

Pliktverket
Att:
Karolinen 651 80
KARLSTAD

Tillsyn enligt personuppgiftslagen (1998:204) – personuppgiftsbehandling i anslutning till Pliktverkets e-tjänst för lämplighetsundersökning

Sammanfattning

Det är inte tillräckligt att enbart med användarnamn i form av personnummer och lösenord i form av en pinkod autentisera användarna då de ansluter till lämplighetsundersökningen via Internet om nuvarande funktionalitet i e-tjänsten ska bestå. Det är dock, som verket själv har påtalat, förenat med svårigheter att införa e-legitimation. Men det finns andra autentiseringsmetoder för användarna som skulle kunna vara aktuella istället för e-legitimation. Om det inte anses möjligt att införa alternativa, starkare, autentiseringsmetoder för inloggning till e-tjänsten anser Datainspektionen att användarnas åtkomst via Internet ska begränsas till enbart uppgifter som varken är känsliga enligt 13 § PuL eller på annat sätt integritetskänsliga.

Att ifyllda uppgifter är fullt synliga för en användare som loggar in igen, med den pinkod som skickats ut, är inte acceptabelt ur ett integritetsskyddsperspektiv. Vi anser att en användare, som loggar ut ur e-tjänsten, inte ska kunna ta del av ifyllda uppgifter igen vid inloggning annat än om hon eller han använder sig av en stark autentiseringsmetod såsom e-legitimation eller motsvarande. När en användare väl signerat sin lämplighetsundersökning anser vi att proceduren ska vara avslutad.

Informationen som Pliktverket ger via sin hemsida rörande hanteringen av personuppgifter i lämplighetsundersökningen ligger enligt vår bedömning nära de krav som ställs enligt PuL. Men den bör kompletteras i några avseenden. Pliktverket bör överväga att lämna den uppdaterade informationen som ges under rubriken "Om webbplatsen" på inloggningssidan till e-tjänsterna. Informationen som ges i brevet som skickas ut inför lämplighetsundersök-

ningen bör, precis som Pliktverket också avser göra, ses över. Datainspektionen anser att informationen i det brev som skickas ut ska motsvara den information som ges via Pliktverkets hemsida efter att verket kompletterat den i enlighet med våra påpekanden.

Datainspektionens beslut

Pliktverket föreläggs att komma in med en skriftlig åtgärdsplan där verket redogör för de förändringar, och därtill knutna förstärkningar av integritetsskyddet, som verket är berett att genomföra ifråga om autentiseringen till e-tjänsten.

Pliktverket föreläggs även att komma in med en skriftlig åtgärdsplan som redogör för vilka åtgärder verket är berett att vidta för att hindra att obehöriga kan ta del av redan ifyllda uppgifter i lämplighetsundersökningen.

Åtgärdsplanen ska innehålla en uppskattning av när de föreslagna åtgärderna kan vara genomförda och vara Datainspektionen tillhanda **senast måndagen den 1 mars 2010**.

Datainspektionen förutsätter att Pliktverket beaktar de synpunkter som getts avseende informationen till de registrerade.

Redogörelse för tillsynsärendet

Datainspektionen genomförde en inspektion hos Pliktverket den 7 maj 2009. Syftet var att kontrollera personuppgiftsbehandlingen i anslutning till e-tjänsten för lämplighetsundersökning inför mönstring. Tillsynen har redovisats genom ett protokoll som översänts till er och ni har yttrat er.

Allmänt om Pliktverket och e-tjänsten "Lämplighetsundersökning"

Pliktverket ansvarar för mönstring, antagningsprövning, inskrivning och redovisning av totalförsvarspliktiga. Verket är en civil myndighet direkt under försvarsdepartementet.

Lämplighetsundersökningen är en egenutvecklad webbaserad e-tjänst som togs i drift 2007. Tjänsten har tillkommit som ett led i försvarets ändrade inriktning och dimensionering. Den syftar i grunden till att identifiera de personer som klarar kraven för militär grundutbildning och kalla dessa till mönstring. Tjänsten riktar sig till både män och kvinnor. Under 2008 svarade 13 500 unga kvinnor samt 71 000 unga män på frågorna i e-tjänsten.

