IMY. Integritetsskydds myndigheten

Vägledning – föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1)

Diarienummer:
IMY-2024-7587

1 Inledning

Genom 6 och 7 §§ i Integritetsskyddsmyndighetens föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1) är det tillåtet för vissa företag att behandla sådana personuppgifter som avses i artikel 10 i dataskyddsförordningen[1] (personuppgifter som rör lagöverträdelser) för kontroller av till exempel kunder, leverantörer och arbetstagare mot så kallade sanktionslistor.

Syftet med vägledningen är att närmare förklara regleringen i 6 och 7 §§ för att underlätta tillämpningen för de företag som omfattas av föreskrifterna.

2 Företag under Finansinspektionens tillsyn

Det framgår av 6 § första stycket att bestämmelsen avser företag som står under Finansinspektionens tillsyn.

Med företag under Finansinspektionens tillsyn avses företag med Finansinspektionens tillstånd att erbjuda finansiella tjänster, såsom exempelvis banker och kreditmarknadsföretag[2], företag som tillhandahåller betaltjänster[3], fondbolag[4], försäkringsföretag[5], försäkringsförmedlare[6], företag som driver verksamhet med konsumentkrediter[7] och värdepappersinstitut[8]. Vidare avses företag som är registrerade hos Finansinspektionen och endast delvis står under Finansinspektionens tillsyn. Ett exempel på sådana företag är finansiella institut[9].

3 Föreskrifter och regelverk på finansmarknadsområdet

Utöver kravet i 6 § första stycket på att företag ska stå under Finansinspektionens tillsyn för att få behandla personuppgifter som rör lagöverträdelser för kontroller mot sanktionslistor krävs att behandlingen är nödvändig för att efterleva lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, andra föreskrifter eller regelverk på finansmarknadsområdet utfärdade av utländska myndigheter, EU-organ eller mellanstatliga organisationer.

Exempel på föreskrifter och regelverk som avses i 6 § första stycket är:

- Lagen (2004:297) om bank- och finansieringsrörelse
- Lagen (2007:528) om värdepappersmarknaden
- Regelverk utfärdade av U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC)
- Rekommendationer från Financial Action Task Force (FATF)

---

[1] 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 (allmän dataskyddsförordning).
[2] 13 kap. 2 § lagen (2004:297) om bank- och finansieringsrörelse.
[3] 8 kap. 1 § lagen (2010:751) om betaltjänster.
[4] 10 kap. 1 § lagen (2004:46) om värdepappersfonder.
[5] 17 kap. 2 § försäkringsrörelselagen (2010:2043).
[6] 8 kap. 3 § lagen (2018:1219) om försäkringsdistribution.
[7] 16 § lagen (2014:275) om viss verksamhet med konsumentkrediter.
[8] 23 kap. 1 § lagen (2007:528) om värdepappersmarknaden.
[9] 8 § lagen (1996:1006) om valutaväxling och annan finansiell verksamhet.

- Riktlinjer från de europeiska tillsynsmyndigheterna European Banking Authority (EBA), European Securities and Markets Authority (ESMA) och European Insurance and Occupational Pensions Authority (EIOPA)

4 Utländsk lagstiftning och regelverk på import- eller exportområdet

Utöver kravet i 7 § första stycket på att företag ska stå under Inspektionen för strategiska produkters eller Strålsäkerhetsmyndighetens tillsyn för att få behandla personuppgifter som rör lagöverträdelser för kontroller mot sanktionslistor krävs att behandlingen är nödvändig för att efterleva krav enligt utländsk lagstiftning eller andra regelverk på import- eller exportområdet utfärdade av utländska myndigheter eller Förenta nationerna.

Exempel på utländsk lagstiftning och regelverk som avses i 7 § första stycket är:

- Den amerikanska lagen The Arms Export Control Act (AECA) som implementeras genom International Traffic in Arms Regulations (ITAR) och som hanteras av U.S. Departement of State.
- Den amerikanska lagen The Export Control Reform Act (ECRA) som implementeras genom Export Administration Regulations (EAR) och som hanteras av U.S. Department of Commerce.

5 Nödvändighetsrekvisitet

Kravet på att behandlingen ska vara nödvändig för att efterleva de föreskrifter och regelverk samt utländsk lagstiftning som avses i 6 och 7 §§ ska tolkas på samma sätt som nödvändighetskravet i artikel 6.1 i dataskyddsförordningen. Det krävs inte att föreskrifterna och regelverken ställer krav på kontroller mot sanktionslistor för att behandlingen ska anses vara nödvändig.

Ett exempel är att det kan vara nödvändigt för exempelvis en bank att behandla personuppgifter som rör lagöverträdelser genom kontroller mot sanktionslistor för att efterleva kraven på kundkännedom enligt lagen om åtgärder mot penningtvätt och finansiering av terrorism.

6 Sanktionslistor fastställda i demokratisk ordning och allmänt tillgängliga

En förutsättning för att företag som omfattas av 6 och 7 §§ ska få utföra kontroller mot sanktionslistor är att dessa listor är fastställda i demokratisk ordning och allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser. Detta innebär att exempelvis interna listor som upprättas av enskilda företag eller koncerner inte omfattas av bestämmelserna.

Nedan framgår exempel på sanktionslistor som IMY har bedömt vara fastställda i demokratisk ordning och som är allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser.[10]

[10] Se exempelvis IMY:s beslut IMY-2022-12123.

6.1 Av FN utfärdad sanktionslista

- United Nations Security Council Consolidated List

6.2 Av amerikanska myndigheter utfärdade sanktionslistor

U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC):

- Specially Designated Nationals List (“SDN-listan”)
- Consolidated Sanctions List

U.S. Department of State:

- List of Administratively Debarred Parties
- List of Statutorily Debarred Parties
- CAATSA Section 231(e) – Defence and Intelligence Sectors of the Government of the Russian Federation
- Terrorist Exclusion List

U.S. Department of Commerce - Bureau of Industry and Security (BIS):

- Denied Persons List
- Entity List
- Unverified List

6.3 Av brittiska myndigheter utfärdade sanktionslistor

Home Office:

- Proscribed Terrorist Organisations

HM Treasury – Office of Financial Sanctions Implementation:

- Consolidated List of Financial Sanctions Targets in the UK

7 Sanktionslistor utfärdade av EU

EU kan besluta om internationella sanktioner inom ramen för den gemensamma utrikes- och säkerhetspolitiken. Sanktionslistor utfärdade av EU, t.ex. European Union Consolidated Financial Sanctions List, genomförs sedan i EU-förordningar som blir direkt tillämpliga i svensk nationell rätt. För kontroller mot sådana listor krävs inget tillstånd från IMY.[11]

8 Krav på att kunna skilja på äkta och falska träffar

Företag som utför kontroller mot sanktionslistor behöver vidta integritetsskyddande åtgärder i syfte att säkerställa att eventuella träffar som uppstår vid kontrollerna är äkta. En sådan åtgärd kan vara att ha rutiner som säkerställer att den person som finns upptagen på en sanktionslista och som ett företag får träff på vid kontroll mot

[11] 5 § 2 förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

sanktionslistan utgör samma person som den person företaget avsett att kontrollera, exempelvis en person som företaget avser att ingå en affärsförbindelse med.