HARVEST
ADVOKATBYRÅ

Att vara compliant med AML-regelverket och GDPR – vanliga utmaningar och risker

2025-03-12

Agenda

1) Avstamp och tillämpliga regler

2) Exempel på gränsdragningsproblem mellan regelverken – vanliga utmaningar i praktiken

3) Vilka risker finns och hur kan man som verksamhetsutövare säkerställa compliance med de båda regelverken?

Avstamp och tillämpliga regler

Dataskyddsförordningen (”GDPR”)

Rättslig grund

- *Samtycke*
- *Avtal med den registrerade*
- *Skydda grundläggande intresse*
- *Myndighetsutövning och uppgift av allmänt intresse*
- *Intresseavvägning*
- *Rättslig förpliktelse*
  - Behandlingen är *nödvändig* för att fullgöra förpliktelser enligt lagar och regler
  - IMY: skälet till personuppgiftsbehandlingen ska framgå tydligt
  - EDPB anger att fyra villkor ska vara uppfyllda:
    - Framgå av EU-lagstiftning eller nationell lagstiftning
    - Fastställa en tydlig och specifik skyldighet att behandla personuppgifter
    - Förpliktelsen ska åtminstone definiera ändamålet med behandlingen
    - Skyldigheten åligger den personuppgiftsansvarige

Dataskyddsförordningen (”GDPR”)

Vissa personuppgifter har starkare skydd

- *Personuppgifter som rör lagöverträdelser*
- *Känsliga personuppgifter*
- *Andra integritetskänsliga uppgifter, t.ex. personnummer, löneuppgifter*

Lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (”PTL”)

Behandling av personuppgifter enligt PTL

5 kap. 2 §

En verksamhetsutövare får behandla personuppgifter i syfte att kunna fullgöra sina skyldigheter enligt denna lag.

Behandling av känsliga personuppgifter

5 kap. 5 §

(...) får behandlas endast om det är nödvändigt för att
1. bedöma om kunden är en person i politiskt utsatt ställning eller familjemedlem eller känd medarbetare till en sådan person enligt 1 kap. 8-10 §§,
2. bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §,
3. uppfylla övervakningsskyldigheten enligt 4 kap. 1 §,
4. bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §,
5. lämna uppgifter enligt 4 kap. 3 och 6 §§, och
6. lämna uppgifter i samverkan enligt 4 a kap.

Behandling av personuppgifter om lagöverträdelser

5 kap. 6 §

(...) får behandlas endast om det är nödvändigt för att
1. bedöma den risk som kan förknippas med kundrelationen enligt 2 kap. 3 §,
2. uppfylla övervakningsskyldigheten enligt 4 kap. 1 §,
3. bedöma misstänkta transaktioner och aktiviteter enligt 4 kap. 2 §,
4. lämna uppgifter enligt 4 kap. 3 och 6 §§, och
5. lämna uppgifter i samverkan enligt 4 a kap.

Exempel på gränsdragningsproblem mellan regelverken – vanliga utmaningar i praktiken

Kontroll av om kunden eller kundens verkliga huvudman är en politiskt utsatt person

Vad säger PTL?

”En verksamhetsutövare ska bedöma om kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person.”

När kan uppgifterna behandlas i praktiken?

- Om kunden (fysisk person)
- Om verklig huvudman
- Gäller det även samtliga av kundens styrelseledamöter, VD och andra företrädare?

Kontroll av kunder och kunders verkliga huvudmän mot sanktionslistor

Vad säger PTL?

- Begränsade möjligheter till kontroll mot sanktionslistor enligt PTL
- IMY:s föreskrifter om behandling av personuppgifter som rör lagöverträdelser (IMYFS 2024:1)

Företag under Finansinspektionens tillsyn

6 § Företag under Finansinspektionens tillsyn får behandla personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning för kontroller mot sanktionslistor, om

1. behandlingen är nödvändig för att efterleva lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, andra föreskrifter på finansmarknadsområdet eller regelverk på det området utfärdade av utländska myndigheter, EU-organ eller mellanstatliga organisationer,
2. sanktionslistorna är fastställda i demokratisk ordning och allmänt tillgängliga på utfärdande myndigheters eller mellanstatliga organisationers webbplatser, och
3. företaget har vidtagit relevanta skyddsåtgärder för att kunna skilja på äkta och falska träffar.