E-tjänsten innebär att målgruppen gör en självvärdering via Internet, bestående av ett antal frågor om bland annat hälsa, fysisk prestationsförmåga, in-

tressen och skolgång. Tjänsten medför bland annat stora besparingar för Pliktverket och ett förbättrat underlag för mönstringen. Tjänsten innebär dessutom förenklingar för de personer som eventuellt ska kallas till mönstring.

Efter att ha loggat in i e-tjänsten besvarar användaren ett 60-tal frågor. Dessa frågor är grupperade i sex olika avsnitt, nämligen "Min hälsa", "Min skoltid", "Min personlighet", "Mitt sociala liv", "Min inställning till att göra lumpen" och "Allmänna frågor". Frågorna utgörs i allt väsentligt av så kallade flervalsfrågor eller kryssfrågor. E-tjänsten innehåller inga så kallade öppna frågor, där användaren skulle kunna lämna uppgifter om i princip vad som helst. Användaren kan inte heller bifoga elektroniska dokument.

Pliktverket har uppgett att tillämplig lagstiftning rörande hanteringen av personuppgifter i e-tjänsten är dels lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga, dels personuppgiftslagen i tillämpliga delar samt också Pliktverkets interna bestämmelser om gallring av upptagningar i systemen Plis och Syom – PIB 2008:12.

Pliktverket är personuppgiftsansvarigt för den behandling av personuppgifter som utförs inom ramen för e-tjänsten och anser att personuppgiftsansvaret inträder i och med att de erbjuder tjänsten till presumtiva användare.

Skäl för beslutet

Tillämpliga bestämmelser

Enligt 2 kap. 1 § lagen om totalförsvarsplikt är alla totalförsvarspliktiga skyldiga att på begäran av bl.a. Pliktverket lämna nödvändiga uppgifter om sig själva, i syfte att deras förutsättningar att fullgöra värnplikt eller civilplikt ska kunna utredas.

För Pliktverkets verksamhet gäller lagen (1998:938), samt anslutande förordningen (1998:1229), om behandling av personuppgifter om totalförsvarspliktiga. I lagens 4 § sägs att om inget annat följer av registerlagen eller av föreskrifter som meddelats med stöd av lagen, tillämpas personuppgiftslagen (1998:204) vid behandling av personuppgifter om totalförsvarspliktiga.

I vare sig lagen om behandling av personuppgifter om totalförsvarspliktiga eller den anslutande förordningen finns särskilda bestämmelser om information till registrerade eller säkerhet kring personuppgiftsbehandling. Inte heller den PIB som uppgetts vara tillämplig på personuppgiftsbehandlingen i e-

tjänsten innehåller sådana bestämmelser. Vi bedömer därför att PuL:s bestämmelser gäller i dessa delar.

Enligt personuppgiftslagen 23-25 §§ ska den personuppgiftsansvarige själv-
mant lämna information om behandlingen av personuppgifter till de registre-
rade. Informationen ska omfatta följande uppgifter:

- a) uppgift om den personuppgiftsansvariges identitet (informationen bör innehålla namn, adress, telefonnummer, organisationsnummer och i förekommande fall e-postadress),
- b) uppgift om ändamålen med behandlingen,
- c) all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna (kategorier av mottagare), skyldighet (för den enskilde) att lämna uppgifter, rätten att ansöka om information (gratis registerutdrag en gång per år), och rätten till rättelse.

Av 31 § PuL följer att den personuppgiftsansvarige är skyldig att vidta säkerhetsåtgärder, såväl tekniska som organisatoriska, för att skydda de personuppgifter som behandlas. För att skapa ett lämpligt 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 som finns tillgängliga på marknaden samt vad det kostar att genomföra åtgärderna.

Information

Pliktverket lämnar information till användarna om behandlingen av personuppgifter. Informationen lämnas dels i de informationsbrev som skickas till användaren, dels på en särskild sida efter det att användaren loggat in på e-tjänsten i fråga. Informationen i brevet lyder

"Dina uppgifter är sekretesskyddade. Uppgifterna som du lämnar i lämplighetsundersökningen ansvarar Pliktverket för och uppgifterna är sekretesskyddade enligt 7 kapitlet 1 c och 12 §§ sekretesslagen (1980:100)".

