Dnr
TRAFICOM/461816/04.04.04.01/2020
1.6.2021

Traficoms promemoria om kriterier för bedömning av tillförlitligheten hos aktörer som ges tillgång till tjänster på någon annans vägnar

Innehållsförteckning

1 Promemorians syfte och bakgrund

Enligt lagen om transportservice har tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt (tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt) för tjänster på någon annans vägnar rätt att på förhand ange bedömningskriterier på basis av vilka de kan bedöma tillförlitligheten hos leverantörer (leverantörer som har rätt till tillgång till tjänster på någon annans vägnar) som begär tillträde till gränssnitt för tjänster på någon annans vägnar.

Syftet med denna promemoria är att förtydliga hur Transport- och kommunikationsverket Traficom (nedan Traficom) i egenskap av behörig övervakande myndighet tolkar den ovannämnda rätten för tjänsteleverantörer som är skyldiga att ge tillträde att ange bedömningskriterier.

Traficoms promemoria syftar till att bland annat identifiera med hjälp av hurdana typer av kriterier tjänsteleverantörer som är skyldiga att ge tillträde skulle kunna bedöma tillförlitligheten hos aktörer som har rätt till tillgång till tjänster på någon annans vägnar samt hjälpa dem att identifiera hurdana bedömningskriterier som är rättvisa, rimliga och icke-diskriminerande. Traficom bedömer dock lagenligheten hos bedömningskriterierna som aktörerna har angett från fall till fall.

Promemorian är inte en mall för bedömningskriterier, och aktörerna själva ansvarar för att ange sina bedömningskriterier. Promemorian är inte heller en fullständig förteckning över bedömningskriterier, och kriterierna som presenteras här bildar ingen enhetlig helhet.

Traficom övervakar dataskyddet för tjänster på någon annans vägnar till de delar det är fråga om hur rättvisa, rimliga och icke-diskriminerande bedömningskriterierna och avtalsvillkoren för dataskyddet är. Därtill övervakar Traficom att de aktörer som är skyldiga att ge tillträde till gränssnitt uppfyller skyldigheten att med beaktande av dataskyddet ge tillträde till gränssnitt för tjänster på någon annans vägnar enligt lagen om transportservice.

Till stöd för upprättandet av promemorian har Traficom ordnat fem verkstäder, där aktörerna har kunnat framföra sina synpunkter på bedömningskriterierna.
Den 6 november 2020 skickade Traficom ett utkast till promemoria om bedömningskriterierna till aktörerna för utlåtande. Utlåtanden kunde lämnas in fram till den 27 november 2020, och 19 utlåtanden lämnades in till Traficom i ärendet. I utlåtandena ägnades i Traficoms uppfattning särskild uppmärksamhet åt dataskyddsfrågor i genomförandemodellen för tillgång till tjänster på någon annans vägnar, där kunden identifieras genom att man jämför informationen i användarkonton.

Utlåtanderesponsen beaktades i den nya versionen av utkastet, som skickades till aktörerna för utlåtande den 10 maj 2021, och genom att man

lät göra dataskyddsutredningen som nämns nedan. Utlåtanden kunde lämnas in fram till den 26 maj 2021, och 11 utlåtanden lämnades in till Traficom i ärendet.

I promemorian har man strävat efter att beakta all respons som kommit in under processens gång.

Traficom lät advokatbyrån Bird & Bird utreda kraven som dataskyddslagstiftningen ställer och som den personuppgiftsansvarige ska beakta i genomförandet av jämförelsemodellen visavi tjänster på någon annans vägnar.[1]

Utredningen gäller de krav som dataskyddslagstiftningen ställer på den personuppgiftsansvarige. I utredningen tas inte ställning till tolkningen av skyldigheterna enligt lagen om transportservice. Traficom övervakar inte förverkligandet av den personuppgiftsansvariges skyldigheter ur dataskyddslagstiftningens synvinkel. Utredningen och resultatet av den är inte ett övervakningsverktyg för Traficom eller Traficoms officiella tolkning.

Beredningsprocessen för promemorian beskrivs på bilden ovan.

2 Vad betyder tillgång till tjänster på någon annans vägnar?

Enligt 156 § i lagen om transportservice ska en leverantör av mobilitets- eller kombinationstjänster, som inkluderar ett system med användarkonton, ge andra leverantörer av mobilitets- eller

[1] https://liikkumisenrajapinnat.fi/sites/default/files/media/file/Puolesta-asioinnin%20vertailumallin%20tietosuojavelvoitteet%20%202021%2004%2014.pdf

kombinationstjänster tillgång till sitt försäljningsgränssnitt och möjliggöra för dessa att på begäran av de som använder tjänsten och på deras vägnar skaffa biljettprodukter som berättigar till användning av en rabatt, en ersättning eller något annat specialvillkor eller andra produkter som berättigar till användning av tjänsten med utnyttjande av identifierings- och användaruppgifter som finns i tjänsten om den som använder tjänsten.

