Innovative Security

Origo och GDPR

Information och rekommendationer angående Origo och GDPR

Innehåll

Origo och GDPR

Information och rekommendationer angående Origo och GDPR

GDPR

Detta dokument beskriver hur Origo kan användas för att uppfylla de krav som GDPR ställer på hantering av personuppgifter. Upplägget i dokumentet är som följer:

Först presenteras GDPR:s grundläggande principer, vilka rättigheter de registrerade har enligt GDPR som vi bedömer är relevanta för Origo samt hur Origo uppfyller dessa.

Därefter ges rekommendationer om best practice för att GDPR-anpassa en Origo-installation.

Notera att om organisationen har en skräddarsydd Origoinstallation från före införandet av GDPR kan ytterligare funktioner behöva införas i samverkan med leverantör.

Observera att detta dokument endast är rådgivande. Kunden ansvarar själv för att anläggningen och hantering av personuppgifter sker i enlighet med GDPR.

Principer

GDPRs grundläggande principer för behandling av personuppgifter är som följer:

- Laglighet, korrekthet och öppenhet – All behandling av personuppgifter måste ha laglig grund och det måste vara tydligt för den registrerade vad som sker med deras personuppgifter.
- Ändamålsbegränsning – Behandling av personuppgifter får enbart vara av överenskommen typ. Personuppgifter får inte användas i andra syften utan överenskommelse med den registrerade.
- Uppgiftsminimering – Enbart nödvändiga personuppgifter skall ingå i behandlingar.
- Korrekthet – De personuppgifter som behandlas skall vara korrekta. Felaktiga personuppgifter skall rättas eller raderas.
- Lagringsminimering – Personuppgifter skall inte sparas längre än vad den lagliga grunden tillåter. Därefter skall personuppgifterna raderas.
- Integritet och konfidentialitet – Personuppgifter skall skyddas så de inte otillbörligen sprids, ändras eller raderas.

Registrerades rättigheter

GDPR definierar ett antal rättigheter som tillfaller de registrerade. De vi anser är relevanta för Origo är följande:

- Rätt till information (1) – I samband med insamling av personuppgifter har den registrerade rätt att få information om vilka uppgifter det gäller, hur de kommer att behandlas, vilken laglig grund som finns för behandlingen, mm.
- Rätt till information (2) – En registrerad person har rätt att begära ut registerutdrag om sina egna personuppgifter samt hur de behandlas.

- Rätt till rättelse – En registrerad person har rätt att begära rättning av personuppgifter som uppfattas som felaktiga.
- Rätt till radering – En registrerad person har rätt att få sina personuppgifter raderade under förutsättning att andra tyngre vägande lagliga skäl inte finns för organisationen att behålla dem.
- Rätt till begränsning av behandling – En registrerad person kan begära att deras personuppgifter ”fryses” och inte längre får behandlas. Detta gäller tex om den registrerade personen anser att personuppgifterna utsatts för olaglig behandling och att de måste bevaras som bevis.
- Rätt till dataportabilitet – Den registrerade har under vissa omständigheter rätt att begära ut sina personuppgifter i ett format som tillåter överföring till ett annat system eller tjänst.

Origo och GDPR

Laglighet, korrekthet och öppenhet

De behandlingar av personuppgifter som utförs i Origo måste täckas av laglig grund. Vanligtvis utgörs detta av avtal (tex anställningsavtal, kontrakt) eller liknande för användarkategorier anställda, konsulter och entreprenörer.

Normalt ligger all hantering av detta helt utanför Origo men om personer kan ange persondata direkt i Origo kan det vara lämpligt att komplettera inmatningsfunktionen med relevanta informationstexter. Om den lagliga grunden omfattar berättigat intresse behöver även de avvägningar som gjorts med avseende på den registrerades rättigheter beskrivas. Om den lagliga grunden är samtycke (tex besökare som anger information om sig själv) kan även en samtyckesfunktion införas direkt i Origo.

I de fall Origo integreras med externa tjänster som drivs av annan aktör måste organisationen verifiera att dessa aktörer uppfyller GDPR och att nödvändiga avtal finns på plats.