Med informationen i brevet menar verket att myndigheten är ansvarig för uppgifterna enligt PuL och att de lämnade uppgifterna även är skyddade enligt sekretesslagen. Pliktverket har uppgett att man avser ändra texten i informationsbrevet så att informationen om behandling av personuppgifterna blir tydligare. I övrigt gäller den särskilda informationen om behandling av personuppgifter som lämnas efter inloggning till e-tjänsten.

Datainspektionens bedömning

Informationen till den registrerade är en viktig del i den enskildes integritets-skydd. Via sin webbsida informerar Pliktverket om hur uppgifterna i lämplighetsundersökningen hanteras. Informationen omfattar följande.

”Uppgifterna som du lämnar i lämplighetsundersökningen registrerar och bearbetar vi i Pliktverkets datoriserade informationssystem Plis.

Vad ska uppgifterna användas till?

Pliktverket måste ha uppgifterna för att kunna bedöma om du har förutsättningar att mönstra (antagningspröva) och göra lumpen. När vi inte längre behöver uppgifterna förstör vi dem.

Pliktverket har ansvar för uppgifterna

Myndigheten har ansvar för hur dina uppgifter behandlas (personuppgiftsansvarig). Det innebär bland annat att vi ska se till att uppgifterna behandlas korrekt och att obehöriga inte kan ta del av dem.

Vem kan ta del av uppgifterna?

Det är bara de medarbetare vid Pliktverket som behöver dina uppgifter för att lösa sina arbetsuppgifter som får ta del av dem. Uppgifterna är skyddade enligt 7 kapitlet 1 c och 12 §§ i sekretesslagen (1980:100).

Du har rätt att få veta vilka uppgifter Pliktverket har om dig

Du kan skriva till Pliktverket och få besked om vilka uppgifter vi har om dig. Eftersom ansökan ska vara undertecknad kan du inte skicka den som e-post. Du kan också begära att vi rättar, spärrar eller tar bort felaktiga uppgifter om dig.”

Informationen som Pliktverket ger via sin hemsida rörande hanteringen av personuppgifter i lämplighetsundersökningen ligger enligt vår bedömning nära de krav som ställs enligt PuL. Men den bör kompletteras i några avseenden. Det bör finnas fylligare information rörande den personuppgiftsansvariges identitet samt vilka mottagare som kan bli aktuella av personuppgifterna. Meningen ”Du kan skriva till Pliktverket och få besked om vilka uppgifter vi har om dig” kan förtydligas något genom att man anger att detta kallas registerutdrag samt att den registrerade har rätt att en gång per år gratis få ett sådant efter ansökan.

Den information som ges i brevet som skickas ut inför lämplighetsundersökningen är för knapphändig för att nå upp till PuL:s krav. Den bör, precis som Pliktverket också avser göra, ses över. Vi anser att informationen i det brev som skickas ut ska motsvara den information som ges via Pliktverkets hemsida efter att verket kompletterat den i enlighet med våra påpekanden.

Informationen på hemsidan ges under rubriken ”Om webbplatsen” och inte i direkt anslutning till inloggningen för e-tjänsterna. I de fall personuppgifter samlas in i samband med användning av Internet, brukar vi rekommendera

att informationen lämnas på en inloggningsbild eller liknande. Pliktverket bör därför överväga att lämna den uppdaterade informationen som ges under rubriken "Om webbplatsen" på inloggningssidan till e-tjänsterna. Med en sådan placering av informationen ökar chanserna att samtliga användare av e-tjänsten får den information som krävs enligt PuL. Verket bör också korrigera informationen till följd av den nya offentlighets- och sekretesslag som trätt ikraft under 2009.

Inloggning och autentisering

För att använda den aktuella e-tjänsten krävs en åttaställig pinkod (sifferkod) och en åttaställig signeringskod (sifferkod). Dessa används för autentisering i samband med inloggning respektive signering av lämplighetsundersökningen efter avslutat ifyllande av svaren. Användarna får koderna tillsända med vanlig post i maskerat kuvert. Om de personliga koderna kommer bort, vilket har inträffat, går det att kontakta Pliktverket och få koderna skickade igen. Vid behov kan Pliktverket skapa nya koder. Pinkoderna skapas genom en slumpgenerator.

