Datasöksystemet
Instruktioner för produktionssättning och underhåll

Dokumentversion 1.0

Instruktioner för produktionssättning och underhåll av datasöksystemet **21.10.2019**

Versionshistorik

Version	Datum	Beskrivning
1.0	21.10.2019	Instruktioner för produktionssättning och underhåll av datasöksystemet

INNEHÅLLSFÖRTECKNING

1 Dokumentets syfte

Detta dokument ingår i Tullens föreskrift 6/2019 om ett övervakningssystem för bank- och betalkonton. Dokumentets syfte är att instruera leverantörer av uppgifter om datasöksystemets produktionssättning och underhåll. Detta dokument kompletteras av beskrivningen av datasöksystemets frågegränssnitt.

Tullen kommer även att offentliggöra denna instruktion på sin webbplats.

2 Terminologi och förkortningar

Term	Förklaring
Övervakningssystem för bank- och betalkonton	Det nationella övervakningssystemet för bank- och betalkonton, som består av Kontoregistret samt datasöksystem, grundar sig på lagen om ett övervakningssystem för bank- och betalkonton 571/2019 samt Europaparlamentets och rådets direktiv (EU) 2018/843 av den 30 maj 2018 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.
Datasöksystemet	Datasöksystemet är ett elektroniskt datasöksystem för bank- och betalkonton som upprätthålls av leverantören av uppgifter, med hjälp av vilket leverantören av uppgifter omedelbart och utan hinder av sekretessbestämmelserna lämnar de uppgifter om sina kunder till den behöriga myndighet som avses i 2. mom. I enlighet med lagen föreskriver Tullen de tekniska kraven på datasöksystemet och varje leverantör av uppgifter implementerar sitt eget datasöksystem, dvs. det finns många datasöksystem.
Personuppgiftsansvarig	I ett decentraliserat datasöksystem ansvarar leverantören av uppgifter i egenskap av personuppgiftsansvarig för att uppgifterna är tillgängliga genom att upprätthålla ett datasöksystem och den behöriga myndigheten ansvarar i egenskap av personuppgiftsansvarig för de uppgifter den hanterar med hjälp av datasöksystemet.
Leverantören av uppgifter/Upprätthållaren av datasöksystemet	Med leverantören av uppgifter avses en part som har en lagstadgad skyldighet att upprätthålla ett datasöksystem, med hjälp av vilket leverantören av uppgifter omedelbart och utan hinder av sekretessbestämmelserna förmedlar de uppgifter om sina kunder till den behöriga myndigheten som fastställs i gällande lagstiftning. Med leverantören av uppgifter avses även en i Finland belägen filial till utländska betalningsinstitut, institut för elektroniska pengar, kreditinstitut och tillhandahållare av virtuell valuta.
Behörig myndighet/Användaren av information	Den behöriga myndighet och advokatförening som definieras i lagen om ett övervakningssystem för bank- och betalkonton och som på grundval av sin behörighet har rätt att motta och behandla information som har förmedlats med hjälp av de datasöksystem som upprätthålls.

Upprätthållning	Med upprätthållning avses datasöksystemets underhållsprocesser, till exempel hantering av tjänstenivån, användarstöd, incidenthantering, problemsökning, hantering av användarrättigheter samt versions- och ändringshantering. Ansvaret för dessa är decentraliserat. Tullen ansvarar endast för de tekniska kraven genom sin föreskrift.

3 Bakgrund och omfattning

Enligt Europaparlamentets och rådets direktiv (EU) 2018/843 ska medlemsstaterna upprätta centraliserade automatiserade mekanismer som tillåter identifiering av innehavare av bank- och betalkonton och bankfack nationellt.

