ÖVERGRIPANDE INFORMATION OM BEHANDLING AV PERSONUPPGIFTER

Branschriktlinjer för tillämpning av Dataskyddsförordningen i fastighetsmäklarverksamhet

1. BAKGRUND

Dataskyddsförordningen (2016/679) utgör ett omfattande regelverk avseende behandling av personuppgifter och innebär både nya och utökade skyldigheter för personuppgiftsansvariga samt nya och utökade rättigheter för registrerade.

Denna övergripande information om behandling av personuppgifter beskriver några av de mest framträdande och viktiga delarna i Dataskyddsförordningen. Avsikten är att det ska vara möjligt att på en övergripande nivå skapa sig förståelse rörande hur regelverket ser ut och fungerar.

2. PERSONUPPGIFTSANSVAR

2.1 Bedömning av personuppgiftsansvaret

Personuppgiftsansvarig är enligt personuppgiftslagen och Dataskyddsförordningen den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter, dvs. *varför* och *hur* den aktuella behandlingen av personuppgifter genomförs. Det är den personuppgiftsansvarige som är ansvarig för att se till att behandlingen av personuppgifter sker i enlighet med reglerna i Dataskyddsförordningen. Vem som är personuppgiftsansvarig för en viss behandling av personuppgifter avgörs av en helhetsbedömning av omständigheterna i varje enskilt fall. Avgörande för denna bedömning är dock inte vem som har det formella ansvaret, utan vem som faktiskt har inflytande över behandlingen som utförs. En tumregel är att den som tagit initiativ till en viss behandling även är att anse som personuppgiftsansvarig.

Vidare måste personuppgiftsansvaret preciseras i förhållande till *varje* behandling (t.ex. insamling, överföring, lagring etc.) av personuppgifter som genomförs i ett flöde. Den omständigheten att personuppgiftsansvaret måste identifieras i förhållande till varje behandling är dessutom avgörande för att korrekt information om behandlingen ska kunna lämnas till de registrerade, samt för att det interna register över behandlingar av personuppgifter som den personuppgiftsansvarige kan vara skyldig att föra enligt Dataskyddsförordningen ska uppfylla kraven på vad registret ska innehålla enligt Dataskyddsförordningen.

Ett mäklarföretag är exempelvis personuppgiftsansvarigt för behandlingen av personuppgifter vid fullgörandet av förmedlingsuppdraget eftersom det är mäklarföretaget som har inflytandet över vilka personuppgifter som behandlas, samt för vilka ändamål dessa personuppgifter behandlas. Mäklarföretaget bestämmer således ändamålen med och medlen för behandlingen av personuppgifter inom ramen för förmedlingsuppdragets fullgörande.

Vad gäller mäklarföretag med franchisestruktur är det viktigt att utreda ansvarsförhållandena, särskilt i den mån det kan föreligga ett gemensamt personuppgiftsansvar mellan franchisegivare och franchisetagare. För att göra denna bedömning bör franchisestrukturen analyseras närmare, där närmare ledning t.ex. torde gå att finna i franchiseavtalet.

Om flera personuppgiftsansvariga är inblandade i behandling av personuppgifter och lämnar en gemensam information till den registrerade om behandlingen ska det enligt Datainspektionens tillsynspraxis klart framgå vem som är personuppgiftsansvarig i förhållande till respektive behandling för att den registrerade ska kunna tillvarata sina rättigheter.

2.2 Gemensamt personuppgiftsansvar

Av artikel 26 i Dataskyddsförordningen framgår vidare att i den utsträckning ett *gemensamt* personuppgiftsansvar föreligger ska de gemensamt personuppgiftsansvariga under "öppna former" fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt Dataskyddsförordningen. Detta ska ske genom ett inbördes arrangemang (dvs. någon form av skriftlig överenskommelse) som återspeglar de gemensamt personuppgiftsvarigas respektive roller och förhållande gentemot registrerade. Det väsentliga innehållet i arrangemanget ska enligt samma artikel göras tillgängligt för den registrerade. Innehållet i arrangemanget är dock inte bindande för den registrerade i den meningen att arrangemanget skulle förhindra den registrerade att välja vilken personuppgiftsansvarig som denne vill utöva sina rättigheter gentemot.

Det kan vara lämpligt att dokumentera arrangemanget i ett avtal mellan de företag som är gemensamt personuppgiftsansvariga. Avtalet bör ange (i) för vilka kategorier av behandlingar som företagen är gemensamt personuppgiftsansvariga, (ii) i förhållande till respektive kategori av behandling vem som är ansvarig för att fullgöra skyldigheterna som den personuppgiftsansvarige har enligt Dataskyddsförordningen och särskilt vem som ska säkerställa att information om behandlingen av personuppgifter lämnas till de registrerade och hantera en begäran från en registrerad om utövande av dennes rättigheter enligt Dataskyddsförordningen, samt (iii) en gemensam kontaktpunkt för de personuppgiftsansvariga.

