Dataskydd – för hållbar innovation och digitalisering

*Erica Wiking Häger och Ängla Pändel**

1. Inledning

Först och främst ett stort grattis till det svenska dataskyddet som fyller 50 år! Vi har tillsammans arbetat med dataskydd i mer än 25 år och har förmånen att på daglig basis lämna råd till företag och organisationer om hur de många gånger snåriga dataskyddsreglerna ska tillämpas i praktiken. Det är ett oerhört stimulerande och varierande arbete som ger oss möjlighet att sätta oss in i en mängd olika branschers och organisationers utmaningar rörande dataskydd.

Vi ser att det går olika trender i dataskyddsarbetet. I samband med införandet av dataskyddsförordningen år 2018 kom det naturligen att bli ett stort fokus på att kartlägga personuppgiftsbehandlingar, inrätta dataskyddsfunktioner, anta styrdokument och utbilda medarbetare. I tiden därefter har vi i omgångar sett att fokus bland annat har skiftat till personuppgiftsincidenter, tredje landsöverföringar och en ökad aktivitet i Integritetsskyddsmyndighetens tillsynsverksamhet. Den ständiga utvecklingen av dataskyddet gör att företag löpande behöver följa upp och utveckla sitt dataskyddsarbete.

Många företag har nu kommit in i en mer mogen fas och dataskyddet hanteras ofta på samma sätt som andra etablerade compliance-områden, såsom anti-korruption, konkurrensrätt och handelssanktioner. I viss utsträckning har dataskyddet kommit att uppfattas som en teknisk lagstiftning och som ibland har ett rykte om sig att vara tråkig. Enligt vår uppfattning kan inget vara mer fel. Tvärtom är användning av personuppgifter helt central för många företag, både i den dagliga verksamheten och i företagets arbete med affärsutveckling och innovation. Ett modernt och effektivt dataskyddsarbete blir därmed en förutsättning för företagets fortsatta framgång.

* Advokater, Mannheimer Swartling Advokatbyrå AB.

Vi är övertygade om att dataskyddet kommer att fortsätta att spela en central roll även de kommande 50 åren. Vi förutspår dock att arbetet med dataskydd gradvis kommer att förändras. Mycket av det grundläggande compliance-inriktade arbetet kommer sannolikt att kunna automatiseras och digitaliseras. I stället förväntar vi oss att frågor kring dataskydd kommer att vidgas och att dataskyddets ursprung i mänskliga rättigheter kommer att få en allt större betydelse.

I detta kapitel gör vi ett försök att spana in i framtiden kring frågor som vi tror kommer att bli centrala för alla jurister som arbetar med dataskydd, och då särskilt hur vissa av EU:s initiativ inom hållbarhetsområdet kommer att påverka dataskyddsarbetet.

2. Dataskyddet en hållbarhetsfråga?

2.1 Vad är hållbart företagande?

Hållbart företagande är ett begrepp som är under ständig utveckling och förändring. Det finns därför många olika sätt att beskriva vad som avses med hållbart företagande. En vanlig utgångspunkt är UN Global Compacts Tio Principer, som fastställer principer för hållbarhet inom mänskliga rättigheter, arbetsrätt, miljö och antikorruption. Principerna har sin grund i FN:s allmänna förklaring om de mänskliga rättigheterna, ILO:s deklaration om grundläggande principer och rättigheter i arbetslivet, Rio-deklarationen samt FN:s konvention mot korruption. OECD:s riktlinjer för multinationella företag och FN:s vägledande principer för företag och mänskliga rättigheter är två ytterligare internationella initiativ som syftar till att få företag att verka för hållbarhet i sin verksamhet. OECD:s riktlinjer innehåller rekommendationer om hur multinationella företag bör agera inom bland annat mänskliga rättigheter, arbetsrätt, miljö, antikorruption, konsumentskydd, skatt och affärsetik. Syftet är att främja ansvarsfullt företagande och samarbete mellan företag och samhälle för att uppnå positiva ekonomiska, sociala och miljömässiga resultat. FN:s vägledande principer för företag och mänskliga rättigheter har utvecklats av FN för att adressera den påverkan på mänskliga rättigheter som företag kan ha i sin verksamhet. Principerna betonar företagens ansvar att respektera mänskliga rättigheter och förebygga och mildra eventuell negativ påverkan. En annan viktig referenspunkt är de Globala målen för hållbar utveckling som utgör en uppsättning gemensamma mål för regeringar, myndigheter och företag världen över om hur de, fram till år 2030, behöver arbeta för att utrota fattigdom, stoppa klimatförändringar och skapa fredliga och trygga samhällen. Företag som är medlemmar i Global Compact åtar sig att tillämpa de

Tio Principerna i verksamheten och integrera dem i sina affärsstrategier och verksamhetsprocesser samt låta sig vägledas av de Globala målen i sitt hållbarhetsarbete. EU:s gröna giv, som syftar till att ställa om EU till en modern, resurseffektiv och konkurrenskraftig ekonomi, är också relevant i en beskrivning av hållbart företagande. EU:s gröna giv har lett till en våg av lagstiftningsinitiativ inom hållbarhetsområdet.