Ändamålsbegränsning

Personuppgifter som finns registrerade i Origo får inte användas för andra behandlingar än de som har laglig grund enligt ovan. Vid införande av nya funktioner i Origo är det därför lämpligt att verifiera att de täcks av existerande laglig grund och om detta inte är tydligt kan det finnas skäl att se över anställningsavtal mm. Hanteringen av detta ligger dock helt utanför produkten Origo.

Uppgiftsminimering

Origo hanterar enbart personuppgifter som överenskommits med kund kompletterat med vissa tekniska data som krävs för att systemet skall fungera. Personuppgifterna matas antingen in direkt i Origo eller hämtas från integrerade system. Vilka personuppgifter det rör sig om går att utläsa av Origos systemspecifikation. Finns ytterligare frågor (eller om exempel på faktiskt innehåll önskas) tillhandahålls även en rapport som hämtar ut alla personuppgifter om en utpekad person.

Önskas en genomgång för att eventuellt ytterligare minimera antalet personuppgifter kan detta genomföras i samverkan med leverantören. Identifieras personuppgiftstyper som ej är nödvändiga för den behandling som Origo utför i verksamheten kan dessa tas bort ur systemet i samverkan med leverantören.

Korrekthet

I Origo uppdateras normalt personuppgifter då ändringar sker i de integrerade systemen och detta gör att Origos uppgifter alltid skall vara aktuella. Då flera persondatakällor är integrerade skall det vara tydligt vilket system som är ägare till vilka uppgifter och det systemet skall korrigera informationen i de andra systemen. I de fall personuppgifter enbart anges genom inmatning i Origo skall användare med tillräcklig behörighet kunna redigera personuppgifterna. Hur detta är uppsatt varierar dock mellan olika installationer. Konsultera leverantören om ni önskar hjälp med att analysera hur er installation fungerar.

Lagringsminimering

Personuppgifter får inte lagras längre än vad medges enligt den lagliga grunden. Vid integration med tex HR-system raderas därför normalt personer och persondata i Origo (och dess undersystem) då motsvarande data raderas i HR-systemet. Då flera persondatakällor är integrerade skall det vara tydligt vilket system som är ägare till vilka uppgifter och det systemet skall initiera radering av motsvarande information i Origo och de andra systemen. I de fall personuppgifter enbart anges genom inmatning i Origo skall användare med tillräcklig behörighet kunna radera personuppgifterna. Hur detta är uppsatt varierar dock mellan olika installationer. Konsultera leverantören om ni önskar hjälp med att analysera hur er installation fungerar eller om ni vill ändra i existerande funktionalitet.

En annan viktig komponent i lagringsminimering är hanteringen av ärendehistorik och loggar. Både ärendehistorik och loggar betraktas som ”livedata” i Origo och är åtkomlig för användare. I aktuella versioner av Origo raderas automatiskt ärendehistorik äldre än maximalt 90 dagar. Hur länge loggposter sparas är konfigurerbart och ett tidsintervall som passar kunden måste anges i systemet.

Säkerhetskopiering hanteras utanför Origo men rekommendationen är att organisationen har strikta processer för hantering av säkerhetskopior av Origos databas. Säkerhetskopior bör tas regelbundet och måste sparas säkert. Säkerhetskopior får dock inte sparas längre än vad organisationen har rätt till enligt den lagliga grund som gäller för behandlingen av personuppgifterna. Det kan vara relevant för organisationen att utreda om berättigat intresse behöver användas för att motivera lagringstider utöver tex avtalslängd, väga dessa intressen mot de registrerades integritetskrav och dokumentera detta.

Integritet och konfidentialitet

I Origo sker alltid åtkomstkontroll innan en användare kan få tillgång till personuppgifter. Rekommenderat är att använda SSO (Single sign-on) i Origo för att garantera att organisationens policy för lösenordshantering efterlevs. Vilka personuppgifter som en användare kan se beror på användarens roll i Origo.