3. GRUNDLÄGGANDE PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

All behandling av personuppgifter ska följa de grundläggande principerna för behandling i artikel 5 i Dataskyddsförordningen. Dessa grundläggande principer utgör Dataskyddsförordningens yttersta ramverk och den registrerade kan exempelvis inte samtycka till att den personuppgiftsansvarige behandlar personuppgifter i strid med dessa grundläggande principer. Det är därför av stor vikt att dessa principer observeras vid all behandling av personuppgifter, vilken typ av behandling som genomförs. De grundläggande principerna anges i avsnitt 3.1 – 3.7 nedan.

3.1 Laglighet

Behandling av personuppgifter är endast tillåten under förutsättning att behandlingen är laglig. Detta innebär bl.a. att personuppgiftsansvariga måste följa gällande lagstiftning vid behandling av personuppgifter och behandlingen ska alltid ske i enlighet med Dataskyddsförordningen.

3.2 Ändamålsbegränsning

Personuppgifter får endast behandlas för uttryckligt angivna och specifika ändamål. Vidare får personuppgifter inte behandlas för ändamål som är oförenliga med de ursprungliga ändamålen för vilka personuppgifterna samlades in. Det är därför inte tillåtet att använda redan insamlade uppgifter för helt andra ändamål än de för vilka uppgifterna samlades in. Exempelvis är det i regel inte tillåtet att samla in personuppgifter för ändamålet att kunna kontakta spekulanter för att sedan i strid med den dataskyddsinformation spekulanten erhållit, sälja spekulantregistret till en tredje part, om inte samtycke inhämtats från spekulanten.

3.3 Uppgiftminimering och lagringsminimering

Personuppgifter får endast behandlas om de är nödvändiga för att uppfylla de ändamål för vilka personuppgifterna ursprungligen samlades in. Personuppgifter ska således endast behandlas när det är nödvändigt och får därför inte behandlas endast för att personuppgifterna kan komma att vara användbara i framtiden (uppgiftsminimering). Av denna anledning är det av stor vikt att den personuppgiftsansvarige noggrant överväger vilka personuppgifter som behövs för respektive behandlingsaktivitet som den personuppgiftsansvarige avser utföra.

Personuppgifter får inte heller lagras för en längre tid än vad som är nödvändigt för att uppfylla ändamålen med behandlingen eller för att följa rättsliga förpliktelser. Det är därför av stor vikt att det finns fastställda gallringstider (dvs. efter vilken tid personuppgifter ska gallras) kopplade till respektive ändamål för behandling av personuppgifter.

Vägledning rörande gallringstider för särskilda typändamål som är typiskt förekommande i mäklarverksamhet är två år.

3.4 Personuppgifter ska vara uppdaterade och korrekta

Personuppgifter ska vara korrekta och uppdaterade. Detta innebär att det inte är tillåtet att behandla felaktiga personuppgifter om den registrerade. Den personuppgiftsansvarige bör därför säkerställa att det finns en rutin på plats som säkerställer att t.ex. kontaktuppgifter till spekulan-ter är uppdaterade och korrekta, så att det inte behandlas inkorrekta uppgifter i ett sådant spekulantregister. En sådan rutin kan exempelvis bestå i att mäklarföretaget i samband med att kontakt tas med en spekulant även ber spekulanten bekräfta att alla uppgifter fortfarande är korrekta.

3.5 Säkerhet

Den personuppgiftsansvarige är skyldig att säkerställa lämplig säkerhet i förhållande till de per-sonuppgifter som behandlas. Säkerheten gäller såväl organisatorisk, fysisk som teknisk säker-het. Det innebär att säkerhetsåtgärderna omfattar allt från interna rutindokument, fysiska åtgär-der som lås på dörrar till fysiska arkiv som omfattas av Dataskyddsförordningen eller till ser-verrum (i den mån servrar är belägna lokalt) och systemtekniska åtgärder såsom t.ex. kryptering. Inga personuppgifter får förekomma i system eller på andra lagringsytor som inte kan garantera en lämplig säkerhet avseende behandlingen.

Säkerhetsnivån ska vara lämplig i förhållande till mängden och typen av personuppgifter som behandlas. Detta innebär att ju fler personuppgifter som behandlas om ett större antal registrerade, desto högre krav ställs på säkerheten kring behandlingen.

3.6 Transparens

Behandling av personuppgifter ska vara transparent i förhållande till den registrerade så att den registrerade har en möjlighet att dels förstå hur och varför dennes personuppgifter behandlas och dels för att den registrerade ska ges möjlighet att utöva sina rättigheter. Transparens säker-ställs bland annat med klara och tydliga informationstexter till registrerade samt åtgärder för att underlätta för registrerade att utöva sina rättigheter i förhållande till behandlingen av deras per-sonuppgifter (såsom t.ex. rätten till tillgång (registerutdrag)).

En närmare beskrivning om vad informationen ska innehålla finns i [vägledning avseende in-formation till registrerade].