Med skyldighet att ge tillträde till tjänster på någon annans vägnar (tillgång till tjänster på någon annans vägnar) enligt lagen om transportservice avses att en leverantör av en mobilitets- eller kombinationstjänst i en specifik tjänst kan köpa personliga reserätter som är knutna till kundens användarkonto eller andra produkter som berättigar till användning av mobilitetstjänsten åt kunden i en annan mobilitets- eller kombinationstjänst. Personliga reserätter och övriga produkter inom mobilitetstjänster baserar sig på det användarkonto som kunden har i den befintliga tjänsten i gränssnittet hos tjänsteleverantören som är skyldig att ge tillträde till gränssnittet. En leverantör som använder tjänster på någon annans vägnar kan således inte på basis av tillgången till tjänster på någon annans vägnar kräva några sådana förmåner som kunden i tjänsten själv inte får. Via tillgången till tjänster på någon annans vägnar behöver en tjänsteleverantör som är skyldig att ge tillträde till gränssnitt på basis av kravet i lagen om transportservice således inte sälja produkter till ett billigare pris än det som erbjudits kunden i tjänsten eller betala provision till den aktör som har rätt till tillgång till tjänster på hens vägnar. Parterna kan komma överens om ett bredare samarbete än den rättsliga skyldigheten i fråga om tjänster på någon annans vägnar.

Vid tjänster på någon annans vägnar är det på så vis fråga om att kunden ber leverantören som har tillgång till tjänster på hens vägnar att använda information som finns i kundens användarkonto i en annan tjänst. Vid tjänster på någon annans vägnar är det dock alltid fråga om en rättshandling mellan två mobilitets- eller kombinationstjänster som baserar sig på ett avtal mellan aktörerna om användning av det aktuella gränssnittet.
Jämförelsemodellen för tillgång till tjänster på någon annans vägnar beskrivs mer i detalj i beskrivningen av Traficoms jämförelsemodell för tillgång till tjänster på någon annans vägnar[2].

Nedan en figur som beskriver tillgång till tjänster på någon annans vägnar.

[2] https://www.liikkumisenrajapinnat.fi/sites/default/files/media/file/Liite%201.1.%20Puolesta-asiointi%20vertailumallin%20kuvaus_.pdf

3 Vad är bedömningskriterier?

Den lagstiftningsmässiga grunden för bedömningskriterierna finns i 156 § 4 mom. i lagen om transportservice, enligt vilket de i [...] 1 mom. avsedda leverantörer av mobilitets- eller kombinationstjänster och aktörer som på deras vägnar ansvarar för biljett- eller betalningssystem samt i 2 mom. avsedda utgivare av biljetter för en mobilitetstjänst som innehåller en rabatt, en ersättning eller ett specialvillkor har dock rätt att enligt på förhand angivna kriterier och villkor bedöma tillförlitligheten hos en sådan leverantör av en mobilitets- eller kombinationstjänst som har rätt till tillgång. Tillgång till uppgifter får inte nekas, om den aktör som begär tillgång har ett tillstånd, ett godkännande, en auditering eller en certifiering för verksamheten i fråga som beviljats av en myndighet eller för motsvarande ändamål av en tredje part som myndigheten befullmäktigat, eller om det annars visas att verksamheten motsvarar en allmänt tillämpad standard eller allmänt accepterade villkor inom branschen. Den som nekas tillgång ska ges sakligt motiverade skäl till detta.

Ovannämnda tjänsteleverantörer som är skyldiga att ge aktörer som har rätt till tillgång till tjänster på någon annans vägnar tillträde till gränssnitt ska enligt 158 § i lagen om transportservice se till att tillträdet kan ske utan att vare sig datasäkerheten eller integritetsskyddet i tjänsten äventyras.

För att tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt ska kunna uppfylla kraven i 158 § i ovannämnda lag samt även på annat sätt säkerställa en fungerande och säker tillgång till tjänster på någon annans vägnar, har de rätt att bedöma tillförlitligheten hos de leverantörer som har rätt till tillgång till tjänster på någon annans vägnar enligt på förhand angivna kriterier och villkor.

