behandlingen av personopplysninger. Hva slags opplysninger deles, hvilket rettslig grunnlag finnes for delingen? Er denne delingen egentlig nødvendig for å oppfylle formålet med avtalen? Det må man ha kontroll på.

2. Gyldighetskontroll

Databehandleravtalene må være gyldige. Minimumskravene fremgår eksplisitt av forordningens artikkel 28 og det er ingen grunn til at avtalen ikke skal oppfylle de kravene som fremgår. For gjennomføringen av gyldighetskontrollen er det en klar anbefaling å ha på plass en sjekkliste for å være sikker på at det blir en strukturert gjennomgang. Dersom man ikke har den juridiske kompetansen til å gjennomføre gyldighetskontrollen, bør dette settes bort til et advokatfirma eller noen med juridisk kompetanse.

3. Risikokontroll

Gyldighetskontrollen kan helt fint vise at samtlige av de avtalene virksomheten er bundet av er gyldige etter artikkel 28, men det er ikke ensbetydende med at avtalene er gode eller ivaretar samtlige av virksomhetens forpliktelser etter forordningen. Artikkel 28 er ikke risikobasert og er i så måte bare uttrykk for minimumskrav. Det medfører at virksomheten må gjøre en kartlegging av avtalens risiko – både kontraktrisiko og personvernrisiko. Hvilken risiko som kan godtas eller ikke, vil som alltid komme an på hvilke typer personopplysninger som behandles og omfanget av behandlingen. Virksomheten bør også ha gjort noen klare valg rundt

hvilke risikoer som kan godtas og hvilke som ikke kan godtas. Et tips her er å gradere risikoene, enten i trafikklys, eller 1-3 graderinger. Da kan dere ta utgangspunkt i de største risikoene først.

4. Dialog

I etterkant av gyldighetskontrollen og risikokontrollen står man med en viss sannsynlighet igjen med en del uavklarte spørsmål, og muligens noen risikoelementer som det bør gjøres noe med. Gå i dialog med leverandøren angående de punktene som er uakseptable, uavklarte eller som ønskes endret. Det er i begge parters, samt den registrertes interesse, at databehandleravtalen ivaretar de registrertes rettigheter på en god måte. Dersom avtalen dateres tilbake til rundt 2018, kan det være gode grunner til å foreslå å inngå en ny avtale, ettersom det har skjedd mye på personvernområdet de siste årene.

5. Fortsett oppfølgingen

GDPR og personvern er i rivende utvikling og er et særlig dynamisk rettsområde. Det medfører at problemstillinger som ikke var viet særlig plass ved forrige kontroll, kan være særlig aktuelle nå. Det anbefales derfor at revisjon av avtalene og leverandørene innlemmes i et årshjul eller liknende og følges opp minimum årlig. Et annet forslag er å innlemme rapporteringskrav til databehandleren – det kan være årlige, eller kvartalsvise. Rapporteringen kan gjerne komme fra virksomheten selv, eller gjennom en tredjepartsuttalelse. Hold databehandlerne ansvarlige for kontraktens innhold – opprettholder de kravene til sikkerhet? Har de nye underleverandører som ikke følger av avtalen eller er godkjent? Har de fulgt slettefristene?

Certificate of Origin og ikke-preferensielle opprinnelsesregler

Stadig flere norske selskaper møter krav om å fremlegge Certificate of Origin når de eksporterer varer til land vi ikke har en handelsavtale med. Dette sertifikatet gir ingen rett til nedsatt preferensiell tollsats, men benyttes som et opprinnelsesbevis i forbindelse med blant annet lisens- og veterinærbestemmelser, kvoter, opprinnelsesmerking og handelsstatistikk.

Tollrådgiver
Helene Øien Hval
Senior Manager, BDO Advokater

Spesielt ved eksport til asiatiske land har vi sett et stort oppsving i at importør ber eksportør eller produsent i Norge fremlegge et Certificate of Origin (CoO) sammen med varene. Dette er et opprinnelsesbevis som brukes for varer med det som kalles ikke-preferensiell opprinnelse. Det betyr at varen ikke har opprinnelse etter en handelsavtale som gir en nedsatt preferensiell tollsats, men likevel kan dokumentere en opprinnelse, for eksempel i Norge.

Ordningen

I tilfeller der Norge ikke har fremforhandlet frihandelsavtaler, har vi gjennom WTO- og GATT-avtalen bundet oss til å innrømme land som eksporterer varer til Norge en MFN-tollsats. MFN står for «Most-Favoured Nation Treatment» (også kalt bestevilkårskravet) og betyr at alle andre land enn de vi har en avtale med, skal få en lik og fastsatt tollsats ved import. Norge kan for eksempel ikke velge å sette tollsatsen på vare fra ett spesifikt land høyere enn fra ett annet. Enkelt sagt bindes alle «ikke-handelspartnere» gjennom bestevilkårskravet, til å gi hverandre lik behandling innenfor alle regler knyttet til handel med varer.

De ikke-preferensielle opprinnelsesreglene benyttes i sammenheng med bestevilkårskravet, blant annet i forbindelse med MFN-tollsats, anti-dumpingtiltak, opprinnelsesmerking, offentlige innkjøp og handelsstatistikk. Disse opprinnelsesreglene er derfor som regel mer liberale enn reglene for preferansetollbehandling, og må ikke blandes sammen.

En vare kan få nasjonal opprinnelse i Norge, uten at varen har rett til preferansetollbehandling iht. frihandelsavtalene.

De ikke-preferensielle reglene har stor betydning ved utførsel til land som har krav om at CoO skal fremlegges ved import. Ved innførsel til Norge kreves normalt ikke dokumentasjon for ikke-preferensiell opprinnelse.