I samband med hållbart företagande förekommer ofta förkortningen ESG. ESG står för Environmental (miljö), Social (samhällsansvar), och Governance (bolagsstyrning). ESG myntades ursprungligen som ett begrepp för att hänvisa till faktorer som kunde beaktas av investerare.[1] Nu används ESG ofta som ett alternativt sätt att hänvisa till hållbarhet, där de centrala områdena för miljö, sociala frågor och bolagsstyrningsfrågor framhävs som något ett företag bör överväga när det hanterar sin påverkan på människor och planeten. Om man ser till ESG-faktorerna så aktualiseras dataskydd framför allt inom Social och Governance, det vill säga inom ”S” och ”G”. Social fokuserar i stor utsträckning på företagens skyldighet att skydda mänskliga rättigheter, medan Governance betonar betydelsen av bolagsstyrning och hållbarhetsredovisning. Dataskydd har emellertid även en koppling till miljön och ”E”-aspekten. Digitalisering och den ständigt ökande dataanvändningen ställer krav på lagring av data. Det innebär till exempel att den som upphandlar tjänster för lagring eller själv lagrar data behöver beakta vilka miljöaspekter exempelvis serverhallar kan ha.[2]

2.2 Dataskydd och mänskliga rättigheter

Iakttagandet av mänskliga rättigheter är en central del av hållbart företagande. Ett av de grundläggande syftena med dataskyddsförordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter och personlig integritet. Genom dataskyddsförordningen och skyddet för den personliga integriteten manifesteras en grundläggande respekt för de mänskliga rättigheter som slås fast i en rad internationella konventioner. De för dataskyddet och integritetsskyddet allra mest centrala mänskliga rättigheterna är:

[1] Global Compact, ”*Who Shares Wins – Connecting Financial Markets to a Changing World*” The Global Compact report, 2005, https://www.unepfi.org/fileadmin/events/2004/stocks/who_cares_wins_global_compact_2004.pdf, och Freshfields rapport.

[2] Se till exempel studien ”*Carbolytics, an analysis of the carbon costs of online tracking*”, https://carbolytics.org. Studien avser koldioxidutsläpp kopplade till uppfyllandet av lagkraven för användningen av cookies.

- Artikel 12 i FN:s allmänna förklaring om de mänskliga rättigheterna och artikel 17 i FN:s konvention om medborgerliga och politiska rättigheter, stadgar att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana angrepp.
- Artikel 8 i Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (”**EKMR**”), stadgar att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Vidare stadgas att offentlig myndighet inte får ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.
- Artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (”**EU-stadgan**”), föreskriver att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer.
- Artikel 8 i EU-stadgan tar specifikt sikte på skyddet för personuppgifter. Här anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne och att dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och få rättelse av dem. Vidare anges att en oberoende myndighet ska kontrollera att dessa regler efterlevs.

Vidare ger den svenska grundlagen alla svenska medborgare vissa grundläggande fri- och rättigheter, oavsett ålder, kön eller härstamning, i förhållande till det allmänna. Skyddet följer av 2 kap. 1 § regeringsformen och omfattar yttrandefrihet, informationsfrihet, mötesfrihet, demonstrationsfrihet, föreningsfrihet och religionsfrihet. Regeringsformen ger även ett grundlagsskydd mot åsiktsregistrering[3] och betydande intrång i den personliga integriteten från det offentliga.[4] De grundläggande fri- och rättigheterna har alla en direkt eller indirekt koppling till behandlingen av personuppgifter och begränsningar av möjligheten till sådan behandling i de fall det kan anses inskränka någon av rättigheterna.

I dataskyddsförordningen görs kopplingen till individens rättigheter i regeln om konsekvensbedömningar i artikel 35, vilken innehåller en uttrycklig referens till fysiska personers rättigheter och friheter. Av

[3] 2 kap. 3 § regeringsformen.
[4] 2 kap. 6 § 2 st. regeringsformen.

artikeln följer att ”*om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter*”. Hänvisningen till de registrerades ”rättigheter och friheter” avser i första hand dataskydd och integritet, men kan även omfatta andra grundläggande rättigheter såsom yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.[5] Även om dataskyddsförordningen främst fokuserar på skyddet av personuppgifter, måste den personuppgiftsansvarige överväga samtliga rättigheter och friheter som den registrerade omfattas av. Detta innebär att de faktorer som ska vägas in till individens fördel sträcker sig bortom rätten till skydd för personuppgifter.

Värt att notera är även att skyddet för personuppgifter och integritet inte enbart är självständiga rättigheter. De lägger också en viktig grund för andra mänskliga rättigheter. Dataskyddet bidrar exempelvis till att skydda journalister och deras arbete, människorättsförsvarare, rätten till fungerande val, rätten att få sin sak prövad i domstol och att skydda människor från diskriminering.

2.3 På vilket sätt kan bristande dataskydd få inverkan på mänskliga rättigheter?

Alla företag behandlar personuppgifter – primärt om anställda, kunder och affärskontakter. Behandlingen kan ske för många olika ändamål såsom marknadsföring, kundvård, personaladministration, rekrytering och produktutveckling. Ofta sker även behandling av personuppgifter som en integrerad del i de tjänster som företag erbjuder sina kunder. Exempel på sådana tjänster är AI-system och sociala medier, där behandling av personuppgifter är en nödvändig förutsättning för själva tjänsten.

All personuppgiftsbehandling måste så klart ske i enlighet med dataskyddsförordningen och annan tillämplig dataskyddslagstiftning. Ibland blir det emellertid fel och ett företag kan komma att – medvetet eller omedvetet – behandla personuppgifter på ett sätt som innebär en överträdelse av såväl dataskyddsförordningen som annan tillämplig dataskyddslagstiftning. Emellertid kan en felaktig behandling av person-

[5] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248, rev 0.1, sid. 7.

uppgifter även innebära en kränkning av mänskliga rättigheter. För att illustrera detta presenterar vi nedan tre fiktiva exempel.

