

A group of business professionals in a meeting, with a teal geometric overlay. The overlay consists of several overlapping hexagons and triangles in shades of teal and dark green, with thin gold lines connecting the vertices. The background shows a woman in a white top on the left, a man in a blue suit in the center, and a woman in a white shirt on the right, all smiling and engaged in conversation. A desk with a keyboard and papers is visible in the foreground.

Vägledning:

behandling av personuppgifter
enligt Dataskyddsförordningen

Datum för senaste uppdateringen: 1 februari 2020

Innehållsförteckning

1. INLEDANDE BESTÄMMELSER.....	5
1.1 BAKGRUND	5
1.2 SYFTE	5
1.3 TILLÄMPNINGSOMRÅDE OCH OMFATTNING	5
2. BEGREPP I VÄGLEDNINGEN	6
3. ALLMÄNT OM MEDLEMMARNAS TJÄNSTER	8
4. PERSONUPPGIFTSANSVARIG, PERSONUPPGIFTSBITRÄDE OCH TREDJE PART	8
4.1 INLEDNING	8
4.2 ALLMÄNT OM ROLLERNA	9
4.2.1 Personuppgiftsansvarig	9
4.2.2 Personuppgiftsbiträde.....	9
4.2.3 Tredje part	10
4.3 EXEMPELSITUATIONER	10
4.3.1 Rekrytering	10
4.3.2 Uthyrning	11
4.3.3 Omställning.....	12
5. LAGLIG GRUND	13
5.1 INLEDNING	13
5.2 SAMTYCKE	13
5.3 AVTAL	14
5.4 INTRESSEAVVÄGNING	15
5.5 RÄTTSLIG FÖRPLIKTELSE	15
5.6 MYNDIGHETSUTÖVNING OCH ALLMÄNT INTRESSE SAMT SKYDD AV GRUNDLÄGGANDE INTRESSE	16
5.6.1 <i>Behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.....</i>	<i>16</i>
5.6.2 <i>Behandling som är nödvändig för att skydda intressen av grundläggande betydelse.....</i>	<i>16</i>
6. REKRYTERINGSFRÅGOR.....	16
6.1 INLEDNING	16
6.2 REKRYTERING UTIFRÅN ANSÖKAN TILL ENSKILD TJÄNST	17
6.2.1 <i>Inledning</i>	<i>17</i>
6.2.2 <i>Laglig grund.....</i>	<i>17</i>
6.2.3 <i>Information till registrerade</i>	<i>17</i>
6.2.4 <i>Medlemsföretag som personuppgiftsbiträde</i>	<i>18</i>
6.3 REKRYTERINGSPLATTFORMAR	18
6.3.1 <i>Inledning</i>	<i>18</i>
6.3.2 <i>Laglig grund.....</i>	<i>18</i>
6.3.3 <i>Information till den registrerade</i>	<i>19</i>
6.3.4 <i>Medlemsföretag som personuppgiftsbiträde</i>	<i>19</i>
7. UTHYRINGSFRÅGOR	19
7.1 INLEDNING	19
7.2 GENERELLT ANGÅENDE UTHYRNING	20
7.2.1 <i>Laglig grund.....</i>	<i>20</i>
7.2.2 <i>Information till den anställda.....</i>	<i>20</i>
7.3 ANSTÄLLDA HOS UNDERLEVERANTÖRER	20
7.3.1 <i>Laglig grund.....</i>	<i>20</i>
7.3.2 <i>Medlemsföretag som personuppgiftsbiträde</i>	<i>20</i>
7.4 INDIVIDUELL PRESTATIONS MÄTNING	21
7.5 SYSTEM FÖR REKRYTERING OCH KOMPETENSDATABASER	21

8. OMSTÄLLNINGSFRÅGOR	21
8.1 INLEDNING	21
8.2 LAGLIG GRUND.....	22
8.3 SÄRSKILT OM ANALYSRESULTAT	22
9. SÄRSKILDA ÖVERGRIPANDE FRÅGOR	22
9.1 PERSONLIGHETS- OCH KOMPETENSTESTER	22
9.1.1 <i>Specifikt om personuppgiftsansvar</i>	22
9.1.2 <i>Laglig grund</i>	23
9.1.3 <i>Information till den registrerade</i>	23
9.2 REFERENSER	24
9.2.1 <i>Laglig grund</i>	24
9.2.2 <i>Information till den registrerade</i>	24
9.3 SEARCH	24
9.3.1 <i>Inledning</i>	24
9.3.2 <i>Laglig grund</i>	24
9.3.3 <i>Information till den registrerade</i>	25
9.4 BEHANDLING AV UPPGIFTER OM LAGÖVERTRÄDELSE	25
9.5 PERSONNUMMER OCH ANDRA NATIONELLA IDENTIFIKATIONSNUMMER	26
9.6 IDENTIFIERING AV ANVÄNDARE	27
9.7 REGISTER ÖVER EJ ÖNSKVÄRDA KANDIDATER	27
9.8 PERSONUPPGIFTER I OSTRUKTURERAT MATERIAL	27
9.9 KREDITUPPLYSNINGAR	27
9.9.1 <i>Inledning</i>	27
9.9.2 <i>Laglig grund</i>	27
9.9.3 <i>Information till den registrerade</i>	28
9.10 ANVÄNDA AV SOCIALA MEDIER.....	28
9.11 RESULTAT FRÅN DROG-, ALKOHOL- OCH ANDRA HÄLSOTESTER	29
9.12 SCREENING MOT SANKTIONSLISTOR	29
9.13 SÄRSKILT ANGÅENDE MEDLEMSFÖRETAG INOM SÄRSKILDA BRANSCHER	30
9.14 SÄKERHETSPRÖVNING ENLIGT SÄKERHETSSKYDDSLAGEN	30
9.14.1 <i>Inledning</i>	30
9.14.2 <i>Medlemsföretaget som personuppgiftsbiträde</i>	31
9.15 DATASKYDDSFÖRORDNINGEN OCH SPECIALLAGSTIFTNING	31
10. ENSKILDAS RÄTTIGHETER	32
10.1 ALLMÄNT	32
10.2 DATAPORTABILITET	32
10.3 REGISTERUTDRAG	32
10.4 RÄTT TILL RÄTTELSE, RADERING OCH BEGRÄNSNING	33
10.5 RÄTT ATT GÖRA INVÄNDNINGAR	34
10.6 IDENTIFIERING	34
11. SÄKERHET OCH SEKRETESS	34
11.1 ALLMÄNT	34
11.2 TEKNISKA SÄKERHETSÅTGÄRDER.....	34
11.2.1 <i>Privacy by design och privacy by default</i>	34
11.2.2 <i>Behörighetskontroll</i>	35
11.2.3 <i>Loggning</i>	35
11.2.4 <i>Åtkomstskydd</i>	35
11.2.5 <i>Brandvägg, VPN m.m.</i>	35
11.2.6 <i>Pseudonymisering och anonymisering</i>	35
11.3 ORGANISATORISKA SÄKERHETSÅTGÄRDER	36
11.3.1 <i>IT- och informationssäkerhetspolicy</i>	36
11.3.2 <i>Kontroll och avstämning</i>	36

11.3.3	<i>Incidenthantering</i>	36
11.3.4	<i>Utbildning</i>	36
12.	RIKTLINJER FÖR LAGRING OCH GALLRING AV PERSONUPPGIFTER	36
12.1	ALLMÄNT	36
12.2	UPPGIFTER OM KANDIDATER	37
12.3	UPPGIFTER OM KONSULTER OCH ANSTÄLLDA	38
12.4	UPPGIFTER OM KUNDER OCH LEVERANTÖRER.....	38
12.5	RADERING OCH GALLRING	39
13.	ÖVERFÖRING AV PERSONUPPGIFTER	39
13.1	ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE PART, TILL EXEMPEL KUNDER OCH MYNDIGHETER	39
13.2	ÖVERFÖRING AV PERSONUPPGIFTER TILL LEVERANTÖRER.....	39
13.3	TREDJELANDSÖVERFÖRINGAR	40
BILAGA 1 –	MATRIS ÖVER LAGLIG GRUND	41

Denna Vägledning är framtagen av Kompetensföretagen tillsammans med en referensgrupp med företrädare för vissa av Kompetensföretagens medlemsföretag. Innehållet i Vägledningen utgår ifrån reglerna i dataskyddsförordningen och baseras på rättsläget per den 31 december 2019 och ska ses som en översikt utifrån en tolkning av dataskyddsregler inom vissa områden. Kompetensföretagen ansvarar inte för handling eller underlåtenhet med anledning av vad som framgår av Vägledningen. Vägledningen ska således endast tillämpas som ett tolkningsunderlag och ska inte uppfattas som en uppmaning till viss handling eller underlåtenhet.

Lagstiftningen på dataskyddsområdet inbegriper dataskyddsförordningen, tillämplig svensk dataskyddslag och speciallagstiftning på dataskyddsområdet. Det faktum att Vägledningens bestämmelser följs undantar inte medlemsföretag från kraven enligt dataskyddsförordningen eller annan tillämplig lag. Vägledningen påverkar inte heller Datainspektionens befogenheter eller uppgifter.

Innehållet i Vägledningen utgör inte juridisk rådgivning och ersätter inte respektive medlemsföretags eget dataskyddsarbete.

Stockholm i februari 2020

Kompetensföretagen

1. INLEDANDE BESTÄMMELSER

1.1 Bakgrund

Kompetensföretagen och en referensgrupp med företrädare från vissa av organisationens medlemsföretag har utarbetat denna vägledning avseende behandling av personuppgifter ("**Vägledningen**") för att precisera hur medlemsföretagen i praktiken kan tillämpa dataskyddsförordningens bestämmelser avseende vissa frågor. Medlemsföretagen i branschen arbetar alltid aktivt för att nå samsyn i de många utmanande frågeställningar som vi ställs inför. I denna Vägledning presenteras Kompetensföretagens tolkning avseende tillämpningen av dataskyddslagstiftningen inom branschen.

1.2 Syfte

Det huvudsakliga syftet med Vägledningen är att underlätta för medlemsföretagens olika verksamhetsområden vid respektive medlemsföretags anpassning till gällande regelverk avseende dataskydd och behandling av personuppgifter. Därutöver ska medlemsföretagen kunna använda Vägledningen som ett verktyg i respektive verksamhet och i relationen med kunden, i frågor som rör dataskydd.

1.3 Tillämpningsområde och omfattning

Vägledningen är en del av de tjänster Kompetensföretagen erbjuder sina medlemsföretag, och kan tillämpas av alla medlemsföretag inom Kompetensföretagen. Vägledningen är inte bindande för medlemsföretag men kan tjäna som ett stöd i medlemsföretagens interna dataskyddsarbete.

Vägledningen reglerar endast den behandling av personuppgifter inom medlemsföretagens verksamheter som är hänförlig till verksamhetsområdena *rekrytering, uthyrning* och *omställning*. Vägledningen reglerar inte hur medlemsföretagen ska utforma och genomföra sitt eget dataskyddsarbete i övrigt. Vägledningen reglerar till exempel inte behandling av personuppgifter som avviker från de situationer som berörs i Vägledningen eller som är hänförlig till andra verksamhetsområden än de ovan nämnda. Exempelvis omfattar Vägledningen inte den interna hanteringen av personuppgifter avseende medlemsföretagens egna anställda, styrelsemedlemmar eller uppdragstagare som inte uthyrs eller på annat sätt direkt berörs av verksamhetsområdena ovan. Vägledningen är inte tillämplig på Kompetensföretagens hantering av personuppgifter, utan gäller för medlemsföretagens personuppgiftshantering.

Vägledningen är således inte uttömmande och redogör därför inte nödvändigtvis för alla krav och skyldigheter som medlemsföretagen kan omfattas av vid behandling av personuppgifter.

2. BEGREPP I VÄGLEDNINGEN

Nedan följer förklaringar av begrepp som återkommande förekommer i vägledningen.

Annan mottagare	En annan part som den personuppgiftsansvarige lämnar uppgifter till och som behandlar personuppgifter för sin egen räkning, till exempel Skatteverket.
Behandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.
Kompetensföretagen	Branschorganisation för företag med verksamhet inom bland annat uthyrning, omställning och rekrytering.
Medlemsföretag(en)	Företag som är medlem i Kompetensföretagen.
Omställning	Uppdrag som innebär att kund avser att säga upp eller har sagt upp en eller flera anställda alternativt av annan anledning önskar omställning eller förändring för anställd/-a, till exempel genom omplacering. Inom ramen för omställningsuppdraget ska medlemsföretaget bl.a. förse deltagaren med analys av förutsättningar för nytt arbete, utbildning och/eller coachning i syfte att finna för deltagaren nytt arbete inklusive att starta egen verksamhet eller på annat sätt göra deltagaren mer attraktiv på arbetsmarknaden. En omställningsprocess kan initieras direkt av kund eller genom att medlemsföretaget får ett uppdrag via anvisning från offentlig sektor till exempel Arbetsförmedling eller kommun.
Personuppgifter	Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Exempel på personuppgifter är namn, kontaktuppgifter, identifikationsnummer, lokaliseringsuppgifter, onlineidentifikatorer eller faktorer som är specifika för en persons fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Personuppgifter kan således vara uppgifter om en kunds inköp, beteende och intresseområden.
Personuppgiftsansvarig	Den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som en personuppgift avser.
Rekrytering	Uppdrag som innebär att kund avser att anställa en eller flera personer, kandidater, som kunden ger medlemsföretaget i uppdrag att välja ut och presentera för kunden. I uppdraget ingår inte att lämna ut uppgifter om kandidater, som inte presenteras av medlemsföretaget för kunden.
Search	Extern sökning i olika kanaler efter lämpliga kandidater för potentiell rekrytering utan på förhand givet tillstånd från kandidaten.

Tredje part	Någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar har befogenhet att behandla personuppgifter.
Underbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning på uppdrag av den personuppgiftsansvariges personuppgiftsbiträde, till exempel en underleverantör till personuppgiftsbiträdet.
Uthyrning	Uppdrag som innebär ett affärsmässigt och rättsligt förhållande mellan medlemsföretag och kund i vilket medlemsföretag mot ersättning ställer egenanställd personal eller personal från underleverantör (uthyrd person) till kundens förfogande för att utföra arbete som hör till kundens verksamhet under kundens kontroll och ledning. Med uppdrag avses den urvalsprocess av uthyrd person som sker vid personaluthyrning och därefter tillhandahållandet av uthyrd person

Övriga personuppgiftsrättsliga begrepp som används men inte definieras i Vägledningen ska ha samma innebörd som enligt definitionskatalogen i artikel 4 i dataskyddsförordningen.