3.7 Ansvarsskyldighet

En viktig del i Dataskyddsförordningen är den ansvarsskyldighet som föreskrivs i de grundläggande principerna för behandling. Detta innebär att det är den personuppgiftsansvarige som bär bevisbördan för att Dataskyddsförordningen följs. Det är således inte upp till den registrerade eller till tillsynsmyndigheterna att bevisa att den personuppgiftsansvarige har brutit mot Dataskyddsförordningen, det är snarare den personuppgiftsansvarige som ska bevisa att den ansvarige följer de regler som föreskrivs i Dataskyddsförordningen. Ovanstående ställer höga krav på den personuppgiftsansvarige att dokumentera policys, rutiner och ställningstaganden, m.m. avseende behandling av personuppgifter.

4. LAGLIG GRUND FÖR BEHANDLING AV PERSONUPPGIFTER

När den personuppgiftsansvarige har säkerställt att de grundläggande principerna kan följas måste en laglig grund för behandlingen identifieras. De lagliga grunderna som den personuppgiftsansvarige kan tillämpa finns i artikel 6 i Dataskyddsförordningen och anges nedan. En laglig grund måste identifieras i förhållande till respektive behandling av personuppgifter.

4.1 Samtycke

Behandling av personuppgifter kan vara tillåten med stöd av den registrerades samtycke. Behandling av personuppgifter ska dock endast ske på grundval av samtycke i den utsträckning ingen annan laglig grund är tillämplig på behandlingen. Detta beror bland annat på att samtycke aktualiserar ytterligare regler i Dataskyddsförordningen (bl.a. reglerna om hur ett giltigt samtycke inhämtas samt att ett samtycke alltid går att återkalla).

Vad gäller reglerna avseende giltigt samtycke innebär dessa att ett samtycke måste vara otvetydigt och ha lämnats frivilligt av den registrerade, efter att den registrerade erhållit klar och tydlig information som säkerställer att den registrerade har förstått samtyckets omfattning. Om samtycke lämnas för flera specifika behandlingsändamål måste den registrerade ha möjlighet att välja vilka ändamål som ska omfattas av samtycket. Detta innebär att ett enda samtycke inte ska omfatta flera behandlingsändamål. Det är därför inte möjligt att med ett klick i en kryssruta samtycka till behandling av personuppgifter för flera ändamål som kräver samtycke, utan det måste finnas flera kryssrutor tillgängliga i sådant fall.

Vidare ska den registrerade alltid ha rätt att återkalla ett lämnat samtycke utan negativa följder. Det ska även vara lika lätt att återkalla ett samtycke som att lämna samtycket.

Samtycke kan normalt sett inte användas som laglig grund för behandling av personuppgifter i förhållande till anställda eller andra registrerade om det föreligger en tydlig obalans mellan den registrerade och den personuppgiftsansvarige, om inte tillämplig lagstiftning uttryckligen anger något annat.

4.2 Nödvändigt för att fullgöra eller ingå ett avtal

Det är tillåtet att behandla den registrerades personuppgifter om behandlingen är nödvändig för att kunna fullgöra- eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås med den registrerade. Det är viktigt att notera att avtalet ska gälla mellan den personuppgiftsansvarige och den registrerade. Det går således inte att använda denna lagliga grund om den personuppgiftsansvariges kontraktuella åtaganden endast gäller i förhållande till en tredje part.

Exempel på när denna lagliga grund kan vara aktuell att använda är i förhållande till administrationen av förmedlingsuppdraget avseende säljare. Eftersom det finns ett förmedlingsavtal med säljaren som ligger till grund för förmedlingsuppdraget är det möjligt att behandla säljarens personuppgifter i den mån behandlingen är nödvändig för att förmedlingsuppdraget ska kunna fullgöras. Se även nedan angående rättsliga förpliktelser.

4.3 Nödvändigt för att efterleva en rättslig förpliktelse

Det är tillåtet att behandla personuppgifter om det är nödvändigt för att fullgöra rättsliga förpliktelser, t.ex. för att kunna fullgöra bokföringsskyldighet eller för att fullgöra regler i Penningtvättslagen avseende kundkännedom. Den rättsliga förpliktelsen ska vara reglerad i svensk rätt eller EU-rätt för att utgöra en rättslig förpliktelse. Vidare ska även rättsliga skyldigheter som framgår av kollektivavtal omfattas av begreppet rättslig förpliktelse enligt lagförslaget till ny dataskyddslag i Sverige.

Ett annat exempel på rättslig förpliktelse är att mäklarföretag kan behandla personuppgifter på grund av att det finns en rättslig förpliktelse att föra anbudsförteckning i enlighet med fastighetsmäklarlagen (2011:666).

4.4 Berättigat intresse (Intresseavvägning)

Det är tillåtet att behandla personuppgifter om den personuppgiftsansvarige har ett berättigat intresse av att behandla personuppgifterna och detta intresse vid en bedömning väger tyngre än den registrerades integritetsintresse. Bedömningen huruvida det föreligger ett sådant berättigat intresse och om det väger tyngre än den registrerades intresse måste göras i förhållande till respektive behandling av personuppgifter i det enskilda fallet. Exempel där behandlingen sannolikt är tillåten med stöd av en intresseavvägning är behandling av personuppgifter som sker när kontaktuppgifter om spekulanter samlas in under visning i syfte att kunna kontakta spekulanterna och undersöka deras vidare intresse av objektet. Mäklarföretaget har då ett berättigat intresse av att kunna följa upp med spekulanter om de är intresserade av att lämna ett bud på objektet.

