Integritetsskydds myndigheten

Danske Bank A/S, Sverige Filial

Diarienummer:
DI-2021-2183

Datum:
2022-09-30

Beslut om tillstånd att behandla personuppgifter om lagöverträdelser

Integritetsskyddsmyndighetens beslut

Danske Bank A/S, Danmark, Sverige Filial (org.nr 516401-9811) får tillstånd att behandla personuppgifter om lagöverträdelser som innefattar brott genom kontroller av nya kunder mot den inom Danske Bank-koncernen förda interna Observationslistan över tidigare kunder som filialer inom Danske Bank-koncernen på grund av krav enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) anmält till Polismyndigheten och sedermera avslutat kundrelationen med i den mån det är nödvändigt för att uppfylla krav inom ramen för penningtvättslagen.

Beslutet gäller tills vidare men kan återkallas om Danske Bank A/S, Danmark, Sverige Filial behandlar eller kan komma att behandla personuppgifter på ett sätt som strider mot de förutsättningar som framgår av motiveringen till detta beslut.

Redogörelse för ärendet

Danske Bank A/S, Danmark, Sverige Filial (Danske Bank) ansöker, om Integritetsskyddsmyndigheten (IMY) anser att det behövs, om tillstånd enligt 3 kap. 9 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) att behandla personuppgifter om lagöverträdelser.

Av ansökan framgår bland annat följande.

Danske Bank är en nordisk bank med verksamhet i tolv länder i hela världen. I Sverige är Danske Bank den femte största banken med 140 000 privatkunder och 34 000 företagskunder.

Danske Bank har en skyldighet att efterleva bestämmelserna i penningtvättslagen och står under Finansinspektionens tillsyn i Sverige.

Enligt 2 kap. 3 § penningtvättslagen är Danske Bank skyldig att bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen (kundens riskprofil). Kundens riskprofil ska bestämmas med utgångspunkt i den allmänna riskbedömningen och verksamhetsutövarens kännedom om kunden.

Som en del av en koncern har Danske Bank en skyldighet att enligt 2 kap. 9 § andra stycket penningtvättslagen att följa gemensamma rutiner och riktlinjer inom koncernen

Postadress:
Box 8114
104 20 Stockholm
Webbplats:
www.imy.se
E-post:
imy@imy.se
Telefon:
08-657 61 00

avseende bland annat informationsutbyte för att säkerställa att information om misstänkt penningtvätt och finansiering av terrorism och andra relevanta uppgifter vid behov sprids till berörda inom koncernen.

Om avvikelser, misstänka aktiviteter eller transaktioner uppmärksammas måste Danske Bank vidta skärpta kundkännedomsåtgärder samt andra nödvändiga åtgärder för att bedöma om det finns skälig grund att misstänka att det är fråga om penningtvätt eller finansiering av terrorism eller att egendom annars härrör från brottslig handling.

Finner Danske Bank att det finns skälig grund för misstanke måste Danske Bank enligt 4 kap. 3 § penningtvättslagen rapportera misstanken till Finanspolisen inom Polismyndigheten. Danske Bank får enligt penningtvättslagen inte informera kunden eller annan utomstående om att en misstanke uppstått, att en rapport lämnats till Finanspolisen eller att informationen lagras.

En banks register över misstänkt penningtvätt eller finansiering av terrorism får enligt huvudregeln i 5 kap. 8 § penningtvättslagen inte samköras med motsvarande register hos annan. Det gäller dock enligt 5 kap. 9 § inte för bankkoncerner där verksamhetsutövarna har hemvist inom EES.