Syftet med övervakningssystemet för bank- och betalkonton är att effektivisera myndigheternas tillgång till information om bank- och betalkonton genom att digitalisera den samt effektivisera myndigheternas förfrågningar så att de riktas till rätt mottagare. I nuläget är tillgången till information manuell och processerna är tröga, långsamma och krävande. Via ett elektroniskt system är informationen tillgänglig betydligt snabbare än den är manuellt. Övergången till ett elektroniskt datasöksystem ökar företagens och medborgarnas dataskydd, eftersom uppgifterna inte längre förmedlas till exempel via fax. Även när det gäller informationens kvalitet är målet att uppnå förbättringar, eftersom den manuella insamlingen av information innebär en större risk för fel än en automatiserad process, dvs. den information som fås via övervakningssystemet för bank- och betalkonton är mer pålitlig och felfri.

Finland har antagit lagen om ett övervakningssystem för bank- och betalkonton (571/2019). I enlighet med det som föreskrivs i lagen består övervakningssystem för bank- och betalkonton av 1) ett bank- och betalkontoregister (senare Kontoregistret) och 2) ett decentraliserat datasöksystem.

4 Presentation av datasöksystemet

Datasöksystemet är ett system som har implementerats av leverantören av uppgifter utifrån Tullens tekniska specifikationer och via vars frågegränssnitt behöriga myndigheter kan göra förfrågningar om de uppgifter som definieras i lagen om ett övervakningssystem för bank- och betalkonton.

Kreditinstitut har underhållsskyldighet för datasöksystem. Betalningsinstitut, institut för elektroniska pengar och tillhandahållare av virtuell valuta kan om de önskar deklaratoriskt upprätthålla ett datasöksystem för att uppfylla sin skyldighet att tillhandahålla information. Anmälan ska göras till Tullen, vilket innebär att de aktörer som deklaratoriskt upprätthåller ett datasöksystem inte behöver leverera information till det Kontoregister som Tullen upprätthåller.

I datasöksystemet ansvarar leverantören av uppgifter i egenskap av personuppgiftsansvarig för uppgifternas tillgänglighet genom att upprätthålla ett datasöksystem och den behöriga myndigheten ansvarar i egenskap av personuppgiftsansvarig för de uppgifter den hanterar med hjälp av datasöksystemet. Bägge personuppgiftsansvariga är skyldiga att övervaka att uppgifterna behandlas lagenligt. Dessutom föreskriver lagen om ett övervakningssystem för bank- och betalkonton att den behöriga myndigheten ska upprätthålla en loggbok över användningen av datasöksystemet, som ska innehålla åtminstone de uppgifter som lagen föreskriver.

Tullen utfärdar en föreskrift om datasöksystemet och stöd för tolkningen av föreskriften, men Tullen ansvarar inte för och övervakar inte produktionssättningen av datasöksystemet.

4.1 Uppgifterna i datasöksystemet

De uppgifter som ska förmedlas till den behöriga myndigheten via datasöksystemet föreskrivs i lagen om ett övervakningssystem för bank- och betalkonton. Uppgifternas tidsperspektiv härleds från 3 kap. 3 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism, som innehåller exakta och avgränsade bestämmelser om uppgifterna om kundkontroll samt bevarandet av dessa. I enlighet med artikel 40.1b i det femte direktivet om penningtvätt tillämpas även förvaringstiden för uppgifterna om kundkontroll på uppgifter som är tillgängliga via de centraliserade mekanismer som avses i artikel 32 a.

4.1.1 Ansvar för uppgifternas felfrihet

I enlighet med EU:s dataskyddsförordning är den personuppgiftsansvariga ansvarsskyldig för att personuppgifterna är exakta och vid behov uppdateras; den personuppgiftsansvariga ska vidta alla möjliga och rimliga åtgärder för att säkerställa att personuppgifter som i förhållande till behandlingsändamålen är inexakta och felaktiga raderas eller korrigeras utan dröjsmål (”exakthet”); den personuppgiftsansvariga har även anmälningsskyldighet. Den personuppgiftsansvariga ska anmäla om korrigering, radering eller begränsning av behandlingen av personuppgifter till varje mottagare som personuppgifterna har lämnats till. I enlighet med lagen om ett övervakningssystem för bank- och betalkonton har den registrerade dock inte rätt att veta till vilka myndigheter uppgifterna redan har lämnats. För att trygga den registrerades rättigheter ska därför den behöriga myndigheten även informeras ifall den registrerade har bestridit felfriheten för de uppgifter som berör den registrerade. Den behöriga myndigheten har dock rätt att använda personuppgifter under den tid som leverantören av uppgifter utreder huruvida uppgifterna är felfria.