För att logga in i e-tjänsten krävs också ett användarnamn, som utgörs av användarens personnummer. Pliktverket anser att lösningen med personnummer är praktisk och att den är tillräcklig ur säkerhetshänseende och anser att stöd finns i registerlagen för att använda personnummer som användarnamn.

Pliktverket har uppgett att man övervägt e-legitimation och att denna metod egentligen är att föredra. I nuläget är det dock förenat med svårigheter och kostnader för underåriga att skaffa e-legitimation, varför Pliktverket bedömer att denna lösning inte är lämplig. Verket har dock möjlighet att snabbt och enkelt lägga till en funktion för e-legitimation. Förutom e-legitimation har inte Pliktverket funderat på annat lämpligt sätt för autentisering. Att använda pinkod och signeringskod som tagits fram via en slumpgenerator anser Pliktverket vara det bästa sättet efter att använda e-legitimation.

Datainspektionens bedömning

Rörande nuvarande autentiseringslösning anser vi att om en användare anmäler att hon eller han har förlorat sin pinkod så ska en nyskapad pinkod tas fram och skickas ut till användaren. Detta ska ske vid varje tillfälle en användare hör av sig och anmäler sin pinkod förlorad. Se dock vidare nedan angående alternativa autentiseringslösningar till den nu använda.

I utredningen "Totalförsvarsplikt och frivillighet – SOU 2009:63" presenteras en ny inriktning rörande den fortsatta skyldigheten att fullgöra värnplikt och civilplikt. Plikten ska vara beroende av att regeringen med hänsyn till för-

svarsberedskapen föreskriver om det. I detta ligger att skyldigheten att fullgöra värnplikt och civilplikt med längre grundutbildning än 60 dagar i framtiden ska omfatta både män och kvinnor. Utredningen analyserar bl.a. skyldigheten att medverka vid en föreskriven utredning om sina personliga förhållanden.

Lämplighetsundersökningen genomförs med stöd av 2 kap. 1 § lagen om totalförsvarsplikt som *annan utredning*. Sådan annan utredning behöver inte genomföras i den enskildes närvaro. Förslagen i utredningen innebär att alla män är skyldiga att svara på frågorna i höstens webbaserade lämplighetsundersökning. För kvinnorna är det frivilligt. Men från och med 1 juli 2010 är lämplighetsundersökningen obligatorisk för alla 18-åriga män och kvinnor.

I ett särtryck (Elektronisk identifiering och underskrift i Sverige) till Vervas rapport 2008:12 (Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar, publicerad i juni 2008) uttrycktes en samlad problembild för dagens e-legitimationer. Bland annat sades där att personer under 16 år inte kan skaffa e-legitimation samt att det för personer mellan 16 och 18 år kan vara svårt att hitta en utfärdare (sid 18 i angivet särtryck). Datainspektionen har inte fått några signaler om att läget har förändrats väsentligt i detta avseende.

Datainspektionen anser att känsliga personuppgifter endast får lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som asymmetrisk kryptering (till exempel e-legitimation), engångslösenord eller motsvarande. Dessutom ska känsliga personuppgifter vara krypterade vid överföring.

Pliktverkets e-tjänst kan anses vara starkt autentiserad gentemot användarna eftersom identiteten för e-tjänstens webbsida säkerställts med ett certifikat som är signerat av en ackrediterad organisation (se också nedan under rubriken "IT-säkerheten i övrigt").

E-tjänsten innebär en omfattande behandling av känsliga personuppgifter enligt PuL:s definition, i form av uppgifter som rör hälsa.

