DANIEL LUNDQVIST OCH HANNA BOGSJÖ

För att säkerhetsföretag ska kunna uppfylla kraven i den nya EU-förordning som ska ersätta PUL krävs hårt arbete.

Dataskyddsförordningen är snart här:

▶ Uppfyller ni kraven i ”nya PUL”?

EU:s nya dataskyddsförordning kommer med all sannolikhet att beslutas under våren och sedan träda ikraft år 2018. Förordningen kommer då helt ersätta dagens personuppgiftslag (PUL) och annan lagstiftning om personuppgiftsbehandling i Sverige. Den nya förordningen innehåller flera viktiga nyheter och stora förändringar jämfört med dagens regelverk. För många företag, inte minst i säkerhetsbranschen, krävs ett omfattande arbete för att kunna uppfylla de nya lagkraven. Ett nödvändigt första steg är att kartlägga dagens personuppgiftsbehandling så snart som möjligt, det är varken praktiskt eller tekniskt genomförbart att vänta tills de nya reglerna träder ikraft.

Skyddet för den personliga integriteten är en grundläggande rättighet för alla EU-medborgare. Mot bakgrund av den snabba tekniska utvecklingen har frågor om personlig integritet och personuppgiftsbehandling aktualiserats i flera uppmärksammade rättsfall i EU-domstolen de senaste åren (exempelvis i domar mot Google och Facebook).

DET ÄR UPPENBART att personlig integritet blir en allt viktigare fråga för kunder, anställda och allmänheten. Frågan står även högt på den politiska dagordningen. I december 2015 träffades en principöverenskommelse mellan EU-kommissionen, EU-parlamentet och Europeiska Rådet om en ny dataskyddsförordning inom EU. Slutligt beslut om det nya regelverket förväntas fattas i april eller maj 2016. Den nya förordningen kommer att träda ikraft två år efter detta beslut, alltså sannolikt under våren 2018. Svenska företag och myndigheter har alltså något mer än två år på sig för att anpassa sin verksamhet till EU:s nya lagstiftning.

Många av grundprinciperna i dagens PUL kommer att vara relevanta även under den nya dataskyddsförordningen. Det kommer till exempel även i framtiden att krävas uttryckligt ändamål och laglig grund för varje behandling, samt att specifik information måste lämnas till registrerade. Även reglerna kring grundläggande rättigheter för de registrerade (som ansökan om registerutdrag), obligatoriska så kallade personuppgiftsbiträdesavtal samt det principiella förbudet mot överföring av personuppgifter till tredje land kommer att behållas.

EN NYHET MED stor betydelse för säkerhetsbranschen är att förordningen innehåller skadeståndssanktionerade åtaganden även för så kallade personuppgiftsbiträden, det vill säga bolag som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett företag som hanterar en databas med information om sina kunders kunder får därmed en ”egen” lagstadgad skyldighet att vidta tekniska och organisatoriska åtgärder för att skydda sådana personuppgifter mot obehörigt intrång och röjande. Enligt PUL är det bara den ansvarige som bär sådant ansvar enligt lag, även om den ansvarige genom avtal ska överföra ansvaret på biträdet. I det nya regelverket blir det alltså ännu viktigare att både kartlägga behandlingar och att klargöra ansvars- och avtalsförhållanden, oavsett om företaget agerar som personuppgiftsansvarig eller personuppgiftsbiträde.

Därutöver innehåller det nya regelverket många nyheter och förändringar som för många säkerhetsföretag kommer att kräva någon grad av organisatoriska, processrelaterade och/eller tekniska förändringar. Några av de viktigaste förändringarna är:

• Det nya regelverket blir en EU-förordning istället för ett EU-direktiv. Detta innebär bl.a. att de nya reglerna gäller direkt som lag i Sverige och därför helt kommer att ersätta den svenska personuppgiftslagen och sannolikt också många registerförfattningar.

• Företag som bryter mot den nya förordningen kan drabbas av mycket höga sanktioner, t.ex. i form av böter på upp till 4 % av global årsomsättning. Riskerna förknippade med att behandla personuppgifter i strid med det nya regelverket kommer alltså att öka väsentligt jämfört med dagens nivåer.

• Undantaget i PUL om så kallad ostrukturerad personuppgiftsbehandling, t.ex. uppgifter i löpande text, kommer att försvinna när den nya förordningen införs. För sådana uppgifter gäller i dagsläget ett förenklat regelverk med väsentligt lägre krav.