En tjänsteleverantör som är skyldig att ge tillträde till gränssnitt ska ange sina bedömningskriterier på förhand, och de ska vara rättvisa, rimliga och icke-diskriminerande. Dessa krav gäller såväl enskilda kriterier för bedömning av tillförlitligheten som bedömningskriterierna som helhet. En tjänsteleverantör som är skyldig att ge tillträde till gränssnitt ska kunna visa och motivera att dess bedömningskriterier är nödvändiga för bedömningen av tillförlitligheten hos aktörer som har rätt till tillgång till tjänster på någon annans vägnar. Om en tjänsteleverantör som är skyldig att ge tillträde till gränssnitt nekar en aktör tillgång ska tjänsteleverantören ge aktören sakligt motiverade skäl till detta.

Bedömningskriterierna gör det enklare för aktörer att redan i förväg förstå vilka villkor de måste uppfylla för att de ska kunna använda tjänster på någon annans vägnar i tjänsten som den ifrågavarande leverantören som är skyldig att ge tillträde till gränssnittet tillhandahåller.

Bedömningskriterierna kan även ändras till exempel om systemen som tjänsteleverantören som är skyldig att ge tillträde till gränssnittet tillhandahåller ändras och det påverkar bedömningen av tillförlitligheten hos aktörer som har rätt till tillgång till tjänster på någon annans vägnar. Även ändringarna ska uppfylla kraven på rättvishet, rimlighet och icke-diskriminering.

4 Exempel på kriterier för bedömning av tillförlitligheten hos leverantörer som har rätt till tillgång till tjänster på någon annans vägnar

Enligt Traficom skulle tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt kunna använda exempelvis följande typer av bedömningskriterier vid bedömning av tillförlitligheten hos leverantörer som begär tillgång till tjänster på någon annans vägnar:

- Leverantörer som har rätt till tillgång till tjänster på någon annans vägnar identifierar kunderna på ett tillförlitligt sätt
- Leverantörer som har rätt till tillgång till tjänster på någon annans vägnar jämför användarkonton på ett tillförlitligt sätt:
  - Datainnehållen lämpar sig för jämförelse
  - Datainnehållen är korrekta/uppgifternas korrekthet intygas
- Informationssäkerheten i tjänsterna som leverantörer som har rätt till tillgång till tjänster tillhandahåller
- Den ekonomiska situationen för leverantörer som har rätt till tillgång till tjänster

- Anseendet för leverantörer som har rätt till tillgång till tjänster på någon annans vägnar.

Kriterierna ovan bildar ingen helhet, utan kan användas till tillämpliga delar. Listan är inte heller uttömmande, utan aktören kan använda också andra kriterier som den anser viktiga och nödvändiga för att kunna bedöma tillförlitligheten.

När det gäller dataskyddet kan man i fråga om bedömningskriterierna förutsätta att leverantören som har rätt till tillgång till tjänster på någon annans vägnar kan visa hurdana åtgärder den har vidtagit för att uppfylla kraven i den allmänna dataskyddsförordningen, till exempel information till de registrerade och förverkligande av de registrerades övriga rättigheter i tjänsten som leverantören tillhandahåller.

4.1 Hur tillförlitlig är identifieringen som leverantörer som ges tillgång till tjänster på någon annans vägnar gör?

4.1.1 Allmänt om identifiering vid tjänster på någon annans vägnar

Enligt 156 § 3 mom. i lagen om transportservice får personuppgifter endast behandlas i den omfattning som behövs för styrkande av någons identitet och för att genomföra kundhändelsen i samband med sådana kundhändelser på någon annans vägnar som avses i 1 och 2 mom. Utöver vad som föreskrivs någon annanstans i lag ska identiteten kunna styrkas på ett särskilt tillförlitligt sätt då tillgång till tjänster på någon annans vägnar grundas eller då den ändras väsentligt. Identiteten ska kunna styrkas också i samband med en kundhändelse på någon annans vägnar.

I en regeringsproposition om lagrummet (RP 145/2017 rd, s. 186) nämns följande om styrkande av identiteten: ”Enligt det föreslagna 3 mom. ska identiteten kunna styrkas synnerligen noggrant när ett kundförhållande grundas eller ändras väsentligt. Också vid varje transaktion på någon annans vägnar bör vederbörandes identitet kunna styrkas. I tekniskt avseende torde det kunna göras med olika lösningar, såsom identifieringskoder, certifikat eller pseudonymer. Till skillnad från PSD2 ska stark identifikation alltså inte krävas. Dessutom är det värt att notera att t.ex. betalningstjänstdirektivet kan förutsätta stark elektronisk identifiering vid betalningsuppdrag.”

I sitt beslut 20/1905/3 av den 10 december 2020 har Helsingfors förvaltningsdomstol ansett att stark identifiering i samband med beviljande av behörighet för tjänster på någon annans vägnar har kunnat betraktas som ett förbjudet och orimligt användarvillkor.

