Personuppgiftspolicy

Syfte

MTD arbetar strukturerat för att behandla personuppgifter på ett korrekt och lagligt sätt. I den här policyn beskrivs övergripande rutiner för hanteringen av personuppgifter. ”Vi” avser i detta dokument genomgående, bolaget MTD eller dess medarbetare.

Mål

Målet med denna policy är att personuppgifter behandlas på ett lagligt och ansvarsfullt sätt inom MTD.

Roller och ansvar

CIO/Dataskyddsombudet har ett övergripande ansvar att driva och övervaka de frågor som behandlas i denna policy. Samtliga chefer är ansvariga för den egna organisationens efterlevnad av policyn.

Hålla och uppdatera register: CIO
IT-säkerhet och incidenthantering: CIO
Utbildning: CIO
Internrevision: CIO

Principer för personuppgiftsbehandling

Vi ska vara ansvarsfulla i vår hantering av personuppgifter, oavsett om det gäller medarbetare, kunder, leverantörer eller andra samarbetspartners. Frågor som på olika sätt berör behandling av personuppgifter finns i alla delar av vår verksamhet och vi uppmuntrar därför till att i samtliga sammanhang beakta våra regler kring personuppgiftsbehandling.

Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Vi ska vara transparanta om vilka uppgifter vi hanterar och se till att de personer som på olika sätt finns registrerade hos MTD kan göra sina rättigheter gällande på ett effektivt sätt.

Insamling av personuppgifter får endast ske för särskilda, uttryckligt angivna, och berättigade ändamål och vi ska bara samla in uppgifter som behövs för detta ändamål. Vi arbetar aktivt med att begränsa lagringen genom att gallra i enlighet med vår gallringspolicy och när det är lämpligt genom automatisk gallring. Vi ska med rimliga åtgärder se till att uppgifterna är korrekta.

För att kunna säkerställa och visa att vi lever upp till lagstiftningens krav ska vi samla all dokumentation avseende vårt dataskyddsarbete på följande ställen: huvudsakligen i vårt ledningssystem på SharePoint samt, för de delar som avser register och avtal, i verktyget Qnister GDPR.

Upphandling av IT-tjänster

När vi upphandlar IT-tjänster, såsom programvara eller drift och support, ska det först genomföras en risk-och sårbarhetsanalys och utefter utfallet välja lösning eller leverantör.

Vid anlitande av personuppgiftsbiträden ska vi endast anlita den som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i lagen och säkerställer att den registrerades rättigheter skyddas. De överväganden som görs, inklusive dokumentation av säkerhetsnivå etc., ska dokumenteras. Vidare ska det tecknas ett personuppgiftsbiträdesavtal.

Vi undviker om möjligt överföring av personuppgifter till tredje land men när det bedöms lämpligt eller nödvändigt får detta endast ske efter att tillräckliga säkerhetsåtgärder har vidtagits och dokumenterats.

IT-Säkerhet

Riskbedömning

Vi ska fortlöpande göra en riskbedömning av den behandling av personuppgifter som vi genomför. Vi ska vidta tekniska och organisatoriska åtgärder för att uppnå en säkerhetsnivå som är lämplig i förhållande till risken. Riskanalys och beslut om åtgärder ska dokumenteras.

Behörigheter

Det ska finnas skriftliga behörighetsinstruktioner för samtliga IT-system som innehåller personuppgifter. Grundprincipen är att behörigheter ska tilldelas så att endast de personer som behöver tillgång till personuppgifterna har åtkomst. Beroende på uppgifternas känslighet kan behörigheterna vara snävare eller vidare.

Incidenthantering

Alla säkerhetsincidenter ska dokumenteras i en incidenthanteringslogg med uppgift om omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Med säkerhetsincident avses en händelse som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

När lagen så föreskriver ska incidenter även rapporteras till Datainspektionen respektive den registrerade.

IT-Policy och IT-Säkerhetspolicy

MTD har antagit en IT-policy och en IT-säkerhetspolicy där våra medarbetares förhållningssätt till IT-miljön regleras mer detaljerat.

Register över behandlingar

MTD ska föra ett register över behandlingar av personuppgifter i verktyget Qnister GDPR. Respektive systemägare är ansvarig för registret. CIO och Dataskyddsombudet tillser att hålla registret uppdaterat löpande.

Konsekvensbedömning

Om en behandling av personuppgifter, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska vi enligt Dataskyddsförordningen före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter: Konsekvensbedömning eller DPIA (Data Protection Impact Assessment).

Även när vi inte når upp till kravet för Konsekvensbedömning ska vi, när det är lämpligt, genomföra en förenklad riskanalys. Analysen blir ett underlag för valet av tekniska och organisatoriska säkerhetsåtgärder.

Inbyggt dataskydd och dataskydd som standard

Vi ska proaktivt utvärdera möjligheterna att genomföra tekniska åtgärder, såsom pseudonymisering och uppgiftsminimering för att effektivt leva upp till kraven i GDPR och skydda den registrerades rättigheter. Vi ska även genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

Utbildning

Medarbetare ska få relevant information och utbildning om behandling av personuppgifter. Vid behov ges fördjupad eller riktad utbildning till dem som hanterar känsliga personuppgifter. Deltagandet i utbildningar ska dokumenteras.

Uppföljning och intern revision

Efterlevnaden av denna policy ska kontrolleras med stickprov och intern revision minst en gång per år. Vi ska löpande utvärdera om vårt dataskyddsarbete lever upp till lagstiftningens krav och genomföra förändringar när det är påkallat.