Det ska noteras att den registrerade alltid har rätt att invända mot behandling som grundas på en intresseavvägning av skäl som är hänförliga till den registrerades specifika situation. Om den registrerade invänder mot behandlingen måste den personuppgiftsansvarige kunna visa ett tvingande berättigat skäl för fortsatt behandling, dvs. ett betydligt starkare berättigat intresse än initialt. I exemplet med att spara spekulanters kontaktuppgifter i försäljningssyfte är det troligt att ett sådant tvingande berättigat skäl inte skulle föreligga om den registrerade skulle invända mot behandlingen. Skulle spekulanten trots invändningen ändå vilja delta i budgivningen, föreligger dock sannolikt ett sådant tvingande berättigat skäl eftersom det annars inte vore möjligt att genomföra budgivningen på ett ändamålsenligt sätt.

4.5 Behandling av känsliga personuppgifter

Känsliga personuppgifter får behandlas om den registrerade har lämnat sitt uttryckliga samtycke eller om behandlingen är tillåten enligt Dataskyddsförordningen eller den föreslagna svenska dataskyddslagen. Inom ramen för förmedlingsuppdraget bör inga känsliga personuppgifter behöva registreras, men om så är fallet krävs som huvudregel uttryckligt samtycke från den registrerade.

Känsliga personuppgifter definieras i Dataskyddsförordningen som uppgift som rör (i) ras eller etniskt ursprung, (ii) politiska åsikter, (iii) religiös eller filosofisk övertygelse, (iv) medlemskap

i fackförening, (v) genetiska eller biometriska uppgifter, (vi) hälsa, eller (vii) sexualliv eller sexuell läggning. Känsliga personuppgifter är således begränsade till endast dessa typer av personuppgifter.

Behandling av känsliga personuppgifter ställer högre krav på säkerheten kring behandlingen. Exempelvis ska åtkomst till känsliga personuppgifter som görs tillgängliga över så kallat öppet nät (t.ex. åtkomst via internet till en molntjänst) skyddas av tvåfaktorsautentisering. Detta innebär att det inte ska vara möjligt att endast logga in med användarnamn och lösenord, utan att ytterligare identifiering krävs (t.ex. mobilt bank-ID).

4.6 Personuppgifter rörande brott

Det finns ett generellt förbud mot att behandla personuppgifter som rör fällande domar i brottmål och överträdelser samt vissa s.k. säkerhetsåtgärder. Undantag från detta förbud gäller om behandlingen är tillåten enligt lag, Datainspektionens föreskrifter eller om Datainspektionen har utfärdat ett särskilt undantag i ett enskilt fall. Det torde vara ett mycket fåtal situationer där ett mäklarföretag kan behandla sådana personuppgifter i enlighet med Dataskyddsförordningen och de föreslagna svenska reglerna på området.

5. SÄKERHET OCH INCIDENTHANTERING

5.1 Tekniska och organisatoriska åtgärder

Den personuppgiftsansvarige är skyldig att vidta tekniska och organisatoriska åtgärder för att skydda personuppgifter från olaglig eller oavsiktlig förlust eller förvanskning, samt från otillåten eller olaglig tillgång till personuppgifter. De säkerhetsåtgärder som vidtas ska vara lämpliga med hänsyn till de särskilda risker som är kopplade till en viss behandling av personuppgifter, samt den nivå av känslighet som är kopplad till personuppgifterna. Exempelvis kräver behandling av känsliga personuppgifter en högre grad av säkerhet och kontroll än behandling av personuppgifter i allmänhet.

Säkerheten är särskilt viktig att beakta för mäklarföretag i sådana databaser som lagrar t.ex. undertecknade köpekontrakt eller andra dokument som kan innehålla integritetskänslig information (t.ex. information om ekonomiska förhållanden). Om den typen av personuppgifter tillgängliggörs över öppet nät (t.ex. om de lagras genom en molntjänst) ska tillgången till uppgifterna typiskt sett styras med tvåfaktorsautentisering, t.ex. genom mobilt bank-ID. För det fall personuppgifterna överförs externt via e-post ska e-postmeddelandet krypteras, t.ex. om låneuppgifter bifogas i ett e-postmeddelande.

5.2 Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen kodifierar principen om s.k. inbyggt dataskydd och dataskydd som standard. Detta innebär att samtliga system och applikationer som behandlar personuppgifter ska vara designade på ett sätt som möjliggör för de registrerade att utöva sina rättigheter enligt tillämplig lagstiftning samt för att säkerställa att personuppgifter behandlas på ett säkert och lagligt sätt. Vidare ska system och applikationer som behandlar personuppgifter vara designade för att i standardfallet efterleva de grundläggande principerna för behandling av personuppgifter. Exempelvis bör direkta identifierare (t.ex. personnummer), som inte är absolut nödvändiga för att uppnå ändamålen med behandlingen, pseudonymiseras (t.ex. genom att byta ut personnumret mot ett anställningsnummer).