> **Exempel 1 – Rekryteringsbolaget (ett företag vars primära verksamhet bygger på behandling av personuppgifter)**
>
> Företag A är en framstående aktör inom rekryteringsbranschen som specialiserar sig på att erbjuda avancerade AI-baserade lösningar för att effektivisera rekryteringsprocessen åt sina kunder. Företagets tjänster omfattar automatiserad CV-analys, bakgrundskontroller, förmågan att förutspå en kandidats framtida prestationer baserat på en ingående analys av kandidatens digitala fotspår samt bedömning av mätning av ansiktsuttryck i samband med intervjuer såsom entusiasm, stabilitet eller nervositet. Företag A:s AI-system har tillgång till stora mängder data från sociala medier, tidigare arbetsgivare och andra källor för att bedöma en kandidats lämplighet för en viss tjänst. Under tiden som Företag A framgångsrikt har utvecklat sina tjänster har det dykt upp frågor om hur företaget behandlar kandidaters personuppgifter.

I Exempel 1 finns risk för flera brister i Företag A:s behandling av personuppgifter. En risk är att den omfattande insamlingen av data medför att AI-systemet har tillgång till och analyserar mer information än vad som krävs för att bedöma en kandidats lämplighet. Detta strider mot principen om uppgiftsminimering i artikel 5.1(c) i dataskyddsförordningen. En annan risk är att personuppgifter som inte är direkt relevanta för en viss befattning läggs till grund för att sortera bort en kandidat. Exempel på sådan icke relevant information är personliga åsikter och intressen som kandidaten har delat online. Detta strider mot principen om ändamålsbegränsning i artikel 5.1(b) i dataskyddsförordningen. Behandlingen kan även leda till att AI-systemet drar felaktiga slutsatser om kandidater, vilket kan få till följd att kandidater missgynnas genom att inte erbjudas en anställning som de skulle kunna vara lämpade för. Vidare kan behandlingen utgöra otillåten profilering enligt artikel 22. Slutligen, kan det vara svårt för Företag A att identifiera en rättslig grund enligt artikel 6 och 9 i dataskyddsförordningen för exempelvis behandling av biometrisk uppgifter genom ansiktsigenkänning.

Exempel 1 belyser även hur ett företags bristande behandling av personuppgifter i förlängningen kan innebära en negativ inverkan på personers mänskliga rättigheter. Det finns en risk att algoritmerna bakom AI-systemet baseras på data som är ofullständig eller ger uttryck för eller baseras på fördomar och att resultatet algoritmerna ger, därmed kan bli diskriminerande och få en negativ effekt för exempelvis personer med funktionsnedsättningar. Mätningen av ansiktsuttryck kan till exempel få ett negativt utfall för en person som har en synnedsättning.

Det är även tänkbart att denna typ av tjänst i förlängningen kan få en negativ inverkan på människors yttrandefrihet, en så kallad ”chilling effect” som uppstår till följd av att individer undviker att yttra sig i vissa frågor av rädsla för negativa effekter. En kandidat kan även uppleva en kränkning av sin rätt till privatliv om kandidaten blir föremål för en alltför omfattande behandling av sina personuppgifter.

Exempel 2 – Spelbolaget (ett företag som blir föremål för en personuppgiftsincident)

Företag B är en aktör inom spelbranschen med global närvaro och anställda i olika länder, bland annat Ryssland och Ukraina. Företagets huvudkontor ligger i Sverige, men kundkretsen finns främst inom EU och i USA. Företag B hanterar och lagrar en stor mängd personuppgifter om sina anställda.

Nyligen har en hackergrupp från Ryssland genomfört en framgångsrik ransomware-attack mot Företag B. Genom attacken har känslig information, inklusive personuppgifter om de anställda, blivit krypterad och stulen. Viss information har även sålts på Darknet. Intrånget har exponerat information om anställdas sexuella läggning, inkomst, boendesituation, familjeförhållanden och fackliga tillhörighet. För vissa anställda har även uppgifter om deras politiska åsikter avslöjats. Det bör noteras att ett av Företag B:s spel, som har en lesbisk huvudkaraktär, har fått massiv kritik och väckt debatt i Ryssland. Politiker har uttalat att spelet strider mot rysk lagstiftning och omedelbart bör förbjudas.

Företag B misstänker att attacken kan vara kopplad till kritiken mot spelets huvudkaraktär. Dessvärre har Företag B upptäckt att deras säkerhetskopior inte är uppdaterade, vilket innebär att betydande arbete riskerar att gå förlorat. Av denna anledning överväger Företag B att betala lösen i form av bitcoins till den ansvariga hackergruppen.

Exempel 2 illustrerar några av de konsekvenser som kan uppstå till följd av en säkerhetsincident. Företag B har drabbats av en allvarlig personuppgiftsincident, vilken med hög sannolikhet kräver såväl anmälan till behörig dataskyddsmyndighet som information till registrerade då det är bekräftat att känsliga personuppgifter för anställda har blivit krypterade och utlämnade. Dessutom väcker incidenten vissa dataskyddsfrågor kring Företag B:s behandling av känsliga personuppgifter, särskilt behandlingen av uppgifter om anställdas sexuella läggning. Incidenten avslöjar även brister i Företag B:s informationssäkerhet.