4.2 Aktörer och roller

Detta kapitel presenterar aktörerna och rollerna för gränssnitten i övervakningssystemet för registret över bank- och betalkonton.

Tabell 1. *Aktörer och roller för gränssnitten i övervakningssystemet för registret över bank- och betalkonton*

Aktörer	**Genomförare av datasöksystemets gränssnitt**	**Användare av datasöksystemets frågegränssnitt**
Användare av information		X
Kreditinstitut	A	
Betalningsinstitut	B	
Institut för elektroniska pengar	B	
Tillhandahållare av virtuell valuta	B	

X) alltid
A) som utgångspunkt
B) genom anmälan

Användarna av uppgifter använder datasöksystemets frågegränssnitt. Dessa är behöriga myndigheter och advokatföreningar. I princip implementerar kreditinstitut datasöksystemets gränssnitt, men med undantagstillstånd av Finansinspektionen kan kreditinstitut bli leverantörer av uppgifter till Kontoregistret. I princip är betalningsinstitut, institut för elektroniska pengar och tillhandahållare av virtuell valuta leverantörer av uppgifter till Kontoregistret, men de kan genom anmälan implementera datasöksystemets gränssnitt.

5 Processbeskrivning

Bild 1 visar ett användningsfallsdiagram över de viktigaste verksamhetsprocesserna i övervakningssystemet för bank- och betalkonton.

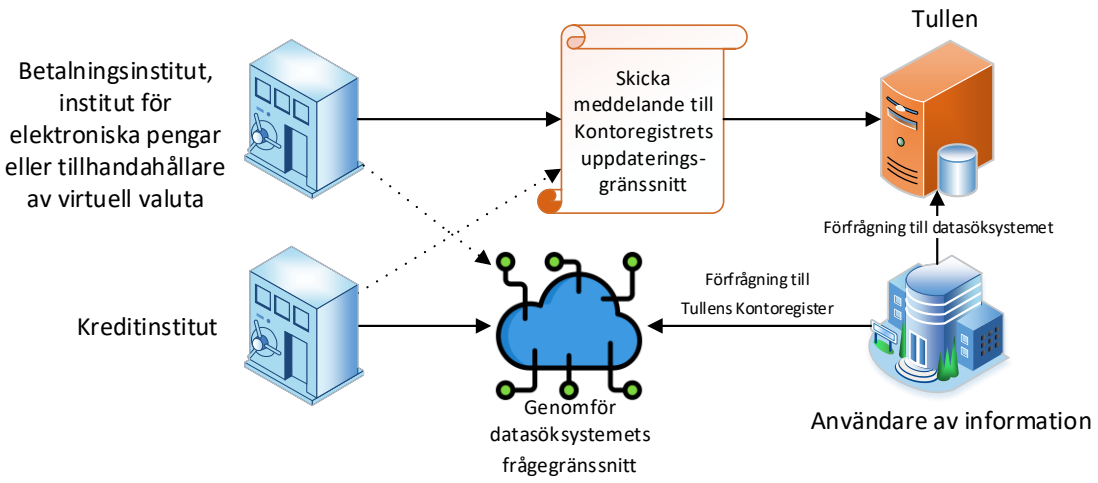

Bild 1: Användningsfallsdiagram.

5.1 Verksamhetsprocessernas förlopp och roller

Den första uppgiften för användaren av uppgifter i datasöksystemets verksamhetsprocess är att ansöka om åtkomsträttigheter till gränssnitten av det kreditinstitut som implementerar gränssnittet eller av en annan leverantör av uppgifter. Behovet av att ansöka om åtkomsträttigheter enligt roll visas i tabell 2.

Användaren av uppgifter måste ansöka om åtkomsträttigheter till gränssnitten separat av varje implementerare av datasöksystemet.

I tabell 2 finns en lista över processtegen i verksamhetsprocesserna för datasöksystemet på en allmän nivå och de tillhörande rollerna.

