Behandling av anställdas personuppgifter – ett antal praktiska scenarion

*Johan Thörn och Johan Sundberg**

1. Inledning

Arbetsgivare behandlar normalt anställdas personuppgifter för ett stort antal ändamål under hela anställningsförhållandet och för en tid därefter. Typiskt sett behandlar också arbetsgivare ett stort antal kategorier av personuppgifter som rör anställda, till exempel i HR-system, vid beräkning och utbetalning av lön, schemaläggning, och i olika IT-system. Därutöver behandlar arbetsgivare normalt särskilda kategorier av personuppgifter (känsliga personuppgifter) om sina anställda, till exempel uppgift om anställdas hälsa i läkarintyg vid sjukskrivning eller i samband med rehabilitering och uppgift om eventuellt fackligt medlemskap för att uppfylla skyldigheter inom arbetsrätten.

Vår erfarenhet är också att arbetsgivare numera i allt större utsträckning vill behandla anställdas personuppgifter för flera ändamål och i flera sammanhang, till exempel i samband med kontroll- och övervakningsåtgärder, införandet av nya tekniska lösningar på arbetsplatsen eller för uppföljning och analys med hjälp av anställdas personuppgifter. Det medför att frågan om en viss behandling av anställdas personuppgifter är tillåten eller inte uppkommer allt oftare.

Vidare kan det konstateras att anställda normalt befinner sig i en beroendeställning i förhållande till arbetsgivaren, innebärande att särskild hänsyn ska tas till de anställdas integritetsintresse vid behandling av deras personuppgifter. Det ojämlika förhållande som – som utgångspunkt – råder mellan arbetsgivaren och den anställde ställer också ökade krav på arbetsgivare att genomföra en noggrann laglighetsanalys för att ta ställning till om en sådan behandling av anställdas personuppgifter är tillåten.

* Advokater. Författarna tackar Sören Öman för genomgång och kloka synpunkter på denna artikel.

Vid en bedömning om en behandling av anställdas personuppgifter i ett enskilt fall är tillåten enligt dataskyddsförordningen (GDPR) och kompletterande lagstiftning krävs inte bara förståelse och kunskap om dataskyddsregler utan även om arbetsrätten. I denna artikel kommer vi att redogöra *dels* för några rättsliga utgångspunkter för behandling av anställdas personuppgifter baserat på vår praktiska erfarenhet som förhoppningsvis kan underlätta din egen laglighetsanalys, *dels* ett antal praktiska scenarion för att illustrera tillämpningen av dataskyddsregler i förhållande till behandling av anställdas personuppgifter.

2. Några rättsliga utgångspunkter

Arbetsrättens betydelse för tolkning och tillämpning av dataskyddsregler

Anställningsförhållandet grundar sig på anställningsavtalet mellan arbetsgivaren och den anställde. Vidare omfattas anställningsförhållandet av ett stort antal arbetsrättsliga lagar, till exempel lagen (1982:80) om anställningsskydd (LAS), semesterlagen (1977:480) och medbestämmandelagen (1976:580) (MBL), samt – i förekommande fall – av kollektivavtal som arbetsgivaren är bunden av.

Såväl arbetsrättsliga lagar som anställningsavtalet och eventuella kollektivavtal får i praktiken betydelse för tolkning och tillämpning av dataskyddsregler vid behandling av anställdas personuppgifter.

Nedan kommer vi att redogöra för några exempel på när arbetsrätten och anställningsförhållandet får betydelse för tolkning och tillämpning av dataskyddsregler kopplat till vissa dataskyddsrättsliga krav, till exempel principerna för behandling av personuppgifter i artikel 5 i GDPR, kravet på rättslig grund i artikel 6 i GDPR och kravet på att genomföra en konsekvensbedömning enligt artikel 35 i GDPR för potentiella ”hög risk”-behandlingar. Vi tar även upp att uppfyllandet av arbetsrättsliga krav, till exempel informations- och förhandlingsplikt enligt MBL också kan få betydelse vid bedömning om en viss behandling av anställdas personuppgifter ska anses vara tillåten. Slutligen tar vi upp vissa aspekter – baserat på vår praktiska erfarenhet – kopplade till dessa krav specifikt i förhållande till behandling av anställdas personuppgifter. Låt oss börja med frågan om personuppgiftsansvar.

Något om personuppgiftsansvaret vid behandling av anställdas personuppgifter

Personuppgiftsansvarig är den aktör som, ensam eller tillsammans med andra aktörer, bestämmer över ändamålen och medlen med en viss behandling av personuppgifter. Annorlunda uttryckt; personuppgiftsansvarig är den som bestämmer *varför* och *hur* personuppgifter ska behandlas i ett enskilt fall och således utövar ett bestämmande inflytande och kontroll över behandlingen av personuppgifter.

Vid behandling av anställdas personuppgifter är utgångspunkten att arbetsgivaren är personuppgiftsansvarig. Detta eftersom arbetsgivaren typiskt sett utövar ett bestämmande inflytande och kontroll över behandlingen av sina anställdas personuppgifter inom ramen för anställningsförhållandet. När anställdas personuppgifter behandlas finns det således en presumtion för att arbetsgivaren är personuppgiftsansvarig för behandlingen (arbetsgivarpresumtionen).

Denna arbetsgivarpresumtion är i praktiken stark. Det krävs således ett förhållandevis litet inflytande över behandlingen av personuppgifter för att arbetsgivaren ska anses vara personuppgiftsansvarig för behandlingen av sina anställdas personuppgifter. Som exempel på att arbetsgivarpresumtionen för personuppgiftsansvar i praktiken är stark kan nämnas att dåvarande Datainspektionen i sin tidigare vägledning om ansvar för personuppgifter som hanteras i system för whistleblowing (oktober 2010) angav att arbetsgivaren är personuppgiftsansvarig för behandlingen av sina anställdas personuppgifter inom ramen för ett sådant system. Detta trots att det vid tidpunkten för vägledningen i praktiken typiskt sett var ett annat bolag, inte sällan ett utländskt moderbolag, som bestämt att systemet ska införas, varför och på vilket sätt behandlingen av personuppgifter i systemet skulle gå till.

Andra (mer aktuella) exempel på denna arbetsgivarpresumtion är från Integritetsskyddsmyndighetens (IMY) tillsynspraxis. IMY har i korthet ansett att arbetsgivaren ansvarar för en behandling av personuppgifter som dess anställda utför så länge det sker inom ramen för tjänsten, även om behandlingen skett i strid med arbetsgivarens policies och riktlinjer på arbetsplatsen. Endast i undantagsfall när anställda för egen räkning hanterar personuppgifter och överskrider sina befogenheter kan behandlingen falla utanför arbetsgivarens ansvar. Se till exempel IMY:s tillsynsbeslut avseende Tullverket om behandling av personuppgifter vid användning av tjänstemobiler (14 mars 2022, diarienummer DI-2020-5868) där arbetsgivaren ansågs ansvarig för att de anställda – i strid med Tullverkets regler – oavsiktligt röjt personuppgifter i form av bilder som tagits i tjänsten på individer som varit föremål för brotts-

misstankar eller ingått i brottsutredningar till en amerikansk molntjänst (Google Foto).

Ett annat exempel är IMY:s tillsynsbeslut avseende Region Skåne (26 april 2023, diarienummer IMY-2022-1290) som rörde en anställd som tappat bort ett okrypterat USB-minne med ett stort antal känsliga patientuppgifter. IMY uttalade i sitt beslut att regionen ansvarar för den behandling av personuppgifter som sker inom ramen för verksamheten även om det är fråga om ett misstag eller en felbedömning som skett av exempelvis en anställd. Det är först om den anställde agerar för andra ändamål, som inte omfattas av arbetsgivarens ändamål, som – enligt IMY – det kan bli fråga om att den anställde eller någon annan aktör är personuppgiftsansvarig för den aktuella behandlingen.

