METODER FÖR IDENTIFIERING PÅ DISTANS VID KUNDIDENTIFIERING OCH IDENTITETSKONTROLL

Identifiering på distans

Behovet av digital identifiering på distans har ökat redan under en längre tid då tjänster tillhandahålls digitalt både i hemlandet och som gränsöverskridande tjänsteproduktion. Upprätthållandet av den nuvarande sociala distanseringen bidrar till att driva på utvecklingen ytterligare.

Vid identifiering på distans är kunden inte fysiskt närvarande när kundrelationen inleds eller i samband med att en transaktion utförs. I sådana fall identifierar den rapporteringsskyldiga kunden genom att inhämta kundkontrolluppgifter och genom att kontrollera kundens identitet med hjälp av en vald metod eller flera valda metoder för identifiering på distans.

Riskbaserat förhållningssätt

Den rapporteringsskyldiga skapar utifrån ett riskbaserat förhållningssätt egna rutiner och minimikriterier för kundkontroll i sina kundrelationer. I den riskbaserade bedömningen vid identifiering på distans ska den rapporteringsskyldiga fästa uppmärksamhet särskilt vid den egna verksamhetens art och hur riskfylld branschen är samt vid verksamhetens omfattning och kundernas geografiska läge. Den rapporterings-skyldiga ska utifrån riskbedömningen bedöma vilka skärpta tilläggsåtgärder för kundkontroll i enlighet med penningtvättslagen som behövs för att den rapporteringsskyldiga ska kunna minska en eventuell förhöjd risk för penningtvätt och finansiering av terrorism i anslutning till identifiering på distans.

Skärpta åtgärder för kundkontroll vid identifiering på distans

Om kunden inte är närvarande vid identifiering och identiteten inte kan kontrolleras (identifiering på distans), ska den rapporteringsskyldiga för att minska risken för penningtvätt och finansiering av terrorism

- kontrollera kundens identitet genom att inhämta ytterligare dokument eller uppgifter från en tillförlitlig källa
- säkerställa att betalningen i samband med en transaktion görs från ett kreditinstituts konto eller betalas in på ett konto
  som tidigare öppnats i kundens namn
- kontrollera en kunds identitet med hjälp av ett i lagen avsett[1] identifieringsverktyg eller med ett kvalificerat certifikat för elektroniska underskrifter[2] eller med någon annan elektronisk identifie-ringsteknik som är datasäker och bevislig.

Vid identifiering på distans kan kundkontroll och kontroll av kundens identitet förutsätta användning av flera olika metoder och inhämtande av ytterligare uppgifter både av kunden och från tillförlitliga källor särskilt då det är fråga om gränsöverskridande tjänster och kundrelationen inleds med en kund som finns i en annan stat. Den rapporteringsskyldiga är ansvarig för att bedöma behovet av skärpta tilläggsåtgärder för kundkontroll.

[1] Lag om stark autentisering och betrodda elektroniska tjänster (617/2009)
[2] Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

Metoder för identifiering på distans

I samband med att en kundrelation inleds identifieras kunden på distans och kundens identitet verifieras med hjälp av en metod eller en kombination av metoder för identifiering på distans. Den rapporterings-skyldiga ska ha tillgång till metoder med vilka den kan kontrollera de uppgifter som kunden ger i samband med identifieringen på distans. De kundkontrollsuppgifter som kunden ger ska kunna kontrolleras med hjälp av uppgifter i offentliga register som klassificeras som tillförlitliga källor. Sådana register är till exempel

- Patent- och registerstyrelsens register, t.ex. handelsregistret och föreningsregistret
- Befolkningsdataregistret hos myndigheten för digitalisering och befolkningsdata
- Suomen asiakastieto Oy:s kreditupplysningsregister[3].

Den rapporteringsskyldiga bör beakta att det i andra stater inte alltid finns uppgifter att tillgå från mot-svarande offentliga register. Om uppgifter finns att tillgå ska den rapporteringsskyldiga bedöma hur aktuella, tillförlitliga och användbara uppgifterna i det utländska registret är. Utöver utredningar från tillförlitliga källor kan för kundkontroll även utgående från den rapporteringsskyldigas riskbedömning utnyttjas t.ex. koder för sociala medier, e-postadresser, telefonnummer som tillhandahålls av en privat tjänsteproducent och där en annan tjänsteproducent redan identifierat kunden t.ex. med hjälp av kreditkortsuppgifter.

