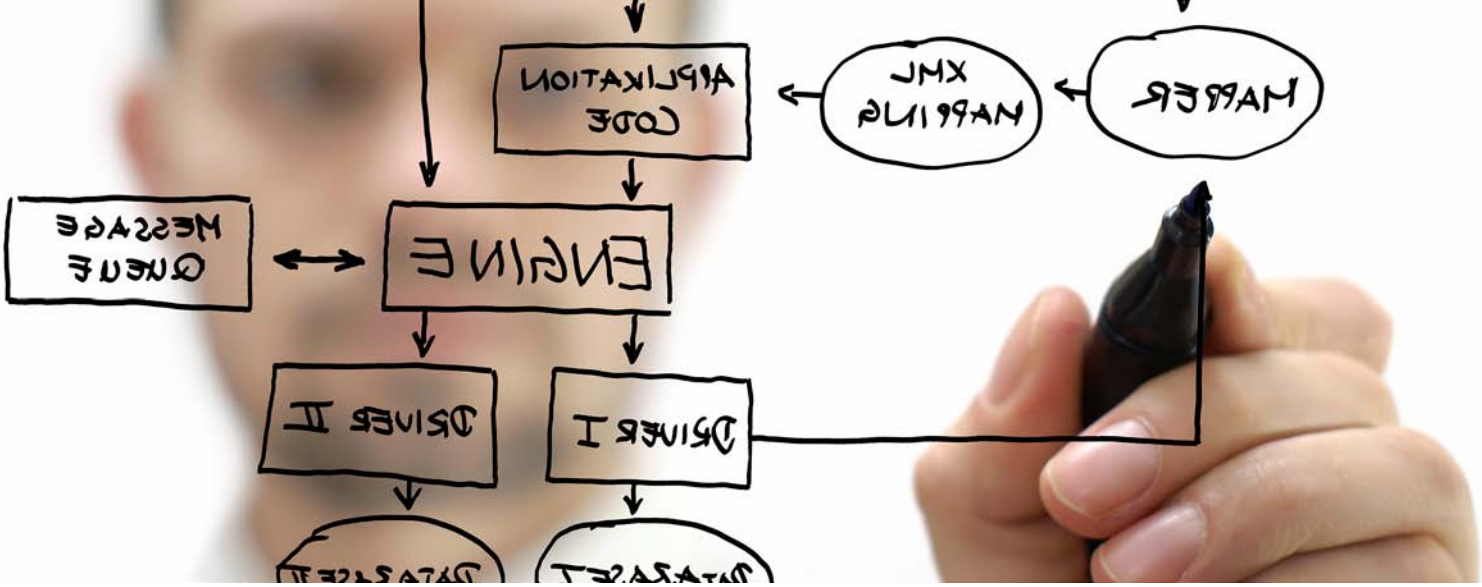

Inbyggd integritet

Privacy by design – Inbyggda mekanismer i IT-system för skydd av den personliga integriteten

Utveckling av tekniska system är ofta komplicerade processer där man måste ta hänsyn till många typer av krav. Inte minst gäller det skyddet av den personliga integriteten. För att undvika fallgropar som blir dyra att åtgärda i efterhand och som gör det svårt att följa lagen är det viktigt att ta hänsyn till integritetsaspekterna i ett tidigt skede i processen.

Några grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha den kvar längre än man behöver och inte använda den till något annat än vad man samlade in den för. Att informera om hur uppgifterna ska behandlas, att begära samtycke och att tillåta insyn i den vidare hanteringen är också led i integritetsskyddet.

Begreppet privacy by design, eller inbyggd integritet som det kallas på svenska, går ut på att låta dessa integritetsfrågor påverka systemets hela livscykel – från förstudie och kravställning via design och utveckling till användning och avveckling. Det här informationsbladet ger en vägledning till hur ett sådant arbete kan utformas.

Inbyggd integritet kan tillämpas på många områden, som till exempel när man tar fram nya standarder och inför ny lagstiftning, men denna vägledning riktar sig främst till de som är

- beställare/kravställare – de som i lagens mening är ansvariga för en behandling av personuppgifter och står i begrepp att införa ett arbetssätt eller ett IT-system för att stödja detta,
- leverantörer av sådana produkter och tjänster,
- på annat sätt involverade i framtagningen av IT-stöd för behandling av person-uppgifter.