Origo bör alltid vara installerat på ett skyddat nätverk så interna integrationer (tex HR-system och passersystem) skyddas. Dessa kan skyddas ytterligare med tex kryptering i de fall produkternas API:er erbjuder detta. Eventuella externa integrationer (mot system utanför det skyddade nätverket) skall alltid skyddas med kryptering, VPN eller motsvarande om personuppgifter överförs.

Origos webbserver kan köras antingen på samma säkra nätverk som applikationsdelen och databasen eller på ett annat nätverk som tillåter webbapplikationen åtkomst till Origos applikationsdel och databas.

Oavsett var Origos webbserver är placerad bör enbart https-anslutningar tillåtas från webbläsare. Åtkomst till webbservern från internet bör inte tillåtas annat än via VPN eller motsvarande.

Rätt till information (1)

Den information som skall meddelas registrerade i samband med registrering hanteras normalt sett av HR eller motsvarande. Se *Laglighet, korrekthet och öppenhet* ovan för rekommendationer då personuppgiftsinmatning sker direkt i Origo.

Rätt till information (2)

Då en registrerad person begär ut information om sina personuppgifter från personuppgiftsansvarige kan den SQL-rapport som levereras tillsammans med Origo användas för att ta ut ett registerutdrag. Detta utdrag innehåller persondata (användarfält i Origo), en förteckning över tilldelade behörigheter samt ett utdrag ur loggen innehållande poster som berör användaren. Registerutdraget sparas i läsbart format.

Personer med inloggningsmöjlighet i Origo kan själv skaffa sig en god bild av vilka personuppgifter som visas i Origo genom att granska sina egna uppgifter på fliken *Mina personuppgifter* i Origo. Denna sida är inte lika komplett som registerutdraget men ger en mer översiktlig bild.

Rätt till rättelse

Om en registrerad person begär och beviljas rättelse kan rättelsen normalt sett ske på två sätt i Origo. Om rättelsen införs i ett integrerar överordnat system (tex HR) medför detta normalt att personuppgifterna automatiskt uppdateras även i Origo. I de fall personuppgifter anges direkt i Origo ska det finnas möjlighet för användare med tillräcklig behörighet att även redigera personuppgifter direkt i Origo. Hur detta är uppsatt varierar dock mellan olika installationer (i vissa fall kan det tex vara nödvändigt att göra rättelsen i passersystemet för att ändringen skall slå igenom). Konsultera leverantören om ni önskar hjälp med att analysera hur er installation fungerar.

Rätt till radering (rätten att bli glömd)

Om en registrerad person begär och beviljas radering kan raderingen normalt sett ske på två sätt i Origo. Om raderingen utförs i ett integrerat överordnat system (tex HR) medför detta normalt att personen raderas även i Origo. I andra fall skall det finnas möjlighet för användare med tillräcklig behörighet att radera personen direkt i Origo. Hur detta är uppsatt varierar dock mellan olika installationer (i vissa fall kan det tex vara nödvändigt att radera personen i passersystemet för att personen skall tas bort i Origo). Konsultera leverantören om ni önskar hjälp med att analysera hur er installation fungerar.

Rätt till begränsning av behandling

Om en registrerad person begär och beviljas begränsning av behandling och detta påverkar de personuppgifter som behandlas av Origo bör detta hanteras på följande sätt. Ett registerutdrag för personen tar ut med hjälp av den rapport som levereras tillsammans med Origo (se *Rätt till information (2)* ovan). En säkerhetskopia av Origos databas skapas av behörig tekniker för att säkerställa att en exakt bild av nuläget bevaras och därefter raderas personen i Origo. Raderingen sker för att säkerställa att berörda personuppgifter inte behandlas ytterligare i Origo t.ex. orsakat av förändringar i integrerade system. Notera att om ett annat system är ägare till personuppgifterna (tex ett HR-system) måste det systemet säkerställa att personen inte skickas ut till Origo igen. Konsultera leverantören om ni önskar hjälp med att analysera hur er installation fungerar.