För att uppfylla dessa krav enligt penningtvättslagen har Danske Bank behov av att kontrollera nya kunder mot en intern lista över kunder som har rapporterats till Finanspolisen för misstänkt penningtvätt eller finansiering av terrorism och vars kundrelation har avslutats efter att ha rapporterats till Finanspolisen och bedömts överskrida Danske Banks riskaptit, den s.k. Observationslistan. Om en kund som förekommer på Observationslistan på nytt ansöker om att bli kund görs en individuell bedömning av kunden utifrån ett riskbaserat angreppssätt. Om misstanken inte kan vederläggas och kunden bedöms överskrida Danske Banks riskaptit för finansiell brottslighet kommer någon ny kundrelation inte att inledas. Om misstanken kan vederläggas och kunden i övrigt inte överskrider Danske Banks riskaptit kan däremot en ny kundrelation inledas.

Observationslistan ska vara gemensam för Danske Bank i Sverige, Danmark, Norge och Finland och samtliga nya kunder till dessa legala enheter ska kontrolleras mot den. Syftet med att kontrollera nya kunder mot Observationslistan är att bygga upp nödvändiga undersökande och förebyggande åtgärder för att säkerställa att kunder som Danske Bank tidigare har bedömt överskrida bankens riskaptit, och som en konsekvens därav fått sin kundrelation avslutad, kommer att upptäckas på ett adekvat sätt om individen ansöker om att bli kund på nytt. Det är Danske Banks erfarenhet att kunder som fått sin kundrelation i ett land därefter försöker ansöka om att bli kund på nytt i andra filialer eller andra länder. Det är därför helt nödvändigt att Observationslistan kombinerar kunder vars kundrelation har avslutats i olika filialer och länder för att säkerställa en heltäckande riskprofil på kunden.

Information till Observationslistan kommer att hämtas från Danske Banks system för misstänkt penningtvätt eller finansiering av terrorism (ANS-system). ANS-systemet är ett centralt system för informationssamling och beslutsfattande beträffande ärenden som rör finansiell brottslighet. En kund kommer inte med automatik att nekas bli kund i banken för att denne förekommer på Observationslistan, en träff innebär enbart en utökad kontroll för att fastställa kundens riskprofil.

Vid den initiala kontrollen mot Observationslistan kommer inte anledningen till att kunden tidigare anmälts till Finanspolisen eller anledningen till att kundrelationen

avslutades att framgå. Genom Observationslistans utformning och innehåll har Danske Bank minimerat antalet uppgifter som är relevanta för att uppnå ändamålet för vilka de behandlas. Av Observationslistan framgår enbart statusen ”Offboarded” samt följande nödvändiga information:

- Namn/företagsnamn,
- Kundens externa ID (personnummer eller organisationsnummer)
- Titel (verklig huvudman, företag och ägarandel)
- Adress
- Landet där kunden bor
- Medborgarskap
- Anställningsnummer för handläggaren inom banken som hanterade avslutandet av kundrelationen

Personuppgifterna på Observationslistan kommer inte att sparas längre än vad som krävs enligt penningtvättslagen, vilket är fem år efter det att kundrelationen avslutats.

Danske Bank A/S har samrått med Finanstilsynet i Danmark beträffande en rad åtgärder mot finansiell brottslighet vilket har inkluderat Observationslistan.

Danske Bank anser att det föreligger en rättslig förpliktelse enligt artikel 6.1 c i dataskyddsförordningen att utföra kontroller av nya kunder mot Observationslistan. Om Danske Bank inte kan genomföra kontroller mot Observationslistan på den rättsliga grunden rättslig förpliktelse anser Danske Bank att personuppgiftsbehandlingen i vart fall kan baseras på en intresseavvägning enligt artikel 6.1 f. Danske Bank ska beakta den kännedom som finns inom koncernen om tidigare misstankar om penningtvätt och finansiering av terrorism. Kontrollen är nödvändig för att förhindra att en kund vars kundrelation avslutats i en filial inte ska kunna vända sig till en annan filial inom Danske Bank och antas som kund utan att de misstankar som uppstått hos den första filialen beaktas. Om Danske Bank inte skulle genomföra kontrollerna ökar risken att Danske Bank utnyttjas för penningtvätt och finansiering av terrorism.