Tabell 2. *Verksamhetsprocessens steg och roller.*

Processteg	Roller
Ansökan om åtkomsträttigheter för gränssnitten	Användare av information
Beviljande av åtkomsträttigheter till datasöksystemets frågegränssnitt	Upprätthållaren av datasöksystemet/leverantören av uppgifter
Förfrågan om uppgifter i datasöksystemets frågegränssnitt	Användare av information

5.2 Tullens stöd

Tullen erbjuder stöd i anknytning till datasöksystemets instruktioner och dess produktionssättning, verksamhetsmodeller och innehåll. Den primära stödformen är de instruktioner som har publicerats på Tullens webbplats. Dessutom kan underhållet kontaktas per telefon och e-post vardagar kl. 6:30–18:00

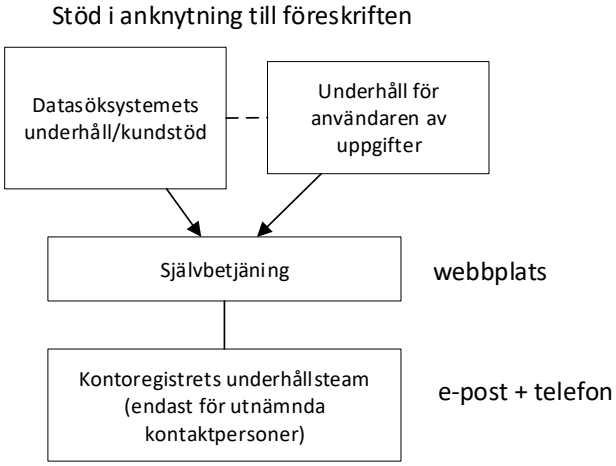

Bild 2. Tullens stöd för verksamhetsmodeller och innehåll

5.3 Leverantörer av uppgifter

I datasöksystemet förmedlas de uppgifter som föreskrivs i lagen om ett övervakningssystem för bank- och betalkonton omedelbart och utan hinder av sekretessbestämmelserna till de behöriga myndigheterna och utan hinder av sekretessbestämmelserna med hjälp av datasöksystem.

5.4 Datasöksystemets frågegränssnitt

Ifall leverantören av uppgifter implementerar datasöksystemet kan användarna av uppgifter göra förfrågningar med hjälp av det. I samband med varje förfrågan om uppgifter ska leverantören av uppgifter autentisera de behöriga myndigheterna med hjälp av ett certifikat (se kapitel 6.1).

En allmän beskrivning av datasöksystemets frågegränssnitt finns i gränssnittsbeskrivningen, kapitel 4.

5.5 Anmälningsförfarande

Tullen ger föreskrifter och instruktioner för produktionssättningen av datasöksystemets frågegränssnitt. Kreditinstitut ska meddela om produktionssättningen av datasöksystemet till Tullen. Samma praxis gäller betalningsinstitut, institut för elektroniska pengar eller tillhandahållare av virtuell valuta som meddelar Tullen om att de implementerar datasöksystemet. Tullen informerar de behöriga myndigheterna, dvs. användarna av uppgifter, om produktionssättningen av datasöksystemet.

Om ett kreditinstitut med Finansinspektionens undantagstillstånd har anslutit sig till Kontoregistret, kan det senare implementera datasöksystemet och övergå till att använda det. När kreditinstitutet meddelar Tullen om beslutet, skickar Tullen en föreskrift och instruktioner för datasöksystemets frågegränssnitt, med hjälp av vilka kreditinstitutet kan implementera datasöksystemet. När kreditinstitutet meddelar att datasöksystemets frågegränssnitt är färdigt och testat, stänger Tullen kreditinstitutets uppdateringsgränssnitt till Kontoregistret. Samma förfaringssätt gäller betalningsinstitut, institut för elektroniska pengar och tillhandahållare av virtuell valuta som redan har tagit Kontoregistret i bruk och senare meddelar att de implementerar datasöksystemet.

5.6 Testning av programgränssnitten för leverans av uppgifter

Integrationen till varje leverantör av uppgifter testas separat.