Företag B behöver emellertid även överväga om incidenten kan innebära direkt fara för anställda och en risk för negativ inverkan på deras mänskliga rättigheter. Det kan inte uteslutas att anställda till följd av incidenten kan komma att utsättas för förföljelse, hot eller ingripanden från myndigheter. Amnesty International har rapporterat om att

det i Ryssland är vanligt förekommande med trakasserier, våld, politiskt motiverade juridiska åtgärder samt repressalier gentemot oppositionella, liksom diskriminering baserad på sexuell läggning. Den lagstiftning som förbjuder främjande av ”icke-traditionella” familjevärden för barn fungerar som ett verktyg för att försvåra för hbtq-relaterad verksamhet och begränsa yttrandefriheten.[6]

Mycket talar för att personuppgiftsincidenten kan komma att ha en negativ inverkan på mänskliga rättigheter, inklusive yttrandefrihet, skydd mot trakasserier, våld och politiskt motiverade juridiska åtgärder samt repressalier och skydd mot diskriminering.

När Företag B bestämmer sig för att betala lösen i form av bitcoins aktualiseras ytterligare risker. Betalning av lösen kan potentiellt innebära en överträdelse av lagar om penningtvätt och finansiering av terrorism. Det finns exempel på fall där betalningar i samband med ransomware-attacker har använts för att finansiera terrorism eller terroristverksamhet. Dessutom kan en betalning strida mot de omfattande sanktioner som till följd av kriget i Ukraina är riktade mot Ryssland. Värt att notera är även att individer som kopplats till olika hackergrupper har utsatts för sanktioner av bland annat USA.[7] Genom att betala lösen till hackergruppen riskerar Företag B således att bryta mot en rad regelverk och därigenom få såväl negativa rättsliga och ekonomiska konsekvenser som negativ publicitet och allvarlig ryktesskada.

Exempel 3 – Techbolaget (ett företag som lämnar ut information till myndigheter)

Företag C är ett svenskt techbolag verksamt inom hälso- och träningsbranschen. Företaget har utvecklat en träningsapplikation för mobiltelefoner som genom en liten handledssändare mäter användarens träningsframsteg. Applikationen samlar in och analyserar omfattande träningsdata, med möjlighet till delning av information med andra användare. Handledssändaren tillverkas av företagets dotterbolag i Kina.

Företaget har inrättat en visselblåsarkanal för att ge anställda möjlighet att anmäla oegentligheter. I visselblåsarsystemet lagras personuppgifter som ingår i anmälningarna. Det kan exempelvis vara namn på visselblåsaren och den person som är föremål för visselblåsningen, beskrivning av de handlingar som anmälts, vilka ibland kan innefatta misstankar om lagöverträdelser.

Nyligen kontaktade en kinesisk myndighet det svenska moderbolaget med en begäran om omedelbar utlämning av personuppgifter om samt-

[6] Se Amnesty International landsrapport om Ryssland, 2022, https://www.amnesty.org/en/location/europe-and-central-asia/russia/report-russia.
[7] Se pressrelease från US Department of the Treasury, 2023, https://home.treasury.gov/news/press-releases/jy1486.

liga anställda i Kina. Företaget har både kinesiska och svenska medborgare som anställda. Myndigheten motiverade begäran med hänvisning till kinesisk lagstiftning och påståenden om att Företag C är skyldigt att tillhandahålla informationen med hänsyn till nationell säkerhet och ökad övervakning av utländska företag.

Företag C får dessutom kontinuerligt förfrågningar från myndigheter, inklusive polis och åklagare både i Kina och Sverige. Dessa förfrågningar avser utlämning av data såsom geolokalisering och kommunikation mellan användare, i syfte att bistå myndigheterna i pågående brottsutredningar.

Exempel 3 belyser några av de svårigheter ett företag ställs inför i samband med utlämnande av personuppgifter till myndigheter. Såvitt gäller dataskydd är överföringar till tredje parter ett förhållandevis väl reglerat område genom dataskyddsförordningen, EU-domstolens praxis och riktlinjer och rekommendationer.[8] Givet att det är myndigheter som begär informationen behöver Företag C emellertid göra en noggrann bedömning innan uppgifterna lämnas ut. Bedömningen behöver beakta såväl svensk som kinesisk lagstiftning, samt internationella standarder för mänskliga rättigheter.

Kina klassificeras som ett land med en noterbar korruptionsrisk enligt Transparency Internationals korruptionsindex (CPI)[9] och det föreligger även risk för kränkningar av mänskliga rättigheter.[10] Bristen på transparens inom den offentliga sektorn och den politiska påverkan på rättsväsendet har skapat förutsättningar för korruption. Samtidigt begränsas yttrandefrihet och pressfrihet genom censur, och minoritetsgruppers rättigheter åsidosätts. Dessa faktorer behöver beaktas av Företag C bland annat inom ramen för en konsekvensbedömning.

Det finns risk att anställda påverkas negativt om informationen skulle lämnas ut. Dessa risker kan potentiellt knyta an till mänskliga rättigheter där ett utlämnande av personuppgifter skulle kunna hota individens rätt till integritet och personlig frihet genom att informationen används på ett sätt som strider mot de anställdas rättigheter eller försvårar för de anställda att skydda sina personliga och privata angelägenheter. De skulle även i extrema situationer kunna resultera i godtyckliga frihets-

[8] Artikel 44–50 dataskyddsförordningen, mål C-311/18, EDPB:s Riktlinje 05/2021 om samspelet mellan artikel 3 (territoriellt tillämpningsområde) och kapitel V (tredjelandsöverföringar) i dataskyddsförordningen, EDPB:s Rekommendation 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder, m.fl.

[9] Transparency International's korruptionsindex för Kina, 2022, https://www.transparency.org/en/countries/china.

