Konsekvensbedömningar avseende dataskydd som kreativa verktyg

Av Stefan Johansson

Personuppgiftsansvariga bör betrakta konsekvensbedömningar, även kallade DPIA:s, som en metod för att utreda och belägga att en behandling är förenlig med GDPR. Detta framstår som särskilt viktigt beträffande behandlingar som gränsar till vad GDPR tillåter.

Stefan Johansson

Gymnasienämnden i Skellefteå kommun blev föremål för den första sanktionsavgiften i Sverige för brott mot GDPR. Fallet rör användande av ansiktsigenkänningsteknik för närvarokontroll i en gymnasieskola. Datainspektionen ansåg i sitt beslut, DI-2019–2221, att behandlingen var oproportionell och att det saknades laglig grund för att behandla känsliga personuppgifter. Någon konsekvensbedömning hade inte genomförts och något förhandssamråd hade inte sökts, trots att detta borde ha skett. Beslutet är överklagat och fallet ligger nu hos Förvaltningsrätten i Stockholm, mål nr 20 577–19.

Syftet med denna artikel är inte att diskutera fallet i sig. Fallet används istället för att illustrera att personuppgiftsansvariga har mer att vinna på att betrakta konsekvensbedömning som ett positivt verktyg för att följa GDPR, än som en administrativ börda.

Bakgrund

Gymnasienämnden syfte var att genom en personuppgiftsbehandling effektivisera den närvarokontroll som enligt lag måste göras i samband med varje lektion. I en grupp på 29 elever gav 22 elever med vårdnadshavare sina medgivande till att medverka i ett pilotprojekt. Övriga 7 elever ville inte medverka. Nämnden ansåg att den tekniske konsulten hade bra kontroll på säkerheten och såg därför inga hinder att genomföra pilotprojektet. Utfallet blev dock en domstolstvist, där sanktionsavgifter och en varning för att i framtiden använda ansiktsigenkänning för närvarokontroll står på spel. Frågan som här ska diskuteras är om en utförligt genomförd konsekvensbedömning skulle ha kunnat förändra detta projektutfall.

När konsekvensbedömning krävs

Reglerna om konsekvensbedömningar finns i artikel 35 GDPR.[1] Lagen kräver att sådana bedömningar genomförs i två fall. Om en planerad behandling leder till hög risk för fysiska personers fri- och rättigheter (artikel 35.1) eller om behandlingen listas i artikel 35.3. Uttryckliga exempel på behandlingar med hög risk kan fastställas enligt artikel 35.4. En sådan lista finns publicerad på Datainspektionens webbplats.[2] Den personuppgiftsansvarige måste alltid själv bedöma och kunna visa om en behandling tillhör någon av dessa kategorier. Skäl 76 anger att bedömningen ska göras på objektiv grund. Eftersom artikel 35 både är omfångsrik och relativt svårförståelig försöker de flesta i praktiken att undvika den. Reaktionen är förståelig, men blir lätt kontraproduktiv.[3]

Rättslig status för skydd av personuppgifter

Inom EU anses människors rätt till skydd av sina personuppgifter tillhöra de grundläggande fri- och rättigheterna. Dessa rättigheter har en stark ställning och anses utgöra den demokratiska rättsstatens fundament på det individuella planet, t.ex.

1 Alla artiklar och skäl från GDPR anges härefter utan förordningens namn.

2 Beträffande den publikationen, inklusive dess rättskällestatus, hänvisas till Datainspektionens beslut DI-2018-13200.

3 I Lov & Data nr 4/2018 finns en artikel på detta tema: ”Konsekvensbedömning avseende dataskydd – riskanalys möter rättighetskrav.”

yttrandefrihet, rörelsefrihet, skydd från godtycklig arrestering m.m. Frågan om varför skydd av personuppgifter har denna höga rättsliga status ska dock inte diskuteras här. I detta sammanhang räcker att konstatera att varje diskussion om GDPR som inte utgår från detta faktum ofrånkomligen hamnar fel. Gällande rätt säger att oavsett hur stor nytta en personuppgiftsansvarig skulle ha av en behandling så måste alltid individens rätt respekteras. Det är i denna kontext som konsekvensbedömningarnas positiva potential framträder.