5.3 Incidenthantering

En nyhet i Dataskyddsförordningen är reglerna avseende hantering av s.k. personuppgiftsincidenter. Personuppgiftsincident är en incident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter som behandlas. Det kan omfatta allt ifrån att en arbetsdator innehållande personuppgifter glöms på ett tåg eller att ett e-postmeddelande med personuppgifter skickas till fel mottagare, till fullbordade hackerattacker. Om en personuppgiftsincident inträffar är den personuppgiftsansvarige skyldig att utreda incidenten och dokumentera att incidenten har inträffat, vilka konsekvenser incidenten fått samt vilka åtgärder den personuppgiftsansvarige ska vidta eller har vidtagit för att säkerställa att motsvarande incident inte sker igen.

Om det är sannolikt att incidenten innebär en risk för de registrerades fri- och rättigheter i förhållande till behandlingen av personuppgifter, ska tillsynsmyndigheten meddelas senast inom 72 timmar från att incidenten upptäcktes. Om incidenten innebär en betydande risk för den personliga integriteten hos de registrerade, ska även de registrerade meddelas om incidenten. Mäklarföretag bör införa klara och tydliga riktlinjer och interna instruktioner för hur personuppgiftsincidenter ska hanteras.

När en personuppgiftsincident ska rapporteras till tillsynsmyndigheten ska en sådan rapport innehålla:

(i) en beskrivning av incidenten och, om möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs, inklusive vilka personuppgifter som omfattas av incidenten;

(ii) namn och kontaktuppgifter till dataskyddsombud (om sådant finns) eller annan kontaktperson hos mäklarföretaget;

(iii) en beskrivning av de sannolika konsekvenserna som incidenten innebär; samt

(iv) en beskrivning av de åtgärder som mäklarföretaget har vidtagit eller kommer att vidta för att åtgärda incidenten eller för att förmildra incidentens negativa effekter.

6. DE REGISTRERADES RÄTTIGHETER

Dataskyddsförordningen introducerar nya och utökade rättigheter som den registrerade kan utöva i förhållande behandlingen av den registrerades personuppgifter. Det är därför av stor vikt att en personuppgiftsansvarig har rutiner som möjliggör för den personuppgiftsansvarige att tillmötesgå en begäran om utövande av rättigheter från den registrerade.

Mäklarföretag behandlar i regel personuppgifter om ett stort antal individer, varför sannolikheten att en individ kan komma att utöva sina rättigheter inte torde vara obetydlig.

6.1 Rätt till information

En registrerad har nästan undantagslöst rätt till information avseende behandlingen av personuppgifter. Det är därför viktigt att det finns en rutin som säkerställer att Mäklarföretaget tillhandahåller information till de kategorier av registrerade vars personuppgifter mäklarföretaget behandlar.

Mer information om informationskravet återfinns i [vägledning avseende information till registrerade].

6.2 Rätt till tillgång (registerutdrag)

Utöver rätten till information ovan har registrerade rätt att på begäran få del av ytterligare information avseende behandlingen av deras personuppgifter samt även i vissa fall få en elektronisk kopia av de personuppgifter som behandlas. En sådan elektronisk kopia ska tillhandahållas i ett vanligt förekommande format inom en månad från att begäran inkommit.

Rätten till registerutdrag innebär att det bör vara möjligt för mäklarföretaget att exportera personuppgifter på individnivå från aktuella system och applikationer. Det ska i sådant fall vara möjligt att exportera samtliga personuppgifter rörande den aktuella individen och sammanställa dessa t.ex. i en elektronisk fil som översänds till den registrerade. Om personuppgifter om en individ behandlas i flera olika system och applikationer bör funktionalitet finnas för att uppgifter ska kunna exporteras från samtliga system och applikationer.

Den ytterligare information som den registrerade har rätt till i samband med ett registerutdrag ska innefatta:

(i) ändamålen med behandlingen;

(ii) de kategorier av personuppgifter som behandlas;

(iii) de mottagare eller kategorier av mottagare till vilka personuppgifter överförs;

(iv) om möjligt, den förutsedda period inom vilken personuppgifterna kommer att behandlas (eller kriterierna för att fastställa denna period);

(v) information om de rättigheter den registrerade har i förhållande till behandlingen;

(vi) rätten att klaga hos tillsynsmyndigheten;

(vii) om uppgifterna samlats in från någon annan än den registrerade, källan till personuppgifterna; samt

(viii) förekomsten av automatiserat beslutsfattande (dvs. automatiserade beslut som har rättsliga eller liknande följer för den registrerade, t.ex. automatiserade beslut om att lämna kredit till en individ), inklusive profilering.

