Dataskydd hos Qliro – säkerhetsåtgärder

På Qliro är våra kunders och användares säkerhet vår högsta prioritet, och vi är fast beslutna att se till att dina personuppgifter är skyddade och säkra.

Hur skyddar vi din information

Qliro har implementerat ett ramverk för dataskydd som består av både organisatoriska och tekniska kontroller, processer och rutiner för att säkerställa att dina personuppgifter hanteras på ett säkert sätt.

Dataskyddsarbete leds av Qliros CISO (Informationssäkerhetschef) och är en del av Qliros ledningssystem för informationssäkerhet som är utformat i enlighet med god säkerhetspraxis samt säkerhetskraven i ISO 27001/27002.

Qliros policy, kontroller och rutiner baseras på riskbedömningar och kompletteras med legala och regulatoriska krav såsom GDPR (EUs Dataskyddsförordning) och omfattar Qliros hela organisation samt våra leverantörer där så är tillämpligt.

Nedan följer en kort översikt över några av de organisatoriska och tekniska säkerhetsåtgärder som implementerats på Qliro.

Organisatoriska säkerhetsåtgärder:

- **Policyer och rutiner för informationssäkerhet och dataskydd,** såsom konsekvensbedömningar avseende dataskydd, inbyggt integritetsskydd, regler för användning av information och utrustning samt åtkomsthantering, har implementerats för att trygga en säkerhetsstandard.

- Vårt **Informationssäkerhetsutbildningsprogram** är obligatoriskt för all personal och inkluderar en mängd olika utbildningsverktyg, utbildningsformer och utbildningsområden. Qliros utbildningsprogrammet planeras på årsbasis och ses kontinuerligt över för att hålla det adekvat och uppdaterat.

- **Rutiner för leverantörsriskhantering** är implementerade för att säkerställa att adekvata säkerhetsåtgärder finns på plats hos våra leverantörer, personuppgiftsbiträden och partners i hela leveranskedjan och inkluderar både

proaktiva och reaktiva kontroller så som due diligence innan avtal, tydliga säkerhetskrav i avtalen samt årliga granskningar av våra leverantörer.

- Våra **rutiner för hantering av säkerhetsincidenter** utvärderas och förbättras kontinuerligt för att säkerställa Qliros förmåga att upptäcka och reagera på säkerhetsincidenter samt säkerställa kontinuiteten i vår verksamhet.

- **Granskningar, revisioner och uppföljningsaktiviteter** genomförs regelbundet både inom respektive affärsfunktion men även av vår risk- och regelefterlevnadsavdelning samt genom internrevisionsfunktionen och av externa oberoende revisionsbyråer.

Tekniska säkerhetsåtgärder:

- **Fysiska säkerhetsåtgärder** har implementerats för att säkerställa att vårt kontor, vår utrustning och våra anläggningar som är ger tillgång till vår IT-miljö är säkra, övervakade och skyddade från obehörig åtkomst och externa miljöhot.

- **Identitets- och åtkomstkontroller** finns på plats för att säkerställa lämplig åtkomsttilldelning (need-to-know), säker autentisering och auktorisering samt spårbarhet och kontroll i samband med åtkomst och användning av information och data.

- **Tekniska verktyg för att** skydda vår information och utrustning från cyberrelaterade hot och attacker, t.ex. spear phishing, skadlig kod eller externa attacker, är implementerade, övervakade och förbättras ständigt för att säkerställa en hög motståndskraft mot cyberhot

- **Åtgärder för att förhindra dataförlust,** t.ex. säkerhetskopior, kryptering (både vid lagring och under överföring) och loggning har implementerats för att säkerställa att information lagras säkert, tillgänglig över tid och på ett kontrollerat sätt.

- **Detekterings- och övervakningsåtgärder implementeras** på flera nivåer inom vår IT-miljö och upprätthåller både proaktiva och reaktiva förmågor och motåtgärder för att säkra vår data.