Enligt lagen om transportservice är grundförutsättningen för tillgång till tjänster på någon annans vägnar att kunden har ett användarkonto i tjänsten som leverantören som är skyldig att ge tillträde tillhandahåller och i en tjänst hos den tjänsteleverantör som ges tillgång (RP 145/2017 rd, s.

186) När konton skapas och i samband med senare åtgärder har aktörerna identifierat kunden.

Med hjälp av denna grundprincip kan man grunda tillgång till tjänster på någon annans vägnar om man genom att jämföra uppgifterna i två användarkonton kan styrka kundens identitet på ett särskilt tillförlitligt sätt och samtidigt använda de identifikationer av kunden som tjänsteleverantören som är skyldig att ge tillträde och leverantören som ges tillgång till tjänster på någon annans vägnar har gjort. Vid tillgång till tjänster på någon annans vägnar identifieras kunderna således genom att man jämför informationen i användarkonton.

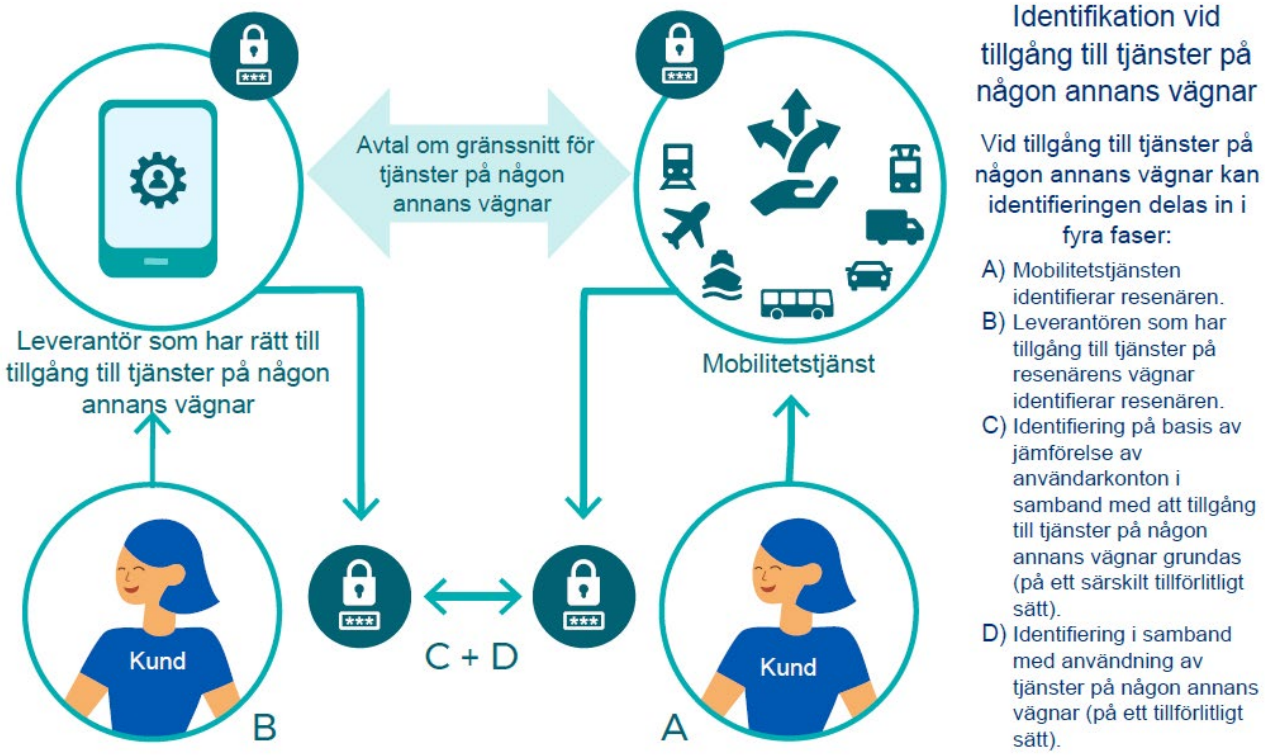

Illustration över de olika faserna av identifikation vid tillgång till tjänster på någon annans vägnar.

4.1.2 Hur tillförlitlig är identifieringen av kunder som utförs av leverantörer som ges tillgång till tjänster på någon annans vägnar?

Tjänsteleverantörer som är skyldiga att ge tillträde kan av leverantörer som har rätt till tillgång till tjänster på någon annans vägnar kräva en tillräckligt hög nivå på identifieringen av kunden för att kunna säkerställa att rätt konton kombineras samt minimera antalet misslyckade jämförelser och eventuella missbruk. Om den identifiering av kunden som leverantören som har rätt till tillgång till tjänster på någon annans vägnar gör inte uppfyller

de på förhand angivna kriterierna för tillförlitlighet kan kundens identitet inte styrkas vid användning av tjänster på dennes vägnar på det mycket tillförlitliga sätt som lagen kräver.