Detta följer även av Europeiska dataskyddsstyrelsens riktlinje om begreppen personuppgiftsansvarig och personuppgiftsbiträde (07/2020, antagen den 7 juli 2021). Av riktlinjen framgår att i princip all behandling av personuppgifter av anställda som sker inom ramen för en organisations verksamhet kan betraktas som att den sker under den organisationens kontroll och därmed att organisationen är personuppgiftsansvarig för behandlingen. Detta gäller naturligtvis då även i förhållande till behandling av anställdas personuppgifter.

Arbetsgivarpresumtionen utesluter så klart inte att en annan aktör i ett enskilt fall kan vara ensam (eller med arbetsgivaren gemensamt) ansvarig för behandlingen av personuppgifter. Det rör sig bara om en presumtion. En bedömning måste således alltid göras i varje enskilt fall avseende vilken eller vilka aktörer som faktiskt i praktiken utövar kontroll och inflytande över behandlingen av personuppgifter, men arbetsgivarpresumtionen kan, enligt vår mening, tillämpas som en rimlig utgångspunkt för en bedömning av personuppgiftsansvaret vid behandling av anställdas personuppgifter.

Arbetsgivarpresumtionen medför även, enligt vår uppfattning, att det i praktiken oftare uppkommer ett *gemensamt personuppgiftsansvar* när flera aktörer är inblandade i behandlingen av anställdas personuppgifter, till exempel i koncerner där moderbolaget inte sällan utövar kontroll och inflytande över behandlingen av personuppgifter på ett sådant sätt att ett gemensamt ansvar uppkommer mellan arbetsgivarbolaget och moderbolaget. Tänk exempelvis koncernövergripande medarbetarundersökningar eller övervakning av koncerngemensamma IT-system.

Principer för behandling av personuppgifter i förhållande till anställdas personuppgifter

Arbetsrättsliga regler och anställningsförhållandet i sig har även omedelbar betydelse för tolkning och tillämpning av principerna för behandling av personuppgifter i artikel 5 i GDPR när anställdas personuppgifter behandlas.

Det kan således konstateras att om en behandling av anställdas personuppgifter skulle stå i strid med arbetsrättsliga regler skulle behandlingen även vara otillåten enligt artikel 5 i GDPR, eftersom behandlingen då skulle stå i strid med principen om laglighet, öppenhet och korrekthet. Detta kan exempelvis aktualiseras i samband med övervakningseller kontrollåtgärder som en arbetsgivare vill införa i förhållande till sina anställda. Om bedömningen är att en sådan kontrollåtgärd inte kan genomföras med stöd av arbetsgivarens arbetsledningsrätt och det saknas stöd i avtal (ett enskilt avtal eller ett kollektivavtal) kan även – om arbetsgivaren trots det väljer att genomföra kontrollåtgärden – eventuell behandling av personuppgifter som sker i samband med åtgärden vara otillåten och i strid med GDPR.

Arbetsrättsliga regler och anställningsförhållandet får även betydelse vid en bedömning om hur länge anställdas personuppgifter får sparas enligt principen om lagringsminimering. En arbetsgivare behöver normalt spara vissa personuppgifter om anställda under hela anställningsförhållandet, till exempel grundläggande personuppgifter om namn, personnummer, tjänst, ansvarsområde etc. Arbetsrätten innehåller även särskilda preskriptionsregler som får betydelse för bestämmande av hur länge en arbetsgivare får bevara personuppgifter för att hantera och bemöta rättsliga krav som rör sina anställda. Dessutom innehåller arbetsrätten, i förekommande fall, särskilda regler om bevarande av dokument och handlingar som får betydelse för att bestämma hur länge arbetsgivaren måste bevara vissa personuppgifter för att uppfylla sina arbetsrättsliga skyldigheter. Ett exempel på det är att en arbetsgivare måste bevara anteckningar om jourtid, övertid och mertid under det aktuella kalenderåret och under två år därefter enligt Arbetsmiljöverkets gällande föreskrift (AFS 1982:17).

Kunskap om arbetsrättsliga regler har således avgörande betydelse för att kunna ta ställning till hur länge anställdas personuppgifter får och bör bevaras i praktiken. Kunskap om arbetsrättsliga regler är således värdefull vid framtagande av rutiner och dokumentation för gallring av anställdas personuppgifter.

Slutligen kan nämnas att anställningsförhållandet i praktiken även kan ha betydelse för tillämpningen av principen om ändamålsbegränsning. Principen innebär – något förenklat – att personuppgifter bara får samlas

in för särskilda och berättigade ändamål och inte återanvändas för något ändamål som är oförenligt med de ursprungliga ändamålen. I praktiken är det mycket vanligt förekommande att arbetsgivare vill vidarebehandla och återanvända anställdas personuppgifter för nya ändamål. För att ta ställning till om behandlingen i sådant fall är tillåten enligt principen om ändamålsbegränsning måste en oförenlighetsbedömning göras mellan de ursprungliga ändamålen för vilka uppgifterna samlades in och de nya tilltänkta ändamålen som arbetsgivaren vill behandla uppgifterna för. I praktiken brukar man fråga sig om den anställde typiskt och objektivt sett kan förvänta sig att arbetsgivaren behandlar de anställdas personuppgifter för det nya ändamålet. Om svaret är jakande anses vidarebehandlingen vara förenlig och tillåten.

IMY har, enligt vår uppfattning, i sin tillsynspraxis varit relativt generös vid bedömningen av vad en anställd typiskt sett kan förvänta sig att en arbetsgivare behandlar anställdas personuppgifter för. Dåvarande Datainspektionen ansåg exempelvis att en anställd typiskt sett kan räkna med att en arbetsgivare vidarebehandlar logguppgifter från ett inpasseringssystem för att utreda konkret misstanke om fusk med arbetstider (kontroll av arbetstid), även om inpasseringssystemet infördes för att upprätthålla säkerheten i lokalerna och säkerställa att endast behöriga vistas i lokalerna (se Datainspektionens tillsynsbeslut den 14 januari 2013 avseende Polisen i Örebro, diarienummer 1369-2012). Tillsynsbeslutet och Datainspektionens syn på oförenlighetsbedömningen illustrerar, enligt vår uppfattning, att anställningsförhållandet i sig kan ge arbetsgivaren ett förhållandevis stort utrymme för att vidarebehandla anställdas personuppgifter för olika ändamål.

Rättslig grund för behandling av anställdas personuppgifter

Arbetsrättsliga regler och avtal (anställningsavtalet och eventuella kollektivavtal) har även betydelse för med vilken rättslig grund enligt artikel 6 i GDPR som arbetsgivaren kan behandla anställdas personuppgifter. Behandling av anställdas personuppgifter som är nödvändig för att uppfylla åtaganden enligt anställningsavtalet, såsom att beräkna och betala ut lön, eller vidta åtgärder med stöd av arbetsledningsrätten, såsom schemaläggning, kan normalt ske med stöd av anställningsavtalet i sig som rättslig grund (artikel 6.1 (b) i GDPR).

Arbetsgivare omfattas även av olika arbetsrättsliga skyldigheter, till exempel skyldigheten att genomföra årliga lönekartläggningar enligt diskrimineringslagen (2008:567). I den utsträckning det är nödvändigt att behandla personuppgifter för att uppfylla arbetsrättsliga skyldigheter kan arbetsgivaren normalt förlita sig på den aktuella rättsliga skyl-

digheten som rättslig grund för behandlingen av personuppgifter (artikel 6.1 (c) i GDPR).