[10] Se Amnesty International's landsrapport om Kina, 2022, https://www.amnesty.org/en/location/asia-and-the-pacific/east-asia/china/report-china/ och FN:s rapport "*OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*", 31 augusti 2022, https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region.

berövanden eller förföljelse som hotar rätten till privatliv eller rätten att få sin sak prövad av en oberoende domstol. Vidare kan risker kopplade till rätten till icke-diskriminering och yttrandefrihet aktualiseras.

Vid förfrågningar från myndigheter ska den personuppgiftsansvarige fastställa den rättsliga grund som tillåter utlämnandet av informationen och bedöma om sådant utlämnande i övrigt är förenligt med dataskyddsförordningen. I många situationer betraktas samarbete med myndigheter som ett vanligt förekommande och berättigat intresse, antingen för den personuppgiftsansvarige eller en tredje part. Vid en sådan bedömning är det emellertid angeläget att väga in de potentiella risker som individer kan ställas inför om informationen lämnas ut till en part där garantier för respekten av mänskliga rättigheter inte kan säkerställas. I dessa fall bör den personuppgiftsansvarige inte lämna ut informationen. Bedömningen bör dokumenteras genom den intresseavvägning eller konsekvensbedömning som dataskyddsförordningen föreskriver.

Sammanfattningsvis belyser våra tre exempel ovan att det finns en viktig koppling mellan företags behandling av personuppgifter och mänskliga rättigheter. Bristande hantering av dataskyddet kan resultera i allvarliga kränkningar av mänskliga rättigheter. Vi menar att detta understryker vikten av att företag arbetar för en bredare förståelse och tillämpning av dataskyddet för att säkerställa att även risker kopplade till mänskliga rättigheter uttryckligen beaktas.

3. EU:s initiativ inom hållbarhet

3.1 Inledning

EU har under senare år tagit flera initiativ för att förmå företag att bidra till en hållbar utveckling och att bättre hantera och rapportera om hållbarhet, både i den egna verksamheten och i värdekedjan. De två lagstiftningsprodukter som enligt vår mening framför allt kommer att få en tydlig bäring på dataskyddet är EU-kommissionens förslag till direktiv om tillbörlig aktsamhet för företag i fråga om hållbarhet (*Eng. Corporate Sustainability Due Diligence Directive*) (”**CSDDD**”)[11] och direktivet om hållbarhetsrapportering (*Eng. Corporate Sustainability Reporting Directive*) (”**CSRD**”)[12]. I CSDDD föreslås regler om obligatorisk tillbörlig aktsamhet avseende mänskliga rättigheter och miljö samt därmed sam-

[11] EU Kommissions förslag till Europaparlamentets och rådets direktiv om tillbörlig aktsamhet för företag i fråga om hållbarhet och om ändring av direktiv (EU) 2019/1937.

[12] Europaparlamentets och rådets direktiv (EU) 2022/2464 av den 14 december 2022 om ändring av förordning (EU) nr 537/2014, direktiv 2004/109/EG, direktiv 2006/43/EG och direktiv 2013/34/EU vad gäller företagens hållbarhetsrapportering.

manhängande bolagsstyrningsfrågor. CSRD rör rapportering om en rad olika hållbarhetsfrågor. Båda initiativen fokuserar brett på hållbarhet, inte enbart påverkan på miljö och klimat utan även påverkan på mänskliga rättigheter.

3.2 CSDDD

På ett övergripande plan syftar CSDDD till att näringslivet ska bidra till en omställning i hållbar riktning. CSDDD är tänkt att etablera ett gemensamt ramverk för företag i syfte att säkerställa så kallad tillbörlig aktsamhet i såväl den egna verksamheten som i värdekedjan (beroende av hur detta begrepp kommer att slutligt definieras) för att motverka negativ påverkan på mänskliga rättigheter, klimat och miljö.[13] I juni 2023 inleddes trepartsförhandlingar mellan Europaparlamentet, Europeiska unionens råd och Europeiska kommissionen med målet att ha ett enats om en slutlig version under 2023.

I det ursprungliga förslaget som lades fram av Kommissionen (vilket kan komma att förändras under trepartsförhandlingarna) följer det av CSDDD att företag ska säkerställa tillbörlig aktsamhet genom att:

- Införa kraven på tillbörlig aktsamhet i företagets policyer och att det ska finnas en policy för tillbörlig aktsamhet, vilken ska innehålla (i) en beskrivning av företagets strategi för tillbörlig aktsamhet, (ii) en uppförandekod som beskriver de regler och principer som ska följas av företagets anställda och dotterbolag, och (iii) en beskrivning av de förfaranden som införts för att tillämpa tillbörlig aktsamhet, inbegripet de åtgärder som vidtagits för att kontrollera efterlevnaden av uppförandekoden och utvidga dess tillämpning till etablerade affärsförbindelser.
- Identifiera faktiska eller potentiella negativa effekter för de mänskliga rättigheterna och negativa miljöeffekter som härrör från företagets egen eller dotterbolagens verksamhet och från deras etablerade affärsförbindelser.
- Vidta lämpliga åtgärder för att förebygga och begränsa potentiella negativa effekter, säkerställa att faktiska negativa effekter upphör och minimera omfattningen av effekterna. Detta kan innebära att ta fram handlingsplaner, och utkräva garantier (s.k. *contractual cascading*), men även att avsluta affärsförbindelser med en partner i vars värdekedja effekten har uppstått. Det kan vidare innebära att i förekommande fall neutralisera negativa effekter genom att betala skadestånd

[13] Artikel 1.1 i CSDDD.