Januari 2012

Datainspektionen

Personuppgiftsansvar

Det är alltid den som bestämmer över hanteringen av personuppgifter som har ansvar för att personuppgiftslagen följs. Ansvaret innebär att se till att det IT-stöd som används inte medför integritetsrisker och därför måste tydliga krav formuleras till leverantören av IT-stödet. Även om en leverantör av IT-produkter normalt inte är ansvarig för de eventuella integritetsproblem som uppstår i samband med användningen av produkten är det viktigt att den har de nödvändiga funktionerna för integritetsskydd.

Även om det istället för en programvara eller hårdvara är en tjänst som levereras (outsourcing eller molntjänster) så är beställaren ansvarig och måste se till att leverantören uppfyller kraven på säkerhet och integritetsskydd.

Checklista för IT-projekt

För att integritetssäkra projektet bör man arbeta på ett strukturerat sätt, ungefär som man förutsätts arbeta när det gäller IT-säkerhet eller kvalitetssäkring. En riskanalys behöver genomföras och man behöver kartlägga konsekvenserna för integriteten för de personer som registreras.

Minimera mängden personuppgifter

IT-system ska helst vara utformade så att så få personuppgifter som möjligt samlas in och hanteras. Fastställ vilka personuppgifter som verkligen krävs för att tillgodose ändamålet, snarare än att se vad som kan finnas tillgängligt. Det gäller såväl vid kravställning och formgivning av ett system som när man samlar in uppgifterna. Ändamålet för behandlingen (det vill säga insamling och övrig hantering) måste bestämmas i förväg och kraven på systemet måste utgå från ändamålet. Olika sätt att att minska integritetsriskerna kan vara att

- begränsa sig till uppgifter som endast indirekt pekar ut en individ,
- begränsa sig till uppgifter som är mindre känsliga,
- ersätta namn, till exempel med psedonymer,
- inte rutinmässigt ha med personnummer som fält i databaser.

Om till exempel ett ärendehanteringssystem kan göra mer med personuppgifter än vad som är tillåtet enligt ändamålet så är det viktigt att det är möjligt att begränsa och spärra de funktionerna för handläggare innan systemet tas i drift.

Begränsa åtkomsten till uppgifterna

Möjligheten att arbeta med och ta del av personuppgifter ska begränsas till de som behöver det för att kunna utföra sina arbetsuppgifter och sättet att arbeta måste vara utformat efter den principen. Ibland sker det naturligt eftersom olika avdelningar och projektgrupper ägnar sig åt sina respektive arbetsuppgifter. Men när uppgifterna samlas i samma IT-system kan det bli lättare att kunna ta del av sådant som inte är relaterat till ens arbetsuppgifter. IT-system bör därför vara utformade med behörighetsstyrning som kan anpassas efter organisationens arbetssätt.

Här bör man först kritiskt granska arbetssättet för att förvissa sig om att det inte i sin tur är framtvingat av IT-system med otillräcklig behörighetsstyrning eller andra brister i säkerhet och integritet.

Ett idealiskt system för kontroll av behörigheter ska kunna se till att identifierade användare kommer åt rätt information enkelt men hindras att komma åt ”fel” information, det vill säga personuppgifter som inte behövs för att lösa ens arbetsuppgift. Segmentering av information kan till exempel vara baserad på medlemskap i grupper eller innehav av roller. Användaren kan ha olika roller i systemet utan att för den skull kunna kombinera den behörighet som hör till skilda roller vid ett och samma tillfälle. Att kräva någon form av dokumenterad motivering (där till exempel ärendenummer anges) för en avvikande sökning i ett register kan höja medvetandet och underlätta uppföljning. Här är fler exempel på hur man kan styra åtkomsten:

Att låta åtkomsten styras och begränsas av arbetsflödet (till exempel ett försäkringsärende eller handläggning av ett ärende hos myndigheter) kan minska integritetsriskerna jämfört med att låta alla register och sökmöjligheter vara helt öppna för samtliga användare hela tiden.