Personuppgiftsbehandling enligt första stycket får endast avse

1. företagets styrelsemedlemmar, fullmaktshavare, ställföreträdare, firmatecknare, ägare, verkliga huvudmän, arbetstagare, arbetssökande, tredjemanspantsättare, borgensmän och motparter i en transaktion,
2. företagets befintliga och presumtiva kunder, leverantörer, samarbetspartners, förmedlare och uppdragstagare,
3. styrelsemedlemmar, fullmaktshavare, ställföreträdare, firmatecknare, ägare, verkliga huvudmän, tredjemanspantsättare, borgensmän och motparter i en transaktion för juridiska personer som avses i 2, och
4. kategorier av personer som är jämförliga med de i 1–3.

När kan uppgifterna behandlas i praktiken?

- Om nödvändigt enligt PTL eller andra föreskrifter och regelverk
- PTL:
  - I samband med riskbedömning av kunder kan det finnas anledning att beakta om kunden har hemvist i en stat som är föremål för bl.a. sanktioner.
  - Motiverat att behandla uppgifter om personer med kopplingar till kunden?
- Nödvändigt?
  - Enligt IMY krävs det inte att föreskrifterna och regelverken ställer krav på kontroller mot sanktionslistor.

Uppgift om medborgarskap och andra kundkännedomsuppgifter

Vad säger PTL?

- Inget krav på att inhämta uppgift om medborgarskap
  - Finansinspektionens praxis (jfr. beslut avs. ClearOn AB, februari 2022)

När kan uppgifterna behandlas i praktiken?

- ”Fullgöra skyldigheter enligt denna lag” (5 kap. 2 § PTL)
- Nödvändig åtgärd?

Vilka risker finns och hur kan man som verksamhetsutövare säkerställa compliance med de båda regelverken?

Frågor om personuppgiftsbehandling ur ett AML-perspektiv

- Trumfar något av regelverken det andra?
  - är det något av regelverken som verksamhetsutövare bör prioritera att vara compliant med?
  - är det bättre att inhämta för många uppgifter än för få?
- Hur ska man förhålla sig till FI:s praxis i de fall FI anger att en uppgift ska inhämtas för att uppfylla PTL trots att det inte anges uttryckligen i lagen?

Risker

- Verksamhetsutövare måna om att göra rätt enligt PTL och minimera sina risker – leder till överträdelse av GDPR?
- Verksamhetsutövare har inte dokumenterat sina egna ställningstaganden
- Bristande ifrågasättande av leverantörers bedömning
- Bristande koppling till generella gallringsrutiner

Slutsatser - att tänka på

- Uttryckligt krav enligt lag eller verksamhetsutövarens egna bedömning att uppgifterna är nödvändiga att inhämta och behandla för att uppfylla PTL?
- Analysera syftet och behovet av behandlingen – säkerställ att detta är dokumenterat
- Regelverken står inte emot varandra - men viktigt att fastställa den rättsliga förpliktelsen enligt PTL för att behandla personuppgiften
- Vid upphandling av nya tjänster och system – säkerställ att ni får information om vilken personuppgiftsbehandling som utförs, vilka sanktionslistor omfattas, hur och var sker lagring etc.
- Kommunikation mellan AML-organisation och dataskyddsorganisation
- Utbilda styrelse och ledning om kraven enligt PTL resp. GDPR

Frågor?

AMIN BELL
ADVOKAT / PARTNER
amin.bell@harvestadvokat.se
076 135 98 00

ANNA CUMZELIUS
ADVOKAT / PARTNER
anna.cumzelius@harvestadvokat.se
076 125 76 00

MALIN BJÖRKLUND
SENIOR ASSOCIATE
malin.bjorklund@harvestadvokat.se
072 333 39 88

Harvest – kontaktuppgifter och sociala medier

+46 8 20 40 11

Engelbrektsplan 1
Box 7225
103 89 Stockholm

info@harvestadvokat.se

Harvest Advokatbyrå AB

harvestadvokatbyra