till drabbade personer och ekonomisk ersättning till drabbade samhällen.
- Inrätta ett klagomålsförfarande för att ge möjlighet för personer och organisationer, som har berättigade farhågor om faktiska eller potentiella negativa effekter för de mänskliga rättigheterna och negativa miljöeffekter med avseende på företagets egen verksamhet, deras dotterbolags verksamhet eller deras värdekedjor, att lämna in klagomål till företaget.
- Övervaka effektiviteten av företagets policyer med avseende på tillbörlig aktsamhet.
- Offentligt kommunicera om tillbörlig aktsamhet genom att årligen på företagets webbplats publicera en översikt över de frågor om mänskliga rättigheter och miljö som omfattas av CSDDD. Sådan kommunikation är inte nödvändig för företag som omfattas av rapporteringskravet i CSRD.
- Enligt CSDDD ska en negativ effekt anses vara väsentlig om agerandet utgör en del av företagets primära verksamhet beroende av risken för allvarlig inverkan på människor eller miljön, antalet individer som påverkas eller kan påverkas, samt omfattningen av faktiska eller potentiella miljöskador, och slutligen hur lätt faktiska eller potentiella skador kan avhjälpas och/eller återställas.

CSDDD har i skäl 67 en uttrycklig referens till dataskydd och integritet. Där anges det att CSDDD ska tillämpas i överensstämmelse med unionens dataskyddslagstiftning och rätten till integritetsskydd och skydd av personuppgifter som fastslås i artiklarna 7 och 8 i EU-stadgan. Vidare anges att all behandling av personuppgifter enligt CSDDD ska ske i enlighet med dataskyddsförordningen, inbegripet kraven på ändamålsbegränsning, uppgiftsminimering och lagringsbegränsning.[14]

Ett nyckelbegrepp i CSDDD är ”negativa effekter för de mänskliga rättigheterna”.[15] Begreppet avser en negativ effekt för skyddade personer till följd av kränkning av någon av de rättigheter eller någon av de förbud som räknas upp i Bilagan till CSDDD, såsom de fastställts i de internationella konventioner som förtecknas i Bilagan till CSDDD. Det innebär att bland annat överträdelse av förbudet mot godtycklig eller olaglig inblandning i en persons privatliv, familj, hem eller korrespondens och angrepp mot personens rykte i enlighet med artikel 17 i FN:s allmänna förklaring om de mänskliga rättigheterna omfattas.

[14] EDPS Formal comments on the Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937.
[15] Artikel 3.1 (c) i CSDDD.

Vi har ovan etablerat kopplingen mellan dataskydd och mänskliga rättigheter. Enligt vår bedömning kan bristande hantering av personuppgifter leda till en kränkning av mänskliga rättigheter, vilket i sin tur kan innebära en sådan negativ effekt som omfattas av CSDDD.

Vårt Exempel 1 ovan är relevant här. I exemplet har vi Företag A vars huvudsakliga affärsidé är att samla in, analysera och dra slutsatser baserat på kandidaters personuppgifter. Företaget använder AI-baserade lösningar, vilket i sig medför en förhöjd risk för potentiella överträdelser av både individens rätt till dataskydd och skyddet för mänskliga rättigheter, exempelvis skyddet mot diskriminering. Förutsatt att Företag A i övrigt omfattas av kraven enligt CSDDD, kan företagets omfattande behandling av personuppgifter och de identifierade riskerna med avseende på mänskliga rättigheter, leda till att Företag A inte bara behöver följa bestämmelserna i dataskyddsförordningen, utan även noggrant överväga och beakta kraven i CSDDD om tillbörlig aktsamhet vid behandlingen av personuppgifter. Om Företag A konstaterar att behandlingen av personuppgifter innebär en faktisk eller potentiell negativ effekt behöver företaget vidta de åtgärder som föreskrivs enligt CSDDD. Detta är ett exempel som är relevant för de flesta företag vars primära verksamhet omfattar behandling av personuppgifter.

Enligt vår tolkning av CSDDD kommer således företag som omfattas av direktivet att behöva bedöma om den egna personuppgiftsbehandlingen eller den behandling som sker i värdekedjan, skulle kunna utgöra en sådan negativ effekt för de mänskliga rättigheterna som avses i CSDDD. Om så är fallet, behöver företaget vidta lämpliga åtgärder för att förebygga och begränsa potentiella negativa effekter, säkerställa att faktiska negativa effekter upphör och minimera omfattningen av effekterna. Vi tror inte att företags personuppgiftsbehandling regelmässigt kommer att innebära skyldigheter enligt CSDDD, men för företag med omfattande och ingripande behandling av personuppgifter kommer CSDDD fortsättningsvis att behöva beaktas i dataskyddsarbetet.

3.3 CSRD

CSRD, som är en revidering och utvidgning av EU-direktivet om icke-finansiell rapportering[16], är en del av EU:s agenda för hållbar finansiering och en nyckelkomponent för att nå målen i EU:s gröna giv. CSRD trädde i kraft i januari 2023 och syftar till att öka tillgången till information om hur företag påverkar människor och miljö samt hur före-

[16] Europaparlamentets och rådets direktiv 2014/95/EU av den 22 oktober 2014 om ändring av direktiv 2013/34/EU vad gäller vissa stora företags och koncerners tillhandahållande av icke-finansiell information och upplysningar om mångfaldspolicy.

tag påverkas av hållbarhetsfrågor. Företag ska rapportera den huvudsakliga faktiska eller potentiella negativa inverkan som kan kopplas till företagets eller koncernens verksamhet och värdekedja, inklusive dess produkter, tjänster, affärsförbindelser och distributionskedja och de huvudsakliga riskerna för företaget eller koncernen med avseende på hållbarhetsfrågor. Utgångspunkten för rapporteringen är principen om dubbel väsentlighet (eller dubbel materialitet), dvs. att rapporteringen ska beskriva både omvärldens inverkan på företaget och företagets påverkan på dess omgivning.

