I stort sett alla företag och organisationer behandlar personuppgifter. Ofta förbisett är den säkerhet som måste omgärda personuppgiftsbehandlingen. Bristande säkerhet vid personuppgiftsbehandling är enligt personuppgiftslagen belagt med straffansvar och skadeståndsskyldighet i förhållande till de vars personuppgifter inte skyddats i tillräcklig omfattning. Datainspektionen, som utövar tillsyn enligt personuppgiftslagen, har granskat ett antal olika verksamheters säkerhet vi behandling av personuppgifter och konstaterat att den i stor utsträckning varit otillräcklig.

JOHAN KAHN OCH **DANIEL SVENSSON**

Krav på säkerhet vid behandling av personuppgifter

ENLIGT 31§ PERSONUPPGIFTSLAGEN är den personuppgiftsansvarige (d.v.s. den som bestämmer ändamål och medel för behandling av personuppgifter) skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas . För att skapa ett sådant skydd för personuppgifterna gäller det att göra en samlad bedömning som tar hänsyn till hur pass känsliga de behandlade personuppgifterna är, riskerna som finns med behandlingen av personuppgifterna, de tekniska möjligheter för skydd och säkerhet som finns tillgängliga, om personuppgifterna omfattas av tystnadsplikt eller sekretess samt vad det kostar att genomföra åtgärderna. Dessutom finns det särskild lagstiftning och särskilda aspekter för exempelvis myndigheter eller personuppgiftsbehandling under patientdatalagen men det berörs inte vidare i denna artikel.

DATAINSPEKTIONEN

Datainspektionen har utfärdat allmänna råd om hur lagens krav på säkerhetsåtgärder ska tolkas och efterlevas. De allmänna råden finns tillgängliga på Datainspektionens webbplats www.datainspektionen.se. De allmänna råden innehåller såväl generella riktlinjer till den personuppgiftsansvarige (t.ex. att kartlägga hotbilden, upprätta säkerhetspolicy och rutiner samt genomföra regelbundna säkerhetstester) som mera konkreta exempel på säkerhetsåtgärder som kan vara lämpliga att vidta. Som direkt framgår av lagtexten, är uppgifternas art helt centralt för bedömningen av vilka säkerhetsåtgärder bör vidtas i det enskilda fallet. Om behandlingen avser känsliga personuppgifter (d.v.s. uppgifter som rör etniskt ursprung, politiska åsikter, religion, fackmedlemskap, hälsa eller sexualliv) ställs avsevärt högre krav på säkerheten.

Datainspektionen har i ett antal intressanta beslut tillämpat lagstiftningens krav på lämpliga säkerhetsåtgärder på konkret fall av personuppgiftsbehandling. Det senaste beslutet fattades den 18 december 2009 och gäller Pliktverkets personuppgiftshantering inom ramen för e-tjänsten Lämplighetsundersökning. Denna tjänst syftar till att identifiera de män och kvinnor som klarar kraven för militär grundutbildning och kalla dessa till mönstring. Tjänsten innebär att målgruppen gör en självvärdering via Internet, bestående av ett antal frågor om bl.a. hälsa, fysisk prestationsförmåga, intressen och skolgång. För inloggning till tjänsten krävs en åttasiffrig pinkod och en signeringskod. Koderna skapas genom en slumpgenerator och tillsänds användarna med post. För inloggning krävs dessutom ett användarnamn, vilket utgörs av användarens personnummer. En användare kan närsomhelst avbryta sin användning av tjänsten och logga in på nytt, varvid de tidigare ifyllda uppgifterna på nytt görs tillgängliga för användaren.

KRÄNKER INTEGRITETEN

Datainspektionen konstaterar att tjänsten Lämplighetsundersökning innebär en omfattande behandling av känsliga personuppgifter i form av uppgifter som rör hälsa. Som redan nämnts medför detta särskilt höga krav på säkerhetsåtgärder enligt personuppgiftslagen. Datainspektionen anser att det därför måste betraktas som en mycket stor integritetskränkning om dessa personuppgifter hamnar i fel händer, t.e.x genom att en annan person än användaren loggar in i tjänsten med användarens inloggningsuppgifter. Den nuvarande autentiseringslösningen, d.v.s. inloggning med unika användarnamn och pinkoder, är därför inte tillräcklig så länge användaren även får tillgång till tidigare ifyllda uppgifter. Om inte Pliktverket implementerar alternativa, starkare, autentiseringsmetoder (såsom exempelvis e-legitimation), anser Datainspektionen att användarnas åtkomst via Internet ska begränsas till enbart uppgifter som varken är känsliga enligt personuppgiftslagens definition eller på annat sätt integritetskänsliga . Sammantaget underkänner alltså Datainspektionen Pliktverkets

säkerhetsåtgärder för e-tjänsten Lämplighetsundersökning och förelägger Pliktverket att upprätta en åtgärdsplan för att uppfylla lagens krav.

ELEKTRONISKA RECEPT

Ett annat intressant beslut gäller Apotekets säkerhetsåtgärder för de personuppgifter som hanteras i samband med överföring av och åtkomst till elektroniska recept enligt lagen om receptregister. Det bör noteras att Datainspektionens beslut är från 2008 och att lagstiftningen om receptregister genomgått avsevärda förändringar, delvis beträffande säkerhetskrav och i förhållande till personuppgiftslagen, i samband med omregleringen av apoteksmarknaden. Datainspektionens beslut är trots det intressant vad gäller tillämpningen av säkerhetskraven i 31 § personuppgiftslagen.

