Delphi

Digitalisering i spåren av Covid-19

Agne Lindberg / Partner / Advokat & **Adam Odmark** / Associate

Digitalisering i spåren av Covid-19

Agne Lindberg / Partner / Advokat & **Adam Odmark** / Associate

Det är mycket fokus på krishantering i Covid-19:s spår, med regeringens olika stödpaket och Corona-virusets direkta juridiska effekter på avtal, anställningsförhållandet, m.m. Det finns givetvis ett liv efter Corona-viruset och alla verksamheter har redan börjat eller kommer snart att fokusera på att komma ur krisen och försöka återgå till en så normal verksamhet som möjligt. Frågan är vad som kommer att vara ”normalt”. Vi tror att övergången till en ”efterkristid” kommer präglas mycket av digitalisering. Digitaliseringen har gjort ett stort språng på grund av Covid-19 med en global begräsning i resor och möten. Därför kommer vi i en serie om tre artiklar på detta tema lyfta fram vad vi tycker är särskilt intressant och viktigt att tänka på i digitaliseringsarbetet. Även i en kristid är det viktigt att göra rätt. Artiklarna kommer ha rubrikerna ”Digitalisering och informationssäkerhet – den rättsliga kartan”, ”Juridiska aspekter och krav på digitalisering – den regulatoriska labyrinten”, samt ”Digitaliseringsavtalet”. Redan i denna artikel ger vi dock en sammanfattande överblick av de viktigaste sakerna att tänka på i digitaliseringsarbetet. Vi har även tagit fram en artikel och genomfört ett webinar om de nya e-handelsreglerna.

Vad är digitalisering?

Digitalisering har blivit något av ett luddigt begrepp vars betydelse olika personer har olika uppfattningar om. Vi vill därför börja med att förtydliga vad vi avser när vi använder det. I vår artikelserie syftar vi på ordet i en bredare bemärkelse. Någon exakt definition är svårt att ge men vi syftar i synnerhet på följande situationer: när en organisation går från analog till digital hantering av något, en generellt ökad användning av digital teknik i samhället, utveckling av ny digital teknik samt verksamhetsförändringar med användning av digital teknik. Typiskt sett handlar det om förändringsarbete såsom att flytta ut funktioner och processer till molnet, att använda olika former av AI som besluts- och verksamhetsstöd samt att utföra olika arbetsuppgifter online.

Digitalisering under och efter krisen

Corona krisen har än så länge mest av nödvändighet lett till en accelererad digitalisering, inte minst beroende på rese- och mötesrestriktioner. Det märks t.ex. på alla som arbetar på distans med hjälp av digitala verktyg. Mycket talar enligt dock enligt oss för att detta storskaliga experiment kommer att få bestående effekter. Acceptansen och viljan att ta till sig nya innovativa verktyg ökar t.ex. i takt med att medarbetare tvingas lära sig hur de fungerar. Arbetsgivare kommer sannolikt även se fördelar med att låta medarbetare fortsätta arbeta hemifrån i högre grad. Det kan i sin tur leda till behov av nya verktyg för mer permanent bruk. Många konsumenter har även ändrat sina konsumtionsvanor. Färre handlar i fysiska butiker men vissa näthandelsbutiker har rent utav sett en kraftigt ökad omsättning. Även detta en effekt som i viss mån lär bestå.

I spåren av finanskrisen 2008 såg vi en kraftig ökning i outsourcingsärenden då inte minst verksamheter inom bank, finans och försäkring la ut stora delar av IT-verksamheten till externa leverantörer och ofta med leveranser från länder med lägre kostnadsläge. Sedan dess har IT-avdelningarna åter vuxit på många håll i landet. Beroende på hur långvarig och djup krisen blir är det inte omöjligt att företag så småningom åter känner sig lockade att outsourca delar av verksamheten till andra länder. Säkerhetsaspekter kan också leda till att företag väljer att flytta tillbaka tjänster till Sverige eller EU. Mycket har dock hänt sedan 2008. Det är möjligt att den tekniska utvecklingen som varit kommer leda till att effektivingar och besparingar genomförs på ett nytt sätt som snarare driver innovation. Kundservice är ett exempel på ett område som redan idag i viss mån har tagits över av verktyg som i varierande grad skulle kunna benämnas som artificiella intelligenser (AI). Det finns säkerligen stor potential för AI att ta över även andra arbetsuppgifter och processer som idag står för stora kostnader. Kanske blir Covid-19 AI:s stora genombrott.

Juridiska aspekter och krav på digitalisering – den regulatoriska labyrinten

Det första regelverk många inser att man måste beakta i digitaliseringsarbetet är förmodligen dataskyddsförordningen (GDPR). Hur omfattande den regulatoriska bördan är varierar beroende på vem man är men det finns långt många flera lagar och regler att beakta än GDPR. I den kommande artikeln på detta tema kommer vi därför guida er igenom några av de viktigaste regelverken att tänka på i digitaliseringsarbetet.