Att bedöma det dataskyddsrättsliga fundamentet

Innan man försöker besvara frågan om behandlingens risknivå aktualiserar förordningens krav på konsekvensbedömning, så kan man börja med att beskriva behandlingens kontext. Det innebär att inventera de grundläggande praktiska frågorna kring behandlingen, som t.ex. dess ändamål, dess konkreta genomförande och vilka kategorier av personuppgifter från vilka kategorier av registrerade som ska behandlas. Dessa delar måste kunna redovisas oavsett om en konsekvensbedömning krävs eller ej, och de är till stor hjälp för det fortsatta arbetet. Genom att börja med behandlingens kontext skapas ett konkret underlag till en första bedömning av behandlingens förhållande till de fundamentala principerna i GDPR. Denna första bedömning är, och bör vara, översiktlig. Dess funktion är att snabbt och tydligt visa på de frågor som kräver svar och indikera det utredningsbehov som finns för att den planerade behandlingen ska vara förenlig med GDPR. Syftet med denna arbetsordning är att kunna ge en relevant uppskattning av den bevisbörda man måste uppfylla för att behandlingen ska möta förordningens krav, oavsett frågan om eventuell risknivå för fysiska personers rättigheter. Därmed får man snabbt upp ögonen för risken att behandlingen är ett dödfött projekt. Bevisbördan kanske är så stor, beträffande t.ex. ändamål och laglig grund, att man helt enkelt inte tror sig kunna uppfylla den. De fundamentala principerna kommer så att säga före risknivån i prövningsordningen avseende en behandlings förenlighet med GDPR. I det aktuella fallet är de kontextuella punkterna ansiktsigenkänning, skolmiljö och närvarokontroll.

> Gällande rätt säger att oavsett hur stor nytta en personuppgiftsansvarig skulle ha av en behandling så måste alltid individens rätt respekteras. Det är i denna kontext som konsekvensbedömningarnas positiva potential framträder

Den första punkten, ansiktsigenkänning, rör biometriska uppgifter. En av de särskilda kategorier av personuppgifter som är förbjudna att behandla enligt artikel 9.1. Kan inget av undantagen i artikel 9.2 tillämpas blir alltså behandlingen olaglig, alldeles oavsett alla andra frågor. Kopplingen till artikel 9.1 indikerar således tydligt att bevisbördan för behandlingens förenlighet med GDPR är hög, oavsett om lagens krav på konsekvensbedömning har inträtt eller ej.

De andra punkterna, skolmiljö och närvarokontroll, rör både myndighetsutövning och relationen mellan myndighet och privatperson. Detta har betydelse för såväl val av rättslig grund som vid bedömningen av om eventuella samtycken är giltiga. Skulle en övertydlig samtyckeshantering enligt artikel 7, i synnerhet avseende samtyckets återkallande, vara en möjlighet att påvisa samtyckets frivillighet, trots eventuell beroendeställning? Skäl 43 poängterar att offentliga myndigheter måste vara extra noga i samtyckesfrågor. Har det någon betydelse att gymnasieelever till största delen är omyndiga, om än ofta över 16 år gamla? Dessa frågors relevans är också oberoende av om en konsekvensbedömning krävs eller ej.