Verktyg för stark elektronisk identifiering enligt lagen om stark autentisering

Transport- och kommunikationsverket Traficom övervakar att lagen om stark autentisering[4] följs. Starka elektroniska identifieringstjänster är för närvarande

- bankernas nätbankskoder
- teleföretagens mobilcertifikat
- identitetskort med medborgarcertifikat från Myndigheten för digitalisering och befolkningsdata utfärdat av polisen
- vissa andra identifieringscertifikat
- olika organisationskort för registrerade leverantörer av tjänster för identifieringsförmedling

För starka elektroniska identifieringsverktyg finns strikta krav, t.ex. skyldighet att innan verksamheten inleds göra en anmälan till Traficom, skyldighet att göra en kvalitetsrevision och skyldighet att anmäla störningar. Traficom upprätthåller en förteckning över identifieringstjänster som uppfyller kraven i lagen.[5]

Annan elektronisk identifieringsteknik

I takt med att teknologin utvecklats är det i samband med lösningar för identifiering på distans möjligt att utnyttja t.ex. artificiell intelligens samt blockkedja-teknologin, vilket gör det möjligt att bygga tjänster och lagra data på ett nytt sätt. Vid identifiering av en kund på distans borde man utnyttja information från olika datakällor genom att jämföra och sammanslå de uppgifter som inhämtats från kunden med de uppgifter som fåtts via tillförlitliga källor.

[3] för syften som avses i kreditupplysningslagen (527/2007).
[4] lag om stark autentisering och betrodda elektroniska tjänster 617/2009
[5] https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/elektronisk-identifiering

Artificiell intelligens utnyttjas för närvarande åtminstone vid ansiktsigenkänning och i kontrollen av riktigheten av fysiska identitetsbevis. Vid digital inledande identifiering[6] kan kunderna identifiera sig själva med mobilutrustning, pass (eller annat identitetsbevis) och sitt ansikte. På marknaden finns tillämpningar som identifierar identitetsbevisens riktighet genom att granska säkerhetsegenskaperna, t.ex. hologrammens äkthet. Beträffande biometriska pass kan tillämpningen läsa passets chip. Tillämpningen identifierar kundens ansikte med hjälp av den ansiktsbild som kunden tagit och det faktum att kunden lever identifieras med hjälp av en rörlig bild.

Processens transparens vid identifiering på distans och förvaring av identifieringsuppgifter

Processen för identifiering på distans ska vara transparent (datasäker och bevislig) och det ska vara möjligt att göra en kontroll i efterhand. Kundens uppgifter ska förvaras enligt den förvaringstid som föreskrivs i penningtvättslagen med beaktande av dataskydd och informationssäkerhet (konfidentialitet, integritet och tillgänglighet). Den person som identifieras ska ge sitt samtycke till identifiering på distans och även samtycket ska förvaras. Den anmälningsskyldiga bör noggrant överväga att begränsa vilka dokument och uppgifter för verifiering av identiteten som godkänns vid identifiering på distans och försäkra sig om att dokumenten är intakta och inte kan editeras. Med tanke på den riskbaserade bedömningen kan det vid identifiering på distans vara motiverat att be vissa kunder om mer omfattande tilläggsutredningar och noggrannare uppgifter.

Utläggning av processen för identifiering på distans

Identifiering på distans köps ofta av en extern tjänsteproducent i form av underleverans. Utläggning av processen för identifiering på distans förutsätter alltid att den rapporteringsskyldiga gör en bedömning av riskerna förknippade med identifieringen på distans och en noggrann planering. Av avtalet ska både förfarandena och båda parternas uppgifter och ansvar framgå. Dessutom ska den rapporteringsskyldiga förutsätta att dokumenteringen om kundförhållandet skickas till den rapporteringsansvariga eller att den finns tillgänglig för den rapporteringsskyldiga utan dröjsmål under hela kundförhållandet och under den förvaringstid som föreskrivs i penningtvättslagen.

Den rapporteringsskyldiga ska sörja för att den har en tillräcklig teknisk kompetens, att ledningen är införstådd och för kontinuitetshanteringen vid utläggning av identifiering på distans. I sådant fall ska den rapporteringsskyldiga ha tekniska färdigheter och kompetens att leda och övervaka den utlagda funktionen. Den rapporteringsskyldiga ska också ha tillräcklig förståelse för den utlagda funktionen för att vid behov kunna återta den utlagda identifieringen på distans för att sköta den internt eller för att överföra den på en ny tjänsteproducent. Den rapporteringsskyldiga är ansvarig för att följa upp kvaliteten av den utlagda tjänsten.

Ansvaret för kundkontrollen samt för den fortlöpande uppföljningen och för iakttagandet av utrednings- och anmälningsskyldigheten är alltid hos den rapporteringsskyldiga i alla situationer.

Detta dokument har upprättats den 29.6.2021 av den undergrupp för tillsynsmyndigheter enligt penningtvättslagen som har inrättats av den nationella myndighetssamarbetsgruppen för förhindrande av penningtvätt och finansiering av terrorism. Ytterligare information om innehållet i dokumentet lämnas av Finansinspektionen. Om du har andra frågor, vänligen vänd dig till din egen tillsynsmyndighet enligt penningtvättslagen.

[6] *Med inledande identifiering* avses verifiering av identiteten hos den som ansöker om ett identifieringsverktyg i samband med att verktyget skaffas. Se lagen om stark autentisering och betrodda elektroniska tjänster (7.8.2009/617)