3. ALLMÄNT OM MEDLEMMARNAS TJÄNSTER

Kompetensföretagens medlemsföretag har verksamhet inom bland annat tjänsteområdena rekrytering, uthyrning och omställning. Utförandet av respektive tjänst kan skilja sig åt från medlemsföretag till medlemsföretag samt över tiden. Vi noterar att det finns andra typer av tjänster, såsom Master/Managed Service Providers (MSP), Recruitment Process Outsourcing (RPO) och Vendor Management Systems (VMS).¹ Vi har dock valt att inte närmare behandla dessa tjänster här.

Ur ett dataskyddsperspektiv innebär tillhandahållandet av olika typer av tjänster att medlemsföretagen intar olika roller beroende på tjänstens karaktär och utförande, och att olika frågeställningar blir relevanta för olika typer av tjänster.

4. PERSONUPPGIFTSANSVARIG, PERSONUPPGIFTSBITRÄDE OCH TREDJE PART

4.1 Inledning

Syftet med ett personuppgiftsansvar är att fördela/allokera ansvar i avsikt att ge de registrerade ett fullgott skydd vid behandling av dennes personuppgifter. Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter (till ett personuppgiftsbiträde), men personuppgiftsansvaret kan aldrig överlåtas.

Medlemsföretagen kan, beroende på omständigheterna, gentemot kunder och leverantörer inta rollen som personuppgiftsansvarig, personuppgiftsbiträde eller tredje part. Olika regler gäller beroende på vilken roll medlemsföretagen intar. Nedan i punkt 4.3 beskrivs exempelsituationer då medlemsföretagen intar respektive roll inom ramen för tjänsteområdena rekrytering, uthyrning och omställning. Särskilda frågor som hänför sig specifikt till tjänsteområdena rekrytering, uthyrning och omställning samt en beskrivning av dessa områden återfinns under avsnitten 6, 7, och 8.

Relationen mellan personuppgiftsansvarig och personuppgiftsbiträde ska alltid regleras i ett så kallat personuppgiftsbiträdesavtal. Sådant avtal ingås inte med s.k. tredje part. Detta utesluter dock inte att medlemsföretagen behandlar motsvarande personuppgifter uteslutande för *eget* ändamål, vilket ju medför ett personuppgiftsansvar. Inget personuppgiftsbiträdesavtal ingås mellan två separata personuppgiftsansvariga när dessa behandlar motsvarande personuppgifter oberoende av varandra (var för sig).

I de exempelsituationer som följer nedan beskrivs som nämnt medlemsföretagens roller avseende personuppgiftsansvar. Det bör dock tilläggas att detta avser specifika exempelsituationer och att det i praktiken kan röra sig om mer komplexa bedömningar. Det är inte alltid all behandling inom ramen för ett uppdrag är hänförlig till en specifik exempelsituation utan gränserna, och därmed personuppgiftsansvaret, kan vara mer flytande. I sådana situationer bör medlemsföretagen särskilt beakta vikten av att bryta ner uppdragets olika komponenter och analysera varje behandling

¹ Jämför World Employment Confederations (WEC) riktlinjer om personuppgiftsansvariga och personuppgiftsbiträden som HR-tjänsteleverantörer. WEC är en medlemsorganisation för aktörer inom arbetsgivarsektorn världen över, deras europeiska verksamhet, som har tagit fram den aktuella vägledningen, representerar aktörer från 30 olika länder.

för sig varvid medlemsföretagen får bedöma vilken roll medlemsföretaget har avseende respektive behandling.

4.2 Allmänt om rollerna

4.2.1 Personuppgiftsansvarig

Medlemsföretaget är personuppgiftsansvarig när den bestämmer *ändamål* och *medel* med behandlingen. I praktiken är det den part som bestämmer *varför* behandlingen ska utföras och *hur* den ska gå till, d.v.s. den som faktiskt har och utövar kontroll över behandlingen som utförs. För att bedöma kontroll bör man bl.a. se till vem som (enligt lag eller avtal) har bestämmanderätten över en viss behandling. Vid svåra avvägningar kan medlemsföretagen, i tillägg till vad som anges ovan, genom en ändamålstolkning av regelverket, se till vilken ansvarsfördelning som framställer bäst skydd för de registrerade. Därutöver kan medlemsföretagen se till vem den registrerade rimligen skulle förvänta sig som ansvarig för behandlingen av dennes personuppgifter.

Ändamål handlar om varför det är nödvändigt att behandla personuppgifterna.

Medel avser såväl hur en behandling går till (vilka personuppgifter som behandlas och hur länge, samt i vilka system som uppgifterna behandlas) som vilka tekniska och organisatoriska åtgärder som omgärdar behandlingen.

Den personuppgiftsansvarige har det yttersta ansvaret för att principerna och skyldigheterna som uppställs i dataskyddsförordningen följs, vilket också ska kunna visas.

Om två eller flera gemensamt och i samråd bestämt att genomföra en viss behandling av personuppgifter, och därigenom gemensamt styr över behovet och ändamålet med behandlingen, kan parterna bedömas som gemensamt personuppgiftsansvariga. Detta gäller även om var och en har givits möjlighet att ensam bestämma över behandlingen. Det torde räcka att medlemsföretagen tillsammans med annan part (till exempel kunden) *kan* bestämma över ändamålen och medlen för behandlingen av personuppgifter för att ett gemensamt personuppgiftsansvar ska uppstå. Gemensamt personuppgiftsansvariga måste komma överens om vem som ansvarar för fullgörandet av de olika skyldigheterna och de registrerades rättigheter som uppställs i dataskyddsförordningen genom att träffa ett särskilt avtal.

4.2.2 Personuppgiftsbiträde

Medlemsföretag är personuppgiftsbiträde när medlemsföretaget behandlar personuppgifter för en personuppgiftsansvarigs räkning, det vill säga den part som bestämmer ändamålen och medlen med behandlingen som medlemsföretaget utför (se till exempel kundens rekryteringsprocess i punkt 4.3.1 nedan).

Ett medlemsföretag som behandlar personuppgifter i egenskap av personuppgiftsbiträde får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige och det personuppgiftsbiträdesavtal som den personuppgiftsansvarige är skyldig att ingå med medlemsföretaget. Ofta behöver även personuppgiftsbiträdet inhämta ett skriftligt tillstånd innan den anlitar en leverantör eller annan tredje part som behandlar de aktuella personuppgifterna.

Flera av de skyldigheter som faller på personuppgiftsansvarig åläggs också personuppgiftsbiträdet, till exempel krav på att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud.

4.2.3 Tredje part

Medlemsföretag är tredje part då ett medlemsföretag på något sätt är inblandad i behandlingen av personuppgifter utan att inta roll som personuppgiftsansvarig, personuppgiftsbiträde eller registrerad. En tredje part är aldrig behörig att behandla personuppgifterna ifråga, inom ramen för den aktuella behandlingen. Detta kan till exempel vara fallet då medlemsföretaget hyr ut personal till en kund, och medlemsföretaget inte utför någon behandling av personuppgifter (se till exempel punkt 4.3.2 nedan).

Som tredje part har medlemsföretaget inget legalt ansvar för den aktuella personuppgiftsbehandlingen och behöver inte uppfylla de krav som ställs på personuppgiftsansvariga och personuppgiftsbiträden enligt dataskyddsförordningen. Det här utesluter självklart inte att part, å sin sida, för eget ändamål utför behandling av motsvarande (likadana) personuppgifter, för vilka denne är personuppgiftsansvarig (s.k. *separat personuppgiftsansvar*).

4.3 Exempelsituationer

4.3.1 Rekrytering

Inom ramen för rekryteringsuppdrag (vars innebörd närmare beskrivs under punkt 6.1) kan medlemsföretagen använda sig av antingen sin egen eller kundens rekryteringsprocess.

Sker rekrytering istället på ett sätt som innebär att medlemsföretaget ställer en person till kundens förfogande (för att under kundens arbetsledning och ansvar utföra rekryteringsuppdraget) gäller istället vad som sägs avseende *uthyrning* i punkt 4.3.2 nedan.

Medlemsföretagets rekryteringsprocess

Då medlemsföretaget använder sig av en egenutvecklad rekryteringsmetod, som i sammanhanget får den innebörd att medlemsföretaget *bestämmer* vilka personuppgifter som ska samlas in, *varifrån* uppgifterna ska samlas in och *hur* behandlingen ska utföras i övrigt, intar medlemsföretaget en så pass självständig ställning att medlemsföretaget är personuppgiftsansvarig inom ramen för rekryteringsuppdraget. Kunden är personuppgiftsansvarig för behandling av alla personuppgifter som, inom ramen för uppdraget, mottas från medlemsföretaget. Kunden behandlar ju aldrig personuppgifter på uppdrag av medlemsföretaget, varför en biträdesrelation är utesluten.

Kundens rekryteringsprocess

Då medlemsföretaget istället använder sig av kundens rekryteringsprocess, där kunden har kontroll över behandlingen av personuppgifter, varpå personuppgifter lämnas från kunden till medlemsföretaget för till exempel bedömning och urval (på uppdrag av kund), intar medlemsföretaget rollen som personuppgiftsbiträde till kunden – som är personuppgiftsansvarig – för de uppgifter som mottas och behandlas för kundens räkning. I en sådan situation är det viktigt att ett personuppgiftsbiträdesavtal ingås mellan medlemsföretaget och kund, som innehåller tydliga instruktioner avseende hur medlemsföretaget får behandla personuppgifterna.

Medlemsföretagets personal arbetar hos kunden

Om medlemsföretagets personal som bistår vid rekrytering behandlar personuppgifter hos kunden under kundens arbetsledning och i kundens system, och personalen är

förhindrad och obehörig att dela personuppgifter med medlemsföretagen, samt medlemsföretagen inte har åtkomst till personuppgifterna på annat sätt, saknar medlemsföretagen all kontakt med personuppgiftsbehandlingen. Medlemsföretagen intar då rollen som *tredje part* (det vill säga medlemsföretaget är varken personuppgiftsansvarig eller personuppgiftsbiträde). Kunden är personuppgiftsansvarig för den behandling av personuppgifter som medlemsföretagens uthyrda arbetstagare utför under rekryteringsprocessen.

Andra situationer i en rekryteringsprocess

I vissa fall förekommer det att såväl kundens som medlemsföretagens respektive rekryteringsprocesser används parallellt. Kund respektive medlemsföretag ansvarar i en sådan situation för den personuppgiftsbehandling som respektive part själv utför, vilket innebär att parterna är separat personuppgiftsansvariga för sin egen respektive behandling. Å andra sidan lutar det senaste årets praxis allt mer mot att gemensamma processer också ska anses innefatta ett gemensamt personuppgiftsansvar, varför en bedömning i varje enskilt fall alltid måste göras.

4.3.2 *Uthyrning*

Inom ramen för uthyrningsuppdrag (vars innebörd närmare beskrivs under punkt 7.1) får uthyrd arbetstagare, när denne arbetar *på plats hos kunden*, i regel tillgång till gemensamma anläggningar på samma villkor som kundens egna anställda. Därutöver ansvarar kunden vanligtvis för inhyrd personal såsom för egen, anställd personal. I regel används kundens utrustning, IT-system och IT-miljö av den inhyrda personalen. Kunden ansvarar därför för inhyrd personals handlingar och underlåtelse samt ansvarar för deras säkerhet.

Personuppgifter i uppdraget

Då en uthyrd arbetstagare behandlar personuppgifter när denne arbetar på plats hos kunden, under ovan nämnda uthyrningsförhållande, och den uthyrde står under kundens ansvar och arbetsledning, är medlemsföretaget vanligtvis obehörig att behandla personuppgifterna och saknar helt tillgång till dessa (exempelvis genom att parterna har ingått sekretessavtal). Medlemsföretaget utför i en sådan situation *ingen behandling* av de personuppgifter som den uthyrde behandlar vid utförandet av sitt uppdrag. Medlemsföretaget betraktas då som *tredje part*. Kunden är ensam personuppgiftsansvarig för den behandling av personuppgifter som den uthyrde utför under uthyrningsförhållandet. Den uthyrde behandlar personuppgifter inom kundens verksamhet för det ändamål som kunden, tillika personuppgiftsansvarig, har bestämt. Det är i sådan situation viktigt att skilja mellan den behandling av personuppgifter som medlemsföretaget respektive den uthyrde utför.

Eftersom medlemsföretagen, under ovan angivna omständigheter, inte behandlar personuppgifterna för kundens räkning finns inte heller något behov av att ingå ett biträdesavtal vid uthyrning.

Personuppgifter som avser den uthyrde arbetstagaren

Behandling av personuppgifter som föranleder ett personuppgiftsansvar hos medlemsföretaget är ofta begränsat till uppgifter om den uthyrde arbetstagaren som är relevanta för anställningsförhållandet med medlemsföretaget, sådan behandling utförs ofta hos medlemsföretaget, i dennes IT-system.

På samma sätt är kunden personuppgiftsansvarig för sådan behandling av den uthyrdes personuppgifter som *kunden* utför med anledning av att den uthyrde arbetar för kunden under kundens arbetsledning och ansvar.

Om medlemsföretaget erhåller personuppgifter från kunden som avser den uthyrde arbetstagaren, är medlemsföretaget och kund separat personuppgiftsansvariga för respektive parts behandling av sådana personuppgifter.

Uthyrning under minimal arbetsledning (s.k. "consulting")

När uthyrd personal i princip saknar kundens direkta arbetsledning och ansvar samt ges tillgång till personuppgifter som kunden ansvarar för, vilka behandlas inom ramen för uppdraget, sker behandlingen av sådana personuppgifter på uppdrag av kunden och för kundens ändamål. Medlemsföretag intar då rollen som personuppgiftsbiträde. Detta gäller endast för den behandling som utförs av uthyrd personal för kundens räkning. Skulle uthyrd personal, inom ramen för uthyrningsförhållandet, behandla personuppgifter för medlemsföretags ändamål intar medlemsföretaget istället rollen som personuppgiftsansvarig.