Tilläggas ska också att en skyldighet enligt ett kollektivavtal, i förekommande fall, enligt dataskyddslagen (2018:218) kan utgöra en rättslig skyldighet i den mening som avses i artikel 6 i GDPR. Detta har, enligt vår mening, i praktiken utökat arbetsgivares möjligheter att säkerställa en robust rättslig grund för behandling av anställdas personuppgifter, exempelvis vid vissa kontroll- och övervakningsåtgärder som sker med stöd av ett lokalt kollektivavtal som arbetsgivaren har träffat med berörda fackliga organisationer. Före GDPR och dataskyddslagen kunde arbetsgivare i praktiken enbart förlita sig på sitt berättigade intresse och en intresseavvägning som rättslig grund för behandling av personuppgifter som följer av ett kollektivavtal. Med det sagt utgör uppfyllandet av en skyldighet enligt ett kollektivavtal, enligt vår uppfattning, normalt ett starkt berättigat intresse, vilket i praktiken kan underlätta intresseavvägningen och öka förutsättningarna för att arbetsgivaren kan genomföra den aktuella behandlingen av personuppgifter.

I sammanhanget förtjänar att framhållas att det är viktigt att i varje enskilt fall faktiskt göra en bedömning *dels* om en rättslig skyldighet som följer av arbetsrätten faktiskt är så tydlig och precis att den utgör en rättslig skyldighet enligt GDPR, *dels* – om så är fallet – om det faktiskt är *nödvändigt* att behandla personuppgifter för att uppfylla den aktuella rättsliga skyldigheten.

Av ingresspunkt 41 i GDPR följer att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsebar för dem som omfattas av den. Enligt förarbetena till dataskyddslagen måste, enligt regeringen, det bedömas från fall till fall vilken *grad* av tydlighet och precision som krävs utifrån behandlingens och verksamhetens karaktär. Ett mer kännbart intrång kräver dock, enligt samma uttalande i förarbetena, att den rättsliga grunden är mer preciserad och därmed gör intrånget förutsebart. Mot bakgrund av dessa uttalanden har IMY i sin tillståndspraxis (se till exempel tillståndsbeslutet avseende Danske Bank, den 30 september 2022, diarienummer DI-2021-2183, med vidare relevanta hänvisningar) konstaterat att en förpliktelse som är alltför svepande och som ger den personuppgiftsansvarige en alltför stor handlingsfrihet i fråga om hur den ska uppfyllas *inte* kan utgöra en rättslig skyldighet i den mening som avses i artikel 6 i GDPR.

Som exempel medför det, enligt vår mening, att skyldigheten enligt arbetsmiljölagen (1977:1160) att arbetsgivaren ska vidta alla åtgärder som behövs för att förebygga att arbetstagaren utsätts för ohälsa eller olycksfall, som utgångspunkt, är alltför svepande för att i sig utgöra en rättslig skyldighet i den mening som avses i artikel 6 i GDPR och för den

delen i den mening som avses i undantaget från förbudet mot behandling av känsliga personuppgifter i artikel 9 i GDPR när behandlingen är nödvändig för att uppfylla arbetsrättsliga skyldigheter. I praktiken påverkar det de rättsliga förutsättningarna för arbetsgivare att genomföra kontrollåtgärder, till exempel förebyggande alkohol- och drogkontroller som inbegriper elektronisk hantering av testresultat (jämför också exempelvis Datainspektionens tillsynsbeslut avseende Region Gävleborg om införande av förebyggande slumpmässiga drogkontroller, den 23 januari 2014, diarienummer 52-2013, där Datainspektionen i och för sig konstaterade – efter att ha konsulterat Arbetsmiljöverket – att det inte fanns någon rättslig skyldighet enligt gällande arbetsmiljöregler att genomföra förebyggande drogkontroller).

Det sagda innebär således att svepande eller otydliga åligganden enligt ett kollektivavtal normalt inte kan utgöra en rättslig skyldighet i den mening som avses i artikel 6 i GDPR. Innan en arbetsgivare förlitar sig på ett åtagande enligt ett kollektivavtal som arbetsgivaren är bunden måste således en noggrann bedömning göras om åtagandet faktiskt uppfyller graden av precision som krävs för att åtagandet ska utgöra en rättslig skyldighet eller – för en privat arbetsgivare – om det är bättre att förlita sig på en intresseavvägning för den aktuella behandlingen.

Som nämnts ovan krävs också att behandlingen av personuppgifter faktiskt är *nödvändig* för att uppfylla den aktuella rättsliga skyldigheten, även om skyldigheten uppfyller kraven på precision och tydlighet för att utgöra en rättslig skyldighet enligt GDPR. Arbetsgivaren måste därför i varje enskilt fall överväga om det är möjligt att uppfylla skyldigheten utan att personuppgifter behandlas.

Som exempel kan nämnas att arbetsgivarens skyldighet enligt diskrimineringslagen att vidta aktiva åtgärder för att undersöka om det finns risk för diskriminering, repressalier eller om det finns andra hinder för enskildas lika rättigheter och möjligheter i verksamheten inte nödvändigtvis medför en rätt att behandla personuppgifter för detta syfte. Det är, enligt vår uppfattning, normalt möjligt att genomföra sådana undersökningar utan att samla in anställdas personuppgifter och då är det inte – strikt sett – nödvändigt att behandla anställdas personuppgifter för att uppfylla denna skyldighet. I praktiken uppkommer dessa frågor inte sällan när en arbetsgivare vill samla in anställdas uppgifter inom ramen för en enkätundersökning eller motsvarande som underlag för en arbetsmiljöutredning under förevändningen att insamlingen är nödvändigt för att uppfylla krav i diskrimineringslagen.

Slutligen ska tilläggas att det förekommer i praktiken att arbetsgivare väljer att inhämta den anställdes samtycke till en viss behandling

av personuppgifter. I sådant fall aktualiseras åtminstone två frågor: (i) vad är det för typ av samtycke och (ii), om det rör sig om ett samtycke som rättslig grund enligt artikel 6.1 (a) i GDPR, är samtycket giltigt?

Vad gäller den första frågan är det inte självklart att ett lämnat samtycke utgör ett samtycke som rättslig grund enligt artikel 6 i GDPR. Det gäller att skilja på samtycke och samtycke brukar vi säga. Det finns situationer där arbetsgivare inhämtar den anställdes *medgivande*, till exempel för att delta i en viss aktivitet, såsom en undersökning eller fotografering vid ett event. Ett sådant medgivande är inte nödvändigtvis samma sak som ett samtycke enligt artikel 6.1 (a) i GDPR. Vår uppfattning är att ett sådant medgivande i stället skulle kunna beaktas inom ramen för en intresseavvägning om arbetsgivaren förlitar sig på sitt berättigade intresse enligt artikel 6.1 (f) i GDPR för den aktuella personuppgiftsbehandlingen. Den anställdes medgivande medför, enligt vår mening, att intresseavvägningen blir mer ”robust”, eftersom integritetsintresset blir mer begränsad i sådant fall.

Vad gäller den andra frågan, om ett samtycke enligt artikel 6.1 (a) i GDPR är giltigt, måste givetvis en bedömning göras i varje enskilt fall. Det förtjänar dock att särskilt framhållas i detta sammanhang att en anställd, som utgångspunkt, inte kan lämna ett giltigt samtycke för arbetsgivarens behandling av personuppgifter, eftersom ett sådant samtycke normalt inte anses vara frivilligt på grund av den beroendeställning som följer av anställningsförhållandet. Kravet på frivillighet är högt ställt (jämför exempelvis Europeiska dataskyddsstyrelsens riktlinje 05/2020 om samtycke). I princip är det tillräckligt att den anställde känner någon form av påtryckning att lämna sitt samtycke för att samtycket ska vara ogiltigt.

