2019-03-12
Olof Junesjö

Informationssäkerhetspolicy (inklusive dataskydd)

Inledning

Hantering av information i allmänhet och personuppgifter i synnerhet är av största vikt för att vi ska kunna bedriva ett ändamålsenligt och effektivt projektarbete. Det är också en trovärdighetsfråga i relation till våra kunder. Denna policy beskriver hur Governo hanterar information på en övergripande nivå. Detta gäller såväl hanteringen av personuppgifter som andra typer av information med särskild fokus på information av känslig karaktär. Vi har i arbetet säkerställt att arbetssätten beskrivna i denna policy är i linje med GDPR.

I bilaga återfinns en kartläggning som genomförts av hur personuppgifter hanteras mer i detalj på Governo.

Denna policy ersätter Governos Dataskyddspolicy (180129) samt Governos Ledningssystem för informationssäkerhetsarbete.

Om dokumentet

Denna policy syftar till att beskriva hur Governo upprätthåller informationssäkerheten, både med avseende på personuppgifter och andra typer av information. Detta dokument innehåller riktlinjer och rutiner för hantering av information inklusive definitioner och ansvarsområden. Dokumentet riktar sig till samtliga anställda på Governo samt de samarbetspartners med tillgång till Governos server och andra digitala och analoga databaser.

Då den största mängden av Governos information finns lagrad digitalt på extern server via en molnlösning ligger tyngden i detta dokument främst vid digital informationshantering och arbetssätt kopplat till detta, men ska även beaktas vid hantering av annan typ av information som kan vara i analog form.

Policyn omfattar samtlig information som hanteras på Governo. Detta innefattar såväl information som innehåller personuppgifters som den som inte gör det. Vad gäller

definitionen av personuppgifter hänvisas till EU:s förordning.[1] Förenklat kan sägas att all sådan information som direkt eller indirekt kan hänvisas till en fysisk person räknas som personuppgifter. Policyn och dess bilaga omfattar både dataskydd (dvs. hantering av anställdas personuppgifter) som integritet (dvs. hantering av kunders personuppgifter).

Organisation för arbetet med informationssäkerhet

Governos högsta ledning i form av bolagets VD och ledningsgrupp arbetar aktivt med att säkerställa att informationssäkerheten upprätthålls.

Ytterst är Governos VD ansvarig för informationssäkerheten på bolaget samt för att IT-ansvarig och övriga berörda har de förutsättningar som krävs för att följa de riktlinjer och rutiner som finns avseende informationssäkerheten. På Governo innehar VD rollen såväl som informationssäkerhetsansvarig som personuppgiftsansvarig.

Rollen informationssäkerhetsansvarig har till uppgift att löpande uppdatera och följa upp detta dokument, att hantera eller ta vidare avvikelser och andra hot i förhållande till informationssäkerheten samt att hålla sig à jour med aktuell lagstiftning. Informationssäkerhetsansvarig är även ansvarig för kommunikation med systemleverantörer i frågan och säkerställer att leverantörsavtalen följer företagets krav på informationssäkerhet.

Informationssäkerhetsansvarig ansvarar för att en genomgång av policyn sker i samband med introduktion av nyanställda. Därefter ansvarar alla anställda för att hålla sig uppdaterade om de riktlinjer och rutiner som redovisas i detta dokument. Som individ är man också ansvarig för att i sina uppdrag och kundkontakter tillse att personuppgifter hanteras enligt denna policy (inkl. bilaga).

Samverkan med andra konsulter och externa leverantörer ska regleras genom avtal och alla ska ha kännedom om Governos riktlinjer och rutiner kring informationssäkerhet samt följa dessa.

Informationssäkerhet på Governo – definition och mål

Informationssäkerhet på Governo definieras som ett tillstånd där information har ett skydd avseenDatde konfidentialitet, spårbarhet, tillgänglighet och riktighet.

