

Tillhandahållare av betrodda tjänster – ny EU-förordning den 1 juli 2016

Den 1 juli 2016 börjar EU:s förordning 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen) att tillämpas i Sverige.

Syftet med förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att skapa en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter inom unionen.

Förordningen är uppdelad i två delar. En del handlar om elektronisk identifiering och för den delen är ansvarig svensk myndighet [E-legitimationsnämnden](#). Den andra delen, där PTS blir tillsynsmyndighet, handlar om betrodda tjänster.

Elektronisk identifiering och elektroniska underskrifter är viktiga förutsättningar för att privatpersoner och företag ska kunna använda digitala tjänster. För att ett system med elektronisk identifiering ska fungera krävs att alla inblandade parter uppfattar det som tillförlitligt. Därför innehåller eIDAS-förordningen en rättslig ram för elektronisk identifiering och så kallade betrodda tjänster och regler för de som tillhandahåller de betrodda tjänsterna.

Vilka berörs av eIDAS-förordningen?

Tillhandahållare av betrodda tjänster

Tillhandahållare av betrodda tjänster som är etablerade inom unionen omfattas av eIDAS-förordningen (artikel 2.1.)

I eIDAS-förordningen (artikel 3 p. 16) definieras en *betrodd tjänst* som en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av någon av följande tjänster:

- Utfärdande av certifikat för elektroniska underskrifter och stämplor
- Validering av underskrifter och stämplor
- Bevarande av underskrifter och stämplor
- Tidsstämpling
- Elektronisk rekommenderad leverans
- Certifikat för autentisering av webbplatser

En *tillhandahållare av en betrodd tjänst* definieras (artikel 3 p.19) som en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerad eller icke kvalificerad tillhandahållare av betrodda tjänster.

Undantag

Som huvudregel omfattas alla tillhandahållare av betrodda tjänster av eIDAS-förordningen.

Det finns dock vissa typer av tillhandahållande av betrodda tjänster som är undantagna från förordningens krav. Det är betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets deltagare endast används inom slutna system (artikel 2.2). Dvs. förordningen gäller inte tillhandahållare av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare och som inte påverkar tredje man. Som exempel nämns system som inrättats inom företag eller offentlig förvaltning för hantering av interna förfaranden. Endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man omfattas av förordningen.

Undantaget från förordningens tillämpningsområde är även bestämmelser i nationell lagstiftning eller unionslagstiftningen som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav (artikel 2.3).

I svensk lagstiftning ställs för närvarande inte några krav på att använda kvalificerade betrodda tjänster vare sig mellan enskilda eller gentemot offentliga organ.

Kvalificerade och icke kvalificerade tillhandahållare

Det är frivilligt att vara en *kvalificerad tillhandahållare* och tillhandahålla *kvalificerade betrodda tjänster*. För att bli kvalificerad ska en tillhandahållare granskas av ett organ för överensstämmelsebedömning och lämna in rapporten från en sådan granskning och en anmälan till PTS. Om PTS bedömer att kraven i förordningen är uppfyllda beviljas status som kvalificerad tillhandahållare. Övriga tillhandahållare benämns *icke kvalificerade tillhandahållare*.

Krav på icke kvalificerade tillhandahållare

Ett fåtal av förordningens bestämmelser berör även icke kvalificerade tillhandahållare. Det är bestämmelserna om:

- Skadeståndsansvar (artikel 13)
- Lämpliga säkerhetsåtgärder (artikel 19.1)
- Skyldighet att rapportera säkerhetsincidenter och integritetsförluster till PTS (artikel 19.2)

Med lämpliga säkerhetsåtgärder avses tekniska och organisatoriska åtgärder som tillhandahållarna ska vidta för att hantera riskerna för säkerheten hos sina betrodda tjänster. Säkerhetsnivån ska stå i proportion till graden av risk med beaktande av teknikutvecklingen. Det innebär att tillhandahållare behöver ha en organisation och roller som kontinuerligt arbetar med att genomföra riskanalyser och utifrån dessa vidta åtgärder som hanterar dessa risker.

Mer stöd från standarder

Mer stöd för säkerhetsarbetet finns i standarderna:

[EN 319 401 General Policy Requirements for Trust Service Providers](#)

[ISO/IEC 27002:2013 Information technology - Security techniques -- Code of practice for information security controls](#)

Säkerhetsincidenter och integritetsförluster ska rapporteras senast inom 24 timmar efter upptäckt. Det som ska rapporteras är sådana säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller de personuppgifter som ingår i tjänsten.

Tillsyn över icke kvalificerade tillhandahållare

PTS kommer att agera genom att bedriva tillsyn när myndigheten tar del av påståenden att en icke kvalificerad tillhandahållare eller en betrodd tjänst som denne tillhandahåller inte uppfyller kraven i förordningen.

Bestämmelser för kvalificerade tillhandahållare

Krav och övriga bestämmelser som rör kvalificerade tillhandahållare beskrivs i PTS dokument [Vägledning - För betrodda tjänster i Sverige enligt eIDAS](#) som finns på PTS webbplats.

Läs mer på PTS webbplats

På PTS webbplats www.pts.se/eidas finns mer information om eIDAS.

Faktablad om eIDAS

PTS-F-2016:3

Publicerat 2016-06-03

Faktablad finns på www.pts.se/faktablad