Rapporteringen ska ske i enlighet med de obligatoriska europeiska standarderna för hållbarhetsrapportering (*Eng. European Sustainability Reporting Standards* (”**ESRS**”)), som tagits fram av EFRAG och antogs av kommissionen i juli 2023. De nya standarderna ska säkerställa jämförbar, tillräcklig och kvalitativ information från företagen om på vilket sätt de påverkar människor, miljö och klimat. Målet är att rapporteringen ska öka transparensen och jämförbarheten eftersom företag kommer att behöva lämna mer omfattande upplysningar och information kopplad till hållbarhet än vad som har gällt under nuvarande regler om hållbarhetsrapportering.

Vi har identifierat flera tydliga kopplingar mellan dataskydd och CSRD. Det finns till att börja med krav att på att beakta integritet i den dubbla väsentlighetsanalysen.[17] Vidare finns det uttryckliga referenser till integritet i de ämnesspecifika standarderna inom det sociala området.[18] Här kan vi se att bolag ska rapportera om integritetsrelaterade risker avseende egna anställda, anställda i värdekedjan samt för konsumenter och slutanvändare. Vidare ska bolag lämna en utförlig beskrivning av den övergripande strategi som bolaget använder för att identifiera och hantera betydande faktiska och potentiella effekter på konsumenter och/eller slutanvändare hänförliga till företagets produkter och/eller tjänster i de fall dessa utgör en risk för konsumenters och/eller slutanvändares integritet.[19]

ESRS koppling till integritetsskyddet blir särskilt tydligt i följande tillämpningskrav (*Eng. application requirements*):

- Integritetsskydd kopplat till skydd mot diskriminering.[20]
- Integritetsskydd i samband med nyttjande av interna rapporteringskanaler som omfattas av förbud mot repressalier.[21]

[17] ESRS 1, Appendix A, AR 16 innehåller en icke-uttömmande lista över ämnen att beakta i den dubbla väsentlighetsanalysen för var och en av ESRS-kategorierna.
[18] ESRS S1, ESRS S2 och ESRS S4.
[19] ESRS S4 – Konsumenter och slutanvändare, Mål – Punkt 2, sid. 224.
[20] ESRS S1-2, Appendix A, AR 25.
[21] ESRS S4-3, Appendix A, AR 22.

- Ett företag ska beakta en allvarlig personuppgiftsincident om den har väsentlig inverkan på konsumenter och/eller slutanvändare.[22]
- När ett företag lämnar upplysningar om initiativ eller processer som syftar till att minska väsentlig negativ effekt, får företaget till exempel beakta initiativ som syftar till att öka medvetenheten om risker för bedrägerier på nätet, vilka leder till en minskning av antalet fall där slutanvändare råkar ut för en kränkning av sin personliga integritet.[23]
- När ett företag lämnar upplysningar om väsentliga risker och möjligheter relaterade till företagets påverkan eller beroende av konsumenter och/eller slutanvändare får företaget beakta att affärsmöjligheter relaterade till företagets påverkan på konsumenter och/eller slutanvändare kan innefatta marknadsdifferentiering och ökad attraktivitet för kunder genom att erbjuda säkra produkter eller tjänster som respekterar integriteten.[24]

Med beaktande av dataskyddets koppling till mänskliga rättigheter är vår uppfattning att ett företags dubbla väsentlighetsanalys i många fall kommer visa att dataskyddet utgör en av bolagets huvudsakliga hållbarhetsrisker. Det skulle till exempel kunna bli resultatet för ett bolag vars primära verksamhet bygger på AI-system, behandling av stora mängder personuppgifter eller övervakning, men även företag med ett stort antal anställda. För att belysa detta ytterligare kan vi åter se till Exempel 1 där Företag A bedriver en verksamhet i vilken det föreligger en tydlig risk för diskriminering, Exempel 2 där den personuppgiftsincident som Företag B har drabbats av kan få långtgående konsekvenser för registrerade och Exempel 3 där Företag C:s anställda behöver skyddas mot repressalier när visselblåsarkanalen används.

Slutbetänkandet från utredningen om hållbarhetsredovisning föreslår en rad ändringar i svensk lag för att införliva CSRD i svensk rätt.[25] Vi noterar dock att inga ändringar föreslås i dataskyddslagstiftningen vilket vi utgår beror på att CSRD inte ska inverka på kraven enligt dataskyddsförordningen.

[22] ESRS S4, Appendix A, AR 1.
[23] ESRS S4-4, Appendix A, AR 36.
[24] ESRS S4-4, Appendix A, AR 37.
[25] SOU 2023:35, Nya regler om hållbarhetsredovisning, Slutbetänkande av utredningen om hållbarhetsredovisning.

4. Hur påverkar dataskyddet genomförandet av EU:s hållbarhetsregelverk?

4.1 Insamling av ny information/behandling av befintlig information för nya ändamål

Genomförandet av CSRD och uppfyllandet av ESRS kommer att få inverkan på företags behandling av personuppgifter. Även om CSRD inte har någon direkt inverkan på dataskyddslagstiftningen medför CSRD krav på nya typer av personuppgiftsbehandling för de företag som träffas av regelverket. Det är tydligt att CSRD innebär krav på informationsinsamling och rapportering vilket i många fall förutsätter en behandling av personuppgifter.