För autentisering av användarna är det mot bakgrund av det ovan sagda alltså inte tillräckligt att enbart med användarnamn i form av personnummer och lösenord i form av en pinkod autentisera användarna då de ansluter till lämplighetsundersökningen via Internet om nuvarande funktionalitet i e-tjänsten ska bestå (jfr vår bedömning nedan under rubriken "Åtkomst till lämnade svar efter avbrutet ifyllande"). Vi anser att nuvarande autentiseringslösning

kan användas för inhämtandet av personuppgifter under förutsättning att användarna inte kan se tidigare ifyllda uppgifter.

Den autentiseringslösning som nu finns är alltså inte tillfredsställande sett ur ett integritetsskyddsperspektiv. Det är dock, som verket själv har påtalat, förknäat med svårigheter att införa e-legitimation. Detta bekräftas av uttalandet i Vervas rapport.

Om utredningskommitténs förslag om åldergränsen 18 år genomförs, hamnar saken i ett helt annat läge. Då öppnar sig markant större möjligheter för Pliktverket att införa e-legitimation som autentisering för e-tjänsten. Det finns dock risk för att det tar tid för förslagen att realiseras. Under denna mellanperiod måste lämplighetsundersökningen kunna fungera med ett tillfredsställande integritetsskydd.

Det finns andra autentiseringsmetoder för användarna som skulle kunna vara aktuella istället för e-legitimation. Dessa skulle kunna verka var och en för sig eller som alternativ till varandra. Olika användare skulle alltså kunna använda olika autentiseringsmetoder beroende på den enskildes förutsättningar. Dessutom skulle de olika autentiseringsmetoderna kunna medge användarna olika grad av åtkomst till personuppgifter i lämplighetsundersökningen. Exempelvis skulle en användare som bara autentiserar sig med en pinkod inte kunna se tidigare ifyllda svar i e-tjänsten.

För de användare som har möjlighet att använda en starkare autentiseringsmetod (exempelvis e-legitimation eller motsvarande) skulle alltså tidigare ifylld information kunna visas vid återinloggning.

Om det inte anses möjligt att införa alternativa, starkare, autentiseringsmetoder för inloggning till e-tjänsten, anser vi att användarnas åtkomst via Internet ska begränsas till enbart uppgifter som varken är känsliga enligt 13 § PuL eller på annat sätt integritetskänsliga.

Pliktverket ska mot bakgrund av det sagda därför föreläggas att komma in med en åtgärdsplan där verket redogör för de förändringar, och därtill knutna förstärkningar av integritetsskyddet, som verket är berett att genomföra ifråga om autentiseringen till e-tjänsten.

Åtgärdsplanen ska också innehålla en uppskattning av när de föreslagna åtgärderna kan vara genomförda.

Åtkomst till lämnade svar efter avbrutet ifyllande

Användaren kan avbryta ifyllandet av uppgifter och återuppta detta vid ett senare tillfälle. De ifyllda uppgifterna ligger kvar i e-tjänsten och är synliga för användaren efter inloggning. Användare kan logga in i e-tjänsten och ta del av och lämna uppgifter även efter signering. Ändringar kan göras efter signering med hjälp av signeringskoden. I samband med signering flyttas svaren över i form av ett pdf-dokument. Om en användare efter signering går in igen, ändrar uppgifter och sedan signerar så genereras ett nytt pdf-dokument. Detta går att göra ända fram till det att tjänsten stängs för året. I princip kan uppgifterna vara åtkomliga för användaren i upp emot ett år.

Pliktverket har övervägt att ändra tjänsten så att en gång ifyllda uppgifter inte ligger synliga vid nästa inloggning, men anser att användarvänligheten för de som fyller i lämplighetsundersökningen ökar drastiskt då användaren kan fortsätta att fylla i frågeformuläret utan att behöva börja om från början. Det är endast den enskilde som ser sina egna svar.

Det första året som tjänsten användes gick det inte att komma åt och ändra uppgifterna efter signering. Detta har Pliktverket modifierat i de senare versionerna för att förbättra för den enskilde och för sina handläggare. Pliktverket har uppgett att det är ett smidigt sätt för användaren att kunna låsa upp sin enkät själv och ändra felaktiga uppgifter eller göra kompletteringar för att därefter återigen signera lämplighetsundersökningen. Varje signerad enkät är en inkommen handling som sparas och kan vid behov tas fram av verkets handläggare. När Pliktverket stänger tjänsten är enkäten låst och beslut fattas därefter med ledning av den sista enkäten som lämnats.