Undantag till rätten till registerutdrag föreligger om begäran är uppenbart orimlig eller om registerutdraget skulle inverka menligt på andra registrerades fri- och rättigheter. Det ska dock noteras att dessa undantag bör tolkas restriktivt och att det alltid är den personuppgiftsansvarige som måste bevisa att det t.ex. är uppenbart orimligt att tillhandahålla ett registerutdrag. Vidare får en personuppgiftsansvarig ta ut en avgift om en registrerad begär ut fler än en kopia av personuppgifterna.

Avseende undantag från rätten till registerutdrag bör särskilt noteras att reglerna i Penningtvättslagen förbjuder att information ges till den registrerade bl.a. avseende anmälan till polisen, se penningtvättslagen 5 kap 7 §.

Utöver rutiner för att säkerställa att registrerade ges möjlighet att utöva rätten till registerutdrag behöver personuppgiftsansvariga även införa rutiner som säkerställer att det är rätt registrerad som får del av registerutdraget. Det bör därför införas någon form av rutin för att identifiera den registrerade. Om en kopia av personuppgifterna förs över till fel mottagare utgör detta en personuppgiftsincident (jfr punkt 5.3 ovan).

6.3 Rätt till rättelse

En registrerad har rätt att begära att få felaktiga personuppgifter rättade. Det ska i detta sammanhang noteras att den personuppgiftsansvarige som utgångspunkt är skyldig att självmant hålla personuppgifter korrekta och uppdaterade, med det finns även en rätt för registrerade att begära rättelse för det fall det är den registrerade som upptäcker felaktigheten.

6.4 Rätt till radering (rätten att bli bortglömd)

Registrerade har under vissa omständigheter rätt att begära att få sina personuppgifter raderade. En sådan rätt föreligger om:

(i) personuppgifterna är inte längre nödvändiga för att uppfylla det ändamål för vilket personuppgifterna ursprungligen samlats in;

(ii) den registrerade har återkallat sitt samtycke och det saknas annan laglig grund för att fortsatt behandla personuppgifterna;

(iii) den registrerade motsätter sig behandling som grundas på en intresseavvägning och det är inte möjligt att uppvisa ett tvingande legitimt intresse som väger tyngre än den registrerades integritetsintresse;

(iv) personuppgifterna har behandlats olagligt;

(v) det finns en rättslig skyldighet att radera personuppgifterna; eller

(vi) personuppgifterna har samlats in från barn inom ramen för ett tillhandahållande av informationssamhällets tjänster.

Rätten till radering är således inte någon rättighet som den registrerade alltid kan åberopa, eftersom den endast gäller under ovanstående förutsättningar.

Rätt till radering ska inte föreligga t.ex. om personuppgifterna behövs för att uppfylla en rättslig förpliktelse som kräver behandling av personuppgifterna eller om den personuppgiftsansvarige behöver personuppgifterna för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Det är därför viktigt att utreda huruvida det faktiskt föreligger en rätt till radering när en sådan begäran inkommer till mäklarföretaget, eftersom det i vissa fall faktiskt föreligger en rättslig skyldighet att fortsatt behandla personuppgifter (t.ex. penningtvättsregler).

6.5 Rätt till behandlingsbegränsning

Registrerade har under vissa omständigheter rätt att begära begränsning av behandlingen av deras personuppgifter. Denna rättighet innebär att den personuppgiftsansvarige bör ha tekniska möjligheter att markera eller flagga personuppgifter som begränsade i syfte att säkerställa att personuppgifterna inte är föremål för vidare behandling (annat än att endast lagras), om inte den registrerade samtycker till vidare behandling.

Rätten till behandlingsbegränsning föreligger i följande situationer:

(i) den registrerade bestrider att personuppgifterna är korrekta, under tiden som den personuppgiftsansvarige utreder om så är fallet;

(ii) om behandlingen är olaglig, men den registrerade inte vill att uppgifterna ska raderas, utan istället begränsas;

(iii) den personuppgiftsansvarige behöver inte längre personuppgifterna, men den registrerade behöver att uppgifterna lagras för att kunna fastställa, göra gällande eller försvara rättsliga anspråk; samt

(iv) den registrerade har invänt mot behandlingen, i väntan på kontroll av om den personuppgiftsansvarige har ett tvingande berättigat skäl att ändå fortsätta behandlingen.

Rätten till begränsning föreligger inte om den personuppgiftsansvarige behöver personuppgifterna för att fastställa, göra gällande eller försvara rättsliga anspråk.

6.6 Rätt till dataportabilitet

För det fall den registrerade själv har tillhandahållit personuppgifterna till den personuppgiftsansvarige och behandlingen grundas på (i) den registrerades samtycke, eller (ii) att behandlingen är nödvändig för att fullgöra eller ingå ett avtal med den registrerade, ska den registrerade ha rätt att på begäran erhålla sådana personuppgifter i ett vanligt förekommande och maskinläsbart format (t.ex. Word, Excel eller PDF), samt ha rätt att överföra sådana personuppgifter till en annan personuppgiftsansvarig.