Danske Bank har därför ett berättigat intresse att utföra kontroller av nya kunder mot Observationslistan. Danske Bank bedömer vidare att upprätthållandet av och kontroller mot Observationslistan är absolut nödvändiga för att uppfylla ändamålet och att ändamålet inte kan uppnås på något annat sätt.

De registrerade som kommer att förekomma på Observationslistan är nuvarande och tidigare kunder till Danske Bank vilka i egenskap av kunder inte kan anses vara en integritetskänslig kategori av registrerade. Eftersom det följer av penningtvättslagen och kunderna informeras om sina skyldigheter får kunderna anses ha en förväntan om att deras aktiviteter och transaktioner övervakas och att eventuella misstankar rapporteras till Finanspolisen. Kunderna måste rimligen förvänta sig att tidigare misstankar om penningtvätt eller finansiering av terrorism kan komma att påverka deras möjligheter att bli kund hos Danske Bank.

Danske Bank har gjort vad den kan för att minska riskerna för kundernas fri- och rättigheter samt vidtagit åtgärder för att behandlingen i övrigt ska vara förenlig med dataskyddsförordningen. Kontrollerna kommer att genomföras av ett begränsat antal personer och i enlighet med Danske Banks nuvarande rutiner för validering av screening och riskklassificering vid on-boarding av kunder. Danske Bank kan skilja på äkta och falska träffar.

Motivering av beslutet

Tillämpliga bestämmelser m.m.

Enligt 2 kap. 3 § penningtvättslagen ska en verksamhetsutövare bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen. Kundens riskprofil ska bestämmas med utgångspunkt i den allmänna riskbedömningen och verksamhetsutövarens kännedom om kunden.

Enligt 5 kap. 6 § penningtvättslagen får personuppgifter om lagöverträdelser behandlas om det är nödvändigt bland annat för att bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §.

En verksamhetsutövares register med uppgifter om misstänkt penningtvätt eller finansiering av terrorism får enligt 5 kap. 8 § penningtvättslagen inte samköras med motsvarande register hos någon annan. Enligt 5 kap. 9 § gäller förbudet dock inte samkörning av register som sker mellan bland annat banker som ingår i samma koncern, om verksamhetsutövarna har hemvist i Sverige eller inom EES.

Det framgår av 2 kap. 9 § penningtvättslagen att en verksamhetsutövare som är det yttersta moderföretaget i en koncern ska fastställa gemensamma rutiner och riktlinjer för koncernen. De gemensamma rutinerna och riktlinjerna ska åtminstone omfatta rutiner och riktlinjer för behandling av personuppgifter och informationsutbyte inom koncernen för att säkerställa att information om misstänkt penningtvätt och finansiering av terrorism och andra relevanta uppgifter vid behov sprids till berörda inom koncernen.

Av artikel 10 i dataskyddsförordningen framgår att behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder får utföras endast under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

IMY har med stöd av 3 kap. 9 § dataskyddslagen och 6 § andra stycket förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringsförordningen) möjlighet att i enskilda fall besluta att andra än myndigheter får behandla personuppgifter som avses i artikel 10 i dataskyddsförordningen. Ett beslut får förenas med villkor.

I förarbetena till dataskyddslagen görs bedömningen att utrymmet för att tillåta behandling av personuppgifter som rör lagöverträdelser är större enligt dataskyddsförordningen jämfört med den tidigare gällande personuppgiftslagen, samt att utrymmet för att avslå en begäran om tillstånd i princip torde vara begränsat till de fall där behandlingen skulle vara oförenlig med dataskyddsförordningen i övrigt, i synnerhet principerna i artikel 5 och kravet på rättslig grund i artikel 6 (prop. 2017/18:105 s. 99 ff).

Av artikel 5.1 a i dataskyddsförordningen följer att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Principen om laglighet innebär bland annat att behandlingen ska ha stöd i någon rättslig grund i artikel 6.1. Principen om korrekthet innefattar en intresseavvägning eller proportionalitetsbedömning, som innebär att behandlingen inte får vara oskälig i förhållande till den registrerade (prop. 2017/18:105 s. 47 f).