4.3.3 *Omställning*

Inom ramen för omställningsuppdrag (vars innebörd närmare beskrivs under punkt 8.1) bistår medlemsföretaget kunden genom att tillämpa sin egen *eller* kundens omställningsprocess.

Medlemsföretagets omställningsprocess

Om ett medlemsföretag använder sin egen omställningsprocess är medlemsföretaget personuppgiftsansvarigt för dessa uppgifter. Det här gäller eftersom medlemsföretaget bestämmer *vilka* personuppgifter som ska samlas in, *varifrån* uppgifterna ska samlas in och *hur* behandlingen ska gå till i övrigt. Medlemmen innehar kontroll över den behandling som utförs.

Kundens omställningsprocess

Om medlemsföretagen bistår *kunden* med omställning utifrån kundens omställningsprocess är kunden att betrakta som personuppgiftsansvarig.

Skulle medlemsföretagen använda egna system för att behandla personuppgifter, för att bistå kunden utifrån *kundens* omställningsprocess, intar medlemsföretagen rollen som personuppgiftsbiträde – eftersom medlemsföretagen nu *behandlar* personuppgifter på uppdrag av kunden. Om den personal som bistår vid omställningen behandlar personuppgifter hos kunden under kundens direkta arbetsledning och i kundens system, och personalen är förhindrad och obehörig att dela personuppgifter med medlemsföretagen, samt medlemsföretagen inte har åtkomst till personuppgifterna på annat sätt, saknar medlemsföretagen all kontakt med personuppgiftsbehandlingen. Medlemsföretagen intar då rollen som *tredje part* (d.v.s. medlemsföretaget är varken personuppgiftsansvarig eller personuppgiftsbiträde). Kunden är personuppgiftsansvarig för den behandling av personuppgifter som medlemsföretagens uthyrda arbetstagare utför när de bistår kunden i omställningsprocessen. Denna situation liknar de situationer som beskrivs ovan i punkt 4.3.1 och 4.3.2 angående rekryteringskonsulter och uthyrd personal.

Andra situationer i en omställningsprocess

I vissa fall förekommer det att såväl kundens som medlemsföretagens respektive omställningsprocesser används parallellt. Kund respektive medlemsföretag ansvarar

i en sådan situation för den personuppgiftsbehandling som respektive part själv utför, vilket innebär att parterna är separat personuppgiftsansvariga för sin egen respektive behandling. Å andra sidan lutar det senaste årets praxis allt mer mot att gemensamma processer också ska anses innefatta ett gemensamt personuppgiftsansvar, varför en bedömning i varje enskilt fall alltid måste göras.

5. LAGLIG GRUND

5.1 Inledning

Personuppgifter ska alltid behandlas på ett lagligt sätt. All behandling ska ha stöd i någon av de sex lagliga grunder som anges i dataskyddsförordningen och som redogörs för här under. Utan en lämplig laglig grund är behandlingen av personuppgifter inte laglig. Eftersom *behandling* omfattar en eller flera åtgärder beträffande personuppgifter, såsom insamling, lagring, bearbetning eller ändring, läsning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring, så är det viktigt att personuppgifter inte hanteras på något sätt innan en laglig grund har identifierats. Det går inte att, vid ett senare tillfälle, byta laglig grund för en pågående personuppgiftsbehandling. Det går till exempel inte att börja använda en intresseavvägning för att det tidigare inhämtade samtycket tas tillbaka eller inte längre är giltigt.

Notera särskilt det som anges nedan om problematiken att använda samtycke som laglig grund i anställningsförhållanden, det bör därför alltid noggrant bedömas om giltigt samtycke kan lämnas i enlighet med vad som följer av avsnitt 5.2. Notera även att det alltid bör bedömas vilken laglig grund som är tillämplig för den aktuella behandlingen och finns det ingen laglig grund som är tillämplig, t.ex. genom att ett giltigt samtycke inte kan lämnas, så är behandlingen inte tillåten enligt dataskyddsförordningen.

Det är viktigt att medlemsföretagen dokumenterar sitt resonemang vid val av laglig grund. Laglig grund ska också informeras den registrerade.

5.2 Samtycke

Samtycke kan inte användas som en generell laglig grund för all personuppgiftsbehandling men kan tillämpas för vissa specifika behandlingar om medlemsföretaget bedömer att den registrerade kan lämna ett giltigt samtycke. För att vara giltigt ska ett samtycke vara ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerade till den aktuella behandlingen av personuppgifter.²

Medlemsföretagen bör särskilt notera kravet på frivillighet och den problematik som finns med användning av samtycke i ojämlika förhållanden. Ett exempel på sådant ojämlikt förhållande är anställningsförhållanden, där det i många fall anses osannolikt att en arbetstagare, på grund av beroendeställningen till arbetsgivaren, kan välja att inte samtycka utan att känna att det kan få konsekvenser från arbetsgivarens håll. De registrerade är inte alltid anställda hos medlemsföretagen men i många fall befinner de sig i en liknande beroendeställning. Medlemsföretagen måste därför, för varje typ

² För mer information om samtycke som laglig grund rekommenderar vi WP29:s riktlinjer i WP259 rev.01 som European Data Protection Board (EDPB) stödjer. Ni hittar dem här: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

av behandling, göra en bedömning av om samtycke kan inhämtas frivilligt med hänsyn till den registrerades beroendeställning. Medlemsföretagen bör särskilt tänka på att den registrerade ska ha möjlighet att välja att inte samtycka till behandlingen, valet att samtycka ska inte på något sätt vara påverkat av ställningen till medlemsföretaget och den registrerade får inte utsättas för någon form av negativa konsekvenser om denne väljer att inte samtycka.

Den ovan anförda problematiken med att inhämta giltigt samtycke är särskild svår då samtycke i många fall är den lagliga grund som bedöms mest lämplig vid t.ex. vissa mer integritetskänsliga behandlingar, såsom kompetensutvärderingar och tester. Särskilt svårt är det att möjliggöra för en kandidat att fortsätta rekryteringsprocessen om denne inte samtycker till aktuell behandling. Det är viktigt att medlemsföretagen är väl medvetna om den problematik som finns och alltid gör en bedömning av om giltigt samtycke kan inhämtas samt säkerställer att den registrerade inte på något vis hamnar i en sämre ställning om denne väljer att inte samtycka.

Samtycket ska vara specifikt, vilket innebär att medlemsföretagen inte får inhämta ett generellt samtycke utan behandlingen som den registrerade samtycker till ska vara specificerad. Samtycket ska vidare vara otvetydigt, det vill säga den registrerade ska samtycka genom en aktiv handling. Inhämtande av samtycket får därför inte ske genom t.ex. en förifylld kryssruta. Den registrerade ska även närsomhelst kunna återkalla sitt samtycke och behandlingen ska då upphöra.

Vid insamling av samtycke ska tydlig information om behandlingen ges, såsom *vem* som begär samtycket, vilken *typ* av personuppgifter som ska behandlas och för vilket *ändamål* den aktuella och separata behandlingen faktiskt sker. Ett samtycke ska inte vävas in bland andra villkor och juridiska texter.

Medlemsföretagen bör dokumentera och spara alla insamlade samtycken, även samtycke som lämnas muntligt ska dokumenteras. Notera även att ett samtycke som laglig grund medför att den registrerade har rätt till dataportabilitet (för vidare information om dataportabilitet, se avsnitt 10.2) avseende uppgifter som den registrerade själv har lämnat.

Om någon av de andra lagliga grunderna är tillämpliga, t.ex. avtal med den registrerade, bör behandlingen grundas på den lagliga grunden istället för samtycke. Om personuppgiftbehandlingen grundas på en annan laglig grund får inte heller samtycke inhämtas för samma behandling. Notera även att särskilda krav och regler finns för samtycke från personer under 18 år.

5.3 Avtal

Avtal som laglig grund kan tillämpas när den aktuella behandlingen behöver ske *för att kunna fullgöra ett avtal som ingåtts med den registrerade*, eller för att kunna vidta åtgärder på begäran av den registrerade innan ett sådan avtal ingås.³

Eftersom denna lagliga grund kräver ett avtal där den registrerade är part tillämpas denna lagliga grund vanligtvis i anställningsförhållanden. Även andra avtal och villkor

³ För mer information om avtal som laglig grund rekommenderar vi EDPB:s riktlinjer 2/2019 av den 8 oktober 2019; https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

kan vara relevanta, till exempel villkor som accepteras av en kandidat vilket medför att medlemsföretagen åtar sig att arbeta aktivt för att hitta en tjänst åt kandidaten.

Som arbetsgivare får medlemsföretagen alltså behandla personuppgifter om en anställd för att kunna uppfylla anställningsavtalet. Exempelvis innefattar detta sådan behandling som krävs för att beräkna lön och för att registrera sjukfrånvaro.

Observera att avtal som laglig grund medför att den registrerade har rätt till dataportabilitet (för vidare information om dataportabilitet, se avsnitt 10.2) avseende uppgifter som den registrerade själv har lämnat.

5.4 Intresseavvägning

Den lagliga grunden intresseavvägning möjliggör behandling av personuppgifter då medlemsföretagets berättigade intressen väger tyngre än den registrerades intresse av skydd för sina personuppgifter. Det krävs dock att behandlingen är nödvändig för det aktuella ändamålet, vilket i sig ska vara tydligt och klart. Behandling av samma personuppgifter får inte senare ske för något annat syfte.⁴

Medlemsföretagens bedömning och avvägning av ovan intressen, vilket ska göras i varje enskilt fall, ska alltid dokumenteras. Detta är viktigt för att kunna visa att medlemsföretagen följer principen om ansvarsskyldighet. Vid en sådan bedömning bör medlemsföretagen fundera över om den registrerade kan förvänta sig att uppgifterna behandlas på avsett vis. En sådan förväntan talar för att medlemsföretagets berättigade intresse väger tyngre än den registrerades intressen.

5.5 Rättslig förpliktelse

Det är lämpligt att stödja personuppgiftsbehandling på rättslig förpliktelse som laglig grund då det finns lagar eller regler som föreskriver att medlemsföretaget *måste* behandla vissa personuppgifter i sin verksamhet. Sådana lagar och regler innefattar både EU-rätt och svensk rätt. I svensk rätt ska den rättsliga förpliktelsen följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller författning. Det innebär att bestämmelser i t.ex. ett kollektivavtal kan medföra att ett medlemsföretag måste behandla personuppgifter för att efterleva kraven i kollektivavtalet.

Försiktighet bör dock iakttas, så att lagar och regler inte tolkas alltför extensivt. För att en rättslig förpliktelse ska utgöra laglig grund för en viss behandling ska det stå klart att behandlingen är nödvändig för att efterleva den aktuella regleringen. Medlemsföretagen är t.ex. vanligtvis skyldiga att redovisa skatt och sociala avgifter avseende arbetstagare och har en bokföringsskyldighet enligt bokföringslagen, vilka båda innefattar behandling av personuppgifter som är nödvändig för att uppfylla den rättsliga förpliktelsen.

⁴ Det finns inga EDPB-riktlinjer avseende intresseavvägning som laglig grund. För mer information om intresseavvägning som laglig grund rekommenderar vi WP29:s yttrande i WP217; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

5.6 Myndighetsutövning och allmänt intresse samt skydd av grundläggande intresse

Avslutningsvis behandlas de två återstående lagliga grunder som vi anser är mindre relevanta för medlemsföretagen då de, bortsett från nedan nämnda fall, har ett begränsat tillämpningsområde i förhållande till medlemsföretagens verksamhet.

5.6.1 *Behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning*

Det är möjligt att behandla personuppgifter i en *myndighetsutövning* som sker på uppdrag av staten, exempelvis genom privata skolor och vårdbolag. All myndighetsutövning ska grundas på lag, förordning eller annan författning.

Behandling som utförs för ett *allmänt intresse* är tillåtet om det finns stöd i lag eller annan författning för den aktuella uppdraget, exempelvis skollagen. Denna lagliga grund är vanligtvis tillämplig inom privat arbetsförmedling, socialtjänst, hälso- och sjukvård, energiförsörjning, skolverksamhet och kollektivtrafik (buss, tåg, flyg).

5.6.2 *Behandling som är nödvändig för att skydda intressen av grundläggande betydelse*

Behandling av personuppgifter är tillåtet om det är nödvändigt för att rädda den registrerades eller någon annan persons liv. Denna lagliga grund, *skydd av grundläggande intresse*, kan bara tillämpas i mycket begränsad omfattning, vid tillfällen då den registrerade inte kan fatta beslut eller lämna samtycke, till exempel då den registrerade insjuknat eller är medvetslös.

6. REKRYTERINGSFRÅGOR

6.1 Inledning

Medlemsföretagen tillhandahåller flera olika tjänster inom rekrytering som föranleder olika frågeställningar. Nedan beskrivs särskilda frågor som ska beaktas i vissa scenarion som kan uppstå inom ramen för medlemsföretagens rekryteringstjänster. Bland annat beskrivs vilken eller vilka lagliga grunder som behandlingen av personuppgifter kan baseras på och vilken information som ska lämnas till kandidaten.

Ett rekryteringsuppdrag innebär i regel att medlemsföretagens kund avser att anställa en eller flera personer och att medlemsföretagen ges i uppdrag att välja ut och presentera en eller flera kandidater för kunden. Som en del av rekryteringsuppdraget får medlemsföretaget i regel i uppdrag att bland annat göra en kandidatsökning, administrera ansökningar och göra ett urval av tänkbara kandidater, vilket kan innefatta djupintervjuer och tester av olika slag. Medlemsföretagen lämnar i anslutning till detta uppgifter om kandidater till kunden, vilka kan utgöras av CV och kompetensprofil, resultat av tester m.m. I rekryteringsuppdragen ingår inte att lämna ut uppgifter om kandidater som inte presenteras som alternativ för kunden.

Det är kunden som beslutar om kandidaten ska anställas.

Notera att de särskilda frågor som anges nedan är exempelfrågor och avsnittet täcker inte alla tänkbara situationer. Vidare kan även det som anges i avsnitten om uthyrning i vissa delar vara aktuellt vid rekrytering och därmed läsas i ljuset av det som anges i detta avsnitt. Medlemsföretagen måste göra en bedömning av respektive behandling och de aktuella omständigheterna.

6.2 Rekrytering utifrån ansökan till enskild tjänst

6.2.1 Inledning

Kandidater kan via medlemsföretagen söka enskilda tjänster hos medlemsföretagens kunder som annonseras av medlemsföretagen.