Om det är tekniskt möjligt ska den personuppgiftsansvarige på den registrerades begäran föra över personuppgifterna direkt till en annan personuppgiftsansvarig. Detta skulle kunna innebära att, om förutsättningarna föreligger, ett mäklarföretag måste föra över personuppgifter som den registrerade själv tillhandahållit och som behandlas med stöd av någon av de ovan angivna grunderna direkt till ett annat mäklarföretag, om den registrerade begär det.

6.7 Rätt att motsätta sig behandling

Den registrerade har rätt att motsätta sig behandling av personuppgifter om behandlingen grundas på en intresseavvägning (artikel 6.1 f)) eller om behandlingen sker för direktmarknadsföringsändamål. Det är därför av stor vikt att det finns rutiner för att säkerställa att en sådan invändning kan hanteras på ett sätt som gör att invändningen skyndsamt handläggs och det utreds huruvida det kan föreligga ett tvingande berättigat skäl till fortsatt behandling. Om invändningsrätten föreligger är det viktigt att omgående efter att ha identifierat att så är fallet, upphöra med den behandling som invändningsrätten omfattar.

Om den registrerade invänder mot behandling som sker med stöd av en intresseavvägning har den personuppgiftsansvarige dock rätt att fortsatt behandla personuppgifterna om den personuppgiftsansvarige kan visa ett tvingande berättigat skäl (se ovan punkt 4.4). Bedömning huruvida ett tvingande berättigat skäl föreligger bör lämpligen göras av en jurist.

Rätten att invända mot behandling av personuppgifter för direktmarknadsföringsändamål innebär att mäklarföretaget upphöra att skicka direktmarknadsföring till den berörda individen om

invändning sker. Mäklarföretaget får hålla en lista över sådana personer som invänt mot behandling för direktmarknadsföringsändamål för att förhindra att dessa personer felaktigt får vidare direktmarknadsföring.

7. INTERNT REGISTER

Både personuppgiftsansvariga och personuppgiftsbiträden är typiskt sett enligt artikel 30 skyldiga att föra ett internt register över de behandlingar av personuppgifter som utförs inom ramen för verksamheten. Enligt Dataskyddsförordningen föreligger som huvudregel inte någon sådan skyldighet för företag med färre än 250 anställda. Om behandlingen (i) sannolikt kommer medföra en hög risk för de registrerades integritet, (ii) inte är tillfällig, eller, (iii) omfattar känsliga personuppgifter eller brottsuppgifter, ska ett register föras trots att företaget har färre än 250 anställda. Av särskild vikt är regeln i (ii) som säger att register alltid ska föras när behandlingen inte är tillfällig. Eftersom de flesta behandlingar som utförs inte är av tillfällig karaktär, innebär det i praktiken att samtliga mäklarföretag kommer att vara skyldiga att föra ett internt register avseende de flesta av personuppgiftsbehandlingarna som utförs.

Det interna registret ska alltid innehålla:

(i) Kontaktuppgifter till den personuppgiftsansvarige (samt dataskyddsombudet om sådant finns).

(ii) Ändamålen med behandlingen.

(iii) En beskrivning av kategorier av registrerade och kategorier av personuppgifter.

(iv) Angivande av eventuella överföringar utanför EU/EES.

(v) Gallringstider avseende de olika kategorierna av uppgifter.

(vi) En allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder som vidtas.

Utöver dessa punkter kan det vara lämpligt att komplettera det interna registret med information som strikt sett inte behöver ingå i det interna registret. Exempel på detta kan vara vilken laglig grund som tillämpas för respektive behandlingsändamål, externa mottagare av personuppgifter samt, i den mån mäklarföretaget behandlar personuppgifter i många olika system, vilka system som omfattas av en viss behandling. Anledningen till detta är att det interna registret blir mer förvaltningsbart, vilket kan underlätta t.ex. vid upprättandet av informationstexter.

8. ÖVERFÖRING AV PERSONUPPGIFTER

8.1 Överföring till andra personuppgiftsansvariga

Om en personuppgiftsansvarig överför personuppgifter till en annan personuppgiftsansvarig sker ett utlämnande av personuppgifterna. Sådan överföring är en behandling i sig vilken kräver att den personuppgiftsansvarige måste ha en laglig grund (artikel 6) för utlämnandet och bl.a. att de grundläggande kraven för behandling av personuppgifter (se punkt 3 ovan) är uppfyllda. Den personuppgiftsansvarige som lämnar ut personuppgifterna ska även säkerställa att de registrerade får information om utlämnandet varvid information bör lämnas om i vart fall kategorin av mottagare, ändamålen med utlämnandet och den lagliga grunden för utlämnandet. I vissa fall kan ytterligare information behöva lämnas, t.ex. kategorierna av utlämnade personuppgifter.

8.2 Överföring till personuppgiftsbiträden

När en personuppgiftsansvarig anlitar ett personuppgiftsbiträde (t.ex. en molntjänstleverantör) för att behandla personuppgifter för den personuppgiftsansvariges räkning måste ett s.k. personuppgiftsbiträdesavtal ingås med personuppgiftsbiträdet. Dataskyddsförordningen innehåller de-taljerade krav på vad ett sådant personuppgiftsbiträdesavtal ska innehålla.