> **Den nya förordningen ställer betydligt högre krav på kontroll och transparens**

• Kraven skärps kring hur giltiga samtycken från registrerade kan inhämtas. Samtycken som lämnats enligt dagens regelverk kan alltså vara ogiltiga när förordningen träder ikraft. Om så är fallet krävs kan det krävas nya samtycken inhämtas, vilket förstås kan bli en omständlig process för många företag.

• Inbyggd integritet, så kallad privacy by design, blir ett uttryckligt krav i den nya förordningen. Detta innebär i korthet att integritetsfrågor ska beaktas och ”byggas in” när IT-system utvecklas och upphandlas.

• Alla säkerhetsincidenter som berör personuppgifter ska rapporteras till dataskyddsmyndigheten (i Sverige sannolikt Datainspektionen) inom 72 timmar. I vissa fall ska även de registrerade informeras om incidenten.

• Två nya rättigheter för de registrerade införs i form av dels en så kallad rätt att bli bortglömd, dels en rätt till så kallad dataportabilitet. Rätten att bli bortglömd innebär att personuppgifter permanent ska raderas på den registrerades begäran, medan dataportabilitet innebär att den registrerade ska kunna begära ut sina personuppgifter i ett standardiserat format så att uppgifterna lätt kan överföras till andra företag.

• Rollen för de nationella dataskyddsmyndigheterna förändras. Bland annat ska en registrerad i Sverige kunna vända sig till den svenska myndigheten (Datainspektionen) med klagomål mot ett bolag i ett annat europeiskt land. Vidare kommer myndigheten att under vissa omständigheter vara skyldig att fatta beslut i de ärenden som anmäls till eller uppkommer hos myndigheten.

• Den nya förordningen är tillämplig för alla företag (även utanför EU) som erbjuder produkter eller tjänster till individer inom EU, eller om företaget bevakar eller inhämtar information om användares beteende inom EU (t.ex. genom s.k. cookies). Detta innebär i praktiken att alla större sociala nätverk och internettjänster kommer omfattas av det nya regelverket.

• För sociala nätverk införs en slags ”åldersgräns”, innebärande att barn under en viss ålder måste inhämta samtycke från sin vårdnadshavare för att registrera sig för det aktuella nätverket. Åldersgränsen ska vara mellan 13-16 år och bestäms av varje medlemsstat. Det är sannolikt att den svenska åldersgränsen kommer sättas så lågt som möjligt, det vill säga vid 13 år.

ÄVEN OM ETT grundläggande syfte med den nya förordningen är att harmonisera regelverket inom hela EU, så finns undantag där nationella regler kommer få genomslag. Det kanske viktigaste undantaget rör personuppgiftsbehandling om anställda, vilket ju är ett område som berör i princip alla företag. Det återstår att se hur det svenska regelverket för sådan personuppgiftsbehandling kommer att se ut.

Sammanfattningsvis kan konstateras att den nya förordningen ställer betydligt högre krav på kontroll och transparens över företags behandling av personuppgifter. Det bästa, och förmodligen enda, sättet att åstadkomma en sådan kontroll och transparens är att göra en övergripande och noggrann kartläggning av alla ”behandlingar” av personuppgifter som förekommer idag. Först därefter kan man sedan bedöma vilka åtgärder som behöver implementeras.

Med säkerhet kommer ett flertal konkreta åtgärder att bli nödvändiga, såsom exempelvis uppdatering av informationstexter gentemot kunder samt översyn av befintliga rutiner för inhämtande av eventuella samtycken från registrerade. Vidare behöver rutiner avseende incidentrapportering till myndigheter införas, samt att krav- och inköpsprocesser kan behöva justeras. Det säger sig självt att det är fråga om åtgärder som för många företag innebär omfattande förändringar, både tekniskt och organisatoriskt. Även om två år kan tyckas vara lång tid så finns alltså ingen tid att spilla. ●

DANIEL LUNDQVIST
Daniel Lundqvist är advokat och delägare i Advokatfirman Kahn Pedersen. Daniel är specialiserad på juridik relaterad till integritetsskydd, datasäkerhet och IT-avtal.

HANNA BOGSJÖ
är biträdande jurist på advokatfirman Kahn Pedersen och arbetar med IT-relaterad juridik, integritetsfrågor, kommersiella avtal och offentlig upphandling.