6.2.2 Laglig grund

Inom ramen för rekryteringstjänsten kan medlemsföretaget behandla personuppgifter om kandidater baserat på det avtal som ingås med kandidaten, den registrerade, för att ta del av rekryteringstjänsten.

Medlemsföretagen kan även komma att istället inhämta kandidatens informerade samtycke, och använda detta samtycke som laglig grund för behandlingen.

Oavsett medlemsföretagens val av laglig grund ska kandidaten, i samband med registreringen av uppgifter, alltid förse med tillräckligt tydlig information om den tilltänkta behandlingen på ett lämpligt och lättillgängligt sätt.

Om samtycke ska användas som laglig grund måste medlemsföretagen säkerställa att den enskilde kan lämna ett giltigt samtycke. Se vidare i avsnitt 5.2 angående problematiken med samtyckets frivillighet i anställningsförhållanden eller därmed jämförbara förhållanden. I en rekryteringssituation är kandidaten ännu inte anställd och om så blir fallet kommer kunden, och inte medlemsföretaget, att vara arbetsgivare. Även om det inte föreligger ett faktiskt anställningsförhållande kan en kandidat i många fall ändå anses vara i en beroendeställning i förhållande till medlemsföretaget. Det är därför viktigt att medlemsföretaget, i enlighet med vad som anges i avsnitt 5.2, noga bedömer om ett frivilligt samtycke kan inhämtas.

Om samtycke används som laglig grund ska medlemsföretagen vidare lämna information om att kandidater när som helst kan dra tillbaka samtycket.

Inom branschen förekommer det även att kandidater vänder sig direkt till medlemsföretagen för att tillhandahålla personuppgifter i syfte att söka efter en tjänst som inte annonserats. Medlemsföretagen ska också i dessa fall säkerställa att laglig grund finns genom att den registrerade, i och med tillhandahållandet av kontaktuppgifter, CV och andra dokument, ingår avtal med medlemsföretaget genom att acceptera användarvillkor för rekryteringstjänsten alternativt lämnar sitt informerade samtycke.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att avtal är den bäst lämpade lagliga grunden. Här avses det avtal som ingås med kandidaten avseende rekryteringstjänsten. Samtycke kan vara en lämplig laglig grund i vissa fall, förutsatt att medlemsföretaget bedömer att det kan lämnas frivilligt.

6.2.3 Information till registrerade

Informationen till kandidaterna bör innehålla instruktioner om att känsliga personuppgifter och uppgifter som saknar relevans för rekryteringen inte ska lämnas om så inte krävs för tjänsten samt att kandidaten ansvarar för att informera eventuella referenser om att deras personuppgifter lämnats ut till medlemsföretaget. Medlemsföretaget bör lämna eventuell ytterligare information om behandlingen av referensens personuppgifter vid sin första kontakt med referensen.

Se vidare under avsnitt 6.3.2 angående laglig grund vid användning av rekryteringsplattformar.

6.2.4 *Medlemsföretag som personuppgiftsbiträde*

Om medlemsföretag agerar som personuppgiftsbiträde gentemot kund behöver medlemsföretaget säkerställa att underleverantör endast behandlar personuppgifter på samma villkor som medlemsföretaget behandlar personuppgifter för kundens räkning. Underleverantören agerar i egenskap av underbiträde i en sådan situation.

6.3 **Rekryteringsplattformar**

6.3.1 *Inledning*

Det förekommer att medlemsföretagen använder sig av olika former av rekryteringsplattformar för att hantera personuppgifter om kandidater. Plattformarna kan innehålla dokument, såsom CV och intervjuanteckningar, med uppgifter om kandidater som var för sig eller tillsammans är integritetskänsliga, och kan därmed innebära en ingående kartläggning av den enskilde. Det är därför av stor vikt att medlemsföretagen säkerställer att personuppgifter i rekryteringsplattformarna hanteras lagligt och säkert.

6.3.2 *Laglig grund*

Den lagliga grunden för att behandla personuppgifter från rekryteringsprocessen i en databas kan antingen vara avtal, samtycke eller intresseavvägning. Det är upp till varje medlemsföretag att bedöma vilken laglig grund som är mest lämplig för behandlingen.

När en kandidat registrerar sig på ett medlemsföretags rekryteringsplattform ingår kandidaten och medlemsföretaget i regel ett avtal om förmedling av potentiella rekryteringar, beroende på hur rekryteringstjänsten är uppbyggd. Medlemsföretaget behandlar i dessa fall de uppgifter som kandidaten laddar upp på rekryteringsplattformen för att kunna fullgöra avtalet med kandidaten.

Om samtycke används som laglig grund måste den registrerade få så pass tydlig information att denne kan ta ställning till om samtycke ska lämnas. Medlemsföretaget ska även säkerställa att samtycket i övrigt är giltigt samt lämna information om att kandidat när som helst kan dra tillbaka samtycket. Se vidare i avsnitt 5.2 och notera särskilt vikten av att säkerställa att samtycket är frivilligt inhämtat.

Om behandlingen grundas på en intresseavvägning måste medlemsföretagen ha ett berättigat intresse av att ta del av uppgifterna, vilket också ska dokumenteras. Vidare måste medlemsföretagen visa på att detta intresse väger tyngre än den registrerades intresse av att behandling inte ska ske. Intresset av att kunna identifiera talangfulla medarbetare och konsulter och erbjuda dem arbete kan för medlemsföretagens typer av verksamheter i regel anses väga tyngre än kandidaternas intresse av att uppgifterna inte behandlas. Att kandidaten själv söker en specifik anställning eller vill vara aktuell för olika anställningar är omständigheter som talar för detta inom just bemannings- och rekryteringsbranschen. Generellt sett är personuppgiftsbehandlingen som medlemsföretagen utför inom ramen för tillhandahållandet av rekryteringsplattformar en förutsättning för att kunna erbjuda de registrerade en effektiv och ändamålsenlig tjänst. Avvägningen måste dock göras för

varje enskild rekryteringsplattform och ta i beaktande bland annat de kategorier av behandlingar som utförs och vilka uppgifter som behandlas.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att avtal, i form av anställningsavtal med den registrerade, är den bäst lämpade lagliga grunden. Med avtal som laglig grund behöver medlemsföretaget inte argumentera för intresseavvägningen eller riskera att samtycke återtas eller anses ogiltigt.

6.3.3 *Information till den registrerade*

De registrerade måste informeras om att uppgifter från rekryteringsprocessen lagras på en rekryteringsplattform under ansökningsförfarandet och att uppgifterna kan komma att sparas längre för framtida rekryteringar. När kandidaten själv söker en anställning samlas personuppgifterna in från den registrerade. I samband med detta ska medlemsföretagen lämna den information som framgår av tillämplig dataskyddslagstiftning.

På rekryteringsplattformar har de registrerade vanligen möjlighet att välja vilket material som laddas upp och vad det innehåller. Medlemsföretagen bör därför vara särskilt noga med att på dessa plattformar informera kandidater som laddar upp CV och andra dokument om att känsliga personuppgifter och uppgifter som saknar relevans för rekryteringen inte ska lämnas samt att kandidaten ansvarar för att informera eventuella referenser om att deras personuppgifter lämnats ut till medlemsföretaget. Medlemsföretagen bör lämna eventuell ytterligare information om behandlingen av referensens personuppgifter vid sin första kontakt med referensen.

Medlemsföretagen kan informera registrerade om hur medlemsföretaget behandlar personuppgifter som en del av tjänstevillkoren på rekryteringsplattformen. Informationen bör då vara utformad på ett tydligt sätt och separat från övriga villkor.

6.3.4 *Medlemsföretag som personuppgiftsbiträde*

Om medlemsföretagen agerar som personuppgiftsbiträde gentemot kund ska medlemsföretagen säkerställa att underleverantör endast behandlar personuppgifter på samma villkor som medlemsföretagen behandlar personuppgifter för kundens räkning. Underleverantören agerar i egenskap av underbiträde i en sådan situation.

7. **UTHYRINGSFRÅGOR**

7.1 **Inledning**

Med uthyrning avses ett förhållande mellan medlemsföretag och kund där medlemsföretaget mot ersättning ställer egen, anställd personal eller underleverantörs personal till kundens förfogande. Personalen står under kundens kontroll, ledning och uppföljning under den överenskomna tiden för uppdraget och ska utföra arbete som hör till kundens verksamhet.

Inom ramen för uthyrningstjänsten genomför medlemsföretaget en urvalsprocess, under vilken medlemsföretaget tar fram en kravprofil och identifierar lämpliga kandidater för uppdraget. Kandidaten presenteras sedan för kunden som tar ställning till om kandidaten ska anlitas för uppdraget.

Notera att de särskilda frågor som anges nedan är exempelfrågor och avsnittet täcker inte alla tänkbara situationer. Vidare kan även det som anges i avsnittet om uthyrning i vissa delar vara aktuellt vid rekrytering och därmed läsas i ljuset av det som anges i

detta avsnitt. Medlemsföretagen måste göra en bedömning av respektive behandling och de aktuella omständigheterna.

7.2 Generellt angående uthyrning

7.2.1 Laglig grund

Medlemsföretagen kan behandla personuppgifter om de anställda som ska hyras ut till kund baserat på anställningsavtalet med den enskilde, med ändamålet att bland annat administrera anställningsförhållandet, så som att betala ut lön eller kontakta den anställda. Medlemsföretagen behandlar även personuppgifter om dessa anställda med ändamålet att matcha individen mot potentiella uppdrag för kund. För att uppfylla dessa ändamål kan det ofta krävas att medlemsföretaget lämnar ut uppgifter om den anställda till kunder och potentiella kunder. Medlemsföretag kan även ha en rättslig skyldighet att överföra personuppgifter om sina anställda och uppdragstagare, så som för att skicka kontrolluppgifter till Skatteverket.

Uppgifter om betyg, omdömen eller andra värderande upplysningar, till exempel från utvecklingssamtal och uppföljning under uppdrag, får behandlas om det är nödvändigt för att administrera anställningsavtalet eller för att uppfylla rättsliga skyldigheter.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att avtal med den anställda, anställningsavtalet, är den bäst lämpade lagliga grunden. Andra lagliga grunder kan dock bli relevanta.

7.2.2 Information till den anställda

Varje anställd hos ett medlemsföretag ska i samband med att anställningsavtalet med medlemsföretaget ingås ges information om den tilltänkta behandlingen av personuppgifter, bland annat att uppgifter kan komma att lämnas ut till kunder och potentiella kunder i syfte att hyra ut den anställda till kund.

7.3 Anställda hos underleverantörer

7.3.1 Laglig grund

Medlemsföretagen kan i regel behandla personuppgifter om anställda hos underleverantörer baserat på en intresseavvägning, förutsatt att medlemsföretaget har gjort en avvägning och dokumenterat denna, alternativt kan personuppgifterna behandlas med den anställdes informerade samtycke som laglig grund. Se ovan i avsnitt 6.3.2 angående krav på giltiga samtycken och dokumenterade intresseavvägningar.

I de fall då anställda hos underleverantörer hyrs ut av medlemsföretagen till kund, är medlemsföretagen skyldiga att säkerställa att underleverantören har rätt att dela uppgifter om den anställda med medlemsföretagen och kunden.

Det går inte att stödja behandling av den anställdes uppgifter på att behandlingen är nödvändig för att uppfylla ett avtal mellan medlemsföretaget och underleverantören, eftersom den anställda inte är part till avtalet.

Mot bakgrund av dessa omständigheter anser Kompetensföretagen att en intresseavvägning är den bäst lämpade lagliga grunden.

7.3.2 Medlemsföretag som personuppgiftsbiträde

Om medlemsföretag skulle agera som personuppgiftsbiträde gentemot kund behöver medlemsföretaget säkerställa att underleverantör endast behandlar personuppgifter

på samma villkor som medlemsföretaget behandlar personuppgifter för kundens räkning. Underleverantören agerar i egenskap av underbiträde i en sådan situation.

7.4 Individuell prestationsmätning

Det förekommer att medlemsföretagen genomför individuell prestationsmätning för att bedöma vilken person som passar för en specifik uthyrning. Behandling av personuppgifter för ändamål som innebär individuell prestationsmätning är laglig om den är nödvändig för att uppfylla anställningsavtalet, till exempel för att beräkna och betala ut lön. Behandling av personuppgifter som innebär individuell prestationsmätning är tillåten för ändamålen att exempelvis planera, organisera, leda och följa upp arbetet om det sker på ett sätt som inte strider mot god sed på arbetsmarknaden eller är kränkande. Behandlingen kan i sådana fall grunda sig på en intresseavvägning.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att avtal med den anställda, anställningsavtalet, är den bäst lämpade lagliga grunden.

7.5 System för rekrytering och kompetensdatabaser

Om medlemsföretagen använder system för rekrytering av anställda får endast uppgifter som är nödvändiga för just detta ändamål behandlas, exempelvis för att bedöma den arbetssökandes karriärmöjligheter och lämplighet genom granskning av omdömen, betyg och kompetenser.

Medlemsföretagen kan även komma att upprätta kompetensdatabaser över anställda och konsulter som hyrs ut eller avses hyras ut. Medlemsföretagen kan som generell utgångspunkt, efter att ha gjort en dokumenterad intresseavvägning och i övrigt i enlighet med god sed på arbetsmarknaden, registrera faktauppgifter om de anställda i kompetensdatabaser. Detta kan avse uppgifter om utbildningar, arbetslivs-erfarenhet, uppdrag, poäng från tester och dylikt.

Behandling av värderande omdömen och dylikt kräver dock som huvudregel att ett giltigt samtycke från arbetstagaren har inhämtats. Värderande omdömen är uppgifter om en person som baseras på någon annans uppfattning eller bedömning, exempelvis uppgifter om hur den registrerade är eller beter sig i intervjuanteckningar, uppgifter om resultat från personlighetstester eller personlighetsprofiler. Faktiska påståenden, så som ett påstående från den registrerade själv att denne är på ett visst sätt, utgör inte ett värderande omdöme. Notera här det som anges i avsnitt 5.2 angående de krav som finns för att ett samtycke ska vara giltigt.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att en intresseavvägning är den bäst lämpade lagliga grunden. Samtycke kan dock krävas för behandling av värderande omdömen.