Av artikel 5.1 följer vidare att uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1 b), att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (artikel 5.1 c), samt att uppgifterna inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (artikel 5.1 e).

Enligt principen om ansvarsskyldighet i artikel 5.2 i dataskyddsförordningen ska den personuppgiftsansvarige ansvara för och kunna visa att behandlingen är förenlig med principerna i artikel 5.1.

Enligt artikel 6.1 i dataskyddsförordningen krävs att en behandling av personuppgifter har stöd i någon av de rättsliga grunder som anges där. Av artikel 6.1 c följer att behandling av personuppgifter är tillåten om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Av artikel 6.1 f följer att behandling av personuppgifter är tillåten om behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter.

Krävs IMY:s tillstånd för behandlingen?

Behandlas personuppgifter som avses i artikel 10 i dataskyddsförordningen?
Information om ett rättsligt förfarande som inletts mot en fysisk person utgör personuppgifter som rör lagöverträdelser som innefattar brott i den mening som avses i artikel 10 i dataskyddsförordningen. Detta innebär att t.ex. uppgifter om att en person är eller har varit föremål för en polisanmälan, en förundersökning, ett åtal eller rättegång i ett brottmål omfattas av skyddet i artikel 10. Den som behandlar personuppgifter genom att utföra kontroller av kunder mot en lista över fysiska personer som har rapporterats till Finanspolisen för misstänkt penningtvätt eller finansiering av terrorism behandlar således personuppgifter om lagöverträdelser som innefattar brott.

Är behandlingen nödvändig för att fullgöra en rättslig förpliktelse (artikel 6.1 c och 5 § kompletteringsförordningen)?
Danske Bank har för det fall Observationslistan anses innehålla uppgifter om lagöverträdelser som innefattar brott uppgett att behandlingen är nödvändig för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras.

Enligt 5 § 2 kompletteringsförordningen får personuppgifter som rör lagöverträdelser som innefattar brott behandlas om behandlingen är nödvändig för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras. För det fall Danske Banks kontroll av nya kunder mot Observationslistan är en personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse behöver Danske Bank inte IMY:s tillstånd för att få behandla uppgifterna i fråga.

Enligt IMY bör 5 § 2 kompletteringsförordningen tolkas med utgångspunkt i artikel 6.1 c i dataskyddsförordningen där det framgår att en personuppgiftsbehandling är laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

Enligt artikel 6.3 i dataskyddsförordningen ska den grund för behandlingen som avses i 6.1 c fastställas i enlighet med unionsrätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Av bestämmelsen framgår vidare att syftet med behandlingen ska fastställas i den rättsliga grunden. Av skäl 41 till EU:s dataskyddsförordning framgår att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsebar för dem som omfattas av den. När det gäller vilken grad av tydlighet och precision som krävs för att behandling av personuppgifter ska anses nödvändig har regeringen i förarbetena till dataskyddslagen uttalat att det måste bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär. Regeringen har vidare uttalat följande. ”Ett mer kännbart intrång, t.ex. behandling av känsliga personuppgifter inom hälso- och sjukvården, kräver att den rättsliga grunden är mer preciserad och därmed gör intrånget förutsebart. Om intrånget är betydande och innebär övervakning eller kartläggning av den enskildes personliga förhållanden krävs dessutom särskilt lagstöd enligt 2 kap. 6 och 20 §§ RF” (prop. 2017/18:105 s. 51).

IMY konstaterar att för att artikel 6.1 c i dataskyddsförordningen ska vara tillämplig krävs en i rättsordningen fastställd rättslig förpliktelse som uppfyller kraven på precision och tydlighet. Om förpliktelsen är för svepande och ger den personuppgiftsansvarige en alltför stor handlingsfrihet i fråga om hur den ska uppfyllas kan den inte utgöra rättslig grund enligt artikel 6.1 c.[1] Bestämmelsen i 5 § 2 kompletteringsförordningen bör tolkas på motsvarande sätt.