Tilläggas ska också att även om den anställde i en viss situation kan lämna ett giltigt samtycke, exempelvis på grund av att det erbjuds rimliga alternativ till att lämna ett samtycke och den anställde har ett genuint fritt val mellan att lämna sitt samtycke eller inte utan att riskera några negativa konsekvenser, är det vanligt förekommande att inhämtade samtycken inte uppfyller de övriga kraven, särskilt på grund av bristande information (se längre ner avseende informations- och transparenskravet vid behandling av anställdas personuppgifter). Samtycke som rättslig grund för behandling av personuppgifter bör – så långt som möjligt – undvikas i allmänhet och särskilt när det gäller anställdas personuppgifter. Samtycke bör således vara en ”sista utväg” som kan övervägas när inga andra alternativ finns.

Behandling av särskilda kategorier av personuppgifter om anställda

Det är vanligt förekommande att arbetsgivare behandlar särskilda kategorier av personuppgifter (känsliga personuppgifter) om anställda, till exempel uppgift om hälsa i samband med sjukskrivning och utbetalning av sjuklön, eller uppgift om fackligt medlemskap för att uppfylla informations- och förhandlingsplikt enligt MBL.

Typiskt sett innebär ovanstående exempel inga större rättsliga problem, eftersom en arbetsgivare för behandlingen normalt sett kan förlita sig på det ovannämnda undantaget i artikel 9.2 i GDPR, som innebär att en personuppgiftsansvarig får behandla känsliga personuppgifter om det är nödvändigt för att ”*fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten*”. Det är dock, som nämnts ovan, viktigt att i varje enskilt fall göra en bedömning om behandlingen faktiskt är nödvändig för att uppfylla en skyldighet (eller utöva en rättighet) inom arbetsrätten. Vår erfarenhet är att arbetsgivare i många fall i praktiken tolkar (eller vill tolka) det aktuella undantaget i artikel 9.2 i GDPR alltför generöst för att undvika att en behandling av känsliga personuppgifter annars skulle vara otillåten.

Vi får förhållandevis ofta frågan om det är möjligt att behandla känsliga personuppgifter om en anställd i samband med tvist med den anställde eller berörda fackliga organisationer. Som tur är finns det ett undantag i artikel 9.2 (f) i GDPR som anger att det är tillåtet att behandla känsliga personuppgifter om det är nödvändigt för att hantera och bemöta rättsliga krav. Detta undantag är typiskt sett tillämpligt i en arbetsrättslig tvist.

Den omständigheten att arbetsgivare normalt behandlar känsliga personuppgifter om sina anställda innebär också att arbetsgivaren måste säkerställa att dessa uppgifter omfattas av särskilt skydd enligt artikel 32 i GDPR. IMY:s tillsynspraxis (se till exempel IMY:s tillsynsbeslut mot Region Uppsala, den 26 januari 2022, diarienummer DI-2019-9457) avseende kryptering av e-postmeddelanden som innehåller känsliga personuppgifter och krav på multifaktorautentisering när sådana uppgifter tillgängliggörs via internet, till exempel via olika portaler, har således betydelse även för behandling av anställdas känsliga personuppgifter.

I praktiken bör således arbetsgivare undvika att exempelvis läkarintyg som styrker sjukfrånvaro skickas per e-post eller att endast användarnamn och lösenord krävs för att logga in i tidredovisningssystemet för att registrera sjukfrånvaro. Vår erfarenhet är dock att lönehanteringssystem, som inte sällan erbjuder möjlighet för anställda att logga in i systemen för tidrapportering över internet, numera i större utsträckning har stöd för inloggning med hjälp av e-legitimation (BankID eller

motsvarande). Det gäller dock att se till att sådan inloggning också är tvingande för de anställda.

Konsekvensbedömning vid behandling av anställdas personuppgifter

Om en behandling (eller en serie behandlingar) av personuppgifter sannolikt leder till en hög integritetsrisk ska den personuppgiftsansvarige först genomföra en konsekvensbedömning enligt artikel 35 i GDPR. Om en konsekvensbedömning utvisar att det fortfarande föreligger en hög risk för berörda individers integritet – trots avhjälpande och riskmitigerande åtgärder – måste den personuppgiftsansvarige begära förhandssamråd med berörd tillsynsmyndighet enligt artikel 36 i GDPR.

Som vägledning vid en bedömning om det föreligger ett krav på att genomföra en konsekvensbedömning har IMY i enlighet med artikel 35.4 i GDPR publicerat en förteckning över när en konsekvensbedömning ska göras. Förteckningen listar nio kriterier och anger att om en behandling (eller en serie behandlingar) uppfyller minst två kriterier ska en konsekvensbedömning göras.

Skälet till att vi tar upp detta krav i detta sammanhang är att ett av de nio kriterierna rör om behandlingen avser personer som av något skäl befinner sig i ett underläge eller i en beroendeställning och därför är sårbara, till exempel anställda. Tilläggas kan också att det av IMY:s vägledning om behandling av personuppgifter i arbetslivet framgår att IMY anser att jobbsökande också befinner sig i motsvarande underläge.

Det betyder således att ett av nio kriterier *automatiskt* är uppfyllt vid behandling av anställdas personuppgifter, varvid det endast krävs ett ytterligare kriterium för att behandlingen ska omfattas av ett krav på genomförande av en konsekvensbedömning. I praktiken innebär det att kontroll- och övervakningsåtgärder, såsom övervakning av IT-system och kamerabevakning på arbetsplatsen, som en arbetsgivare vill genomföra normalt omfattas av ett krav på konsekvensbedömning. Det kan även röra sig om införandet av så kallade visselblåsarsystem enligt reglerna om rapporteringskanaler i lagen (2021:890) om skydd för personer som rapporterar om missförhållanden (visselblåsarlagen).

Innan en ny behandling av anställdas personuppgifter genomförs bör således arbetsgivaren överväga om behandlingen omfattas av kravet på en konsekvensbedömning. Vår rekommendation är att arbetsgivare i vart fall bör göra en enklare riskbedömning – inom ramen för en rutin för hantering av nya och förändrade personuppgiftsbehandlingar – av *varje* ny behandling av anställdas personuppgifter för att bland annat ta ställning till om behandlingen omfattas av kravet på en konsekvens-

bedömning. På så sätt säkerställs ett systematiskt dataskyddsarbete i förhållande till nya eller förändrade personuppgiftsbehandlingar som rör anställdas personuppgifter.

En konsekvensbedömning kan även användas som ett bra underlag inom ramen för eventuella förhandlingar med berörda fackliga organisationer avseende den tilltänkta behandlingen för att – utöver att uppfylla kraven i GDPR – visa att arbetsgivaren tar berörda anställdas integritetsskydd på allvar. Tilläggas ska också att inom ramen för en konsekvensbedömning ska berörda individers representanter rådfrågas, vilket – när det rör sig om anställdas personuppgifter – kan vara skyddsombud på arbetsplatsen eller berörda fackliga organisationer. I praktiken kan arbetsgivaren således uppfylla denna skyldighet samtidigt som eventuell förhandlingsskyldighet enligt MBL. Två flugor i en smäll.

Informations- och transparenskravet – ännu viktigare vid behandling av anställdas personuppgifter?