Pliktverket är medvetet om risken att obehöriga använder e-tjänsten i fråga, bland annat för att lämna felaktiga uppgifter. Pliktverket anser dock att risken för att detta skulle passera oupptäckt är mycket liten, eftersom användaren i slutänden alltid får ett skriftligt beslut med besked om eventuell mönstring. Om en användare får ett beslut om mönstring och inte varit inne i e-tjänsten tar användaren kontakt och förhållandet fångas upp den vägen. Pliktverket har hittills inte fått några indikationer på att någon obehörigen lämnat eller tillskansat sig uppgifter som lämnats i e-tjänsten.

Datainspektionens bedömning

Hantering av personuppgifter i lämplighetsundersökningen innebär en omfattande överföring och lagring av dels känsliga personuppgifter enligt PuL, dels uppgifter som sammantaget kan betraktas som mycket integritetskänsliga. Det måste därför betraktas som en mycket stor integritetskränkning om personuppgifterna hamnar i fel händer, exempelvis om en annan person

än användaren loggar in i lämplighetsundersökningen med användarens inloggningssuppgifter.

Om nuvarande funktionalitet ska bestå utan en tillfredsställande autentiseringslösning anser vi, som ovan sagts, att användarnas åtkomst via Internet ska begränsas till enbart uppgifter som varken är känsliga enligt 13 § PuL eller på annat sätt integritetskänsliga.

Pliktverket har anfört att användarvänligheten för de som fyller i lämplighetsundersökningen drastiskt ökar då användaren kan fortsätta att fylla i frågeformuläret utan att behöva börja om från början. Detta ska naturligtvis inte underskattas och utgör från Pliktverkets perspektiv en viktig komponent. Om en användare inte finner en e-tjänst lättanvänd lämnar hon eller han sannolikt tjänsten. Å andra sidan kan det också hävdas att användare kan komma lämna en tjänst om hon eller han ser integritetsrisker med den.

Att ifyllda uppgifter är fullt synliga för en användare som loggar in igen, med den pinkod som skickats ut, är inte acceptabelt ur ett integritetsskydds perspektiv. Vi anser att en användare, som loggar ut ur e-tjänsten, inte ska kunna ta del av ifyllda uppgifter igen vid inloggning annat än om hon eller han använder sig av en stark autentiseringsmetod såsom e-legitimation eller motsvarande. Med en alternativ funktionalitet skulle de redan ifyllda uppgifterna vid återinloggning exempelvis kunna maskeras så att användare som inte använt en stark autentiseringsmetod ser att uppgifterna är ifyllda men inte kan se innehållet i svaren.

När en användare väl signerat sin lämplighetsundersökning anser vi att proceduren ska vara avslutad. Om en användare efter signering anser sig behöva ändra sina svar bör Pliktverket ha informerat denne om att hon eller han kan kontakta verket för att få genomgå lämplighetsundersökningen igen. Då bör nya autentiserings- och signeringsuppgifter skickas ut.

Mot bakgrund av vad som anförts ovan ska därför Pliktverket föreläggas att komma in med en åtgärdsplan där verket redogör för vilka åtgärder man är berett att vidta för att hindra att obehöriga kan ta del av redan ifyllda uppgifter i lämplighetsundersökningen.

Åtgärdsplanen ska också innehålla en uppskattning av när de föreslagna åtgärderna kan vara genomförda.

IT-säkerheten i övrigt

Pliktverket uppger att identiteten för e-tjänstens webbsida säkerställs med ett certifikat som är signerat av en ackrediterad organisation. Dataöverföringen mellan e-tjänstens webbplats och användarens webbläsare är skyddad med SSL/TLS. Användaren loggas ut automatiskt från e-tjänsten efter viss tid. Denna tid är justerbar.

Datainspektionens bedömning

Vi har inga synpunkter under denna punkt.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skriften vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Britt-Marie Wester, IT-säkerhetsspecialisten Mikael Ejner samt juristen Lars Söderberg, föredragande.

Göran Gräslund

Lars Söderberg