För att inte göra någon besviken vill vi förvarna om att just denna artikel inte kommer innehålla något om skatterätt, konsumenträtt, e-handelsrätt, lagen om offentlig upphandling (LOU) eller lagen om elektronisk kommunikation (LEK). Det sistnämnda med undantag för cookie-regleringen som tills vidare återfinns i LEK.

IT-Säkerhet, informationsskydd och dataskydd

Att skydda IT-lösningar och information är förstås något som är i fokus hos alla men det finns även lagar och regler som ställer krav på säkerhet och ett systematiskt säkerhetsarbete. Vi tänker i synnerhet på förordning 2016/679 (GDPR), direktiv 2016/1148 (NIS-direktivet) och förordning 2019/881 (Cybersecurity Act) – samtliga beslutade om på EU-nivå.

Som kund kan man inte outsourca ansvaret för efterlevnaden av alla dessa krav. De egna medarbetarna måste därför utbildas i regelverken. Det är likväl mycket viktigt att ställa krav på leverantören i dessa avseenden i samband med IT-upphandlingar – något som vi kommer återkomma till i artikeln om digitaliseringsavtalet.

GDPR

GDPR-efterlevnad är numer något självklart för de allra flesta i samband med en IT-upphandling. Det tål dock att påminnas om att det inte räcker med en pappersexercis för att bocka av regelverkets krav. Personuppgiftsbiträdesavtal och dylika dokument är självklart viktigt men man måste t.ex. även bedöma om och tillförsäkra att det finns en säkerhetsnivå som är proportionerlig i förhållande till den tilltänka personuppgiftsbehandlingen. Privacy by design innebär krav på ”inbyggd integritet” – d.v.s. planering och utveckling av IT-system måste genomföras med beaktande av de grundläggande principer för personuppgiftsbehandling som anges i artikel 5 i GDPR (bl.a. uppgiftsminimering, behörighetskontroll, standardinställningar för lagring och radering). Det och mycket mer kommer vi att behandla i den kommande artikeln.

NIS-direktivet

Syftet med NIS-direktivet är att säkerställa en god skyddsnivå för samhällskritisk infrastruktur genom att ställa krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster inom såväl privat som offentlig sektor. De typer av tjänster som omfattas av regelverket är indelade i följande sektorer: energi, transporter,

Advokatfirman Delphi www.delphi.se

bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Förutom att uppfylla säkerhetskrav ska de som omfattas av regelverket göra en anmälan till Myndigheten för samhällsskydd och beredskap (MSB) och om en säkerhetsincident inträffar ska även det anmälas till MSB.

Cybersecurity Act

Under 2019 trädde Cybersecurity Act ikraft (en EU-förordning). Genom förordningen har det inrättats ett omfattande system för certifiering av produkter, processer och tjänster för att säkerställa att de uppfyller gällande standarder för cybersäkerhet. Certifieringen är inledningsvis frivillig men ska bli obligatorisk i EU för särskilt viktiga produkter och aktiviteter. Själva certifieringarna är under utveckling.

Börsregler

Nasdaqs vägledning för intern styrning och kontroll i noterade bolag är högst relevant i sammanhanget. Den innehåller en kravbild för att bolag som är noterade ska ha en god intern styrning och kontroll. Vägledningen ställer bl.a. krav på att det ska finnas interna styrdokument för IT- och informationssäkerhet. Det finns även regler för outsourcad verksamhet, som även kan omfatta användningen av molntjänster. Det ställs krav på att det noterade bolaget ska säkerställa att leverantören upprätthåller intern kontroll för de tjänster som levereras och att avtalet mellan parterna ska reglera den interna kontrollen.

Cookies

Det är inte bara webbsidor som kan placera cookies på slutanvändarnas enheter. Många applikationer placerar ut cookies för alltifrån statistiska ändamål till att kunna bygga en profil om den enskilda användaren och presentera specialanpassat innehåll. I dagsläget återfinns regleringen om cookies i LEK men det pågår sedan många år nu ett arbete inom EU med att ta fram en ny e-Privacy-förordning som kommer ersätta den befintliga regleringen. e-Privacy-förordningen kommer innebära att brott mot cookies-regleringen kan leda till administrativa böter motsvarande de som gäller enligt GDPR, d.v.s. upp till det högsta av 4 % av den globala omsättningen och 20 MEUR. Även om den nya förordningen för närvarande tycks avlägsen (arbetet inom EU går mycket trögt) är dess grundläggande principer kända redan nu. Det finns därför möjlighet att bespara sig mycket av framtida huvudverk genom att tänka till redan nu.

