Hogia Signit är en signeringstjänst som håller högsta klass avseende skydd av användarnas data och integritet. Att säkerställa våra kunders trygghet genomsyrar allt vi gör, från utveckling till drift och underhåll.

Hogia Signit

En central funktion i Hogia Signit är att användaren kan styra och begränsa tillgången till signeringsärenden och hur dokument ska signeras. Tillgången kan begränsas så att dokument enbart kan granskas efter identifiering med BankID. De digitala signaturerna skapas med elektroniska underskriftscertifikat. Detta gör att det går att säkerställa att rätt person har signerat dokumentet och att dokumentet inte har manipulerats efter signering.

Med Hogia Signit kan användaren skapa så kallade Avancerade Elektroniska Underskrifter (AdES) i enlighet med en etablerad europeisk standard som uppfyller kraven i EU-förordningen eIDAS. Det signerade dokumentet innehåller då den kompletta certifikatinformationen. Därmed kan äktheten av dokumentet och dess signaturer alltid valideras elektroniskt av en extern part, oberoende av Signit och Hogia som leverantör.

Att distribuera information via e-post innebär alltid risker. Därför skickas inga dokument eller känsliga personuppgifter via e-post.

Datasäkerhet

Fysisk och logisk säkerhet

Hogia använder marknadsledande teknik för att upptäcka och motverka oönskad aktivitet såsom intrångsförsök och skadlig kod. Hogia använder ett enhetligt system för hantering av infrastruktursäkerhet och verktyg för att förhindra, identifiera och svara på eventuella hot. Vidare använder Hogia ett centraliserat skydd mot kryphål och sårbarheter som uppdateras automatiskt för att inkludera skydd mot nya säkerhetsrisker. All access till data kräver godkänd autentisering. Nätverksarkitekturen är indelad i ett flertal säkerhetszoner för att minimera risken för intrång, åtkomst till data och eventuella skadeverkningar.

All kunddata krypteras över publika nätverk.

Endast ett fåtal säkerhetsklassade och bakgrundskontrollerade personer på Hogia har tillgång till data som kan innehålla personuppgifter eller annan känslig information.

Serverdrift och datalagring görs i säkerhetsklassade och geografiskt åtskilda redundanta serverhallar inom EU. Backuper tas kontinuerligt under dagen.

Hogia har en säkerhetsgrupp som kontinuerligt arbetar med riskutvärderingar i syfte att identifiera, mäta och prioritera säkerhetsrisker. Detta för att proaktivt hitta och stoppa sårbarheter och för att leverera högsta datasäkerhet. Penetrationstester och sårbarhetsscanningar av Hogias applikationer och infrastruktur genomförs kontinuerligt. Dessa planerade intrångsförsök genomförs av externa oberoende säkerhetsföretag i syfte att upptäcka och åtgärda svagheter.

Alla förändringar i IT-miljön följer Hogias uppsatta och dokumenterade ändringshanteringsrutiner. Hogia har formella godkännandeförfaranden innan IT-förändringar genomförs. Våra produktionsmiljöer är separerade från övriga miljöer och kunders produktionsdata används aldrig i utvecklings- eller testsyfte.

Efterlevnad av Dataskyddsförordningen (GDPR)

Hogia har riktlinjer och rutiner för behandling av personuppgifter i enlighet med Dataskyddsförordningen och vidtar nödvändiga tekniska och organisatoriska åtgärder för att skydda personuppgifter.

Hogia har en dataskyddsansvarig som övergripande kontrollerar och följer upp att verksamheten efterlever lagkrav och upprättade riktlinjer som ställs avseende hantering av personuppgifter.

Mer information finns beskrivet och tillgängligt publikt i Hogias integritetspolicy på hogia.se, under länken ”Tekniska och organisatoriska säkerhetsåtgärder”.

Gallring av personuppgifter i Hogia Signit

Användaren av Hogia Signit sparar personuppgifter i systemet avseende de individer som ska signera dokumentet (namn, e-post och eventuellt personnummer). I de fall som dokumentet inte signeras av alla parter gallras personuppgifterna automatiskt bort efter 90 dagar. Om dokumentet däremot signeras av alla parter sparas personuppgifterna i Signit till dess användaren själv väljer att radera dessa via gränssnittet.