8. OMSTÄLLNINGSFÖRFRÅGOR

8.1 Inledning

Med omställning avses när kund ger medlemsföretag i uppdrag att genomföra en omställningsprocess varvid medlemsföretagen bland annat ska förse deltagaren med analys av förutsättningar för nytt arbete, utbildning och/eller coachning i syfte att finna för deltagaren nytt arbete inklusive att starta egen verksamhet eller på annat sätt göra deltagaren mer attraktiv på arbetsmarknaden. Uppdraget kan syfta till att omplacera kundens anställda inom organisationen eller till en annan organisation, coacha medarbetare eller på annat sätt hitta nytt arbete för de anställda eller göra dessa mer

attraktiva på arbetsmarknaden. Medlemsföretaget kan även få uppdrag avseende omställning av arbetslösa till arbete eller utbildning via anvisning från offentlig sektor eller kommuner.

8.2 Laglig grund

Inom ramen för omställningstjänsten kan medlemsföretagen i regel behandla personuppgifter om anställda som deltar i ett program baserat på en intresseavvägning, alternativt deltagarens informerade samtycke som laglig grund. Se ovan i punkt 6.3.2 angående krav på giltiga samtycken och dokumenterade intresseavvägningar.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att en intresseavvägning är den bäst lämpade lagliga grunden.

8.3 Särskilt om analysresultat

Medlemsföretag som tillhandahåller en omställningstjänst ska bland annat göra en analys av den enskildes förutsättningar för nytt arbete, utbildning eller coaching.

Resultatet av analysen av förutsättningar för nytt arbete, utbildning eller coaching kan innehålla en mängd uppgifter som kan anses integritetskänsliga till sin natur, så som uppgifter om hälsa, beteende, skäl för uppsägning m.m.

Analysresultat hos medlemsföretagen bör därför omgärdas av tillräckliga säkerhetsåtgärder mot bakgrund av uppgifternas natur. Bland annat bör därför endast de anställda hos medlemsföretagen som behöver dessa uppgifter för omställningsuppdraget ha tillgång till uppgifterna.

I den utsträckning analysresultat omfattar värderande omdömen i enlighet med avsnitt 7.5 ovan kan behandlingen bara grundas på den registrerades informerade giltiga samtycke.

9. SÄRSKILDA ÖVERGRIPANDE FRÅGOR

9.1 Personlighets- och kompetenstester

9.1.1 Specifikt om personuppgiftsansvar

Det förekommer att medlemsföretagen beställer personlighetstester, profiler eller liknande av externa företag. I sådana situationer är leverantören i regel personuppgiftsbiträde till det beställande medlemsföretaget, förutsatt att behandlingen sker för medlemsföretagets ändamål och att medlemsföretaget bestämmer medlen med behandlingen, till exempel genom att bestämma vilken typ av frågor som ska ställas och vilket urval som ska göras. Medlemsföretagen är som personuppgiftsansvariga skyldiga att säkerställa att ett personuppgiftsbiträdesavtal som uppfyller kraven i tillämplig dataskyddslagstiftning ingås med leverantören.

Det kan även finnas situationer då tjänsten är utformad på ett sådant sätt att leverantören av testverktyget ifråga är personuppgiftsansvarig för behandlingen av personuppgifter inom ramen för testet. Medlemsföretagen är då tredje part i förhållande till leverantörens behandling och blir sedan separat personuppgiftsansvariga för medlemsföretagens behandling av testresultaten. Det är upp till varje medlemsföretag att avgöra huruvida leverantören utgör personuppgiftsansvarig eller personuppgiftsbiträde.

9.1.2 *Laglig grund*

Medlemsföretagens behandling av personuppgifter om personlighets- och kompetenstester, inklusive behandling som sker hos en leverantör som agerar som personuppgiftsbiträde, kan baseras på samtycke från den registrerade. I det fall en extern leverantör är personuppgiftsansvarig för behandlingen inom ramen för testet så är leverantören ansvarig för att inhämta den registrerades samtycke i förhållande till den behandlingen. När sedan medlemsföretaget tar del av uppgifterna måste medlemsföretaget säkerställa att laglig grund finns för medlemsföretagets behandling, vilket också lämpligen är den enskildes samtycke. Medlemsföretagen behöver därför utforma samtycket till att omfatta den behandling som medlemsföretaget är ansvarigt för.

Även behandling som bygger på att medlemsföretagen själva tillhandahåller urvalsverktyg så som personlighets- och kompetenstester kan baseras på den enskildes samtycke.

Vid användande av samtycke i anställningsliknande förhållanden är det viktigt att säkerställa att det samtycke som inhämtas är giltigt i enlighet med vad som anges i avsnitt 5.2.

I viss utsträckning kan även det avtal som finns med den registrerade vara tillämpligt som laglig grund för behandling av personuppgifter inom ramen för personlighets- och kompetenstester. Det förutsätter att det finns ett avtal med den registrerade, till exempel att den registrerade accepterar medlemsföretagens allmänna villkor vid användning av medlemsföretagens rekryteringstjänst. Vidare krävs att den behandling som sker är nödvändig för uppfyllande av detta avtal. Det kan vara exempelvis att de allmänna villkoren föreskriver att medlemsföretaget ska verka för att marknadsföra kandidaten till kunder och presentera dennes kompetenser. I ett sådant fall kan behandling av personuppgifter från till exempel kompetenstester vara nödvändig för att medlemsföretaget ska uppfylla sina åtaganden i avtalet.

Intresseavvägning kan i begränsad utsträckning tillämpas som laglig grund för personlighets- och kompetenstester avseende kandidater för chef- och nyckelpositioner. Sådan behandling är möjlig om det finns ett berättigat intresse för kunden (och därigenom medlemsföretaget som assisterar i kundens rekrytering) att en person i sådan ställning ska ha vissa kvaliteter, i syfte att kunden ska kunna planera, leda och organisera sin verksamhet.

Medlemsföretagen bör i varje enskilt fall ta ställning till om det är nödvändigt att utföra personlighets- och kompetenstester för att tillsätta en specifik tjänst samt säkerställa att omfattningen av sådana tester står i proportion till kraven på den specifika tjänsten. Detta för att säkerställa att personuppgifterna behandlas i enlighet med de principer för behandling av personuppgifter som följer av dataskyddsförordningen, till exempel principerna om uppgiftsminimering och ändamålsbegränsning.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att värderande omdömen såsom resultat från personlighets- och kompetenstester kan behandlas med samtycke som laglig grund, förutsatt att medlemsföretagen kan inhämta ett giltigt samtycke från den registrerade.

9.1.3 *Information till den registrerade*

Kandidater ska informeras om att dessa tester/verktyg kan komma att användas av medlemsföretagen inom ramen för rekryteringsprocessen.

9.2 Referenser

9.2.1 *Laglig grund*

Kontroll av referenser är en vanligt förekommande åtgärd som vidtas under rekryteringsprocessen.

Om en kandidat lämnar uppgifter om referenser, får det anses vara en sådan typ av behandling som berättigar medlemsföretaget att hämta in personuppgifter om kandidaten från referenserna. Medlemsföretagen kan stödja sig på en intresseavvägning som laglig grund för behandlingen, förutsatt att medlemsföretagen på förhand gjort och dokumenterat en sådan avvägning. Det krävs dock uttryckligt samtycke från kandidaten om medlemsföretagen avser inhämta känsliga personuppgifter, exempelvis uppgift om sjukfrånvaro. Ett sådant samtycke bör dokumenteras skriftligt och medlemsföretagen bör säkerställa att det är ett giltigt samtycke. Se vidare i avsnitt 5.2 angående kraven på ett giltigt samtycke.

Medlemsföretagen kan även basera behandling av referensers personuppgifter på en intresseavvägning, förutsatt att medlemsföretagen på förhand gjort och dokumenterat en sådan avvägning.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att en intresseavvägning är den bäst lämpade lagliga grunden.

9.2.2 *Information till den registrerade*

Kandidaterna bör av medlemsföretagen upplysas om att kandidaterna själva ansvarar för att informera eventuella referenser om att deras personuppgifter lämnas ut till medlemsföretagen. Medlemsföretagen ska dock lämna ytterligare information om behandlingen av referensens personuppgifter vid sin första kontakt med referensen. Ett sådant tillvägagångssätt förutsätter att det inte tar mer än en månad till kontakt med referensen tas (och att referensens personuppgifter inte lämnas ut till annan mottagare). I annat fall ska referensen på något sätt erhålla information avseende behandlingen av dess personuppgifter.

9.3 Search

9.3.1 *Inledning*

I detta avsnitt hanteras frågor rörande extern sökning efter lämpliga kandidater för potentiell rekrytering utan på förhand givet tillstånd från kandidaten, även kallat *search* eller *headhunting*. Search förekommer inom ramen för tjänsterna uthyrning och rekrytering på uppdrag av kund samt inom ramen för medlemsföretagens interna rekrytering.

9.3.2 *Laglig grund*

Medlemsföretagen kan vid utförande av *search* behandla personuppgifter om potentiella kandidater med intresseavvägning som laglig grund. Medlemsföretagens berättigade intresse är att kunna hitta talangfulla kandidater för rekryteringsprocesser samt att kunna kontakta eller förmedla jobberbjudanden till sådana kandidater. Intresset av att kunna hitta kandidater och erbjuda dem jobb väger tungt eftersom det främjar rörlighet på arbetsmarknaden och att rätt person hamnar på rätt jobb. Dessutom har medlemsföretagen tungt vägande kommersiella skäl till att söka upp kandidater i olika kanaler eftersom det utgör en viktig del av medlemsföretagens kärnverksamhet. *Search* ligger även i den registrerade kandidatens intresse eftersom

denne får möjlighet att ta del av jobberbjudanden som inte utannonserats offentligt och som är anpassade efter den registrerades kompetenser.

För att medlemsföretaget ska anses ha ett berättigat intresse som väger tyngre än den registrerades intresse får *search* endast ta sikte på sådana uppgifter om den registrerade som är relevanta och av väsentlig betydelse för ett bedöma den registrerades yrkeskvalifikationer samt söka kontakt med den registrerade. *Search* får inte avse uppgifter av rent privat natur såsom exempelvis semesterbilder.

För det fall medlemsföretagen samlar in personuppgifter om registrerade som sedermera inte inkluderas i någon rekryteringsprocess väger medlemsföretagens berättigade intresse, av samma skäl som angivits ovan, tyngre än den registrerades intressen och rättigheter, under förutsättning att den registrerade informeras och har möjlighet att invända mot behandlingen).

Mot bakgrund av dessa omständigheter anser medlemsföretagen att en intresseavvägning är den bäst lämpade lagliga grunden.

9.3.3 *Information till den registrerade*

Vid *search* inhämtas personuppgifter utan den registrerades vetskap från en annan källa än den registrerade själv. Den registrerade ska informeras om att dennes personuppgifter insamlats av medlemsföretagen senast en månad från det att uppgifterna samlades in eller, om uppgifterna samlats in för att ta kontakt med den registrerade, vid det första kontakttillfället. Om uppgifterna ska lämnas ut till en annan mottagare ska medlemsföretagen bedöma om det finns en laglig grund att lämna ut uppgifterna och den registrerade ska informeras innan sådan utlämning sker.

Ovanstående innebär att den registrerade ska informeras om den behandling som kommer att ske när den registrerades personuppgifter har samlats in genom *search*, i samband med att rekryteringsprocess inleds eller innan uppgifter om den registrerade delas med kund.

9.4 **Behandling av uppgifter om lagöverträdelser**

Medlemsföretagen kan, utifrån viss kravställning, behöva kontrollera anställda eller kandidaters bakgrund genom att begära att få se utdrag ur belastningsregister eller andra handlingar som kan innehålla uppgifter om lagöverträdelser. Beroende på tjänst, kan denna typ av kontroller vara vanligt förekommande. Särskilt de medlemsföretag som tillhandahåller tjänster inom vård-, omsorgs- och pedagogikbranschen har starkt vägande skäl för att administrera kontroller mot belastningsregister. Dessa medlemsföretag har i vissa fall även en rättslig skyldighet att genomföra sådana kontroller, till exempel avseende vissa säkerhetskänsliga verksamheter och skolor.

Som framgår av första stycket ovan kan medlemsföretagen i samband med ansökningsprocessen och under pågående anställning komma att ställa frågor om och begära att en kandidat eller anställd ska uppvisa utdrag ur belastningsregistret. Medlemsföretagen får registrera att uppgifter hämtats ur belastningsregistret under förutsättning att dokumentet och uppgifterna förstörs omgående. Däremot får medlemsföretagen inte utan lagstöd registrera och spara uppgifter ur belastningsregistret eller andra uppgifter eller uttalanden rörande lagöverträdelser som är hänförliga till sådana uppgifter. Medlemsföretagen får spara allmän information eller iakttagelser om kandidaten såsom rena omständigheter, t.ex. uttryck som "Kandidaten uttalade att [...]", eller "Kandidaten uppträdde hotfullt", om så faktiskt

är fallet. Omständigheter rörande uppgifter om lagöverträdelser, exempelvis att en kandidat berättar att denne begått ett brott, får dock aldrig sparas.

Medlemsföretagen har generellt ingen rätt att behandla personuppgifter om brottslighet, såsom misstanke om brott⁵, domar i brottmål, häktningar och andra tvångsingripanden om inte regeringen eller tillsynsmyndigheten beslutat om det. Att en kandidat eller anställd samtycker till behandling av brottsuppgifter berättigar inte medlemsföretagen att frånga förbudet. Undantag har meddelats i vissa fall. Sådana undantag avser behandling av enstaka uppgifter om lagöverträdelser (eller misstankar om lagöverträdelser) då uppgiften är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk, eller då uppgiften krävs för att fullgöra en anmälningsskyldighet enligt lag eller då det finns stöd av annan lagstiftning att utföra behandlingen.

Uppgifter om näringsförbud kan vara, men är inte per automatik, uppgifter om lagöverträdelser eller misstanke om sådana. Medlemsföretagen bör, i det fall det är nödvändigt att inhämta uppgifter om näringsförbud, tillämpa samma förhållningssätt som anges ovan om utdrag ur belastningsregistret.

9.5 Personnummer och andra nationella identifikationsnummer

Medlemsföretagen får, utan samtycke, enbart behandla personnummer om det är klart motiverat med hänsyn till behandlingens ändamål, vikten av säker identifiering eller något annat beaktansvärt skäl.

