Tekniska och organisatoriska skyddsåtgärder

Enligt artikel 32 i dataskyddsförordningen ansvarar den som behandlar personuppgifter för att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda dessa. Vid bedömningen ska beaktas den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Särskild hänsyn ska tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller för obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

För att skydda informationen behöver därför åtgärder vidtas avseende informationssäkerhet som säkerhetsställer riktighet, konfidentialitet och tillgänglighet. Åtgärderna är organisatoriska, tekniska samt fysiska.

Organisatoriska säkerhetsåtgärder

Organisatoriska säkerhetsåtgärder handlar om det administrativa säkerhetsarbetet som till exempel utbildning, sekretessförbindelser, behörighetsstyrning av åtkomst, dokumentation av rutiner, instruktioner och riktlinjer. Därutöver ska det göras regelbundna dokumenterade kontroller och revisioner av säkerhetsåtgärderna.

Tekniska säkerhetsåtgärder

Tekniska säkerhetsåtgärder syftar till att IT-tekniskt försvåra eller förhindra intrång samt i förekommande fall vid misstanke om incidenter kunna följa upp händelser genom t ex logganalys. Exempel på tekniska säkerhetsåtgärder är flerfaktorsautentisering, brandväggar, kryptering, behörighetssystem, loggning, övervakning, säkerhetskopiering, antivirusskydd, aktiv förvaltning av programvaror innefattande versionshantering samt säkerhetspatchning.

Fysiska säkerhetsåtgärder

Fysisk säkerhet ska förebygga att obehöriga får tillträde till byggnader, lokaler, kontor etc. där de kan få tillgång till uppgifter de inte har rätt att ta del av.

Av betydelse i detta avseende är sådant som hur datorer och lagringsmedier förvaras, zonindelning, direktlarm till bevakningsbolag, säkerhetsdörrar eller om andra har tillträde till byggnaden/lokalen/kontoret.

Inför SCB:s sekretessprövning

För att SCB ska kunna genomföra en sekretessprövning inför ett utlämnande till en organisation eller en enskild forskare måste de organisatoriska, tekniska och fysiska skyddsåtgärderna beskrivas.

I samband med sekretessprövningen kommer redogörelsen granskas av SCB:s rättssekretariat och säkerhetsorganisation för att säkerställa att kraven på skydd enligt artikel 32 i dataskyddsförordningen är uppfyllda. Om projektet inte kan redogöra för att ett fullgott skydd finns kommer SCB inte att kunna lämna ut det begärda materialet med hänvisning till sekretess. Den sekretessbestämmelse som främst blir aktuell vid en sådan prövning är den s.k. dataskyddssekretessen i 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). I korthet innebär bestämmelsen att sekretess gäller för personuppgifter (direkta eller indirekta) om det kan antas att uppgifterna efter ett utlämnande kommer att behandlas i strid med EU:s dataskyddsförordning exempelvis genom att kravet på tekniska och organisatoriska säkerhetsåtgärder inte är uppfyllt.