Informations- och transparenskravet i artikel 12–14 i GDPR gäller givetvis även vid behandling av anställdas personuppgifter. Vår erfarenhet är dock att verksamheter typiskt sett lägger mer tid och resurser på externa informationstexter för att uppfylla informations- och transparenskravet i GDPR i jämförelse med interna informationstexter. Ur ett praktiskt riskperspektiv kanske det framstår som rimligt, eftersom en extern informationstext – som normalt är publicerad på den externa webbplatsen – är tillgänglig för vem som helst att läsa, men vi vill ändå framhålla att den interna informationstexten är minst lika viktig. En bristfällig och illa utformad intern informationstext om behandling av anställdas personuppgifter kan – utöver bristande regelefterlevnad – medföra utmaningar i praktiken.

Bakgrunden till detta är att en informationstext om behandling av personuppgifter återger en ram för den behandling av personuppgifter som den personuppgiftsansvarige genomför och har kommunicerat till berörda registrerade individer. Det innebär bland annat att om den personuppgiftsansvarige till exempel vill samla in ytterligare kategorier av personuppgifter för ett befintligt ändamål, vidarebehandla redan insamlade personuppgifter för ett nytt ändamål eller dela personuppgifter med en ny mottagare måste – utöver att en laglighetsanalys först måste genomföras – informationstexten uppdateras för att täcka den nya eller förändrade personuppgiftsbehandlingen. Den uppdaterade informationstexten måste sedan kommuniceras på lämpligt sätt till berörda individer *innan* behandlingen genomförs (jämför bestämmelserna i artikel 13.3 respektive artikel 14.4 i GDPR). Det är därför viktigt att säker-

ställa att det finns interna rutiner på plats inom ramen för verksamheten för att säkerställa förändringshantering av informationstexter.

Vår erfarenhet är att en bristfällig informationstext om behandling av anställdas personuppgifter kan sätta käppar i hjulen i praktiken i anställningsärenden där arbetsgivaren misstänker att den anställde är illojal eller har begått oegentligheter. I sådant fall genomför arbetsgivaren normalt en utredning och vill inom ramen för en sådan utredning samla in och vidarebehandla ett stort antal personuppgifter om den anställde för att bekräfta misstankarna. Det är, enligt vår uppfattning, inte ovanligt att arbetsgivarens informationstext inte uppfyller (det högt ställda) informations- och transparenskravet och inte heller täcker den aktuella behandlingen. Arbetsgivaren ställs då normalt inför problematiken och den otacksamma situationen att välja mellan att uppfylla informations- och transparenskravet genom att göra nödvändiga uppdateringar av den interna informationstexten och kommunicera till den berörda anställde och samtidigt potentiellt äventyra sin utredning eller – potentiellt i strid med informations- och transparenskravet – avvakta med att lämna information till dess att utredningen färdigställts. Denna situation hade inte uppstått om arbetsgivaren noga utformat sin interna informationstext från början, men det är så klart lätt att vara efterklok.

Det förtjänar därför att sägas i sammanhanget att det är svårt att skriva en informationstext som både uppfyller informations- och transparenskravet (även om tillsynspraxis och vägledningar numera har förtydligat kraven något) och samtidigt täcker alla möjliga tänkbara scenarion som kan uppstå inom ramen för ett anställningsförhållande. Det är därför viktigt att ha rätt strategier och principer för utformning av informationstexter som täcker de vanligast förekommande situationerna som inbegriper behandling av anställdas personuppgifter, särskilt de situationer som till sin natur kan vara känsliga eller jobbiga. Tilläggas kan att vi brukar tillämpa som en handlingsregel vid utformning av informationstexter att ju känsligare en behandling av personuppgifter är desto tydligare måste den anges i en informationstext. Denna handlingsregel gör sig särskilt gällande när det rör sig om behandling av anställdas personuppgifter. Med det sagt övergår vi nu till några praktiska scenarion.

3. Några praktiska scenarion

Nedan redogör vi från några praktiska scenarion för att illustrera tillämpningen av dataskyddsregler i förhållande till behandling av anställdas personuppgifter, men också vilken betydelse uppfyllande av krav

enligt arbetsrättsliga regler kan ha för den aktuella behandlingen av personuppgifter. Samtliga scenarion nedan är fiktiva, men vi har hämtat inspiration från verkligheten. Det är vidare inom ramen för denna artikel inte möjligt att uttömmande analysera samtliga rättsliga krav ur ett dataskyddsperspektiv i förhållande till varje scenario. Se därför våra kommentarer och slutsatser till respektive scenario bara som en utgångspunkt för din egen bedömning av likartade scenarion.

Genomförandet av medarbetarundersökning för att kartlägga medarbetares levnadsvanor och främja arbetet med mångfald och jämställdhet på arbetsplatsen

Spelföretaget Bitar Spelproduktion tar mångfald och jämställdhet på stort allvar. Som ett led i företagets mångfalds- och jämställdhetsarbete planerar HR-avdelningen att genomföra en medarbetarundersökning. Syftet med medarbetarundersökningen är att kartlägga samtliga anställdas levnadsvanor. HR-chefen Lisa Johansson tänker att det skulle ge ett bra underlag för att kunna göra eventuella nödvändiga anpassningar av arbetsmiljön. Det är viktigt att alla medarbetare känner sig välkomna och inkluderade på arbetsplatsen, menar Lisa Johansson. Dessutom följer det av diskrimineringslagen att en arbetsgivare måste undersöka förhållandena på arbetsplatsen för att motverka diskriminering.

Spelföretaget tar hjälp av en extern leverantör specialiserad på enkätundersökningar för att genomföra medarbetarundersökningen. Leverantören utlovar att undersökningen genomförs anonymt genom att alla svar sammanställs och presenteras i en aggregerad rapport för bolaget. Lisa Johansson har dock själv bestämt vilka frågor som ska ställas. Bland annat innehåller undersökningen frågor om medarbetaren tränar regelbundet, om medarbetaren har någon familj eller inte, och om medarbetaren föredrar någon viss könsidentitet. För att samla in så bra svar så möjligt innehåller svarsformuläret fritextfält. Det är viktigt att de anställda får möjlighet att motivera sina svar, menar hon.

Lisa Johansson inser att det kan röra sig om känsliga frågor, men syftet är ju beaktansvärt och dessutom tar företaget sina skyldigheter enligt diskrimineringslagen på allvar. Därtill, och icke desto mindre, lämnar medarbetaren sitt samtycke när medarbetaren fyller i undersökningen. Det har Lisa Johansson sett till, efter att ha konsulterat sin arbetsrättsjurist. Då kan det ju rimligen inte vara några problem?

När företaget skickar ut enkäten blir inte responsen som Lisa Johansson hade förväntat sig. Vissa anställda besvarar enkäten, men flera anställda menar att arbetsgivaren inte har något att göra med deras privatliv och vägrar fylla i enkäten. Vad skulle Bitar Spelproduktion och Lisa

Johansson ha tänkt på ur ett dataskyddsperspektiv innan undersökningen genomfördes?

Den första frågan är vem som är personuppgiftsansvarig för behandlingen av personuppgifter som undersökningen medför. Den andra frågan är, om spelföretaget anses vara personuppgiftsansvarig, om insamlingen och behandlingen är tillåten. I detta avseende är det relevant att ifrågasätta om insamlingen och behandlingen är proportionerlig i förhållande till ändamålet med undersökningen och om det finns någon rättslig grund för behandlingen, samt – om det bedöms att känsliga personuppgifter behandlas – om det finns något tillämpligt undantag för att behandla känsliga personuppgifter. Nedan kommenterar vi samtliga dessa frågeställningar.

