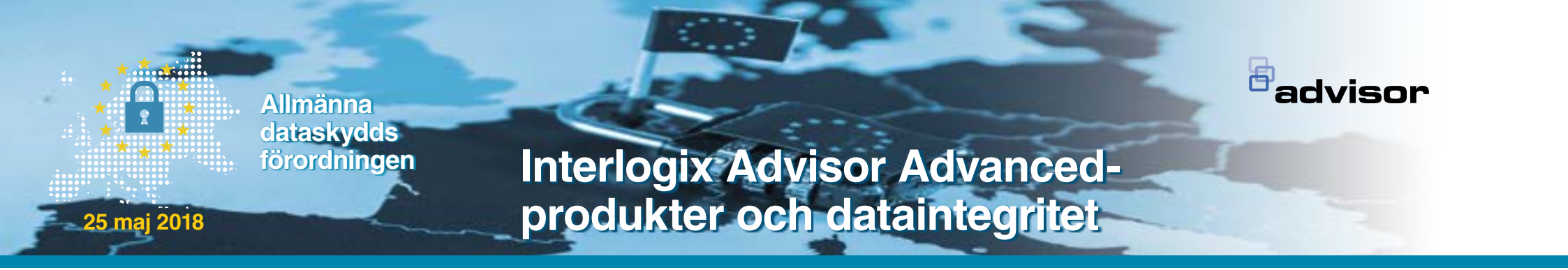

advisor

Interlogix Advisor Advanced-produkter och dataintegritet

Allmänna dataskyddsförordningen (GDPR)

Den allmänna dataskyddsförordningen (General Data Protection Regulation, "GDPR"), som trädde i kraft 25 maj 2018, tillhandahåller regler för att skydda personuppgifter. Personuppgifter avser all information relaterad till en identifierad eller identifierbar fysisk person, som kan identifieras direkt eller indirekt, särskilt genom hänvisning till ett identifikationsnummer eller genom en eller flera faktorer som är specifika för hans/hennes fysiska, fysiologiska, mentala, ekonomiska, kulturella eller sociala identitet. Mer information om GDPR finns tillgänglig på: **http://www.eugdpr.org**

En av de mer betydande ändringarna av EU:s regelverk avseende dataintegritet innefattar GDPR:s utökade lagstadgande, såsom den gäller för alla entiteter etablerade inom EU, oavsett om behandlingen äger rum i EU eller inte, och för alla entiteter som behandlar personuppgifterna för en registrerad som är bosatt i EU med hjälp av entiteter som inte är etablerade i EU.

United Technologies Corporation värdesätter GDPR:s betydelse och har på en global nivå implementerat bindande företagsbestämmelser (Binding Corporate Rules, "BCR"), som inkluderar vår integritetspolicy och vårt interna policyrelaterade företagsstyrningssystem. BCR anses vara den gyllene standarden för dataskydd. Våra BCR finns allmänt tillgängliga på flera olika språk (**http://www.utc.com/Pages/Privacy.aspx**).

Hur påverkar detta Advisor Advanced-produkterna?

Advisor Advanced-produkterna, utvecklade av UTC Fire & Security Americas Corporation, Inc. (som driver verksamhet som "Interlogix"), består av ett produktutbud som tillhandahåller säkerhet för egendomar genom att inbrottslarm och funktioner för tillträdeskontroll installeras. Våra produkter inkluderar maskinvara såsom säkerhetskontrollpaneler, expanderare, tangentbord och läsare, samt programvara för att konfigurera och hantera olika lösningar. Personuppgifter krävs för att de olika systemen ska fungera. Installatören arbetar med dig som kund och slutanvändare för att definiera vilka slags personuppgifter som ska anges som en del av installations- och driftsättningsprocessen. Eftersom Interlogix inte installerar eller driftsätter Advisor Advanced-produkterna, är installatören och slutanvändaren ansvariga för att fastställa att insamlingen och användningen av personuppgifterna överensstämmer med kraven som ställs i GDPR.

Samtidigt som slutanvändaren är slutgiltigt ansvarig för inmatningen, behandlingen och hanteringen av personuppgifter i Advisor Advanced-produkterna, stödjer Interlogix slutanvändaren att göra dataintegriteten förenlig genom att införliva integritetskraven i produktutformningen. Interlogix är förbundna av inbyggd integritet.

Våra produkter är utformade att stödja slutanvändaren i enlighet med hur slutanvändaren fastställer vilka personuppgifter som ska matas in i systemet. Interlogix produkter erbjuder varierande säkerhetsnivåer för att skydda personuppgifterna för de individer som har tillträde till slutanvändarnas anläggningar. Hänsyn tas till branschstandarder och krypteringsmetoder som är förenliga med ISO. Dessa kan konfigureras eller installeras i systemet, t.ex. DESFire EV1 mellan kort och läsare, kryptering mellan kontroller och server, samt HTTPS för en säker anslutning mellan Advisor Management-programmets server och slutanvändarna. Dessutom stödjer programmet omfattande systemrestriktioner för att begränsa tillträdet till dem som är godkända.

Förutom utformningen av produkten kan installatören hjälpa slutanvändaren att fastställa hur de obligatoriska och valbara fälten i våra produkter skall hanteras. Installatören kan ge ytterligare information om vilka uppgifter och loggar slutanvändaren kan se och vilka säkerhetskopior som skapas under installationen, driftsättningen och produktunderhållet.