Ett företag ska enligt 2 kap. 3 § penningtvättslagen vidta åtgärder som syftar till att förhindra att det utnyttjas för penningtvätt och finansiering av terrorism. Åtgärderna ska anpassas efter risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism, ett s.k. riskbaserat förhållningssätt. Det riskbaserade förhållningssättet innebär att verksamhetsutövare har utrymme för egna bedömningar i fråga om vad som utgör en tillräcklig kontroll av kundens identitet. För det fall en allmän hänvisning till en verksamhetsutövares skyldighet att bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen skulle innebära en rättslig förpliktelse att behandla uppgifter om lagöverträdelser skulle detta betyda en väsentlig utvidgning av möjligheterna att behandla personuppgifter om lagöverträdelser.

Kraven på kundkännedom är uppfyllda om åtgärderna för kundkännedom kan vidtas i en sådan omfattning att risken för penningtvätt och finansiering av terrorism i den enskilda kundrelationen kan hanteras, dvs. hållas på en acceptabel nivå. Det riskbaserade synsättet bygger också på att brister avseende en eller flera åtgärder för kundkännedom ska kunna läkas genom att den fortlöpande uppföljningen och övervakningen av affärsrelationen skärps.

IMY bedömer att bestämmelsen i 2 kap. 3 § penningtvättslagen är för otydlig och oprecis för att anses utgöra en rättslig förpliktelse av sådan precision och tydlighet att den kan ligga till grund för den aktuella behandlingen av personuppgifter. Danske Banks behandling av personuppgifter som rör lagöverträdelser kan därmed inte ske med stöd av 5 § 2 kompletteringsförordningen.

[1] Jfr SOU 2017:39 s. 114 f., Artikel 29-gruppens yttrande 6/2014, WP 217, s. 20 f. och Förvaltningsrätten i Stockholms dom 2020-06-17 i mål nr 9379-19 och 9408-19.

Danske Bank har således inte rättslig grund för den aktuella behandlingen i artikel 6.1 c i dataskyddsförordningen. Danske Bank behöver därmed IMY:s tillstånd enligt 3 kap. 9 § dataskyddslagen för att få behandla uppgifterna i fråga.

Ska tillstånd ges?

För att IMY ska kunna bifalla Danske Banks begäran om tillstånd att behandla personuppgifter som rör lagöverträdelser som innefattar brott, ska Danske Bank i enlighet med principen om ansvarsskyldighet kunna visa att behandlingen är förenlig med dataskyddsförordningen, särskilt artiklarna 5 och 6.

IMY konstaterar att det av Danske Bank uppgivna ändamålet att leva upp till kraven i penningtvättslagen är ett sådant särskilt, uttryckligt angivet och berättigat ändamål som avses i artikel 5.1 b i dataskyddsförordningen.

Är behandlingen nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intresse (artikel 6.1 f)?

Danske Bank uppger att för det fall IMY:s tillstånd krävs för kontroller mot Observationslistan så kan behandlingen baseras på en sådan intresseavvägning som sägs i artikel 6.1 f i dataskyddsförordningen.

För att personuppgiftsbehandlingen ska kunna stödjas på artikel 6.1 f i dataskyddsförordningen krävs att Danske Bank kan visa att 1) det finns ett berättigat intresse, 2) behandlingen av personuppgifter är nödvändig för ett ändamål som rör det berättigade intresset och 3) att de registrerades grundläggande fri- och rättigheter inte väger tyngre än det berättigade intresset.

Har Danske Bank ett berättigat intresse?