Men innan vi kommer in på dessa frågeställningar kanske den som läser noggrant noterade skrivningen att leverantören som spelföretaget anlitar i scenariot menar att undersökningen genomförs anonymt. I detta avseende kan det konstateras att även om spelföretaget endast får del av en aggregerad rapport kommer leverantören att behandla personuppgifter om spelföretagets anställda när de lämnar sina svar på undersökningen. Detta eftersom det normalt är tekniskt möjligt att koppla ihop svaren med den anställde som lämnat svaret. Dessutom kan det konstateras att undersökningen innehåller fritextfält som i sig kan innehålla (och troligen kommer att innehålla) personuppgifter. Det är därför en högst rimlig utgångspunkt att både spelföretaget och leverantören kommer att behandla personuppgifter i samband med genomförandet av undersökningen och att reglerna i GDPR är tillämpliga på behandlingen.

Vad gäller då den första frågan om *personuppgiftsansvar* kan det konstateras att arbetsgivarpresumtionen indikerar att spelföretaget är personuppgiftsansvarigt för behandlingen av de anställdas personuppgifter i samband med genomförandet av undersökningen. Det finns inget som tydligt antyder att den externa leverantören skulle utöva något bestämmande inflytande och kontroll över några nödvändiga faktorer för bestämmandet av personuppgiftsansvaret, såsom vilka uppgifter som samlas in och varför. Tvärtom är det tydligt att det är HR-chefen som för företagets räkning har bestämt vilka frågor som ska ställas och därigenom vilka uppgifter som ska samlas in och varför. Bedömningen är därför – föga förvånande – att det är spelföretaget som är (ensamt) personuppgiftsansvarig för behandlingen. Det betyder också att leverantören är ett personuppgiftsbiträde i förhållande till spelföretaget när leverantören behandlar personuppgifter på uppdrag av spelföretaget i samband med undersökningen.

I praktiken är det mycket viktigt att göra en noggrann bedömning av de berörda aktörernas ansvarsroller enligt GDPR. Om leverantören hade utövat ett visst bestämmande inflytande över undersökningen, till exempel genom att föreslå vissa frågeställningar är det sannolikt att ett gemensamt personuppgiftsansvar hade uppstått mellan leverantören och spelföretaget som arbetsgivare. Till synes små skillnader i de faktiska omständigheterna kan således påverka ansvarsanalysen. Djävulen finns i detaljerna som man säger.

Baserat på beskrivningen av scenariot är det dock oklart om det finns ett personuppgiftsbiträdesavtal på plats mellan spelföretaget och leverantören i enlighet med artikel 28.4 i GDPR, men vi får här utgå från att så är fallet. Det är också oklart om spelföretaget genomförde någon riskbedömning av leverantören ur ett dataskyddsperspektiv för att säkerställa att leverantören kan lämna tillräckliga garantier för att – förenklat uttryckt – skydda de anställdas personuppgifter på ett tillräckligt sätt. Med tanke på vad leverantören uppgivit om anonym insamling får vi nog anta att spelföretaget missade detta, men det påverkar inte frågan om behandlingen i sig är tillåten eller inte. Vi får också inom ramen för denna analys anta att leverantören kommer att behandla uppgifterna inom EU/EES-området och därmed att inga tredjelandsöverföringar kommer att ske.

Beträffande den andra frågan om insamlingen och behandlingen är *tillåten* är det korta svaret högst sannolikt nekande. För det första kan det konstateras att även om ändamålet är beaktansvärt (förbättra och skapa bättre förutsättningar för mångfald och jämlikhet på arbetsplatsen) och sannolikt berättigat enligt principen om ändamålsbegränsning är det tveksamt om insamlingen är förenlig med uppgiftsminimeringsprincipen och proportionerlig i förhållande till syftet med behandlingen (jämför ingresspunkt 39 i GDPR). Detta särskilt mot bakgrund av att diskrimineringslagens krav på aktiva åtgärder för att undersöka om det finns risker för diskriminering etc. *inte*, enligt vår uppfattning, innebär en skyldighet för arbetsgivaren att samla in information om de anställdas levnadsvanor på individnivå. Det finns sannolikt mindre integritetskränkande – eller mer integritetsvänliga – sätt att uppfylla detta krav. Dessutom framgår det av bakgrundsbeskrivningen att svarsformuläret innehåller fritextfält. Det finns således en betydande risk för att fler uppgifter än vad som är nödvändigt samlas in enbart av denna anledning. Vår bedömning är därför att det är troligt att behandlingen strider mot principerna för behandling av personuppgifter i artikel 5 i GDPR och därmed är otillåten.

Tilläggas ska också att det vår uppfattning att IMY i sin tillsynspraxis i många fall konstaterar att en behandling är otillåten redan vid en

bedömning av behandlingens förenlighet med principerna om behandling av personuppgifter i artikel 5 i GDPR. Se till exempel det första tillsynsbeslutet (den 20 augusti 2019, diarienummer DI-2019-2221) där dåvarande Datainspektionen påförde en sanktionsavgift enligt GDPR. Beslutet rörde gymnasienämnden i Skellefteå kommun som infört – förvisso som ett test – ansiktsigenkänning för närvarokontroll av elever. Intressant nog var den fråga som främst uppmärksammades i förhållande till beslutet om elevernas samtycke till behandlingen var giltiga, men den frågan saknar – strikt sett – betydelse när behandlingen redan bedömdes vara otillåten, då den stod i strid med principerna i artikel 5 i GDPR. Det fanns, enligt IMY, mer integritetsvänliga sätt att genomföra närvarokontroll av eleverna på.

Av pedagogiska skäl kommenterar vi ändå i det följande även frågan om rättslig grund för behandlingen av personuppgifter i samband med undersökningen. Av bakgrunden framgår att HR-chefen sett till att den anställde lämnar sitt samtycke – som det får förstås, även om det inte är helt klart – till behandlingen av personuppgifter genom att delta i undersökningen. Ett samtycke som rättslig grund är högst sannolikt inte giltigt i detta fall, eftersom det inte kan anses vara frivilligt lämnat när arbetsgivaren begär att den anställde ska delta i undersökningen. Det framgår inte av beskrivningen om deltagandet i undersökningen var genuint frivilligt, men sammanhanget talar för att så inte var fallet, även om den anställde ”samtycker” till deltagandet.

Spelföretaget kan inte heller, enligt vår mening, förlita sig på rättslig förpliktelse enligt artikel 6.1 (c) i GDPR som rättslig grund av det skäl som vi har angivit ovan, det vill säga att det inte finns någon rättslig skyldighet för en arbetsgivare att kartlägga de anställdas levnadsvanor och personliga förhållanden på individnivå enligt diskrimineringslagen.

Den enda tänkbara rättsliga grunden i detta fall är spelföretagets berättigade intresse av att genomföra undersökningen inom ramen för en intresseavvägning enligt artikel 6.1 (f) i GDPR, men det är enligt vår uppfattning (högst) tveksamt om en sådan intresseavvägning skulle falla ut till spelföretagets förmån, särskilt mot bakgrund av uppgifternas känslighet. Eftersom undersökningen inte framstår som frivillig får också, enligt vår uppfattning, den anställdes ”samtycke” begränsad betydelse inom ramen för en intresseavvägning. Om undersökningen *faktiskt* var frivillig och den anställde *medgav* deltagandet skulle emellertid förutsättningarna för spelföretaget att kunna förlita sig på en intresseavvägning som rättslig grund i detta fall ha varit väsentligt bättre.

Därutöver kan det konstateras att uppgift om en anställdes könsidentitet sannolikt utgör en uppgift om sexuell läggning, som är en känslig personuppgift enligt artikel 9 i GDPR. Eventuellt kan uppgifter

om den anställdes familj också utgöra indirekta känsliga personuppgifter beroende på vad den anställde svarar på frågan. I sammanhanget kan det noteras att EU-domstolen i en dom (mål *Vyriausioji tarnybinės etikos komisija*, C-184/20) ansett att uppgift om relation kan utgöra en indirekt uppgift om sexuell läggning och således utgöra en känslig personuppgift.