Om det inte finns samtycke till att behandla personnummer är det medlemsföretagen som ska göra bedömningen om intresset av att använda personnummer väger tillräckligt tungt för att motivera behandlingen. Om det finns annan uppgift som kan användas istället för personnummer och samma resultat kan uppnås genom att använda den uppgiften saknas i regel skäl att använda personnummer.

Medlemsföretagen får exempelvis behandla personnummer för administration avseende anställda och uppdragstagare samt för att kunna lämna uppgifter till myndigheter. Medlemsföretagen får även använda personnummer när säker identifiering är viktigt. Så är till exempel fallet vid fysisk och digital behörighetsadministration för att kontrollera tillgång till personuppgifterna. Säker identifiering har också ansetts särskilt viktig i exempelvis vårdregister, inom socialtjänsten, i bank- och försäkringsverksamhet och för utförande av betalningsuppdrag m.m. Detta innebär att medlemsföretagen som utför bemanningsuppdrag inom dessa områden kan ha särskilda skäl att använda sig av personnummer. Medlemsföretagen får även behandla personnummer i de fall där identifiering annars är osäker till följd av att exempelvis namn eller annan identifieringsuppgift är okänd.

Behovet av säker identifiering av användare av medlemsföretagens tjänster kan således utgöra skäl för att behandla personnummer. Det ovan angivna innebär därtill att de medlemsföretag som kunder med verksamhet inom områdena vård, omsorg och pedagogik har starkt vägande skäl att behandla personnummer. Behandling av

⁵ Det råder viss osäkerhet om misstanke om brott utgör en personuppgift som rör lagöverträdelser. Datainspektionen anger att myndigheten ännu inte kan ta ställning till detta och kommer att kunna ge mer vägledning senare. Konsensus i EU-medlemsstater verkar dock mer och mer gå mot en tolkning där misstanke om brott omfattas.

personnummer är regelmässigt en förutsättning för att kunna presentera kandidater för kund när det gäller sådana tjänster, på grund av den stora vikten av säker identifiering.

9.6 Identifiering av användare

Medlemsföretagen bör tillhandahålla metoder för säker identifiering av användare av medlemsföretagens tjänster, såsom kandidater.

Medlemsföretagen bör informera samtliga användare om att användaren är skyldig att hålla sina användaruppgifter hemliga för att förhindra bedrägerier och obehörig användning av tjänsterna.

9.7 Register över ej önskvärda kandidater

Medlemsföretagen får *inte* upprätta så kallade spärrlistor med tidigare anställda, kandidater m.m. i form av uppgifter om att någon inte är lämplig för återanställning om det inte finns tungt vägande skäl för en sådan typ av behandling, exempelvis om det ställs särskilt hårda krav på redlighet och förtroende för den specifika tjänsten – såsom vid arbete på förskolor. Det gäller dock endast i specifika fall då medlemsföretagens intresse av att behandla registrerades personuppgifter för att ha möjlighet att bedriva sin verksamhet kan anses överväga den registrerades intresse av skydd för sina personuppgifter. Laglig grund för behandlingen är således en intresseavvägning.

9.8 Personuppgifter i ostrukturerat material

Varje medlemsföretag ansvarar för att genomföra interna projekt för att säkerställa att den behandling som tidigare fallit under den så kallade missbruksregeln, det vill säga behandling av personuppgifter i ostrukturerat material så som e-post och dokument, utförs i enlighet med de krav som följer av dataskyddsförordningen.

9.9 Kreditupplysningar

9.9.1 Inledning

Medlemsföretagen kan komma att inhämta kreditupplysningar inom ramen för rekryterings- och uthyrningsprocesser för att undersöka om kandidater har eventuella betalningsanmärkningar.

9.9.2 Laglig grund

För kreditupplysningar kan avtal med den registrerade användas som laglig grund för den personuppgiftsbehandling som utförs. Avtal kan användas som laglig grund om behandling är nödvändig för fullgörande av avtal med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan sådant avtal ingås. Avtalet i fråga är anställningsavtalet och det kan således användas som laglig grund före avtalet ingåtts, förutsatt att det kan ses som en åtgärd på begäran av den registrerade i enlighet med vad som anges nedan.

Kreditupplysning är en sådan åtgärd som vanligtvis vidtas innan ett anställningsavtal träffas. Behandlingen är laglig under förutsättning att kandidaten på förhand informerats om att kreditupplysning kommer att genomföras för alla som vill komma i fråga för att ingå anställningsavtalet samt att ansökan betraktas som en begäran om att kreditupplysning ska vidtas.

Alternativt kan intresseavvägning användas som laglig grund för behandling av uppgifter om kreditupplysningar. Medlemsföretagen kan ha ett berättigat intresse av

att behandla personuppgifter om kreditupplysningar för att göra en ekonomisk riskbedömning av den enskilda, i de fall en sådan bedömning kan anses nödvändig för tjänsten ifråga.

Medlemsföretagen kan således själva göra en bedömning av vilken laglig grund som är mest lämplig utifrån det ovan anförda. Det är dock viktigt att medlemsföretagen är konsekventa och håller sig till den lagliga grund som medlemsföretagen bedömt vara lämplig.

Kreditupplysning i samband med rekrytering och uthyrning får enbart inhämtas om medlemsföretaget i rekryterings- eller uthyrningsprocessen har ett faktiskt behov att ta del av uppgifterna, det vill säga en anledning att göra en ekonomisk riskbedömning beträffande den registrerade. Ett sådant behov kan vara att kandidaten i sin anställning skulle komma att ha ett stort ekonomiskt ansvar. Det kan även finnas fall där det finns en rättslig skyldighet att vidta sådana åtgärder, då rättslig förpliktelse blir laglig grund för behandlingen.

Ofta används så kallade kreditupplysningsföretag för att förse medlemsföretag med information om den registrerade. Medlemsföretagen ska säkerställa att dessa företag har en process på plats för säker hantering av personuppgifter. Kreditupplysningsföretagen är personuppgiftsansvariga inom ramen för sin egen tjänst och den behandling av personuppgifter som detta innebär.

Mot bakgrund av dessa omständigheter anser medlemsföretagen att avtal, och då anställningsavtalet med den registrerade, är den bäst lämpade lagliga grunden.

9.9.3 *Information till den registrerade*

Vid kreditupplysningar inhämtas inte personuppgifterna direkt från den registrerade. Detta innebär att medlemsföretagen ska ge särskild ytterligare information om den tilltänkta behandlingen till den registrerade, till exempel information om källan varifrån uppgifterna hämtats, i enlighet med tillämplig dataskyddslagstiftning.

9.10 **Användandet av sociala medier**

Om tjänster på sociala medier används i rekryteringssyfte ska medlemsföretaget särskilt säkerställa att det finns en laglig grund för behandlingen, att vid var tid gällande villkor för tjänsten följs samt att den enskilde ges information om medlemsföretagens personuppgiftsbehandling genom sociala medier.

Beroende på hur medlemsföretaget använder sociala medier kan ledning för laglig grund och behandlingen i övrigt hämtas i andra avsnitt i denna vägledning. Se avsnitt 6.3 avseende rekryteringsplattformar som tillhandahålls av en social medieleverantör samt avsnitt 9.3.2 angående search via sociala medier.

Inför granskning av profiler, även om detta sker löpande under anställningen, bör medlemsföretagen beakta om kanalen vanligen används i professionella eller privata sammanhang eller om den enskilde kan ha anledning att anta att profilen och de uppgifter som den enskilde delar offentligt kan komma att användas av rekryterings- och bemanningsföretag. Att den enskilde har en öppen profil på exempelvis sociala medier kan inte i sig tas till intäkt för att det är fritt fram att behandla dennes personuppgifter för medlemsföretagens egna syften. Däremot kan det av sammanhanget framgå att den enskilde avser att rikta sig mot potentiella arbetsgivare eller på annat sätt framhåller professionella kvalifikationer eller intressen. Se vidare ovan under avsnitt 9.3 angående *search*.

9.11 Resultat från drog-, alkohol- och andra hälsotester

Medlemsföretagen kan komma att genomföra tester av enskildas hälsa för att säkerställa arbetskapacitet och lämplighet för en viss tjänst.

Resultat från sådana tester är en uppgift om hälsa. Behandlingen kan vara tillåten bland annat om den är nödvändig för bedömningen av en arbetstagares arbetskapacitet avseende en särskild tjänst, om den följer av krav i lag eller om den är nödvändig för att värna om liv eller hälsa. Exempel på sådana tjänster där det kan bli aktuellt med drog-, alkohol eller andra hälsotester är tjänster inom transport och vård.

I en rekryteringsprocess bör nämnda tester endast genomföras om det är nödvändigt för den aktuella tjänsten och en laglig grund därmed kan fastställas enligt ovan. Testen utförs då för kundens ändamål och ska endast utföras i enlighet med kundens instruktioner innebärandes att kunden är personuppgiftsansvarig och medlemsföretaget personuppgiftsbiträde. Medlemsföretaget bör då ha rutiner för att på instruktion från kunden endast utföra sådana tester när det är nödvändigt för att upprätthålla säkerhet och förtroende för personalen.

I det fall tester sker vid uthyrning under den registrerades pågående uppdrag, på kundens uppmaning och under kundens arbetsledning är kunden personuppgiftsansvarig. Kunden är då skyldig att tillse att det finns laglig grund för behandlingen. Medlemsföretagen bör inte ta del av dessa personuppgifter om det inte är nödvändigt av samma skäl som anges ovan, förutsatt att medlemsföretaget inte tar del av några uppgifter är medlemsföretaget tredje part.

Om medlemsföretag eller kund utför drog-, alkohol eller hälsotester på de egna anställda är medlemsföretag eller kund personuppgiftsansvarig för sin egen behandling av personuppgifter.

9.12 Screening mot sanktionslistor

Kunder till medlemsföretagen kan komma att ställa krav på att anställda och kandidater kontrolleras mot olika sanktionslistor och andra typer av register. Medlemsföretagen får endast göra sådana kontroller under kontroll av myndighet eller om Datainspektionen beviljat undantag för sådan typ av behandling. Medlemsföretagen bör därför ha rutiner på plats för att hantera begäran om så kallad "screening" mot sanktionslistor m.m.

Datainspektionen har meddelat undantag för vissa organisationer att behandla personuppgifter om lagöverträdelse i syfte att genomföra kontroller mot specifika sanktionslistor. Exempelvis har Bankföreningen medgivit ett sådant särskilt undantag för behandling som utförs av föreningens medlemmar.

Dessa undantag avser vanligen kontroll av kunders personuppgifter och det finns ännu inte något beviljat undantag avseende kontroll av personuppgifter om anställda eller kandidater. I det fall en av ett medlemsföretags kunder har fått ett undantag beviljat av Datainspektionen är det därför av stor vikt att kontrollera om tillståndet omfattar kontroll mot endast kunddatabaser, eller om det omfattar även kontroll av anställda och kandidater.

I det fall en kund önskar att medlemsföretaget genomför en kontroll, och den är tillåten enligt vad som ovan anförts, behandlar medlemsföretaget i regel personuppgifter för kundens räkning och agerar därmed som personuppgiftsbiträde. Medlemsföretaget

behöver då inte ha ett eget separat tillstånd, utan avgörande för behandlingens tillåtlighet är att kunden har ett tillstånd som omfattar den aktuella behandlingen.

9.13 Särskilt angående medlemsföretag inom särskilda branscher

Vissa av Kompetensföretagens medlemsföretag kan komma att behandla en stor mängd känsliga personuppgifter, och utföra typer av behandlingar som krävs för den kategori av tjänster som dessa medlemsföretag normalt rekryterar till eller ställer egen personal till förfogande för.

Bland annat kan det krävas att medlemsföretag inom vård- och omsorgsbranschen inhämtar hälsodeklaration med sanningsförsäkran avseende smittsamma sjukdomar från alla som ska rekryteras. Medlemsföretag gör även löpande kontroller av personal samt lagrar uppgifter om hur många kontroller som gjorts för att upprätthålla säkerhet avseende smittskydd.

Socialstyrelsen kräver vidare att vissa medlemsföretag säkerställer patientsäkerhet genom att kunna intyga att medlemsföretagens personal har godkänd legitimation, uppfyller språkkrav samt har giltig förskrivarkod. För att kunna uppfylla Socialstyrelsens, hälso- och sjukvårdslagens och övriga föreskrifter och myndigheters krav kan medlemsföretagen även komma att behandla uppgifter om etnicitet, modersmål, var utbildning så som läkarutbildning utförts och ID-handling med foto.

Samtliga dessa behandlingar som berörs ovan krävs regelmässigt för att dessa medlemsföretag ska kunna erbjuda tjänster inom ramen för rekrytering, uthyrning och omställning, samt för att medlemsföretagen och/eller kunden ska kunna agera i enlighet med tillämplig lagstiftning. Dessa medlemsföretag ska därför säkerställa att behandlingarna omgärdas av tillräckliga säkerhetsåtgärder och att endast de uppgifter som behövs för att uppfylla ändamålen med en viss typ av behandling behandlas, samt att det finns en laglig grund för respektive behandling.

9.14 Säkerhetsprövning enligt säkerhetsskyddslagen

9.14.1 Inledning

Medlemsföretagen kan komma i kontakt med verksamheter som behandlar säkerhetskänslig information och därmed omfattas av säkerhetsskyddslag (2018:585), vilken trädde i kraft den 1 april 2019. Aktörer som ska anställa eller anlita en person som genom anställning, eller på annat sätt, till exempel genom uthyrning, ska delta i säkerhetskänslig verksamhet ska säkerställa att en säkerhetsprövning genomförs av personen i fråga. Ställningstagandet avseende anställningen och ansvar för den bedömning som görs har den som beslutar om anställning eller deltagande i den säkerhetskänsliga verksamheten, alltså kunden. Kunden är således personuppgiftsansvarig och ansvarar för att säkerställa att behandlingen dels är tillåten i enlighet med dataskyddsförordningen dels påkallad samt utförd i enlighet med säkerhetsskyddslagen. Medlemsföretagen kan dock komma att genomföra utredningen på uppdrag av kunden, vilken sedan ligger till grund för kundens ställningstagande och beslut om anställning.