Danske Bank har uppgett sig ha ett berättigat intresse att kontrollera kunder mot Observationslistan för att leva upp till kraven att motverka penningtvätt och finansiering av terrorism genom att följa gemensamma rutiner och riktlinjer inom koncernen avseende bland annat informationsutbyte för att säkerställa att information om misstänkt penningtvätt och finansiering av terrorism och andra relevanta uppgifter vid behov sprids till berörda inom Danske Bank. Kontrollen är nödvändig för att förhindra att en kund vars kundrelation avslutats i en filial inte ska kunna vända sig till en annan filial inom Danske Bank-koncernen och antas som kund utan att de misstankar som uppstått hos den första filialen beaktas. Personuppgifterna kommer inte att sparas längre än vad som krävs enligt penningtvättslagen vilket är fem år efter det att kundrelationen avslutats.

IMY konstaterar att det intresse som Danske Bank har hänvisat till är ett sådant berättigat intresse som avses i artikel 6.1 f i dataskyddsförordningen.

Är behandlingen av personuppgifter nödvändig för det berättigade intresset?

Nödvändighetskriteriet i artikel 6.1 f i dataskyddsförordningen ska ses mot bakgrund av att undantag och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är absolut nödvändigt. Vidare följer av skäl 39 till dataskyddsförordningen att personuppgifter endast bör behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

Av praxis följer vidare att kravet på nödvändighet ska prövas tillsammans med principen om uppgiftsminimering enligt artikel 5.1 c i dataskyddsförordningen, som föreskriver att de personuppgifter som samlas in ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

IMY konstaterar att Danske Bank bedriver en sådan verksamhet som lagstiftaren bedömt typiskt sett kunna utnyttjas för penningtvätt och finansiering av terrorism.

Danske Bank har en skyldighet att bedöma kundens riskprofil. En riskfaktor som kan vara relevant för bedömningen är om Danske Bank känner till att kunden varit föremål för rapportering om misstänkta transaktioner.

I propositionen Ytterligare åtgärder mot penningtvätt och finansiering av terrorism (prop. 2016/17:173 s. 313) framhöll regeringen att ska det vara tillåtet för verksamhetsutövare som ingår i samma koncern samt verksamhetsutövare som bedriver gränsöverskridande verksamhet via filial att samköra sina register. Detta undantag från samkörningsförbudet är begränsat till kreditinstitut och finansiella institut, som bedöms ha störst behov av samkörning. Det är moderföretaget i en koncern som ska fastställa gemensamma rutiner och riktlinjer för koncernen. De gemensamma rutinerna och riktlinjerna ska bland annat avse informationsutbyte inom koncernen samt gemensamma rutiner och riktlinjer för behandling av personuppgifter. Information ska kunna delas mellan moder- och dotterbolag och mellan dotterbolagen. Rutiner och riktlinjer för informationsutbyte ska säkerställa att det finns en intern kommunikation om misstankar om penningtvätt eller finansiering av terrorism. Om ett dotterbolag lämnar en rapport om sådana misstankar till Finanspolisen förutsätts denna information i regel delas med övriga delar av verksamheten. Sådan information kan vara relevant för den allmänna riskbedömningen. Informationen kan också syfta till att säkerställa att den kund som rapporterats inte kan bli kund i ett annat dotterbolag, eller i vart fall att information om rapporteringen beaktas vid riskklassificeringen. Det praktiskt genomförbara sättet att åstadkomma sådana kontroller som åligger Danske Bank är att utföra kontroller mot Observationslistan där uppgifter behandlas om kunder som tidigare rapporterats till Finanspolisen och vars kundrelation avslutats.

Mot denna bakgrund har Danske Bank visat att den tilltänkta behandlingen av personuppgifter är nödvändig för det berättigade intresset. Det innebär att Danske Bank har visat att personuppgiftsbehandlingen lever upp till principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen.

Intresseavvägning

Slutligen krävs det att de registrerades grundläggande fri- och rättigheter inte väger tyngre än det berättigande intresset.