EU-domstolens bedömning i domen har för övrigt också betydelse för så kallade anhöriglistor, som är vanligt förekommande att arbetsgivare sparar, om en sådan lista innehåller information om typ av relation. Rekommendationen är således att inte spara uppgift om typ av relation utan bara registrera namn och kontaktuppgifter till den person som den anställde uppgivit som anhörig.

För att spelbolaget i detta fall ska kunna behandla känsliga personuppgifter krävs således ett tillämpligt undantag i artikel 9.2 i GDPR. Eftersom bolaget inte kan förlita sig på de anställdas samtycke till behandlingen och då det inte finns någon rättslig skyldighet enligt diskrimineringslagen att samla in de aktuella uppgifterna har vi i detta fall mycket svårt att se att det finns ett tillämpligt undantag. Även av denna anledning skulle således behandlingen vara otillåten.

Scenariot aktualiserar även andra frågeställningar ur ett dataskyddsperspektiv som vi inte har berört ovan och som vi inte har utrymme att närmare analysera inom ramen för denna artikel, men som ändå förtjänar att nämnas kort. Dessa frågeställningar inkluderar till exempel om spelbolaget har uppfyllt informations- och transparenskravet i GDPR i detta fall (täcker spelbolagets information om behandling av anställdas personuppgifter den aktuella behandlingen?), vilka tekniska och organisatoriska åtgärder som har vidtagits för att skydda de anställdas personuppgifter enligt artikel 32 i GDPR, hur tjänsten för att genomföra enkätundersökningar förhåller sig till principerna om inbyggt dataskydd och dataskydd som standard enligt artikel 25 i GDPR (särskilt när formuläret innehåller fritextfält), samt om behandlingen kräver en konsekvensbedömning enligt artikel 35 i GDPR (troligen eftersom känsliga personuppgifter om anställda skulle behandlas). Låt oss i stället gå till nästa praktiska scenario.

GPS-spårningen av servicebilarna

Elfirman Karlssons & Partners verksamhet expanderar och firman har därför införskaffat flera nya servicebilar som firmans elektriker använder i tjänsten. Eftersom det vore bra att ha koll på var elektrikerna befinner sig har ägaren Linus Karlsson installerat GPS-spårning i samtliga servicebilar. Då kan vi både se till att elektrikerna gör vad de ska på dagarna,

men det skulle också underlätta planeringen av deras körscheman mellan olika uppdrag resonerar Linus Karlsson. Han inser dock att det kan vara lite känsligt med GPS-spårning och han har därför varken informerat de anställda eller informerat facket om detta. Det är enklast så, tänker han. Dessutom tillhör servicebilarna firman och utgör arbetsverktyg, konstaterar han för sig själv. Då borde det ligga inom ramen för firmans bestämmanderätt att ta reda på var bilarna håller hus, tänker han.

Mycket riktigt visade det sig vara en bra idé att installera GPS-tekniken i servicebilarna. I samband med sina dagliga genomgångar av servicebilarnas förflyttningar har Linus Karlsson fattat misstanke om att en av elektrikerna fuskar med arbetstiden genom att ta mycket längre raster än vad som följer av anställningsavtalet och personalhandboken. Efter det att Linus Karlsson konfronterat elektrikern med sina misstankar reagerar den fackliga organisationen. Facket påstår nu att han brutit mot dataskyddsregler och att firman dessutom skulle ha förhandlat med facket innan han installerade GPS-tekniken i servicebilarna. Vad skulle elfirman och Linus Karlsson ha tänkt på ur ett dataskyddsperspektiv innan han installerade GPS-tekniken i bilarna?

Den huvudsakliga frågan i scenariot är om behandlingen av personuppgifter som GPS-spårningen av servicebilarna innebär är tillåten. Vi återkommer till denna fråga strax. Även i detta scenario uppkommer frågan om GPS-spårningen i servicebilarna faktiskt utgör en behandling av personuppgifter som rör elfirmans anställda. Vi får dock utgå från att det är möjligt att, i vart fall indirekt, koppla en servicebil till en viss anställd, till exempel genom tjänstgöringslistor eller om de anställda särskilt tilldelats vissa servicebilar. Detta är tillräckligt för att servicebilens position ska utgöra en personuppgift om den anställde som använder servicebilen i tjänsten. Det är därför en rimlig utgångspunkt att GPS-spårningen i servicebilarna skulle utgöra en behandling av elfirmans anställdas personuppgifter.

Vad gäller då frågan om behandlingens tillåtlighet kan det inledningsvis konstateras att elfirman installerat GPS-spårningen i servicebilarna för två olika ändamål, *dels* för att kontrollera var de anställda är när de utför sina uppdrag, *dels* för att planera elektrikernas körscheman. Vidare framgår av scenariot att elfirman också använder positioneringsinformationen från en av servicebilarna för att utreda en misstanke om att en av de anställda fuskar med arbetstiden, vilket får anses vara ett annat ändamål än att kontrollera var de anställda är när de utför sina uppdrag. En laglighetsanalys måste således genomföras i förhållande till respektive behandling av positioneringsinformationen för respektive ändamål.

I sammanhanget förtjänar att sägas att i praktiken noterar vi ofta att arbetsgivare missar att en laglighetsanalys måste genomföras för respektive identifierad behandling av personuppgifter. Det är enkelt att tro att en bedömning enbart kan göras i förhållande till ett system, en tjänst eller – som i detta fall – användningen av en viss teknisk lösning för spårning. Men en laglighetsanalys ur ett dataskyddsperspektiv måste således genomföras i förhållande till respektive ändamål som elfirman använder GPS-spårningen för.

Principerna för behandling av personuppgifter innebär i förhållande till kontrollåtgärder och övervakning bland annat att ändamålet med behandlingen, som kontrollerna eller övervakningen innebär, måste vara *sakligt motiverat* i den specifika verksamheten. Kontrollerna eller övervakning ska med andra ord ske för ett berättigat ändamål enligt principen om ändamålsbegränsning. Därutöver får inte behandlingen vara för omfattande eller närgången med hänsyn till ändamålet mot bakgrund av principen om uppgiftsminimering. Detta betyder att arbetsgivaren i det enskilda fallet måste kunna bevisa att ändamålet inte kan uppnås på ett annat sätt genom mindre integritetskränkande sätt. Går det inte att bevisa är behandlingen som övervakningen eller kontrollerna innebär oproportionerlig och således i strid med principerna för behandling av personuppgifter i GDPR.

Av IMY:s vägledning om kontrollåtgärder och övervakning följer att det, som huvudregel, inte är tillåtet för en arbetsgivare att använda ett IT-system för att i realtid eller på annat sätt regelmässigt övervaka hur de anställda utför sina arbetsuppgifter eller när de tar raster. I linje med detta anger IMY också i sin vägledning att det normalt inte är tillåtet att använda positioneringssystem för att kontrollera hur länge den anställda arbetar eller tar raster.

Mot denna bakgrund kan det konstateras att elfirmans användning av GPS-spårningen för att kontrollera var de anställda är när de utför sina uppdrag sannolikt står i strid med principerna för behandling av personuppgifter och således redan av denna anledning är otillåten.

Vad gäller användningen av GPS-spårningen för att planera elektrikernas körscheman kan det konstateras att detta bör vara ett berättigat syfte för en elfirma som genomför uppdrag på olika platser. IMY anger i sin vägledning om positioneringssystem som exempel på berättigade ändamål fördelning av resurser respektive logistik, vilket är ändamål som får anses vara snarlika med ändamålet planering av körscheman. Elfirman måste dock säkerställa att behandlingen av positioneringsinformationen för att planera körscheman inte sker på ett alltför närgånget sätt. Det betyder bland annat att om elfirman kan använda sig av aggregerade uppgifter för att uppfylla ändamålet så ska inte uppgifter

på individnivå användas. Baserat på bakgrundsbeskrivningen är det inte helt klart hur elfirman har tänkt att använda positioneringsinformationen för att planera körscheman, men vi får här utgå från att användningen av positioneringsinformationen sker på en lämplig nivå.