Rätt till dataportabilitet

Om en registrerad person begär och beviljas dataportabilitet hanteras det enligt följande. Ett registerutdrag för personen tas ut med hjälp av den rapport som levereras tillsammans med Origo (se *Rätt till information (2)* ovan). Registerutdraget sparas i maskinläsbart format och kan lämnas ut till den registrerade. Om personens begäran om dataportabilitet även innebär en flytt från Origo till ett annat system bör personen även raderas (se *Rätt till radering* ovan)

Best practice för säkerhet i Origo

I denna sektion presenteras en rad olika åtgärder och rekommendationer som kan användas som en checklista för att utvärdera och säkerställa att organisationens Origoinstallation uppfyller GDPR från ett åtkomst- och säkerhetsperspektiv. Notera att GDPR inte pekar på några specifika säkerhetslösningar, lagstiftningen är avsedd att vara helt teknikneutral, utan hänvisar till branchstandarder, best practice och liknande. Att säkra ett system är därför att betrakta som ett löpande arbete och nya säkerhetslösningar bör utredas och värderas när de blir tillgängliga.

Servrar

- Se till att servrarna är fysiskt skyddade – t.ex. låst serverrum eller liknande.
- Skydda åtkomst till servrarna. Enbart nödvändiga konton bör kunna logga in. Se till att dessa konton har lämplig lösenordspolicy etc.
- Exponera inte servrarna mot publika nät (Internet eller andra osäkra nät).
- Säkra extern åtkomst. All onödig åtkomst bör förhindras och krypteras om nödvändig, t.ex. VPN-anslutningar eller motsvarande.
- Kör inga onödiga program eller tjänster på servrarna för att minimera exponeringsytan.
- Håll operativsystemet uppdaterat med de senaste uppdateringarna från Microsoft.

Databas

- Inför rutiner för hur regelbundna backuper hanteras, lagras och tas bort. Backuperna måste lagras på ett säkert sätt och bör tas bort efter en överenskommen tid som inte överstiger vad den lagliga grunden för behandlingen medger.
- Kryptera backuper. Mer information: https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/backup-encryption. Notera att inbyggt krypteringsstöd saknas i SQL Express varför uppgradering eller separat krypteringslösning rekommenderas.

- Skydda åtkomst till SQL Server. Se till att enbart nödvändiga konton (t.ex. Origo) kan logga in i SQL Server.
- Kryptera externa anslutningar till SQL Server om nödvändigt. Mer information: https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine. Om SQL Server och Origo kör på samma server behövs inte detta.
- Tillåt extern åtkomst till SQL Server endast om det är nödvändigt. Är extern åtkomst nödvändig (t.ex. Origo och SQL Server kör på olika servrar) bör endast detta tillåtas i brandvägg. Mer information: https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access.
- Håll SQL Server uppdaterad med de senaste uppdateringarna från Microsoft.
- Mer information om säkerhet i SQL Server: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server.

Nätverk

- Origo, SQL Server och anslutna interna system (såsom passersystem och andra säkerhetssystem) bör köra på sitt egna separerade säkerhetsnätverk. Separationen kan vara fysisk (separat infrastruktur) eller virtuell (VLAN eller krypterad tunnling etc.).
- Åtkomst till säkerhetsnätet bör vara begränsat. Lämplig brandvägg bör användas mellan säkerhetsnät och andra nät.
- Enbart Origos webbsidor bör exponeras utanför säkerhetsnätet (se Webbserver).

Webbserver (IIS)

- Webbserver bör ej exponeras direkt mot Internet.
- Webbservern bör konfigureras för enbart HTTPS åtkomst. Mer information: https://docs.microsoft.com/sv-se/iis/manage/configuring-security/how-to-set-up-ssl-on-iis och https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts. För att genomföra detta behövs ett utfärdat certifikat från en Certificate Authority (CA) eller ett självsignerat certifikat. Om ett självsignerat certifikat används måste alla webbläsare som ska komma åt Origo konfigureras för att lita på detta certifikat.
- Håll IIS uppdaterad med de senaste uppdateringarna från Microsoft.
- Mer information om säkerhet i IIS: https://docs.microsoft.com/en-us/iis/manage/configuring-security/index.