Målen för Governos informationssäkerhetsarbete delas in efter dessa fyra områden:

- **Konfidentialitet** – Informationen är skyddad från obehörig åtkomst och spridning. Individer tar som utgångspunkt endast del av för arbetet relevant information och sprider inte information till obehöriga.
- **Spårbarhet** – Informationens historik i termer av källor och förändringsinsatser framgår i den utsträckning det inte strider mot annan lagstiftning eller mot principerna om konfidentialitet.

[1]

- **Tillgänglighet** – Informationen kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid.
- **Riktighet** – Den information som handhas är tillförlitlig och korrekt. Informationen ska skyddas från medveten och omedveten manipulation som skulle kunna korrumpera dess tillförlitlighet.

Konfidentialitet

Konfidentialitet och skydd av personuppgifter säkerställs dels genom tekniska lösningar i termer av behörighetsnivåer för information som lagras på servern där behörighet styr vem som har den tekniska tillgången till informationen, och dels genom arbets- och förhållningssätt som följer principerna i detta dokument och där medarbetare eller andra individer med tillgång till servern och andra databaser endast tar del av information med relevans för deras arbetsuppgifter. För information med högre säkerhetsklassificeringar, delvis nivå 2 och samtlig information med säkerhetsnivå 1 skyddas av behörighetsnivåer i de fall de lagras på Governos server.

Det finns tydliga rutiner för att reglera behörigheter för tillgång till information, vilket kan variera på projekt- och delprojektsnivå.

Användare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks, samt tillse att utrustningen inte utsätts för obehörigt användande. Pappersdokument, övriga lagringsmedia samt anteckningar på t.ex. whiteboard i arbetsrum måste hanteras i enlighet med hur informationen har klassats.

Samtliga lokala hårddiskar i medarbetarnas datorer är krypterade, vilket försvårar eventuella intrång.

Spårbarhet

Spårbarhet säkerställs dels genom versionshantering, dels genom tekniska lösningar kopplade till Governos upphandlade molnlösning.

Tillgänglighet

Tillgången till relevant information upprätthålls även den genom Governos upphandlade molnlösning och de SLA:er som etablerats i relation till leverantören.

Riktighet

Informationens riktighet säkerställs genom handhavanderutiner där konsulterna i teamen stöttar varandra. Gällande skydd från medveten och omedveten manipulation upprätthålls det genom Governos upphandlade molnlösning.

Processer inom informationssäkerhetsområdet

Processerna inom informationssäkerhetsområdet kan delas in i xx övergripande typer:

- Informationsklassning och -hantering
- Uppföljning av informationssäkerhetsarbetet
- Avvikelse- och undantagshantering
- Återkommande personuppgiftsanalys
- Leverantörshantering

Informationsklassning och -hantering

För att avgöra hur information i specifika projekt ska hanteras behöver en informationsklassning genomföras. En övergripande bedömning utifrån informationssäkerhetsperspektivet sker i projektstart i samrådan med kunden. Klassningen avgör hur informationen hanteras under och efter projektet. Projektledare ansvarar för att klassningen revideras i det det fall det är aktuellt. På Governo hanteras en stor mängd information för kunders räkning. Denna information ska alltid klassas och hanteras i linje med de krav som ställs från respektive kund.

I framtagandet av informationsklasserna har vi utgått ifrån Klassas SKLs KLASSA-verktyg med anpassning till Governos verksamhet.

Säkerhetsnivå 3

Information där spridning, avsaknad av spårbarhet, avbrott i åtkomst och oriktig information enbart har ringa eller ingen effekt för egen eller annan organisations verksamhet eller för enskild person. I allmänhet offentlig information samt icke känsliga personuppgifter.

Projekt som bedöms innehålla information på säkerhetsnivå 3 hanteras digitalt på Governos molnlösning utan restriktioner för användarna.

Säkerhetsnivå 2

Sådan information som om den kommer i orätta händer kan medföra skada för företaget, kund eller enskild person. Information endast avsedd för egen personal och/eller utpekade personer hos kund. Känsliga personuppgifter enligt GDPR.