Kriterierna för identifikationens tillförlitlighet ska vara rättvisa, rimliga och icke-diskriminerande.

Huvudprincipen är att tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt kan förutsätta högst en sådan nivå på tillförlitligheten hos de uppgifter som används för att identifiera kunden som krävs av kunden själv. Om till exempel identifieringen av kunden i användarkonton hos en tjänsteleverantör som är skyldig att ge tillträde till gränssnitt baserar sig på namnet samt ett (verifierat) telefonnummer och en (verifierad) e-postadress kan man inte kräva mer än det av leverantören som ges tillgång till tjänster på någon annans vägnar.

En tjänsteleverantör som är skyldig att ge tillträde till gränssnitt måste öppna gränssnittet först när nivån på tillförlitligheten hos identifikationen som leverantören som ges tillträde utför uppnås.

4.2 Hur tillförlitliga är användarkonton hos leverantörer som ges tillgång till tjänster på någon annans vägnar vid jämförelse?

4.2.1 Allmänt

Som nämns ovan identifieras användaren av tjänsten och hens kundkonto enligt Traficoms tolkning genom att man utnyttjar de identifikationer som leverantören som ges tillgång till tjänster på någon annans vägnar och tjänsteleverantören som är skyldig att ge tillträde till gränssnitt har gjort samt deras jämförelser av uppgifterna i användarkontona på det mycket tillförlitliga sätt som lagen kräver.

Vid tillgång till tjänster på någon annans vägnar ska man behandla så lite personuppgifter som möjligt, men dock i sådan utsträckning att styrkandet av identiteten ”på ett särskilt tillförlitligt sätt” enligt lagen om transportservice inte äventyras.

Tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt har rätt att med hjälp av bedömningskriterier försäkra sig om att leverantören som ges tillträde till tjänster på någon annans vägnar är tillförlitlig även när det gäller datainnehållen i användarkonton, så att det säkert är samma kunds konton som kombineras vid användningen av tjänster på någon annans vägnar.

Denna bedömning kan göras ur två olika synvinklar: 1) Har leverantören som ges tillgång till tjänster på någon annans vägnar sådana typer av datainnehåll som kan jämföras med användarkontona i tjänsten som leverantören som är skyldig att ge tillträde tillhandahåller? och 2) På vilket sätt säkerställs att dessa datainnehåll är korrekta?

4.2.2 Hur väl lämpar sig datainnehållen i användarkonton hos leverantörer som ges tillgång till tjänster på någon annans vägnar för jämförelse?

För att det ska vara möjligt att jämföra användarkonton bör leverantören som ges tillgång till tjänster på någon annans vägnar ha några sådana datainnehåll om kunden som även finns i användarkonton i tjänsten som leverantören som är skyldig att ge tillträde till gränssnitt tillhandahåller. Dessutom ska datainnehållen gå att särskilja tillräckligt väl, så att rätt kontoinnehavare identifieras.

Eftersom bedömningskriterierna ska vara rimliga, kan tjänsteleverantören som är skyldig att ge tillträde till gränssnitt inte kräva fler datainnehåll av leverantören som ges tillgång till tjänster än vad som är nödvändigt för att identifiera kunden. Därtill ska aktörerna beakta principen om uppgiftsminimering enligt EU:s allmänna dataskyddsförordning, vilken begränsar deras möjligheter att samla in personuppgifter om användarna.

När en leverantör som är skyldig att ge tillträde till gränssnitt anger bedömningskriterier för de datainnehåll som krävs borde den beakta också kundens erfarenhet av att använda tjänsten som leverantören som ges tillträde tillhandahåller. Till exempel skulle kravet på långa kundnummer som jämförelseuppgift i tjänsten hos leverantören som är skyldig att ge tillträde i regel kunna betraktas som orimligt, om kunden får reda på det endast genom att logga in i sitt användarkonto i den aktuella leverantörens tjänst.

Jämförelsen ska med andra ord göras med beaktande av kundens användarerfarenhet och med ett så litet antal olika typer av datainnehåll som möjligt, men de datainnehåll som används vid jämförelse av dessa måste identifiera kunden på ett effektivt sätt.

4.2.3 Hur korrekta är datainnehållen hos leverantörer som ges tillgång till tjänster på någon annans vägnar samt hur verifieras uppgifterna?