Beträffande användningen av positioneringsinformation för att utreda misstanken om att en av de anställda fuskar med arbetstiden kan det konstateras att detta enligt IMY:s vägledning kan vara ett berättigat ändamål när det finns en konkret misstanke om att den anställde på ett allvarligt sätt missbrukar arbetsgivarens förtroende. Av bakgrundsbeskrivningen synes dock framgå att uppgifterna inte samlas in för detta ändamål, utan snarare att elfirman vill *vidarebehandla* uppgifterna som samlats in för de två ursprungliga ändamålen för detta nya ändamål.

Frågan uppstår då om denna vidarebehandling skulle vara förenlig med principen om ändamålsbegränsning. Av principen om ändamålsbegränsning framgår att insamlade personuppgifter inte får vidarebehandlas för ett nytt ändamål som – något förenklat – är oförenligt med de ursprungliga ändamålen. Frågan är således om de anställda i detta fall typiskt och objektivt sett kan förvänta sig att arbetsgivaren behandlar positioneringsinformationen för att i ett enskilt fall utreda en konkret misstanke om fusk med arbetstiden. Som nämnts har IMY i sin tillsynspraxis varit relativt generös i förhållande till denna oförenlighetsprövning vid arbetsgivares behandling av personuppgifter inom ramen för anställningsförhållandet. Det är således en rimlig utgångspunkt i detta fall att en anställd typiskt och objektivt faktiskt kan räkna med att en arbetsgivare använder insamlad positioneringsinformation (eller annan logginformation) i ett konkret fall för att utreda misstanke om fusk. Vår uppfattning är således att det finns goda rättsliga förutsättningar för att konstatera att vidarebehandlingen skulle vara tillåten enligt principen om ändamålsbegränsning.

Nästa frågeställning är om det finns någon rättslig grund för *dels* behandlingen för att använda positioneringsinformationen för planering av körscheman, *dels* för vidarebehandlingen av positioneringsinformationen för att utreda misstanken om fusk med arbetstiden.

Vad gäller *vidarebehandlingen* av positioneringsinformationen för att utreda misstanken om fusk med arbetstiden kan det konstateras att det av ingresspunkt 50 till GDPR följer att en vidarebehandling som uppfyller principen om ändamålsbegränsning inte kräver en separat rättslig grund, utan kan ske med stöd av samma rättsliga grund som behandlingen av uppgifterna för det ursprungliga ändamålet. Det är en nyhet i GDPR som ibland kan ge upphov till en del huvudbry. Som exempel är oklart om det även gäller undantag från förbudet att behandla känsliga personuppgifter i artikel 9 i GDPR, vilket får betydelse när känsliga per-

sonuppgifter vidarebehandlas. Sannolikt krävs att det finns ett tillämpligt undantag i artikel 9 i GDPR och att ingresspunkt 50 i GDPR endast täcker rättslig grund för *behandlingen* i artikel 6 i GDPR. Scenariot inbegripet dock – som tur är – inte behandling av känsliga personuppgifter så vi kan lämna denna fråga så länge.

Vad gäller då den rättsliga grunden för behandlingen av positioneringsinformationen för det ursprungliga ändamålet att planera körscheman är den rättsliga grund som i detta fall skulle vara tillämplig – mot bakgrund av att det rör sig om en privat arbetsgivare – elfirmans berättigade intresse inom ramen för en intresseavvägning av att genomföra behandlingen enligt artikel 6.1 (f) i GDPR. Elfirman skulle dock behöva göra en noggrann intresseavvägning i detta fall och överväga vilka åtgärder som kan vidtas för att minska integritetsriskerna. Vi får här nöja oss med att konstatera att det troligen finns förutsättningar för elfirman att förlita sig på sitt berättigade intresse som rättslig grund för behandlingen av positioneringsinformationen för att planera körscheman. I sådant fall skulle även vidarebehandlingen av positioneringsinformationen för att utreda misstanke om fusk med arbetstiden vara tillåten och kunna ske med stöd av samma rättsliga grund.

I sammanhanget ska tilläggas att det är sannolikt att behandlingen av positioneringsinformation i detta fall också skulle omfattas av ett krav på att genomföra en konsekvensbedömning enligt artikel 35 i GDPR *innan* behandlingen påbörjas, särskilt eftersom det rör sig om anställda och positioneringsinformation, som utgör integritetskänsliga uppgifter. Elfirman skulle således ha upprättat en konsekvensbedömning innan elfirman installerade GPS-tekniken i servicebilarna. Inom ramen för konsekvensbedömningen skulle elfirman ha inhämtat synpunkter från berörda fackliga organisationer eller skyddsombudet på arbetsplatsen i egenskap av representanter för de anställda. Vår erfarenhet är att samråd med fackliga organisationer eller skyddsombud kan ge värdefullt underlag för ytterligare riskmitigerande åtgärder och för bedömningen om arbetsgivaren kan förlita sig på sitt berättigade intresse av att genomföra behandlingen inom ramen för en intresseavvägning.

Det framgår inte av bakgrundsbeskrivningen om elfirman är bunden av kollektivavtal. Den omständigheten att den fackliga organisationen menar att frågan om införandet av GPS-spårningen i servicebilarna skulle ha förhandlats antyder i och för sig det. Om elfirman är bunden av kollektivavtal är det vår uppfattning att införandet av GPS-spårningen sannolikt skulle ha varit förhandlingspliktig. Konsekvensbedömningen skulle i sådant fall ha utgjort bra underlag för en sådan förhandling.

Scenariot aktualiserar ytterligare frågeställningar som måste övervägas, men som vi inte har utrymme att närmare beröra här, till exempel

säkerhet och skydd för positioneringsinformationen, inklusive lämplig behörighetsstyrning och åtkomstkontroller till systemet, samt frågan om hur elfirman bör uppfylla informations- och transparenskravet i GDPR (av bakgrundsbeskrivningen framgår att ingen information lämnats).

Det kan dock tilläggas att den omständigheten att ingen information lämnats om behandlingen inte i sig innebär att behandlingen blir otillåten, men om elfirman vill använda positioneringsinformationen i ett efterföljande anställningsärende – om det konstateras att den anställde faktiskt fuskat med arbetstiden – skulle det innebära en riskexponering i den meningen att den anställde (eller den fackliga organisationen för den anställdes räkning) skulle kunna framställa krav på skadestånd för brott mot informations- och transparenskravet i GDPR mot elfirman.

Linus Karlsson skulle nog – så här i efterhand – ha avstått från att installera GPS-tekniken i servicebilarna, i vart fall till dess att han tagit hjälp för att göra det på rätt sätt. Vår erfarenhet är dock att detta scenario i många fall återspeglar hur det kan gå till i verkligheten.

4. Slutord

Behandling av anställdas personuppgifter är alltid en aktuell fråga. I takt med att arbetsgivare vill införa nya tekniska lösningar, IT-system eller genomföra nya initiativ på arbetsplatsen blir det ännu viktigare att noga utreda de dataskyddsrättsliga frågorna som uppkommer. Men som våra praktiska scenarion illustrerar är det i praktiken ofta lättare sagt än gjort. Vår förhoppning är således att vi i denna artikel har givit några värdefulla praktiska tips och råd som kan underlätta din egen analys av om en viss behandling av anställdas personuppgifter uppfyller kraven i GDPR.