Projekt som bedöms innehålla information på säkerhetsnivå 2 hanteras digitalt på Governos molnlösning utan restriktioner för användarna. I vissa fall kan delar av projekten behörighetsklassas.

Säkerhetsnivå 1

Sådan information som om den kommer i orätta händer kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person.

Sådan information som påverkas av lagkrav anförbara till ett visst verksamhetsområde. T.ex. information från kunder med särskilda krav om sekretess.

Oriktig information kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person.

Mycket strikt kontroll av i princip all data.

Projekt som bedöms innehålla information på säkerhetsnivå 1 hanteras digitalt på Governos molnlösning med insyn enbart för de konsulter som arbetar i uppdraget. Konsulterna skriver på sekretessavtal. I projekt klassade på säkerhetsnivå 1 ska dokument inte skickas via e-post externt (där e-posten inte är krypterad) utan enbart laddas ner direkt från molnlösningen. I de fall lagring sker i kundens miljö är kunden ansvarig för informationssäkerheten.

Uppföljning av informationssäkerhetsarbetet

Informationssäkerhetsansvarig följer minst årligen upp det interna informationssäkerhetsarbetet, rutinerna i detta dokument samt relevanta leverantörsavtal. Informationssäkerhetsansvarig stämmer löpande av informationssäkerhetsarbetet med företagets ledningsgrupp och IT-ansvarig.

Avvikelse- och undantagshantering

Alla anställda har ansvar för att rapportera avvikelser, undantag eller andra faktorer som kan påverka informationssäkerheten till informationssäkerhetsansvarig eller annan relevant person.

Vid informationssäkerhetsincidenter är det informationssäkerhetsansvarig som i första hand hanterar dessa samt tillser att adekvata åtgärder vidtas och följs upp för att förhindra upprepning av incidenter.

Beslut med bäring på informationssäkerheten fattas av företagets VD. Informationssäkerhetsansvarig har mandat att vid akuta situationer fatta beslut för att förhindra eller avstyra allvarliga incidenter med direkt påverkan på informationssäkerheten.

Återkommande personuppgiftsanalys

För att upprätthålla ett gott dataskydd har vi tagit fram en process som innehåller följande moment:

- Kartlägga – identifiering av alla personuppgifter som vi hanterar.
- Definiera – framtagande av definitioner på samtliga personuppgifter för de olika målgrupperna i form av vilken information som samlas in, hur detta sker, hur samtycke inhämtas, hur informationen lagras, vilka som har åtkomst och när informationen raderas.
- Utbilda – utbildning av samtliga medarbetare i hur Governo hanterar personuppgifter enligt denna policyn.
- Hantera – löpande hantering av personuppgifter för de som samlar in och har åtkomst till informationen.

Leverantörshantering

Alla leverantörsrelationer regleras i avtal där informationssäkerhetens fyra områden beaktas och samtycke till personuppgiftslagring medges. I detta ingår bl.a.:

- att en leverantör ska kunna säkerställa att Governo och bolagets kunders krav på konfidentialitet och sekretess kan upprätthållas samt redovisa hur detta säkerställs,
- att det med tydlighet ska framgå vilken rätt en leverantör har att ändra, manipulera eller på andra sätt hantera innehållet i information som leverantören har tillgång till, t.ex. genom att det lagras på en extern server samt under vilka omständigheter detta i sådana fall får göras,
- vilka servicenivåer som leverantören förbinder sig att upprätthålla samt hur de säkerställer att detta följs.

För att säkerställa godtagbara nivåer utifrån ett informationssäkerhetsperspektiv granskas alla leverantörsavtal av bolagets informationssäkerhetsansvarig innan avtal ingås.

Governo har fattat beslut om outsourcing av sin it-miljö vilket bl.a. innebär informationshantering via molnlagring av tredje part. För närvarande hanteras tjänsten av Quality of service där relationen styrs via upprättat avtal. Detta avtal följer Governos informationssäkerhetspolicy.