En förutsättning för att jämförelsen som nämns ovan ska fungera är att uppgifterna som används för att jämföra användarkonton är korrekta och aktuella, så att samma kunds datainnehåll kan kombineras med varandra i jämförelsen. På så vis kan tjänsteleverantören som är skyldig att ge tillträde till gränssnitt kräva att åtminstone ett datainnehåll ska vara verifierat i eller i samband med den identifikation som leverantören som ges tillträde till tjänster på någon annans vägnar har gjort. Verifieringen kan ske på olika sätt beroende på datatypen. Till exempel hanteringen av

telefonnummer kan verifieras med sms, medan adressuppgifter kan verifieras i befolkningsdatasystemet.

Personuppgiftsansvariga åläggs att ha korrekta och aktuella uppgifter i sina användarkonton även genom den allmänna dataskyddsförordningens krav på korrekta uppgifter.

4.2.4 Datainnehållen hos tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt och verifieringen av dem

I lagen om trafikservice åläggs tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt inte att ändra datainnehållen i sina användarkonton eller sätten att verifiera dem. Utgångspunkten kan således anses vara att datainnehållen som sådana i användarkonton hos tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt även gör det möjligt för aktörer att använda tjänster på någon annans vägnar. På så vis kan tjänsteleverantörer som är skyldiga att ge tillträde inte neka tillgång till tjänster på någon annans vägnar genom att hänvisa till att datainnehållen i användarkontona inte gör det möjligt för aktörer att använda tjänster på någon annans vägnar utan att äventyra dataskyddet och informationssäkerheten.

Tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt kan dock, till exempel med tanke på dataskyddet, anse det nödvändigt att förbättra sina användarkonton som används för tjänster på någon annans vägnar, till exempel när det gäller datainnehåll eller verifiering av uppgifter. Dataskyddslagstiftningen förutsätter minimering av uppgifter, men samtidigt även uppgifternas integritet samt att de är konfidentiella och korrekta. Dataskyddslagstiftningen hindrar inte att man kan behandla även nya men endast nödvändiga datainnehåll för att genomföra användningen av tjänster på någon annans vägnar, om de uppgifter som redan finns i användarkontona inte kan anses uppfylla kravet på styrkande av kundens identitet enligt lagen om transportservice.

4.3 Informationssäkerheten hos leverantörer som ges tillgång till tjänster på någon annans vägnar som bedömningskriterium

4.3.1 Sekretessgrad, integritet och tillgänglighet

Med upprätthållande av informationssäkerheten avses de tekniska och organisationsmässiga åtgärder som aktören vidtar för att säkerställa webb- och informationssystemens integritet och tillgänglighet samt att informationen hålls konfidentiell.

Sekretess (confidentiality) innebär att endast personer som har behörighet

till det har tillgång till uppgifterna. Detta förutsätter i praktiken att såväl informationen som de som har rätt till den definieras på en tillräckligt hög nivå.

Integritet (integrity) innebär att en uppgift eller ett system inte kan ändras eller förstöras utan behörighet under hela dess livscykel och att eventuella obehöriga ändringar upptäcks.

Tillgänglighet (availability) innebär att en uppgift eller ett system kan användas när det behövs. Tillgänglighet innebär även tillräcklig kapacitet med tanke på användningsbehovet samt vid behov även skydd mot oavsiktliga och avsiktliga överlastningsangrepp.

4.3.2 Faktorer som påverkar nivån på informationssäkerheten i tjänster hos leverantörer som ges tillträde till tjänster på någon annans vägnar

Identifiering av uppgifter som ska skyddas samt risken

För att information och informationssystem ska kunna skyddas effektivt och ekonomiskt ska man identifiera vilka de viktigaste områdena att skydda är samt de största hoten mot dem. Det är omöjligt och/eller för dyrt att skydda allt mot alla hot. För att kunna dimensionera informationssäkerhets- och dataskyddskontrollerna rätt behövs därför en systematisk hotanalys, där man typiskt bedömer riskerna som är förknippade med verksamheten utifrån sannolikheten för dem samt allvarlighetsgraden hos konsekvenserna av dem.

En tjänsteleverantör som är skyldig att ge tillträde till gränssnitt kan kräva att leverantörer som ges tillträde till tjänster på någon annans vägnar vidtar tekniska och organisationsmässiga åtgärder för att upprätthålla informationssäkerheten som står i relation till hotets allvar och sannolikhet, kostnaderna för åtgärderna samt de tekniska och organisationsmässiga kontroller som finns tillgängliga för att avvärja hotet. Man kan i allmänhet inte kräva att en risk undanröjs helt och hållet, men man kan kräva att den minskas till en godtagbar nivå (kvarstående risk).