Utöver behörighetssystem kan även kryptering av lagrad information vara ett sätt att begränsa åtkomsten för till exempel systemadministrativ personal.

Skydda uppgifterna

IT-system som hanterar personuppgifter ska redan från början ha stöd för säkerhetsfunktioner. Särskilt tjänster som exponeras mot Internet måste utvecklas med säkerhet som grundfilosofi och så långt det är möjligt vara byggda för att kunna motstå förekommande typer av angrepp. Att lägga till säkerhetsfunktioner, särskilt oplanerade sådana, i efterhand kan bli dyrt och orsaka driftstörningar. Ju känsligare uppgifter, desto högre säkerhetsnivå krävs. Utöver behörighetsstyrning bör det exempelvis finnas :

- Funktioner för autentisering, minst lösenord, med tillhörande rutiner och funktioner för säker hantering och möjlighet att ansluta systemet till extern kontohantering.
- Möjlighet att använda kryptering
  - vid kommunikation över Internet,
  - i databaser,
  - på mobila enheter.
- Rutiner och tydlig information om säkerhet till systemets användare.
- En logg som kan användas till att utreda felaktig åtkomst till personuppgifter.
- Stöd för säkerhetskopiering.
- Säker utplåning, det vill säga skydd mot att data läcker ut efter att hela eller delar av systemet tagits ur drift och skrotats. Bör inkludera metoder för radering och förstöring av lagringsmedia. Risken för läckage minskar om till exempel hårddiskar och usb-minnen är krypterade från början.

Tänk också på att loggar och säkerhetskopior är fristående delar och i sig kan innebära en integritetsrisk, inbyggd integritet bör tillämpas även på dessa. Loggar innehåller personuppgifter om de som arbetar i systemet och måste därför hanteras på ett integritetssäkert sätt. Säkerhetskopior som sparas länge kan komma att innehålla personuppgifter som borde raderats tidigare. Automatiska metoder för gallring kan behövas.

Låt systemet styra användaren rätt

Användarvänlighet är viktigt för att integritetssäkra ett system och det måste byggas in från början. Exempel på lämpliga egenskaper:

- "Integritet som standard" – att systemets arbetsflöde automatiskt styr användaren mot ett integritetssäkert arbetssätt och att grundinställningarna är satta så att inte mer information än nödvändigt samlas in eller visas.
- När uppgifterna inte längre behövs ska de tas bort. Funktioner för att gallra (radera) uppgifter automatiskt förenklar.
- Myndigheter kan behöva användarvänliga funktioner för att effektivt kunna avskilja data för arkivering.
- Transparens – att ge de registrerade insyn:
  - Med funktioner för att på begäran från enskilda individer enkelt kunna lämna lagstadgade så kallade registerutdrag om deras uppgifter förekommer i systemet.
  - Med ett gränssnitt för att låta den registrerade själv få insyn.
  - Genom att i en logg enkelt kunna visa till vilka andra organisationer information har lämnats ut till.
- När man ska göra utdrag för rapporter eller statistik ska man kunna välja bort den information som inte är relevant. Anonymisering kan ofta användas.
- Stöd för samtycke och återtagande av samtycke – I många fall krävs samtycke för att registrera viss information eller för att vissa funktioner ska få användas.
- Funktioner i användargränssnittet som begränsar möjligheten att skriva in sådant som inte får skrivas in. Ett skolsystem för elevomdömen bör till exempel utformas så att antalet fritextfält minskas. Därmed minskar risken att otillåtna och kränkande omdömen matas in.
- Tydlig information till de som lämnar uppgifter om sig själva om hur uppgifterna kommer att behandlas. En sådan information kan sammanfattas i en integritets-policy.

Sammanfattning

Genom att beakta integritetsfrågorna från början till slut, under systemets hela livscykel, kan man dramatiskt öka förmågan att följa gällande lagar och höja säkerheten. Samtidigt minskar man risken för onödiga kostnader och tidsödande arbetsinsatser som uppstår när försöker lindra integritetsproblem i efterhand.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

Datainspektionen