Efterlevnad av det immaterialrättsliga regelverket

Det finns en mängd immaterialrättsliga aspekter att tänka på i digitaliseringsarbetet. Den förmodligen viktigaste är att säkerställa att IT-upphandlingen leder till att ni erhåller tillräckliga rättigheter för att ni ska kunna göra vad ni har tänkt er. På detta område kommer inte minst open source (OS) in i bilden. Det är viktigt att noggrant beakta vilka licensvillkor som gäller för den OS-programvara som ni tänkt använda er av och säkerställa att ni efterlever licensvillkoren. Brister i detta arbete kan i värsta fall leda till en talan om intrång i någon annans immateriella rättigheter eller att någon använder hot om en sådan talan som påtryckningsmedel för att ni ska träffa ett dyrbart licensavtal på kommersiella villkor.

Allmänna handlingar och OSL

Verksamheter som omfattas av offentlighetsprincipen måste i digitaliseringsarbetet beakta delvis svårtolkade krav i bland annat offentlighets- och sekretesslagen (OSL) och arkivlagen. Allmänhetens möjlighet att ta del av allmänna handlingar får t.ex. inte äventyras genom att myndigheten väljer att byta ut ett IT-system eller att digitalisera ett tidigare analogt arkiv och sekretesskyddade uppgifter får inte röjas i strid med OSL.

Att efterleva arkivlagen är i princip ett praktiskt problem som hanteras genom tekniska lösningar. Att undvika att röja uppgifter i strid med OSL är mer juridiskt komplicerat. OSL förutsätter att en bedömning i flera led görs innan sekretesskyddade uppgifter riskerar att röjas till följd av att t.ex. en ny digital lösning tas i bruk.

När vi fördjupar oss i denna för offentlig sektor centrala fråga kommer vi även behandla frågan om den amerikanska CLOUD Act-lagstiftningen och röjande-begreppet. CLOUD Act innebär i korthet att brottsbekämpande myndigheter i USA under vissa bestämda förutsättningar har rätt att kräva tillgång till data som vissa leverantörer av bl.a. molntjänster har tillgång till, oavsett vem som ”äger” datan och utan geografiska begränsningar.

”Röjande-begreppet” är ett centralt begrepp i OSL. Trots detta finns det inte någon definition av begreppet i OSL, förarbetena är mycket gamla och innehåller knappt något av värde idag och rättspraxis är även den gammal och skral. Allt detta har banat väg för det stora genomslag som eSams uttalande om röjande-begreppet från 2018 fått (eSam är ett program för samverkan kring digitalisering mellan Sveriges kommuner och regioner (SKR) och ett flertal statliga myndigheter). Den centrala delen av uttalandet lyder:

”Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående.”

Efter att ha fått utstå kritik följdes uttalandet under 2019 upp med något mer utförlig argumentation i en vägledning om sekretess och persondataskydd i samband med outsourcing. eSams slutsats förblev dock densamma.

Vår uppfattning är att eSams bedömning är tveksam. Sekretessreglerade uppgifter röjs inte med automatik till amerikanska myndigheter genom att de görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats. Vi kommer att fördjupa oss i detta ämne i den kommande artikeln men redan nu finns två artiklar om CLOUD Act, OSL och röjande-begreppet att läsa här (CLOUD Act och röjande-begreppet enligt OSL) och här (Replik på eSams uttalanden om ”röjande-begreppet” enligt OSL).

Branschspecifika regulatoriska krav

För aktörer som agerar på en reglerad marknad som t.ex. försäkringsbolag, banker kreditinstitut, värdepappersföretag, betalningsinstitut m.fl. finns branschspecifika regler riktlinjer att bakat i digitaliseringsarbetet. Reglerna träffar inte alla köp av digitala tjänster och produkter men den står under Finansinspektionens tillsyn behöver alltid ha dem i åtanke.

I denna del av den kommande artikeln kommer vi bl.a. att fördjupa oss i den europeiska bankmyndigheten (EBA):s riktlinjer för outsourcing som trädde ikraft under 2019 och Finansinspektionens föreskrifter av relevans vid outsourcing. Exempel på utmaningar som regelverken innebär är bland annat:

- Strikta krav på innehållet i outsourcingavtalet
- Krav på att göra en risk- och sårbarhetsanalys (pre-outsourcing analysis) före outsourcing
- Krav på att föra ett register över samtliga outsourcingavtal

EBA:s riktlinjer från 2019 ställer även krav på genomgång av befintliga outsourcingavtal för att säkerställa att de uppfyller de nya riktlinjerna.