Vid bedömning av allvaret hos ett hot ska åtminstone följande beaktas:

1. typ av information som ska skyddas (till exempel krav på behandlingen av personuppgifter eller på hanteringen av certifikatnycklar),

2. hur kritisk funktionen som ska skyddas är med tanke på systemets integritet
och

3. omfattningen av eventuella personuppgiftsincidenter samt ekonomiska och övriga skador när hotet förverkligas.

Vid bedömning av sannolikheten för ett hot ska åtminstone följande beaktas:

1. den rådande och aktuella kunskapen om webbtjänsterna samt
2. de informationssäkerhetsrisker som riktar sig till den bakomliggande plattformsinfrastrukturen.

Vad skyddar man i synnerhet vid tjänster på någon annans vägnar?

På grund av användarkontona är det särskilt viktigt att värna om sekretess och integritet i fråga om personuppgifter vid tjänster på någon annans vägnar (dataskydd). Ett av särdragen är en korrekt sammankoppling av kundernas konton mellan leverantören som ges tillträde till tjänster på någon annans vägnar och leverantören av mobilitetstjänsten.

Andra områden som kräver skydd är till exempel affärshemligheter som systemen innehåller och integriteten i fråga om penningrörelsen samt överlag att informationssystemens integritet bevaras även vid felsituationer och åtminstone vid vanliga webbattacker. Vid fastställandet av målnivån för tillgängligheten till informationssystemen och tjänsterna är det ofta värt att tänka på omfattningen av skador som orsakas av avbrott (till exempel ekonomiska förluster och/eller förlust av anseende) och dimensionera åtgärderna för att skydda tillgängligheten enligt det. På samma sätt som det vanligtvis inte är vettigt att minska en kvarstående risk till noll, lönar det sig i allmänhet inte heller att sträva efter en hundraprocentig tillgänglighet, bland annat på grund av de kostnader som det medför.

4.3.3 Vad kan tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt i bedömningskriterierna kräva i fråga om informationssäkerheten i tjänsterna som en leverantör som ges tillträde tillhandahåller?

Kraven kan grovt delas in i två delområden: beaktande av säkerheten i allmänhet inom organisationens verksamhet (administrativ säkerhet) och teknisk säkerhet i informationssystemen som används inom tjänster på någon annans vägnar.

1) Till det administrativa området kan man anse att en realistisk och systematisk hotanalys av den egna verksamheten hör, utifrån vilken de kvarstående riskerna har minskats till en godtagbar nivå. Organisationen ska bland annat definiera de personer och verksamhetsprocesser som är viktiga för säkerheten och inkludera dem i den dagliga verksamheten.

2) Av den tekniska säkerheten hos informationssystem som används vid tjänster på någon annans vägnar kan krävas att allmän god informationssäkerhetspraxis följs på en konkret nivå. På ett allmänt plan omfattar sådan praxis bland annat följande (listan är inte uttömmande):

- Aktuella informationssäkerhetsuppdateringar i systemen
- God praxis inom administrationen av användarrättigheter
- Ändamålsenliga höjningar av informationssäkerheten samt praxis för upprätthållande av den
- Tillräckligt skydd av datakommunikationen (kryptering/sekretess, integritet, tillförlitlig identifiering av motparten)
- Tydligt definierade, säkra, robusta och testade implementeringar av gränssnitt.

Det är även möjligt att kräva intyg över att de ovanstående kraven uppfylls av leverantörer som ges tillträde till tjänster på någon annans vägnar. Sådana intyg kan vara till exempel rimligen färska självutvärderingar eller utvärderingar gjorda av tredje parter. Rapporter producerade med hjälp av (halv)automatiska informationssäkerhetsverktyg kan också vara ett sätt att visa den tekniska säkerhetsnivån.

Ingendera parten kan dock utkontraktera sitt ansvar i fråga om informationssäkerhet och dataskydd till någon annan part. Till exempel ska tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt se till att deras egna implementeringar av gränssnitt skyddas på lämpligt sätt.

Kriterier för bedömning av informationssäkerheten

För att bedömningen av informationssäkerheten ska vara heltäckande och jämförbar är det möjligt att använda befintliga kriterier och verktyg. Bland dessa finns det såväl mer allmänna kriterier framtagna för säkerställande av den administrativa säkerheten som mer tekniska kriterier för granskning av informationssystem.

Exempel på mer allmänna kriterier är bland annat

- standarderna i ISO 27000-serien
- Traficoms Cybermätare.

Exempel på mer tekniska kriterier är bland annat

- OWASP Top Ten Web Application Security Risks, Mobile Security Testing Guide
- PCI DSS.