Detta kan inkludera behandling av personuppgifter såsom namn, information kopplad till anställningen eller andra uppgifter om anställda, leverantörer, kunder eller andra berörda parter. Denna nya behandling utgör sannolikt inte något problem för de företag som träffas av regelverken då den rättsliga grunden för behandlingen sannolikt kan hämtas från CSRD direkt i form av en rättslig förpliktelse eller genom det berättigade intresse företaget har av att uppfylla kraven enligt CSRD och vidta erforderliga åtgärder. Däremot blir det viktigt för företag att uppdatera tillämpliga register, rutiner eller informationsgivning med beaktande av dessa nya behandlingar för att försäkra sig om att kraven enligt dataskyddslagstiftningen iakttas parallellt med de nya kraven enligt CSRD.

Även CSDDD kan komma att påverka företags nuvarande dataskyddsarbete. När företag som träffas av CSDDD utför de granskningar och bedömningar som krävs kan det innebära ett behov av att samla in och behandla data som innehåller personuppgifter. Till exempel kan företagen behöva samla in information om sina leverantörers arbetsvillkor, miljöpåverkan eller koldioxidutsläpp. Denna information kan innehålla personuppgifter om de anställda som i vissa fall även kan vara känslig. En situation är exempelvis i samband med att ett företag önskar tillmötesgå leverantörers, samarbetspartners och investerares ökade krav på transparens kring mångfald. Mångfaldsrapportering kommer i många fall vara problematisk för företag då det generellt saknas rättslig grund enligt dataskyddsförordningen för behandlingen av de känsliga personuppgifter som mångfaldsrapportering omfattar, samtidigt utgör transparens och åtgärder som syftar till att öka mångfalden ofta en viktig del av företagets hållbarhetsarbete. Vid sådana konflikter är det viktigt att företaget säkerställer att det har lämpliga mekanismer på plats för att hantera de nya hållbarhetskraven utan att bryta mot kraven enligt dataskyddslagstiftningen.

Även den behandling av personuppgifter som hänför sig till kraven i CSDDD behöver följa och inte inverka menligt på det skydd som ges enligt dataskyddsförordningen. Det innebär sannolikt att inte heller företag som träffas av kraven enligt CSDDD kommer att möta några problem med att parallellt följa kraven i CSDDD och dataskyddsförordningen. Däremot är det upp till företaget att försäkra sig om att efterlevnaden av CSDDD sker i enlighet med samtliga krav enligt dataskyddsförordningen och att erforderliga justeringar i det befintliga dataskyddsarbetet görs.

4.2 Ett breddat dataskyddsarbete

Att dataskyddet är så mycket mer än en teknisk lagstiftning och att dataskyddet har en stark koppling till mänskliga rättigheter är känt. Vad detta innebär i relation till de nya hållbarhetsregelverken kan däremot komma att bli företagens nästa stora utmaning. För företag vars verksamhet innefattar behandling av stora mängder personuppgifter, eller som är exponerade för högriskbehandling på grund av de personuppgifter de hanterar, tror vi att de nya hållbarhetsregelverken CSRD och CSDDD kommer att få betydande konsekvenser som kräver särskilda anpassningar av det nuvarande dataskyddsarbetet.

Utöver att endast uppfylla de förpliktelser som följer av dataskyddsförordningen kommer CSRD och CSDDD medföra krav på företag att i ett tidigt skede identifiera faktiska eller potentiella negativa effekter hänförliga till den personliga integriteten och vidta åtgärder för att begränsa negativa konsekvenser. Vidare kan företags behandling av personuppgifter och åtgärder kopplade till integritetsrisker och incidenter utgöra sådan information som ska rapporteras enligt CSRD. Även om det framgår att CSRD och CSDDD inte ska inverka på dataskyddsförordningen så finns det en stark koppling mellan regelverken när det kommer till företag vars verksamheter är beroende av behandling av personuppgifter. Det innebär att nya krav ställs på företag att inte bara uppfylla dataskyddslagstiftningen utan även att uppfylla de krav som ställs enligt hållbarhetslagstiftningen. Vidare blir företags insyn i och bedömning av affärsrelationer viktigare än tidigare. Företagen måste granska och utvärdera sina befintliga partnerskap och affärsrelationer för att säkerställa att samarbetspartners följer liknande standarder för tillbörlig aktsamhet och integritetsskydd. Särskild vikt ligger på att hantera potentiella negativa effekter som kan sträcka sig över hela värdekedjan. Sammantaget innebär detta att företag måste bredda sitt dataskyddsarbete.

5. Framtidens dataskyddsarbete

Mot bakgrund av de ökade hållbarhetskrav som företag har att beakta, särskilt de krav som förväntas komma att följa av CSDD och redan följer av CSRD, är vår uppfattning att dataskyddsarbetet kommer att få en ny dimension. Dataskyddet är en hållbarhetsfråga och kommer att behöva integreras i företags strategiska hållbarhetsarbete på ett tydligare sätt. Det innebär även att såväl dataskyddsombud som företagets dataskyddsjurister kommer att behöva samarbeta med hållbarhetsteamen i långt större utsträckning än vad som är fallet idag i de flesta organisationer. Vi är övertygade om att denna utveckling kommer att göra dataskyddsarbetet än mer intressant och attraktivt för jurister, och även innebära att dataskyddet tydligare knyter an till sina rötter i mänskliga rättigheter. Företag som anpassar sitt dataskyddsarbete till dessa nya förutsättningar kommer att ha utmärkta möjligheter att lyckas med hållbar innovation och digitalisering. Vi ser med tillförsikt fram emot att följa dataskyddets fortsatta utveckling!