Identifiera
Se till att du vet var personuppgifterna förvaras.

Rätta sig efter
Hantera behandling, åtkomst till och radering av personuppgifter och rätta dig efter de registrerades begäran.

Skydda
Etablera säkra procedurer för att skydda personuppgifter.

Registrera
För register över dina procedurer.

Övervaka
Förebygg uppgiftsbrott och rapportera dem.

interlogix
United Technologies

Allmänna dataskydds förordningen

Interlogix Advisor Advanced-produkter och dataintegritet

Cybersäkerhet

Interlogix är förbundna av cybersäkerhet när det gäller dess Advisor Advanced-produkter och -tjänster vilket skyddar personuppgifterna. Interlogix arbetar kontinuerligt med att förbättra sina produkter med dessa mål i åtanke. För att stödja det har Interlogix moderföretag United Technologies Corporation (UTC) en utsedd produktsäkerhetsansvarig.

Advisor Advanced-produkterna låter slutanvändaren lagra personuppgifter i produkten. Den unika identifieringsinformationen (ID) och associerade åtkomsträttigheter finns tillgängliga via säkerhetskontrollpaneler för omedelbart beslutsfattande. Uppvisande av ett identifierande ID (pinkod eller kort) i en läsare matchas med det identifierande ID som finns registrerat i systemet och åtkomst till begärda funktioner eller dörrar/hissar beviljas eller avfärdas, beroende på säkerhetsreglerna som är konfigurerade av systeminstallatören vid slutanvändarens anläggning.

Användningen av personuppgifter är avgörande för en slutanvändares säkerhetskontrollsystem för att hantera rörelserna och tillträdet till begärda funktioner för anställda och besökare. De enda uppgiftsfält som är obligatoriska i Advisor Management är ett namn och – om det krävs – en identifiering (passerkort, PIN) som används för att koppla identifieringen av en person och ställa in behörigheten för var och när användaren kan få åtkomst till den begärda funktionen eller tillträdet.

Exempel på fält som konfigureras för att optimera säkerhetshanteringen i Advisor Management är: interna och externa nummer (ofta använda för att samla in interna HR-nummer eller interna ID-nummer); e-postadress; kön; foto; samt behörighetsnivåer. Dessa uppgifter kan tillhandahållas från en HR-databas genom ett säkert utbyte av uppgifter med regelbundna intervall. Åtkomsten till uppgiftsfälten och möjligheten att lägga till eller ändra baseras på slutanvändarnas beslut och kontrolleras av behörigheter som är konfigurerbara av slutanvändaren.

Säkerhetskontrollpanelerna lagrar uppgifter som händelser i händelsehistorikloggarna. Posterna i händelsehistorikloggarna innehåller en händelsebeskrivning som innefattar: tid och datum för när händelsen inträffade. Slutanvändaren kan också konfigurera loggarna att innehålla ytterligare information för att identifiera den involverade personen och platsen för händelsen. En persons namn kan även skickas till en larmcentral för att den som är involverad i en händelse ska identifieras och lämplig åtgärd vidtas. Vid intrångslarm är lagringen av händelserna och larmrapporteringen i linje med säkerhetsgodkännanden som t.ex. EN50131.

Assistera med dataintegritet

Advisor Management erbjuder slutanvändarens administratörer möjligheten att definiera tillstånd för att säkerställa att individer har åtkomsträttigheter till de funktioner och uppgifter i programmet som krävs för att de ska kunna utföra sina arbetsuppgifter, samt möjligheten att definiera vilken typ av åtkomst som är lämplig.

Advisors säkerhetskontrollpaneler är bara tillgängliga för privilegierade individer (installatörer etc.), vilka endast har åtkomst till funktions- och konfigurationsuppgifter baserat på det tillstånd som tilldelats dem av slutanvändaren.

Advisor Management kan användas för att konfigurera passer- och inbrottslarmskontroll samt larmövervakningsmiljöer, inklusive användarnas åtkomstbehörighet. Det tillhandahåller lösenordstvång och har möjlighet att stödja enkla inloggningar. Systemåtkomsten kan vara restriktiv och begränsad till en individs funktionella ansvar genom segmentering av maskinvara, plats, program och funktioner, samt läs- och redigeringsrättigheter.

Alla händelser som detekteras av en sensor skickas till säkerhetskontrollpanelen och överförs sedan till ett anslutet säkerhetshanteringsprogram, såsom Advisor Management eller till ett konfigurations- eller diagnostikverktyg för registrering och diagnos. Ytterligare personuppgifter kan även skickas till en larmövervakningscentral för att följa upp larm, beroende på den konfiguration som har ställts in och beslutats av slutanvändaren.

För varje händelse som är relaterad till tillträde genom dörrar eller intrångsområden, noteras händelsebeskrivningen och associerade uppgifter och sparas först i maskinvaran i enlighet med de säkerhetsreglerande kraven. När dessa händelser sedan ansluts till Advisor Management-programmet, överförs de också och lagras i det programmet. Detta möjliggör och tillåter en senare verifiering av händelserna av behörig personal – om och när det krävs – och så länge som det är nödvändigt. Lagrandet av uppgifterna fastställs av slutanvändaren: Advisor Advanced-produkter tillhandahåller ingen standardmässig raderingsperiod, men gör det möjligt för slutanvändaren att definiera en sådan.

Ref. 1543 – Advisor SE – 1031