Säkerhetsprövningen syftar till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen och i övrigt är pålitlig från säkerhetssynpunkt. Prövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas, och följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår. Omfattningen av säkerhetsprövningen beror på vilken säkerhetsklass anställningen är placerad i, vilket bland annat baseras på

den typ av uppgifter som den anställda kommer att få ta del av. Anställningar eller annat deltagande i säkerhetskänslig verksamhet som endast innebär hantering av information i den lägsta säkerhetsskyddsklassen, *begränsat hemlig*, ska inte placeras i någon säkerhetsklass eftersom ett röjande av sådan information endast kan medföra ringa skada.⁶

För att undvika eventuella onödiga integritetsintrång bör säkerhetsprövningen utföras under ett *senare* skede i rekryteringsprocessen. Medlemsföretagen bör dock tidigt informera kandidaterna om den prövning som kunden enligt lag måste genomföra.

9.14.2 *Medlemsföretaget som personuppgiftsbiträde*

Kunden är som nämnt personuppgiftsansvarig för behandling av personuppgifter inom ramen för en säkerhetsprövning och i de fall medlemsföretag ska genomföra eller assistera kunden i en sådan prövning blir medlemsföretaget personuppgiftsbiträde.

Innan en kund uppdrar åt ett medlemsföretag att genomföra eller assistera vid en säkerhetsprövning bör kunden beakta att det är fråga om integritetskänslig uppgifter samt iaktta tillämpliga sekretessbestämmelser. Om kunden bedömer att det är lämpligt att ta hjälp av medlemsföretaget ska kunden och medlemsföretaget ingå ett personuppgiftsbiträdesavtal där kunden fastställer vilka skyldigheter som åligger medlemsföretaget, bland annat bör åtkomsten till personuppgifter begränsas till personer som behöver uppgifterna för att kunna utföra sitt arbete och att dessa får instruktioner om hur uppgifterna får användas.

Det åligger kunden att säkerställa att laglig grund för behandlingen finns, att de registrerade informeras, att uppgifterna inte sparas längre än nödvändigt etc. Medlemsföretaget får som personuppgiftsbiträde endast behandla personuppgifter i enlighet med instruktionerna från kunden.

9.15 **Dataskyddsförordningen och speciallagstiftning**

Dataskyddsförordningen är från och med den 25 maj 2018 direkt tillämplig som lag i Sverige och bestämmelserna i förordningen är tvingande. Det kan dock finnas annan lagstiftning som ställer kompletterande krav på hanteringen av personuppgifter i den mån det är möjligt att göra undantag eller förtydliganden i förhållande till dataskyddsförordningen.

I den mån speciallagstiftning på dataskyddsområdet är tillämplig på medlemsföretagens personuppgiftsbehandling på verksamhetsspecifik nivå bör medlemsföretagen informera sig om samt följa sådan speciallagstiftning. Dataskyddslagen, som innehåller kompletterande bestämmelser till dataskyddsförordningen, är tänkt att vara subsidiär i förhållande till sådan speciallagstiftning och kommer därmed att vara tillämplig i verksamheter som omfattas av särskild speciallagstiftning endast om inget annat följer av lag eller föreskrift.

⁶ Detta framgår av prop. 2017/18:89 s. 83.

10. ENSKILDAS RÄTTIGHETER

10.1 Allmänt

Att uppfylla enskilda individers rättigheter är en viktig del av medlemsföretagens dataskyddsarbete. Detta är viktigt både för att upprätthålla förtroende för branschen och för att medlemsföretagen ska kunna erbjuda effektiva tjänster inom ett område där det är särskilt viktigt att uppgifter om enskilda, så som kandidater, är uppdaterade, korrekta och endast behandlas så länge som krävs för att uppnå ändamålet. Det bör därför finnas tydliga policyer och riktlinjer på plats hos medlemsföretaget för att i varje enskilt fall kunna tillvarata enskildas rättigheter i enlighet med dataskyddsförordningen.

10.2 Dataportabilitet

Medlemsföretag ska på den registrerades begäran utan avgift tillhandahålla den registrerade de personuppgifter som rör honom eller henne, och som den registrerade tillhandahållit medlemsföretaget, i ett strukturerat, allmänt använt och maskinläsbart format. Rätten omfattar både personuppgifter som tillhandahållits aktivt genom exempelvis registreringar på medlemsföretagets hemsidor och passivt genom användning av medlemsföretagets tjänster.

Den registrerade har enbart rätt att begära portering av personuppgifter som behandlas med stöd antingen av samtycke eller för att fullgöra ett avtal till vilket den registrerade är part och det gäller bara sådana personuppgifter som den registrerade själv har lämnat.

Medlemsföretagen bör implementera verktyg som möjliggör för den registrerade att ladda ned eller, när det är möjligt och tillämpligt, direkt överföra sina uppgifter till en annan personuppgiftsansvarig. Den registrerade ska därvid kunna välja vilka uppgifter som ska överföras (porteras).

10.3 Registerutdrag

Den registrerade har rätt att vända sig till medlemsföretaget för att få information om de personuppgifter som medlemsföretaget behandlar om personen, genom ett så kallat registerutdrag.

I egenskap av personuppgiftsansvarig har respektive medlemsföretag en skyldighet att lämna ett sådant registerutdrag. Ett registerutdrag ska omfatta information om *vilka* personuppgifter om den registrerade som medlemsföretaget behandlar samt *hur* uppgifterna behandlas (bl.a. varifrån uppgifterna kommer, ändamålet med behandlingen, till vilka kategorier av mottagare uppgifterna lämnats ut och information om lagringstider och ev. överföring av uppgifter till tredje land). Den registrerade har alltså ingen egentlig rätt enligt dataskyddsregelverket att få ut enskilda dokument eller handlingar som sådana, även om det i vissa situationer skulle kunna vara det mest effektiva tillvägagångssättet. Dessutom kan sådana dokument omfatta även andra registrerades personuppgifter, vilka särskilt behöver strykas ifall sådant utlämnande ändå skulle ske.

Om begäran görs i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat. Utdraget ska vanligtvis tillhandahållas till den registrerade senast en månad från dess att begäran mottagits.

10.4 Rätt till rättelse, radering och begränsning

Rätt till rättelse

Alla personuppgifter som behandlas ska vara sakligt riktiga och aktuella i förhållande till det ändamål för vilket de behandlas. Medlemsföretagen ska säkerställa att de personuppgifter som behandlas är riktiga och uppdaterade. Personuppgifter som är felaktiga, ofullständiga eller irrelevanta ska rättas eller raderas.

Varje registrerad har en rätt att kontakta ett medlemsföretag och få felaktiga personuppgifter rättade. Efter mottagandet av en sådan upplysning, om att en uppgift som rör den registrerade är felaktig, ska uppgiften rättas utan onödigt dröjsmål. De registrerade har även en rätt att komplettera med personuppgifter som saknas och som kan vara relevanta för det ändamål för vilket personuppgifterna behandlas.

Att bestämma när en uppgift är felaktig kan vara komplext. Som tumregel kan sägas att personuppgifter bedöms som felaktiga om de inte stämmer överens med faktiska omständigheter och verkligheten. En kandidat kan emellertid anse att en bedömning av dennes kompetens är missvisande och fel. Sådan bedömning *kan* såklart vara felaktig, men om bedömningen är ett ärligt och sant resultat i en rekryteringsprocess så är den inte felaktig på sådant sätt att den föranleder rättelse.

En följd av en rättelse på den registrerades begäran är att medlemsföretaget måste informera även dem som de har lämnat ut uppgifter till om att uppgifterna har rättats. Detta gäller dock inte om det är alltför betungande, eller omöjligt.

Rätt till radering

Om den registrerade begär radering av personuppgifter som rör honom eller henne ska medlemsföretagen radera uppgifterna om de inte längre är nödvändiga för något av de ändamål de samlades in för under förutsättning att det inte finns lagkrav på att uppgifterna inte får raderas.

Därutöver kan medlemsföretagen tvingas radera personuppgifterna bl.a. om behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket eller om den enskilde motsätter sig personuppgiftsbehandling som sker med en intresseavvägning som laglig grund, och det inte finns berättigade skäl som väger tyngre än den enskildes intresse.

Undantag från rätten till radering medges för att tillgodose andra viktiga rättigheter, som till exempel rätten till yttrandefrihet och informationsfrihet, samt för uppfyllandet av en rättslig förpliktelse.

Rätt till begränsning av behandling

Medlemsföretagen ska se till att den registrerades rätt till begränsning efterlevs. Med begränsning av behandling menas att uppgifterna markeras för att enbart behandlas för vissa särskilda ändamål. En rätt att begära begränsning föreligger när den registrerade anser att uppgifterna är felaktiga och har begärt att de rättas. Under tiden uppgifternas korrekthet utreds ska behandlingen av uppgifterna begränsas. När en begränsning upphör (till exempel då utredningen om uppgifternas korrekthet är klar) ska den registrerade ges information om detta.

10.5 Rätt att göra invändningar

Medlemsföretagen ska tillgodose den registrerades rätt att invända mot behandling av dennes personuppgifter om den aktuella behandlingen stöds på uppgift av allmänt intresse, myndighetsutövning eller intresseavvägning som laglig grund.

Om den registrerade invänder mot sådan behandling får medlemsföretagen fortsätta att behandla personuppgifterna endast om medlemsföretagen kan visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Den registrerade har rätt att invända mot behandling av personuppgifter för direktmarknadsföring. Detta får som följd att personuppgifterna inte längre får behandlas för sådana ändamål.

10.6 Identifiering

Medlemsföretagen bör inrätta processer för säker identifiering för att säkerställa att varje individ kan identifiera sig vid utövandet av dennes rättigheter. Så kan exempelvis ske genom införande av tekniska lösningar för tvåfaktorsidentifiering.

11. SÄKERHET OCH SEKRETESS

11.1 Allmänt

Personuppgifter ska av medlemsföretagen alltid behandlas på ett sätt som säkerställer en hög nivå av säkerhet med användning av lämpliga tekniska eller organisatoriska åtgärder. Medlemsföretagen ska också alltid behandla uppgifter om enskildas personliga förhållanden konfidentiellt. Nedan beskrivs vanliga tekniska och organisatoriska säkerhetsåtgärder som kan anses utgöra en rimlig nivå som medlemsföretagen bör eftersträva för att uppfylla de säkerhetskrav som ställs i dataskyddsförordningen, utifrån den typ av tjänster som medlemsföretag inom bemanningsbranschen tillhandahåller. Medlemsföretagen ska slutligt själva avgöra vilka åtgärder som är lämpliga att vidta inom ramen för medlemsföretagens verksamhet och organisation.

11.2 Tekniska säkerhetsåtgärder

11.2.1 *Privacy by design och privacy by default*

Principen om *privacy by design* (sv. inbyggt dataskydd) innebär i korthet att integritetsfrågor ska beaktas under IT-systemens hela livscykel, till exempel genom att man inför åtkomstbegränsningar, minimerar mängden personuppgifter och inrättar stöd för säkerhetsfunktioner redan när system utvecklas. Medlemsföretagen kan i ljuset av denna princip välja att genomföra lämpliga tekniska och organisatoriska åtgärder för olika faser i systemens livscykler för att effektivt kunna beakta andra dataskyddsprinciper, såsom principen om uppgiftsminimering. I praktiken kan detta innebära att medlemsföretagen måste ta höjd för såväl kravställning som egen utveckling avseende de system som innehåller personuppgifter, särskilt sådana som innehåller en stor mängd uppgifter om exempelvis kandidater eller utlyrd personal.

Principen om *privacy by default* (sv. dataskydd som standard) innebär i korthet ett krav på att genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Det innebär att det minst

integritetskränkande alternativet ska vara den förvalda inställningen i systemet. I praktiken kan detta ställa krav på medlemsföretagen att utforma exempelvis rekryteringsplattformar och andra tjänster så att endast de uppgifter som krävs för ändamålet i fråga behandlas.

11.2.2 *Behörighetskontroll*

För att minimera riskerna för att personuppgifter behandlas felaktigt eller sprids i alltför vida kretsar kan medlemsföretagen införa tekniska lösningar för effektiv behörighetskontroll i de system som innehåller personuppgifter. Medlemsföretagens verksamhet är sådan att flera personer kan behöva ha åtkomst till personuppgifter för att tillhandahålla de tjänster som medlemsföretagen erbjuder. Samtidigt ska endast de personer som behöver åtkomst till uppgifterna för att utföra sina arbetsuppgifter ges sådan åtkomst. Detta innebär att enbart de som har sådana roller som kräver att de behandlar personuppgifter för att uppfylla de ändamål för vilka medlemsföretaget behandlar personuppgifterna ska ha behörighet att komma åt uppgifterna. Exempelvis bör personal som arbetar med rekrytering av konsulter till medlemsföretagen ges tillgång till alla personuppgifter om konsulten som behövs för rekryteringsprocessen, medan medlemsföretagens ekonomipersonal inte behöver ges tillgång till sådana uppgifter. Olika behörighetsnivåer kan därvid behöva införas i systemen.

11.2.3 *Loggning*

Åtkomst till personuppgifter i medlemsföretagens system bör kunna följas upp i efterhand genom loggar, där det ska framgå vem som har haft åtkomst samt tidpunkten för åtkomsten.

11.2.4 *Åtkomstskydd*

Medlemsföretagen bör vidta lämpliga säkerhetsåtgärder för att skydda personuppgifter mot obehörig åtkomst. Sådant skydd kan åstadkommas på olika sätt. Ett alternativ är att hålla datorutrustning, servrar och dylikt som innehåller personuppgifter inlåsta så att enbart behörig personal kan komma åt dem. Andra alternativ är exempelvis kryptering av data och lösenordsskydd av enheter såsom datorer och mobiler. Åtgärderna kan användas enskilt eller i kombination för att skapa starkare skydd. Vilka åtgärder som bör vidtas i det enskilda fallet beror på hur stora riskerna är, vilka tekniska möjligheter som finns och på kostnaderna. Medlemsföretagen ansvarar själva för att bedöma vilka åtgärder som är lämpliga. Åtkomst till system som innehåller stora mängder personuppgifter inklusive känsliga uppgifter, såsom rekryteringsplattformar, kräver i regel en högre nivå av säkerhet.

11.2.5 *Brandvägg, VPN m.m.*

Det finns flera alternativa lösningar för att minimera risken för obehörig extern åtkomst till personuppgifter. IT-system kan bland annat skyddas genom brandväggar, VPN, skyddade överföringar m.m.

