Dataskyddsombudets kommentar på konsekvensbedömning rörande skolrobot, Alingsås kommun

Allmän kommentar

Dataskyddsombudet har blivit ombedd av förvaltningen att lämna kommentarer på en konsekvensbedömning som genomförts inför införandet av en skolrobot. Personuppgiftsbehandlingen syftar till att i enlighet med 24 kapitlet 20§ i Skollagen kunna tillhandahålla och bedriva särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under en längre tid. Sådan undervisning ska så långt som möjligt motsvara den undervisning som eleven inte kan delta i.

Dataskyddsombudet anser att förvaltningen lyckats väl i beskrivningen av ändamål. Kommunen har ett uppdrag att tillhandahålla utbildning även under speciella förhållanden enligt skollagen och detta presenteras på ett lättbegripligt sätt i konsekvensbedömningens inledning. Förvaltningen motiverar i konsekvensbedömningen väl och har en viss jämförelse mellan olika alternativa lösningar. Man jämför Skolroboten mot Google meet och presenterar varför skolroboten är att föredra. Förvaltningen jämför dock enbart två it system som potentiella lösningar för att klara uppdraget och dessa är båda lösningar som är eller samarbetar med amerikanska företag. Förvaltningen skulle kunna utveckla denna del genom att argumentera utifrån fler potentiella lösningar så som att lärare reser till eleven och undervisar eller genom enklare systemstöd som inte innebär livestream över internet. Alternativt undersöka möjligheterna till alternativa leverantörer verksamma inom Europa. Dataskyddsombudet menar inte med denna kommentar att dessa alternativ per automatik skulle vara att föredra men att utreda även sådana alternativ och argumentera utifrån påverkan på integriteten skulle ge ytterligare en dimension och visa på att man utvärderat även dessa upplägg för att klara uppdraget och ändamålet och motivera varför förvaltningen väljer det ena framför det andra.

Överlag är konsekvensbedömningen bra och förvaltningen både resonerar och motiverar de vägval man gör på ett bra och tydligt sätt.

Riskanalysen

Till konsekvensbedömningen presenteras också en riskanalys som redogör för potentiella risker i användandet av skolroboten. Riskanalysen lyfter relevanta risker med fokus på integritet vilket är helt rätt. Riskanalysen är inspirerad av ett tänk som är vanligt förekommande inom informationssäkerhetsarbetet med konsekvens och sannolikhet som mätvärden. Så kan man göra för att räkna ut ett riskvärde och metoden ger en uppfattning om hur pass allvarlig en risk kan vara både före och efter en genomförd åtgärd. En viktig skillnad i konsekvensbedömningsarbetet jämfört med en risk och sårbarhetsanalys inom informationssäkerhetsarbetet är ju dock att konsekvensbedömningen saknar en riskaptit. Det vill säga att förvaltningen ska kunna visa att behandlingen går att utföra samtidigt som GDPR efterlevs.

Här blir det viktigt att fundera ett varv med tanke på riskerna rörande tredjelandsöverföringar. Nu har ju leverantören gjort ett noggrant arbete med att stärka säkerheten och minimera andelen överföringar, undvika lagring och använder stark krypteringsteknik. Frågan som kvarstår är dock om det räcker för att kunna visa på att behandlingen är laglig utifrån GDPRs definition. Leverantören har valt att ha kvar de amerikanska underleverantörerna och då förs ansvaret att säkerställa efterlevnaden i med de potentiella överföringarna till den personuppgiftsansvariga. Alingsås kommun har ju fattat ett beslut att försiktighetsprincipen råder vid anskaffningar som innebär risk för tredjelandsöverföringar för ca 1 år sedan. Förvaltningen bör ställa sig frågan om systemet är lämpligt i förhållande till det beslutet.

Techlaw som är en juridikbyrå med inriktning på dataskydd har skrivit en intressant analys rörande problematiken med användandet av AWS som är den underleverantör som lyfts fram mest frekvent i konsekvensbedömningen. De skriver bland annat:

”Trots att AWS användare kan välja specifika datacenter, som till exempel datacenter i Sverige eller på Irland, förekommer överföringar av personuppgifter till USA eller andra länder. Detta framgår tydligt av punkt 12.1 i AWS biträdesavtal:

“AWS will not transfer Customer Data from Customer’s selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.”

Vidare framgår det av standardavtalsklausulerna (som är en del av biträdesavtalet) att personuppgifter överförs till USA. Att bestämma att databehandling i AWS ska ske i en specifik region utesluter således inte att AWS kommer att överföra personuppgifter till USA och andra tredjeländer. Följaktligen innebär användning av AWS en risk att överföra personuppgifter till USA i strid med GDPR och en risk för sanktionsavgifter.”

Hela analysen går att läsa här: https://techlaw.se/analys-amazon-web-services-och-gdpr-vad-galler/

Med anledning av detta är det viktigt att förvaltningen säkerställer så att skyddsåtgärderna man vidtar för att minimera riskerna eliminerar risken för tredjelandsöverföringar av de registrerades uppgifter. Om det fortfarande finns risk eller om det är tveksamt om skyddsåtgärderna är tillräckliga bör förvaltningen överväga förhandsamråd med IMY.

Alternativt så kan förvaltningen undersöka om det går att förhandla med leverantören så att det inte förekommer några underleverantörer som medför risk för tredjelandsöverföringar.

Till sist bör också nämnas att riskanalysen är bra genomförd. Åtgärderna känns rimliga och skattningen lika så. Det är dock viktigt att poängtera att åtgärderna är viktiga att åtgärda före implementering. De tekniska finns ju i regel inbyggda i IT-miljön men de organisatoriska i form av rutiner och arbetssätt är viktiga att förankra så de är på plats redan från start.

Dataskyddsombud,

Johan Bergström & Malin Ericsson