Företag som omfattas av penningtvättslagens regelverk ska bedöma sina kunders riskprofil med utgångspunkt i en allmän riskbedömning där det särskilt ska beaktas vilka slags produkter och tjänster företaget tillhandahåller. Särskilt stora krav ställs på kreditinstitut som Danske Bank som tillhandahåller produkter och tjänster som kan utnyttjas för penningtvätt och finansiering av terrorism i stor omfattning med svåra konsekvenser som följd. Lagstiftaren har i en särskild bestämmelse i 5 kap. 9 § andra stycket penningtvättslagen gjort ett undantag från förbudet att samköra penningtvättsregister och tillåtit att bland annat kreditinstitut får samköra sina egna penningtvättsregister på koncernnivå på grund av den stora risk för penningtvätt och finansiering av terrorism som föreligger i kreditinstituts verksamhet. Det åligger

moderföretaget i en bankkoncern att fastställa gemensamma rutiner och riktlinjer för koncernen avseende behandling av personuppgifter och informationsutbyte inom koncernen för att säkerställa att information om misstänkt penningtvätt och finansiering av terrorism sprids till berörda inom koncernen. Danske Bank har således ett mycket tungt vägande intresse av den aktuella personuppgiftsbehandlingen.

Behovet av att kunna utföra kontroller mot en koncernintern lista om lagöverträdelser som innefattar brott måste vägas mot den risk för intrång i de registrerades personliga integritet som personuppgiftsbehandlingen innebär.

IMY konstaterar att Observationslistan innehåller uppgifter enbart om nuvarande och tidigare kunder till Danske Bank som Danske Bank anmält till Finanspolisen och sedermera avslutat kundförhållandet med. Kunderna informeras om skyldigheter enligt penningtvättslagen och kan enligt IMY:s mening förvänta sig att deras aktiviteter och transaktioner övervakas och att eventuella misstankar rapporteras till Finanspolisen. Kunderna kan vidare förvänta sig att tidigare misstankar om penningtvätt eller finansiering av terrorism kan påverka deras möjligheter att bli kund på nytt hos Danske Bank.

IMY konstaterar att Danske Bank har vidtagit en integritetsskyddande åtgärd genom att införa rutiner för att skilja på s.k. äkta och falska träffar vid kontroller mot Observationslistan. Detta för att undvika felaktiga utpekanden av personer och en felaktig behandling av personuppgifter. Kontrollerna kommer vidare att genomföras av endast ett begränsat antal personer. Uppgifterna på Observationslistan kommer att gallras fem år efter det att kundförhållandet avslutades.

Sammanfattningsvis har Danske Bank visat att det berättigade intresset väger tyngre än de registrerades integritetsintresse.

Sammanfattande bedömning

Det ovanstående innebär att Danske Bank har visat att personuppgiftsbehandlingen kan stödjas på den rättsliga grund som åberopats av Danske Bank, dvs. artikel 6.1 f i dataskyddsförordningen. Danske Bank har vidare visat att behandlingen av personuppgifter är förenlig med principerna om laglighet, uppgiftsminimering och lagringsminimering enligt artikel 5.1 a, c och e. Det innebär att det föreligger förutsättningar för IMY att ge Danske Bank tillstånd att behandla personuppgifter som rör lagöverträdelser vid kontroller av nya kunder mot den inom Danske Bank-koncernen förda interna Observationslistan.

Villkor

Beslutet förutsätter att Danske Bank behandlar personuppgifter i enlighet med bestämmelserna i dataskyddsförordningen. Beslutet kan komma att återkallas om det visar sig att Danske Bank behandlar eller kan komma att behandla personuppgifter på ett sätt som strider mot dataskyddsförordningen.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av avdelningsdirektören Hans Kärnlöf. Vid den slutliga handläggningen har även rättschefen David Törngren och enhetschefen Catharina Fernquist medverkat.

Lena Lindgren Schelin, 2022-09-30 (Det här är en elektronisk signatur)

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Integritetsskyddsmyndigheten måste ha fått ert överklagande inom tre veckor från den dag ni fick del av beslutet, annars kan överklagandet inte prövas. Integritetsskyddsmyndigheten sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om Integritetsskyddsmyndigheten inte själv ändrar beslutet på det sätt ni har begärt.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.