11.2.6 *Pseudonymisering och anonymisering*

I de fall pseudonymisering och anonymisering är möjliga och lämpliga åtgärder bör medlemsföretagen tillämpa sådana åtgärder för att skydda de personuppgifter som behandlas av medlemsföretagen. Detta kan exempelvis åstadkommas genom att anonymisera eller pseudonymisera personuppgifter om kandidater i de fall en fullständig profil inte behöver användas i det enskilda fallet.

11.3 Organisatoriska säkerhetsåtgärder

11.3.1 IT- och informationssäkerhetspolicy

För att skapa kontroll över organisationens informationstillgångar och säkerställa att lämpliga säkerhetsåtgärder vidtas kan en IT- och informationssäkerhetspolicy implementeras inom organisationen. IT- och informationssäkerhetspolicyn bör närmare fastställa och beskriva innebörden av de åtgärder som medlemsföretagen beslutar att vidta. I policyn bör organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål avseende säkerhet redovisas. Policyn bör omprövas och uppdateras löpande för att säkerställa att den anpassas till aktuellt behov av skydd.

11.3.2 Kontroll och avstämning

För att säkerställa att organisationen följer uppsatta regler, riktlinjer och policyer på dataskyddsområdet, inklusive men inte begränsat till bestämmelserna i denna Vägledning, bör det införas rutiner för intern kontroll och övervakning.

11.3.3 Incidenthantering

Det bör även finnas rutiner för att rapportera och följa upp säkerhetsincidenter. Sådana rutiner bör innehålla en åtgärdsplan för hantering, identifiering, utvärdering och mitigering av personuppgiftsincidenter, inbegripet rapportering till tillsynsmyndigheten samt information till registrerade inom de tidsramar som följer av tillämplig dataskyddslagstiftning.

11.3.4 Utbildning

För att minska risken för felaktig hantering av personuppgifter bör organisationen se till att anställda som i sin tjänst behandlar personuppgifter har lämplig utbildning. Anställda bör känna till vad de får och inte får göra, vilka risker behandlingen medför och vad felaktig hantering kan få för konsekvenser.

12. RIKTLINJER FÖR LAGRING OCH GALLRING AV PERSONUPPGIFTER

12.1 Allmänt

Personuppgifter får inte sparas under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När personuppgifter inte längre är nödvändiga, eller lagringen på annat sätt är oförenlig med de grundläggande principerna i dataskyddsförordningen, ska uppgifterna gallras, dvs. raderas eller anonymiseras.

Eftersom Vägledningen inte kan reglera samtliga situationer när radering och gallring ska ske, bör medlemsföretagen ha policyer och riktlinjer på plats avseende lagring och gallring av personuppgifter. Riktlinjerna bör implementeras och tillämpas i hela medlemsföretagens organisationer.

Utöver uppställningen nedan kan det i annan lagstiftning finnas krav på bevarande av information som innebär att vissa uppgifter ska sparas hos medlemsföretagen under längre tid än vad som framgår nedan. Exempel på sådan specialreglering är lagringskrav i bokföringslagen och krav på att spara uppgifter om anställda i upp till tio år i vissa fall. Detta kan innebära att endast viss information om den enskilde är tillåten att spara.

12.2 Uppgifter om kandidater

Det kan finnas tungt vägande skäl för medlemsföretagen att lagra personuppgifter om kandidater under en sådan tid som kandidaterna är intressanta för nya tjänster. Detta är en viktig del av de tjänster medlemsföretagen i regel erbjuder. På motsvarande sätt bör kandidaterna i regel ha ett stort intresse av att deras personuppgifter sparas av bemanningsföretag under sådan tid som kandidaten är intresserad av att söka ett nytt jobb. I regel har slutkandidater, dvs. kandidater som kommit långt i rekryteringsprocesser ett större intresse av att deras personuppgifter lagras.

Därtill ställs det vissa krav i lag på att medlemsföretagen ska spara uppgifter under en viss tid. Bland annat är medlemsföretagen i regel skyldiga att spara vissa personuppgifter från ett rekryteringsförfarande under två (2) år på grund av diskrimineringslagstiftningen.

Det kan även finnas fall där medlemsföretagens kunder ställer krav på att spara uppgifter om kandidater under viss tid, till exempel för att göra egna granskningar och kontrollera urvalsprocessen. Om kunden bestämmer lagringstid ska kunden även vara den som bestämmer hur och varför personuppgiftsbehandling sker och därmed vara personuppgiftsansvarig för behandlingen. Kunden ansvarar då för att personuppgifterna inte lagras längre än vad som är nödvändigt för den aktuella behandlingen och medlemsföretagen ansvarar för att följa kundens instruktioner.

Baserat på övervägandena ovan och utifrån branschpraxis kan, som en generell utgångspunkt, medlemsföretagen lagra kandidaters personuppgifter enligt uppställningen nedan. Laglig grund för behandlingen kan vara dels rättslig förpliktelse, i enlighet med till exempel diskrimineringslagstiftningen, dels medlemsföretagens berättigade intresse att behandla relevanta personuppgifter om kandidater en tid efter anställningsförfarandet (i enlighet med vad som följer av branschpraxis). Det är viktigt att medlemsföretagen endast lagrar personuppgifter av betydelse för nämnda syften och att övriga uppgifter gallras.

Bevarandet av personuppgifter styrs dock i varje enskilt fall av det specifika ändamål för vilket uppgifterna sparas.

1. **Situation:** Registrering på rekryteringsplattform eller på annat sätt kontakt med medlemsföretaget för att visa intresse för rekryteringstjänsterna eller en enskild tjänst.

Tid: I tre (3) år efter det att kandidaten senast var aktiv, till exempel genom att söka jobb, uppdatera kontaktuppgifter och CV eller kontakta medlemsföretag.

2. **Situation:** Insamling av uppgifter under ansöknings-/rekryteringsprocessen, så som själva ansökan inklusive men inte begränsat till CV och personligt brev, intervjuanteckningar och uppgifter från referenser.

Tid: Så länge uppgifterna är nödvändiga för ansökningsförfarandet och därefter i tre (3) år.

3. **Situation:** Ansöknings-/rekryteringsprocessen för slutkandidat, själva ansökan inklusive men inte begränsat till CV och personligt brev, intervjuanteckningar och uppgifter från referenser.

Tid: Så länge uppgifterna är nödvändiga för ansökningsförfarandet och därefter i tre (3) år.

Observera att om uppgifterna ska sparas under en längre tid för framtida rekrytering så utgör det ett annat syfte och det krävs antingen samtycke från kandidaten eller att kandidaten genom att ingå avtal om exempelvis rekryteringstjänster aktivt visat ett intresse och godtagit att uppgifterna sparas under längre tid för sådana ändamål. Medlemsföretagen kan exempelvis, vid insamling av personuppgifter för rekrytering till en specifik tjänst, erbjuda de registrerade att kryssa i en ruta om de önskar att deras uppgifter behandlas i syfte att medlemsföretagen ska kunna kontakta den registrerade med nya jobberbjudanden.

Uppgifterna kan även sparas under längre tid än vad som framgår av uppställningen ovan om kandidaten aktivt visat ett intresse av andra tjänster än den tjänst som ursprungligen söktes, till exempel genom att kontakta medlemsföretaget för att vara tillgänglig för exempelvis nya jobberbjudanden. Sådan typ av interaktion mellan kandidat och medlemsföretag bör dokumenteras skriftligt. Det bör i sådan dokumentation framgå vilket det ursprungliga ändamålet varit för bevarandet respektive det nya ändamålet.

12.3 Uppgifter om konsulter och anställda

Som en generell utgångspunkt kan medlemsföretagen lagra konsulter och anställdas personuppgifter enligt uppställningen nedan.

Bevarandet av personuppgifter styrs dock i varje enskilt fall av det specifika ändamål för vilket uppgifterna sparas.

1. **Anställning/uppdrag och anställnings-/uppdragsavtal;** under avtalsförhållandet och därefter i tio (10) år.
2. **Uppgifter om kompetenser;** under avtalsförhållandet.
3. **Kontrolluppgifter;** tills dess att medlemsföretagets pensionsåtaganden upphört.
4. **Uppgifter om inloggningar och enskildas användning av utrustning;** i normalfallet endast så länge som uppgifterna används för utredning i enlighet med den information som lämnats till den anställda, om inte uppgifterna är nödvändiga för ytterligare interna kontroller vid misstanke om överträdelser av interna riktlinjer eller lagregler.

Övriga uppgifter, så som noteringar om den anställda, information från uppföljningssamtal, lönerrevisioner, statistik, kontaktuppgifter m.m., bör som huvudregel raderas när anställningsförhållandet avslutas.

12.4 Uppgifter om kunder och leverantörer

Som en generell utgångspunkt kan medlemsföretagen lagra kunders och leverantörers personuppgifter enligt uppställningen nedan.

Bevarandet av personuppgifter styrs dock i varje enskilt fall av det specifika ändamål för vilket uppgifterna sparas.

1. **Kund- och leverantörsavtal samt uppgifter om affärshändelser,** såsom uppgifter om tidrapporter, uppdrag, lön, faktura, deklarationer, bokslut; under avtalsförhållandet och därefter för sju (7) år när det gäller bokföringsdata samt tio (10) år när det gäller avtalet i övrigt.
2. **Kontaktuppgifter;** under den tid medlemsföretaget bedömer att uppgifterna är nödvändiga för att upprätthålla relationen med kunden/leverantören.

Radering ska ske när medlemsföretaget får kännedom om att uppgifterna inte längre är adekvata eller relevanta för ändamålet, eller på begäran av kontaktpersonerna.

12.5 Radering och gallring

Medlemsföretagen ansvarar för att inrätta processer för radering och gallring i alla system i enlighet med uppställda tidsgränser ovan.

Detta ställer krav på medlemsföretagen att säkerställa att det finns processer på plats för att kontrollera för vilka ändamål och baserat på vilka lagliga grunder personuppgifter sparas hos medlemsföretagen.

I praktiken innebär detta att om en kandidat vill bli raderad efter en rekryteringsprocess bör medlemsföretaget säkerställa att uppgifterna som sparas endast behålls för att uppfylla ändamålen att uppfylla kraven i diskrimineringslagstiftningen.

13. ÖVERFÖRING AV PERSONUPPGIFTER

13.1 Överföring av personuppgifter till tredje part, till exempel kunder och myndigheter

Medlemsföretagen behöver inom ramen för sina verksamheter löpande överföra personuppgifter till kunder, och i förekommande fall till andra bemanningsföretag så som underleverantörer eller samarbetspartners inom ramen för en överenskommelse med dessa. Vid varje överföring krävs det att medlemsföretagen säkerställer att överföringen är laglig och att individens rättigheter respekteras samt att individerna har informerats om sådana typer av överföringar. Medlemsföretagen behöver också fastställa uppdelningen av personuppgiftsansvar för respektive part (i enlighet med avsnitt 4), vilket är avgörande för medlemsföretagens skyldigheter enligt dataskyddsförordningen.

13.2 Överföring av personuppgifter till leverantörer

Flera av de tjänster medlemsföretagen erbjuder kan komma att utföras helt eller delvis av tredje part, såsom leverantörer av externa system och personlighetstester m.m. Om en sådan tredje part behandlar personuppgifter för ett medlemsföretags räkning anses denna part utgöra personuppgiftsbiträde. Varje medlemsföretag är skyldigt att säkerställa att personuppgiftsbiträdesavtal som uppfyller kraven i dataskyddsförordningen ingås med samtliga personuppgiftsbiträden.

Medlemsföretag kan använda sig av system från externa leverantörer för hantering av personuppgifter om kandidater m.m., till exempel system för e-post, rekryteringsplattformar och ärendehanteringssystem. Beroende på hur systemet är uppbyggt och används kan leverantören vara personuppgiftsbiträde till ett medlemsföretag, särskilt i de fall då den tekniska driften hanteras av leverantören på ett sådant sätt att personuppgifter lagras av leverantören för medlemsföretagets räkning. Det kan även finnas situationer där både leverantör och kund är personuppgiftsansvariga för den behandling av personuppgifter som utförs inom ramen för systemet. Varje medlemsföretag är skyldigt att gentemot såväl enskilda individer som externa parter säkerställa att det tydligt framgår vilken part som är personuppgiftsansvarig respektive personuppgiftsbiträde för de personuppgifter som hanteras. Baserat på sådana överväganden ska medlemsföretaget ingå avtal som reflekterar relationerna och uppfyller kraven i tillämplig dataskyddslagstiftning.

13.3 Tredjelandsöverföringar

Medlemsföretagen får endast överföra personuppgifter utanför EES-området om det finns en laglig grund för överföringen. Medlemsföretagen ska, om sådan överföring sker, informera den registrerade om överföringen samt hänvisa till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

BILAGA 1 – MATRIS ÖVER LAGLIG GRUND

Område	Laglig grund	Avsnitt
Rekrytering till enskild tjänst	Avtal (avseende rekryteringstjänst)	6.2.2
Rekryteringsplattformar	Avtal (avseende rekryteringstjänst)	6.3.2
Uthyrning	Avtal (anställningsavtalet)	7.2.1
Anställda hos underleverantörer	Intresseavvägning	7.3.1
Individuell prestationsmätning	Avtal (anställningsavtalet)	7.4
System för rekrytering och kompetensdatabaser	Intresseavvägning	7.5
Omställningsfrågor	Intresseavvägning	8.2
Analysresultat	Samtycke	8.3
Personlighets- och kompetenstester	Samtycke	9.1.2
Referenser	Intresseavvägning	9.2.1
Search (headhunting)	Intresseavvägning	9.3.2
Uppgifter om lagöverträdelser	Får ej behandlas	9.4
Register över ej önskvärda kandidater	Intresseavvägning	9.7
Kreditupplysningar	Avtal (anställningsavtalet)	9.9.2
Användandet av sociala medier	Intresseavvägning	9.10

Kompetensföretagen är en arbetsgivar- och branschorganisation för personaluthyrnings-, omställnings- och rekryteringsföretag med ca 700 medlemsföretag. Kompetensföretagen ingår i Almega och är medlem i Svenskt Näringsliv.

Branschen erbjuder kunder och medarbetare stor flexibilitet och trygghet. Grunden för verksamheten är att kunderna får tillgång till rätt kompetens vid rätt tillfälle för att kunna verka effektivt. Medarbetarna får möjlighet att utvecklas på en föränderlig arbetsmarknad med den trygghet som erfarenhet och kompetens från många olika arbetsplatser ger.

Kompetensföretagen
● almega

Läs mer på <http://www.kompetensforetagen.se>