Tullen genomför en API-förfrågan med hjälp av vilken förfrågningar om uppgifter kan riktas till leverantörer av uppgifter. Vid testningen är avsikten att säkerställa funktionaliteten för åtminstone alla de datatyper som ifrågavarande leverantör av uppgifter i sin produktion kommer att skicka till Kontoregistret. Funktionen för datasöksystemets gränssnitt testas genom att i Tullens kundmiljö skicka API-förfrågningar till uppgifteleverantörers system och verifiera de svar som fås.

6 Dataskydd

Datasöksystemets dataskydd grundar sig på skydd av dataöverföringsförbindelserna med TLS-kryptering. I systemet identifierar leverantörer av uppgifter och användare av uppgifter varandra med hjälp av servercertifikat. Dessutom är den formella meddelandetrafiken digitalt signerad.

Förbindelserna i kontoregistrets uppdateringsgränssnitt ska vara skyddade med TLS-kryptering med TLS-protokollets version 1.2 eller högre. Båda ändarna av förbindelsen identifieras med servercertifikat genom ömsesidig TLS-autentisering. Kraven på servercertifikaten har beskrivits i kapitel 6.1.

Meddelandenas innehåll ska vara signerat som SOAP XML-poster med hjälp av signaturcertifikat. Signaturcertifikaten har beskrivits närmare i kapitel 6.1.

6.1 Krav på certifikat

I datasöksystemet skyddas externa förbindelser med certifikat. Datasöksystemets leverantör av uppgifter och användare av uppgifter ska för detta ändamål förvärva server- och systemsignaturcertifikat som uppfyller certifikatkraven och installera dem på sitt system. För signerande av meddelanden behövs dessutom ett signaturcertifikat. Tekniskt sett kan samma certifikat fungera både som server- och systemsignaturcertifikat, eller så kan certifikaten vara separata. I allmänhet installeras servercertifikatet på den frontend-server som sköter datakommunikationsförbindelser och signaturcertifikatet på den backend-server som formulerar svaren.

Den part som formulerar och förmedlar svar på förfrågningar från användarna av uppgifter ansöker om certifikaten. Om leverantören av uppgifter själv genomför dessa skeden, söks certifikatet för leverantören av uppgifter. Om man utnyttjar en tjänsteleverantör som formulerar och förmedlar meddelandena på den anmälningsskyldigas vägnar, ska verifikatet sökas av tjänsteleverantören. I sådana fall ska den anmälningsskyldiga befullmäktiga tjänsteleverantören att signera de meddelanden som ska skickas.

6.2 Förnyande av certifikat och kostnader

Certifikatet ska förnyas i god tid före det går ut. Ett utgånget certifikat får inte användas. Om inte annat har överenskommits av parterna ska leverantören av uppgifter meddela den behöriga myndigheten om förnyandet av sitt certifikat minst en månad innan det tas i bruk och skicka en kopia av certifikatet.

Även den behöriga myndigheten, dvs. användaren av uppgifter, ska regelbundet förnya sina certifikat hos certifikatleverantören. Detta meddelas inte separat till anmälningsskyldiga leverantörer av uppgifter, eftersom det antas att leverantören av uppgifter kontrollerar den behöriga myndighetens certifikat mot en lista över godkända certifierare. Giltigheten för behöriga myndigheters certifikat kan kontrolleras i Befolkningsregistercentralens certifikatkatalog.

Enligt 4 § 3. mom. samt 8 § i lagen om ett övervakningssystem för bank- och betalkonton har den behöriga myndigheten rätt att få uppgifterna avgiftsfritt och därför står leverantören av uppgifter för kostnaderna för det certifikat den använder.

7 Servicenivå

Den behöriga myndighetens svar på förfrågningar ska vara tillgängliga ”omedelbart” och ”ofiltrerat”.

Datasöksystemets frågegränssnitt bör vara tillgängligt 24/7, men tillgänglighetskravet är 99,5 % av tiden mellan 07:00 och 22:00. Hur kravet på tillgänglighet uppfylls beräknas som ett medelvärde per kalendermånad.