Datainspektionen konstaterade inledningsvis dels att Apoteket behandlar mycket integritetskänsliga personuppgifter inom ramen för den s.k. nationella receptbrevlådan och receptregistret, dels att Apotekets hantering av elektroniska recept innebär en omfattande överföring och lagring av känsliga personuppgifter som rör en stor del av befolkningen. En oskyddad överföring av elektroniska recept innebär därför en avsevärd integritetsrisk. Datainspektionen noterar också att tillgång till uppgifterna för Apotekets anställda kan utgöra en integritetskränkning om och i den mån den anställde inte haft behov av sådan tillgång.

Datainspektionen fann i beslutet att Apotekets säkerhetslösningar var otillräckliga i tre avseenden. För det första saknades adekvata rutiner för uppföljning av behandlingshistoriken (logg) för åtkomsten till personuppgifterna i den nationella receptbrevlådan och receptregistret. Apoteket förelades i denna del att genom stickprovskontroller göra systematiska och återkommande uppföljningar i syfte att upptäcka obehörig åtkomst till dessa personuppgifter. För det andra bedömdes kommunikationssäkerheten i Apotekets mottagande av elektroniska recept inte uppfylla kraven på säkerhetsåtgärder enligt personuppgiftslagen, eftersom överföringen inte var krypterad i samtliga fall. För det tredje ansågs autentisering med användarnamn och lösenord för inloggning till tjänsten e-Dos inte uppfylla personuppgiftslagens krav på säkerhetsåtgärder. Eftersom tjänsten innehåller känsliga personuppgifter, måste användarnas identitet säkerställas med en teknisk funktion som ger stark autentisering (t.ex. e-legitimation, SITHS-certifikat eller engångslösenord).

Utöver detta beslut, har Datainspektionen gjort motsvarande uttalanden i äldre beslut avseende säkerhetsåtgärder vid behandling av känsliga personuppgifter. Varken Socialnämnden i Nacka kommun eller Barn- och utbildningsnämnden i Nynäshamns kommun ansågs uppfylla lagens krav eftersom överföring av känsliga personuppgifter utfördes i öppna nät utan kryptering. I det senare fallet saknades dessutom nödvändiga loggar för behandlingshistorik.

STRÄNGA KRAV

Av Datainspektionens praxis står klart att det ställs mycket stränga krav på säkerhetsåtgärder för att skydda känsliga personuppgifter. Det är dock viktigt att understryka att lagens krav inte är begränsade till att omfatta endast känsliga personuppgifter. Den personuppgiftsansvarige är ansvarig för att se till att all personuppgiftshantering är föremål för lämpliga säkerhetsåtgärder för att förhindra obehörig användning eller åtkomst.

De mest grundläggande åtgärderna som bör vidtas är att göra en inventering av potentiella hot och upprätta en säkerhetspolicy för verksamheten. Vidare måste möjliga fysiska säkerhetsåtgärder övervägas, såsom t.ex. låsutrustning, fönstergaller, inpasseringskontroller, larmutrustning, placering och märkning av utrustning samt skydd mot rök, vatten och eld.

DANIEL SVENSSON är jur.kand. och biträdande jurist på Advokatfirman Delphi. Daniel arbetar huvudsakligen i Delphis ITC/IP-grupp och biträder svenska och internationella klienter i olika affärsjuridiska frågor, med särskild tonvikt mot IT-rätt, outsourcing, integritetsskyddsfrågor, immaterialrätt och kommersiell avtalsrätt.

KÄNSLIGA PERSONUPPGIFTER

Alla databaser eller andra sammanställningar av personuppgifter måste ha dels en behandlingshistorik (logg) med regelbunden kontroll och uppföljning, dels ett adekvat system för behörighetskontroll för att identifiera och autentisera användarens identitet. Vad gäller kravet på behandlingshistorik, bör en sådan logg innehålla information om läsning, ändring, utplåning eller kopiering av personuppgifter. Så länge inga känsliga personuppgifter behandlas, tyder Datainspektionens praxis på att användarunika inloggningsuppgifter medför ett tillräckligt skydd mot obehörig åtkomst. När det är fråga om känsliga personuppgifter krävs dock starkare autentiseringsmekanismer, som e-legitimation, engångslösenord, aktiva behörighetskort eller biometriska metoder (t.ex. fingeravtryck). När det gäller överföring av känsliga personuppgifter via Internet eller andra öppna nätverk, bör sådan överföring skyddas mot obehörig åtkomst genom assymetrisk kryptering eller annan teknisk lösning med motsvarande skydd. Vid kryptering är det givetvis också essentiellt att krypteringsnycklarna förvaras och skyddas på lämpligt sätt.

Säkerhet för personuppgiftsbehandling är en komplex fråga särskilt i ljuset av att skyddsåtgärderna i sig inte heller får stå i strid med personuppgiftslagen. Exempelvis vid anvädning av biometriskt baserade autentiseringslösningar bör lagligheten analyseras mot bakgrund av personuppgiftslagens regler. ■

JOHAN KAHN // johan.kahn@delphilaw.com

Johan är advokat och delägare i Advokatfirman Delphi i Stockholm. Han arbetar med affärsjuridik och då särskilt IT-rätt, integritetsskyddsfrågor, outsourcing, immaterialrätt samt kommersiell avtalsrätt. Frågor om skydd och säkerhet, så kallad säkerhetsjuridik, är ständigt aktuella och under den här vinjetten delar Johan med sig av sina kunskaper och erfarenheter.