Den tredje punkten, närvarokontroll, är även behandlingens ändamål. Hur förhåller sig behandlingens sätt att uppfylla det ändamålet till de grundläggande dataskyddsprinciperna i artikel 5.1? Hur viktig är närvarokontrollen sett till skolverksamheten som helhet, ur elevers, gymnasienämndens och samhällets perspektiv? Vilka avvägningar mellan dessa intressen kan göras, i enlighet med skäl 4? Är det ens rimligt att använda biometriska uppgifter för närvarokontroll i skolan? Används ansiktsigenkänning av andra myndigheter i andra sammanhang? Vilka analogier och distinktioner kan i så fall göras gentemot dessa för att påvisa att projektets personuppgiftsbehandling är helt rimlig i relation till dess ändamål? Hur fungerar t.ex. det tekniska system som hanterar närvarokontrollen? Blir slutresultatet ett utskrivet papper med kryss i en ruta, som vid manuell närvarohantering, eller skapas en stor databas med olika sökmöjligheter? Om inte full efterlevnad av de grundläggande dataskyddsprinciperna kan visas, artikel 5.2, är behandlingen lika olaglig som om den saknade rättslig grund. Även detta är oberoende av om lagen kräver en konsekvensbedömning eller ej.

De punkter som berörs i detta fall är emellertid så tunga, att en konsekvensbedömning bör genomföras oavsett om kravet på en sådan har aktualiserats eller ej. Det stora skälet är den heltäckande och strukturerade framställningsform som konsekvensbedömningen erbjuder. Det ligger på något sätt i sakens na-

tur att så svårbesvarade legala frågor som dem i det aktuella fallet utreds i detalj och följs upp med en uttömmande diskussion om de risker som de registrerades och eventuellt andra människors fri- och rättigheter utsätts för genom projektet. Vilka tekniska och organisatoriska skyddsåtgärder kommer vidtas för att neutralisera dessa risker? Hur garanteras därutöver att de registrerade kan utöva sina rättigheter? Dessa naturliga följdfrågor, som med all rätt kan ställas oberoende av om någon konsekvensbedömning krävs eller ej, har sina givna platser i en konsekvensbedömning. Genom att självmant behandla dem kan det visas att projektet inte utsätter några fysiska personers fri- och rättigheter för ökad risk jämfört med de system för närvarokontroll som finns idag.

Konsekvensbedömningar är kreativ juridik

Det är ett ofrånkomligt faktum att den tekniska utvecklingen alltid ligger före lagstiftningen. Kombinationen av ansvarsskyldighetsprincipen och den riskbaserade metoden, som bägge genomsyrar GDPR, kan betraktas som ett rättsligt sätt att hantera denna verklighet. Den personuppgiftsansvarige åläggs de facto att själv skapa det underlag som ska användas för att avgöra om en behandling följer GDPR eller ej. Det ligger därför tydligt i den personuppgiftsansvariges eget intresse att skapa ett så bra underlag som möjligt, för att därigenom bättre kunna argumentera för sin sak. Oberoende av om lagen kräver en konsekvensbedömning för en behandling kan således den personuppgiftsansvarige använda det verktyget för att mer eller mindre utforma sin egen dataskyddsrättliga verklighet. Det kreativa spelrummet för väl valda ord baserade på tydligt rättskällestöd framstår onekligen som stort. Syftet med att genomföra konsekvensbedömning i ett fall som detta, med svåra principiella frågor, är således proaktivt, att desarmera en potentiell brist.

Svaret på frågan, om gymnasienämnden hade fått ett bättre projektutfall om de hade genomfört en gedigen konsekvensbedömning, förblir ändå öppet. De rättsliga frågor som projektet väcker är onekligen stora och konsekvensbedömningar är bara en metod att finna svar. Det finns ingen garanti för att de svar man finner är dem man verkligen vill ha. Men det framstår som ett rimligt antagande att en utförlig konsekvensbedömning i god tid hade identifierat de invändningar som Datainspektionen reste och som nu stoppar projektet. I så fall skulle gymnasienämnden ha haft kvar hela frågan på sitt eget bord istället för hos domstolen. De hade då själva kunnat besluta att t.ex. lägga ned projektet eller ändra i projektupplägget och bearbeta sin rättsliga argumentation. I bägge fallen hade gymnasienämnden haft större handlingsfrihet än vad den har idag.

Stefan Johansson är jurist & försäljningschef på Datakollen.