För försäkringsverksamheter har den europeiska försäkringsmyndigheten – EIOPA – i februari 2020 tagit fram riktlinjer för outsourcing till molntjänstleverantörer. Även detta regelverk reglerar krav på innehåll i avtalet, dokumentationskrav och regler kring riskbedömning både av tjänst och leverantör. Det finns även långtgående krav på revisionsrättigheter för kunden.

Artificiell intelligens (AI)

Det finns visserligen inga bindande regler som specifikt träffar organisationer som utvecklar eller använder sig av teknik som kan betraktas som AI. De regler som vi behandlat ovan omfattar dock även AI och ger då upphov till unika och svåra tillämpningsfrågor. Vem bestämmer ändamål och medel (och är därmed personuppgiftsansvarig) för personuppgifter som en AI på eget initiativ väljer att behandla? Vem ansvarar för skador som AI:n orsakar? Vem äger rättigheterna till produkter som skapats av en artificiell intelligens? Vilket skydd finns för den data som en AI behöver för att kunna tränas och den data som träningen ger upphov till? Detta är exempel på frågor som vi kommer att behandla i den kommande artikeln om AI.

Digitaliseringsavtalet

Det finns många anledningar till att lägga krut på att få

till ett bra avtal. Ett bra avtal hjälper er att se till att ni får det ni vill ha och att kostnaderna inte skenar. Det hjälper er även att säkerställa efterlevnad med de regulatoriska krav som omfattar er verksamhet. Ett dåligt avtal kan å andra sidan leda till att hela digitaliseringsprojektet havererar och får läggas ned. Ofta utan möjlighet att få tillbaka några pengar från leverantören. När haverier sker i offentlig sektor får vi ofta höra talas om det om det gäller tillräckligt mycket pengar. Under de senaste åren har vi sett flera exempel på det (utan att nämna några utsatta vid namn). När haverier sker i den privata sektorn får allmänheten sällan höra talas om det men det sker och kostar precis lika mycket pengar där.

Ibland kan vissa avtal knappt vänta med att tecknas för att verksamheten ska kunna fortsätta i dessa tider. Det får man ha förståelse för även om det självklart innebär ett risktagande i sig. Erfarenheten från tidigare kriser är dock att akuta åtgärder ofta blir permanenta. Vi vill därför slå ett slag för att göra avtalet ordentligt även om det är bråttom.

Leveransavtalet och tjänsteavtalet

Man kan förenklat säga att det finns två huvudsakliga typer av IT-avtal: leveransavtal och tjänsteavtal. Vi kommer i den kommande artikeln om digitaliseringsavtalet att fördjupa oss i dessa avtalstyper, dess komponenter och vanliga fallgropar.

Leveransavtalet tar sikte på leverans av något som går att avgränsa och som har en tidpunkt för när hela eller delar av leveransen ska vara fullgjord. Man kan och behöver även mäta om den verkligen har fullgjorts. Om leverans enligt avtalet inte sker i tid föreligger en försening. Efter fullgjord leverans har leverantören typiskt sett ett felansvar. Systemleveransavtalet är ett typexempel på leveransavtal.

Tjänsteavtalet innebär att leverantören ska leverera något över en längre tid. Det finns inte heller någon tydlig avlämningspunkt utifrån vilken man kan mäta om leverans skett i tid eller inte. Leveransen mäts istället oftast med andra typer av kvalitetsmått i form av servicenivåer och key performance indicators (KPI:er). Två exempel på traditionella typer av tjänsteavtal på IT-området är drifts- och systemförvaltningsavtalet. Molntjänsteavtalet är ett mer modernt exempel och det är denna typ av tjänsteavtal som vi kommer att fördjupa oss i den kommande artikeln.

Köp av standardiserade produkter

I vissa fall finns det inte några större möjligheter att som kund påverka avtalet. Det gäller ofta vid köp av standardiserade molntjänster och programvara från stora leverantörer. Vi kommer inte fördjupa oss i det i den kommande artikeln men kan här och nu ge två konkreta tips för dessa situationer. Det ena är att kontrollera om leverantören erbjuder alternativa standardvillkor. AWS och Microsoft erbjuder t.ex. särskilda tilläggsavtal för aktörer inom den finansiella sektorn. Det andra tipset är att göra en ordentlig risk- och sårbarhetsanalys som beslutsunderlag inför köpbeslutet. Analysen bör bl.a. innefatta en kartläggning av vilka risker som avtalet ger upphov till, vad konsekvensen blir om respektive risk förverkligas, hur stor sannolikheten för det är och om det finns några åtgärder som ni kan vidta för att påverka allt detta i riskmitigerande riktning.

Kontakt:
Agne Lindberg / Partner / Advokat
agne.lindberg@delphi.se

Adam Odmark / Associate
adam.odmark@delphi.se