8.3 Skiljelinje mellan överföring till personuppgiftsbiträde eller till annan personuppgiftsan-svarig

Det är viktigt att identifiera i vilken egenskap mottagaren av personuppgifterna kommer att be-handla personuppgifterna, dvs. i egenskap av personuppgiftsbiträde eller personuppgiftsansva-rig. Om mottagaren är personuppgiftsansvarig kommer överföringen att utgöra en behandling i sig, vilken behöver laglig grund och dessutom behöver inbegripas i den information som de registrerade har rätt till.

Om mottagaren är personuppgiftsbiträde inbegrips dock överföringen i den huvudsakliga be-handlingen och något särskild laglig grund är inte nödvändig för sådan överföring. Istället måste ett personuppgiftsbiträdesavtal ingås med personuppgiftsbiträdet, vilket inte är fallet om över-föringen görs till en annan personuppgiftsansvarig.

8.4 Överföringar utanför EU/EES

Om mäklarföretaget överför personuppgifter till en mottagare som är lokaliserad utanför EU/EES, behöver mäklarföretaget säkerställa att samtliga krav som ställs i Dataskyddsförord-ningen efterlevs. Detta inkluderar bl.a. att säkerställa en adekvat skyddsnivå för personuppgif-terna genom att t.ex. ingå Europeiska Kommissionens standardavtalsklausuler (eller motsva-rande från tid till annan gällande ramverk) med mottagande part. Standardavtalsklausulerna finns i två versioner, en version för överföring från en personuppgiftsansvarig till en annan per-sonuppgiftsansvarig och en version för överföring från en personuppgiftsansvarig till ett personuppgiftsbiträde.

9. DATASKYDDSOMBUD

Under vissa förutsättningar är den personuppgiftsansvarige skyldig att utnämna ett dataskydds-ombud som bl.a. ska informera och ge råd, övervaka behandlingen av personuppgifter och fun-gera som en kontaktpunkt för tillsynsmyndigheten. Ett dataskyddsombud ska utnämnas bl.a. om:

(i) kärnverksamheten består av behandling som innebär regelbunden och systematisk övervakning av registrerade i stor omfattning; eller

(ii) kärnverksamheten består av behandling av känsliga personuppgifter eller brottsuppgif-ter i stor omfattning.

Mot bakgrund av ovanstående bör de flesta mäklarföretag inte ha någon skyldighet enligt Data-skyddsförordningen att utnämna ett dataskyddsombud. Större organisationer bör dock överväga att ändå utnämna ett dataskyddsombud eller utse en person med motsvarande funktion som kan utöva en kontrollfunktion avseende de olika behandlingar av personuppgifter som genomförs av mäklarföretaget.

10. PERSONUPPGIFTER I FRITEXTFÄLT OCH OSTRUKTURERAT MATERIAL

10.1 Allmänt om behandling av personuppgifter i fritextfält

När personuppgifter behandlas i fritextfält är det mycket viktigt att vidta åtgärder för att säkerställa att inte fler personuppgifter än nödvändigt behandlas, framför allt för att inte riskera att bryta mot principen om uppgiftminimering. Vid användningen av fritextfält finns alltid en risk att personuppgifter av mer eller mindre känslig karaktär behandlas. Detta kan exempelvis vara fallet om en mäklare gjort ett besök hos en potentiell säljare och för in fritextanteckningar i ett CRM-system eller liknande. Mäklaren kan i detta fall potentiellt skriva t.ex. att den potentielle säljaren varit sjuk och inte kunnat närvara vid mötet, vilket skulle innebära en behandling av känsliga personuppgifter (hälsouppgifter), sannolikt utan laglig grund.

Av denna anledning är det viktigt att begränsa antalet fritextfält i så stor utsträckning som möjligt. När fritextfält används, bör det alltid finnas någon instruktion kopplat till användningen, t.ex. med riktlinjer kring vad mäklaren typiskt sett inte får skriva i ett fritextfält.

10.2 Behandling av personuppgifter i e-post

Eftersom behandling av personuppgifter i e-post omfattas av Dataskyddsförordningens regler, är det viktigt att mäklarföretaget har rutiner för behandling av personuppgifter i e-postkorrespondens. En stor utmaning vad gäller behandling av personuppgifter i e-post är att lämna information till de registrerade vars personuppgifter mäklarföretaget behandlar.

Vad gäller personuppgifter som behandlas hos en person som skickar ett mail till mäklarföretaget, kan det finnas anledning att se över möjligheten till ett automatiskt svar som skickas till avsändaren vid första e-postkontakt. Ett sådant automatiskt svar kan då innehålla en hänvisning till en personuppgiftsinformation som kan återfinnas på mäklarföretagets webbplats.

Vad gäller personuppgifter rörande personer som inte är en del av e-postkorrespondensen (t.ex. om en person nämns i korrespondens mellan två eller flera personer) är utgångspunkten ofta att någon information inte behöver lämnas.