

Vår referens: Dnr 20-11383, Aktilaga: 17, Datum: 2020-12-04

Kivra Sverige AB

Beslut – avskrivning av tillsyn med anledning av driftstörning i den betrodda tjänsten som Kivra Sverige AB tillhandahåller

Saken

Tillsyn enligt artikel 17.3 b eIDAS-förordningen¹.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

Bakgrund

Kivra Sverige AB (Kivra) är en tillhandahållare av en betrodd tjänst enligt artikel 3.16 a eIDAS-förordningen.

Enligt artikel 19.1 eIDAS-förordningen ska tillhandahållare av betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänsterna som de tillhandahåller. En viktig organisatorisk säkerhetsåtgärd kan vara att ha en fastställd och dokumenterad förändringsprocess för hur planerade förändringar ska genomföras, testas och driftsättas.

¹ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

Under augusti 2020 incidentrapporterade² Kivra tre driftstörningar i den betrodda tjänsten som Kivra tillhandahåller, i enlighet med artikel 19.2 i eIDAS-förordningen. Incidenterna påverkade tjänstens tillgänglighet.

I den första incidentrapporten, som inträffade den 25 augusti 2020, uppger Kivra att tjänsten var otillgänglig i 38 minuter. Den andra incidenten, som inträffade 27 augusti 2020, pågick i 14 minuter. Den tredje incidenten, som inträffade 31 augusti 2020, pågick i 1 timme och 50 minuter.

Inom ramen för tillsynen har PTS haft ett tillsynsmöte med representanter från Kivra samt tagit del av skriftliga svar på kompletterande frågor. Vid mötet och i de skriftliga svaren har Kivra redogjort för sina processer för förändringshantering och genomförande av riskanalys, samt de åtgärder som vidtagits för att säkerställa att alla i organisationen följer dessa. Vidare har Kivra informerat om att bolaget har infört en process för att minska risken för liknande incidenter. Kivra har även redogjort för en kortsiktig och en långsiktig plan för att stärka tillgängligheten i den betrodda tjänsten.

Skäl

Tillämpliga bestämmelser

Enligt artikel 17.1 i eIDAS förordningen ska det i varje medlemsstat utses ett tillsynsorgan.

PTS är, enligt 4 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Tillsynsmyndigheten ska enligt artikel 17.3 b eIDAS-förordningen vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i förordningen.

Av artikel 19.1 i eIDAS-förordningen framgår att tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster de tillhandahåller.

² Dnr 20-9730, 20-9786 och 20-9913

PTS bedömning

Fel och incidenter i samband med förändringshantering utgör en stor risk för säkerheten i betrodda tjänster. Enligt PTS bedömning är det en förutsättning för att en tillhandahållare ska anses kunna bedriva ett godtagbart säkerhetsarbete enligt eIDAS-förordningen att tillhandahållaren tillämpar ändamålsenliga processer för förändringshantering och genomförande av riskanalys.

Inom ramen för tillsynen har Kivra redogjort för sin förändringsprocess vilken, enligt PTS bedömning, utgår från en etablerad standard, samt sin process för att göra riskbedömningar. Vidare har Kivra klarlagt vilka åtgärder som vidtagits för att se till att förändringsprocessen följs av alla medarbetare i organisationen.

PTS bedömer att de åtgärder Kivra har vidtagit är lämpliga åtgärder för att minska risken för att liknande incidenter händer igen.

PTS bedömer sammantaget att bolaget vid tidpunkten för tillsynen visat att de bedriver ett systematiskt säkerhetsarbete där de kan identifiera risker och vidta relevanta åtgärder i enlighet med artikel 19.1 eIDAS-förordningen.

PTS bedömer därmed att det inte finns skäl att fortsätta tillsynen och avskriver ärendet från vidare handläggning.

Beslutet har fattats av enhetschef Karin Lodin. I ärendets slutliga handläggning har även handläggarna Anders Franzén, Mikael Ejner, Bahare Sadeghi Gazani och Åsa Gihl (föredragande) deltagit.