Statsförvaltningen har även publicerat kriterier och anvisningar med utgångspunkt i skyddet av information som vanligtvis klassificeras av en myndighet. Dessa kriterier är bland annat den nationella kriteriesamlingen för säkerhetsauditering (Katakri), säkerhetskriterierna för molntjänster (PiTuKri) och flera VAHTI-anvisningar. Som sådan är lämpligheten hos dessa för att bedöma informationssäkerheten i tjänster som leverantörer som ges tillträde tillhandahåller dock begränsad på grund av den ställvis höga kravnivån i de ovanstående kriterierna.

4.4 Ekonomiska bedömningskriterier

Syftet med de ekonomiska bedömningskriterierna är att säkerställa att aktörer som begär tillträde till gränssnitt har tillräckliga ekonomiska resurser för att kunna använda tjänster på någon annans vägnar på ett säkert sätt.

4.4.1 Krav på registrering som näringsidkare som bedömningskriterium

Utgångspunkten enligt lagen är skyldigheten att ge alla tillträde till gränssnitt, men tjänsteleverantörer som är skyldiga att ge tillträde har dock rätt att bedöma andra aktörers tillförlitlighet ur ekonomisk synvinkel.

Man kan kräva att företag som begär tillträde till gränssnitt ska ha ett FO-nummer i Finland eller något annat bevis på att företaget är registrerat som näringsidkare någon annanstans i EU. Inom EU används åtminstone det så kallade VAT-numret, som visar att den som begär tillträde är momsskyldig. Skatteförvaltningens anvisningar säger att när ”ett momsskyldigt företag idkar handel med ett företag som registrerats som momsskyldigt i ett annat EU-land antecknar företaget förutom sitt FO-nummer även momsnumret på fakturan.”

Företag eller sammanslutningar som är verksamma i Finland är skyldiga att anmäla grundande och ändringar i verksamheten samt avslutande av verksamhet till Patent- och registerstyrelsen (PRH) samt Skatteförvaltningen (i PRH:s handelsregister, föreningsregister eller stiftelseregister samt Skatteförvaltningens momsregister, förskottsuppbördsregister och arbetsgivarregister).

Utdrag och intyg ur PRH:s och Skatteförvaltningens register som nämns ovan ger antydningar om att aktören är tillförlitlig också ur ekonomisk synvinkel.

4.4.2 Tillräckliga ekonomiska resurser för att använda tjänster på någon annans vägnar

Det kan krävas att leverantörer som ges tillträde till tjänster på någon annans vägnar har tillräckliga ekonomiska förutsättningar för att på ett säkert sätt bedriva den verksamhet som gränssnittet öppnas för. Vid bedömning av om de ekonomiska resurserna är tillräckliga kan till exempel följande kriterier användas:

Ett företag har sannolikt inte ekonomiska förutsättningar för att bedriva verksamheten om

- företaget har förlorat över hälften av sitt angivna aktiekapital (aktiebolag) eller över hälften av sina tillgångar enligt bokslutet (öppet bolag eller kommanditbolag) på grund av ackumulerade förluster

- företaget har försatts i konkurs eller har inlett företagssanering på grund av insolvens eller på grund av sin situationen skulle kunna bli föremål för det.

4.5 Företagets anseende som kriterium för bedömning av tillförlitligheten

Bedömningskriterier som baserar sig på företagets anseende kan säkerställa att inga missbruk eller allvarliga brister är förknippade med verksamheten för leverantörer som ges tillträde till tjänster på någon annans vägnar.

Vid tillämpning av kriterier som baserar sig på ett företags anseende har tjänsteleverantörer som är skyldiga att ge tillträde till gränssnitt bevisskyldighet om de på dessa grunder vägrar att öppna gränssnitt för leverantörer som begär tillträde. Även i detta fall ska kriterierna vara rättvisa, rimliga och icke-diskriminerande. Vid övervägning får man till exempel beakta fel och försummelser endast för en rimlig tidsperiod. Kriterier som gäller ett företags anseende har likheter med de frivilliga uteslutningsgrunder som beskrivs i lagen om offentlig upphandling och koncession.

Kriterier som bedömer ett företags anseende kan delas in i allmänna och bilaterala grunder för att inte öppna ett gränssnitt på basis av motpartens anseende.

En tjänsteleverantör som är skyldig att ge tillträde till gränssnitt ska dock betrakta leverantörer som har rätt till tillgång till tjänster på någon annans vägnar som pålitliga aktörer om de har vidtagit konkreta tekniska åtgärder samt åtgärder visavi organisationen och personalen med hjälp av vilka man kan förhindra nya straffbara handlingar, fel eller försummelser. När det gäller detta är det leverantörerna som använder tjänster på någon annans vägnar som är bevisskyldiga.