Pensionsmyndigheten
Box 38 190
100 64 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204)- Pensionsmyndighetens webbtjänst Dina Pensionssidor

Datainspektionens beslut

Datainspektionen konstaterar att det föreligger brister när det gäller it-säkerheten när Pensionsmyndigheten ger enskilda tillgång till integritetskänsliga personuppgifter via tjänsten Dina Pensionssidor efter autentisering med enbart personlig kod.

Datainspektionen förelägger Pensionsmyndigheten enligt 45 § första stycket personuppgiftslagen att vidta åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter om fondval i tjänsten samt uppgifter som ger en samlad bild av en enskilds hela pension, det vill säga personens allmänna pension, tjänstepension och privata pension i tjänsten Dina Pensionssidor, genom att införa stark autentisering.

Datainspektionen förutsätter att Pensionsmyndigheten gör en bedömning av vilka säkerhetsåtgärder som bör vidtas för att skydda övriga uppgifter som avser uppgifter om enskildas personliga ekonomiska förhållanden i Pensionsmyndighetens tjänst Dina Pensionssidor. Vid bedömningen av vilken säkerhetsnivå som är lämplig ska Pensionsmyndigheten utgå från känsligheten på de olika uppgifterna, riskerna med behandlingen, de tekniska möjligheter som finns samt kostnaderna för att genomföra de olika säkerhetsåtgärderna.

Redogörelse för tillsynsärendet

Datainspektionen har inlett tillsyn mot Pensionsmyndigheten i syfte att granska Pensionsmyndighetens webbaserade tjänst Dina pensionssidor och hur den förhåller sig till kraven på säkerhetsåtgärder i gällande dataskyddslagstiftning.

Tjänsten Dina pensionssidor använder idag två sätt att säkerställa användarens identitet vid inloggning till tjänsten, antingen sker det via e-legitimation eller personlig kod. En del funktioner i tjänsten är tillgängliga endast efter inloggning med e-legitimation, såsom exempelvis byte av fond, byte från fondförsäkring till traditionell försäkring, val av efterlevandeskydd och ändring av utbetalningskonto.

De uppgifter och funktioner som är tillgängliga vid inloggning med personlig kod för enskilda är följande:

- Den enskildes intjänade allmänna pension, både inkomstpension och premiepension
- Den enskildes digitala Orange kuvert
- Den enskildes utbetalningar
- Den enskildes efterlevandekonto
- Den enskildes premiepensionskonto med fondinformation och värdeförändring
- Den enskilde kan göra en pensionsprognos för hela sin pension baserat både på sin allmänna pension, tjänstepension och privata pension.
- Den enskilde kan beräkna för uttag av premiepensionen
- Den enskilde kan byta personlig kod
- Den enskilde kan avbeställa brevutskick av det Orange kuvertet
- Den enskilde kan ta del av sina kontaktuppgifter

Pensionsmyndigheten har uppgett följande. Myndigheten har valt att tillåta identifiering med hjälp av personlig kod främst för att möjliggöra för dem som av olika anledningar inte kan få någon e-legitimation, men även för att möjliggöra identifiering för användare som av olika anledningar inte har möjlighet att anpassa sig till ny teknik. Pensionsmyndigheten anser att inloggning med personlig kod är en tillräckligt säker inloggning med

beaktande av risken för integritetsintrång eller annan skada i enlighet med 111 kap. 6 § socialförsäkringsbalken. Den bedömningen gör Pensionsmyndigheten med hänsyn dels till de uppgifter användarna kan få tillgång till, dels till hur koden hanteras. Användaren kan vid inloggning med den personliga koden endast ta del av information, medan däremot förändringar som på något sätt påverkar pensionen kräver e-legitimation. Pensionsmyndigheten har även hänvisat till ett beslut från Justitiekanslern (JK) (2003-02-21, dnr 1980-02-42) rörande att skadeståndsanspråk enligt 48 § personuppgiftslagen som riktats mot staten med anledning av att personuppgifter (bekräftelse på hur premiepensionsmedel hade placerats) hade sänts i ett kuvert som inte varit förslutet. JK ansåg att någon rätt till kränkningsersättning inte förelåg, med beaktande av uppgifternas art och den begränsade risken för spridning av uppgifterna.

Pensionsmyndigheten har också hänvisat till lagstiftarens uttalande i förarbetena till aktuella bestämmelser i socialförsäkringsbalken där det anges att det ankommer på de aktuella myndigheterna att avgöra och precisera vilka former för identifiering som ska tillämpas (prop 2003/04:40 s. 33 f). Vidare har Pensionsmyndigheten angett att Prognos till alla är en flerårig satsning för att öka antalet användare av pensionsprognostjänsten minpension.se. Det är den tjänst som används när pensionsspararen på Dina pensionssidor gör en prognos för hela den framtida pensionen. Myndigheten har anfört att en eventuell avveckling av den personliga koden inte är realistisk under de närmsta åren beroende på Prognos till alla som pågår fram till och med 2017.

Skäl för beslutet

Tillämpliga bestämmelser och Datainspektionens tillämpning

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad de skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är. 31 § personuppgiftslagen är en implementering av artikel 17 i dataskyddsdirektivet 95/46/EG och paragrafen ska enligt författningskommentaren ha samma innebörd som artikeln (prop 1997/98:44 s. 136).

Vid behandling av personuppgifter i Pensionsmyndighetens självbetjäningstjänster gäller utöver 31 § personuppgiftslagen också 111 kap. 5 och 6 §§ socialförsäkringsbalken. Bestämmelser i socialförsäkringsbalken är enligt dess förarbeten en precisering av bestämmelsen i 31 § personuppgiftslagen. [1] Enligt 111 kap. 5 § socialförsäkringsbalken ska en enskild som lämnar uppgifter i samband med att han eller hon använder en självbetjäningstjänst använda en sådan elektronisk signatur som avses i lagen (2000:832) om kvalificerade elektroniska signaturer. Vid tillgång till personuppgifter ska certifikat till vilken en säker identifieringsmetod är knuten användas för kontroll av användarens identitet. Denna identifieringsmetod avser en form av stark autentisering. Stark autentisering, också kallad flerfaktorsautentisering, kan realiseras på olika sätt. Det kan ske exempelvis med e-legitimation, men även andra tekniska funktioner för asymmetrisk kryptering samt vissa lösningar för engångslösenord och liknande kan användas.

Enligt Datainspektionens allmänna råd är uppgifter om enskilds personliga och ekonomiska förhållanden inom bankväsendet normalt att anse som integritetskänsliga. Ett uttryck för att det är fråga om integritetskänsliga uppgifter kan vidare vara att uppgifterna omfattas av sekretess för uppgifter om enskilda enligt Offentlighet och sekretesslagen (2009:400). Datainspektionen har i sin tillämpning av 31 § personuppgiftslagen tidigare krävt att integritetskänsliga personuppgifter får lämnas ut via öppet nät, endast till identifierade användare vars identitet är säkerställd med stark autentisering. Datainspektionen har ansett att uppgift om tillgångar, sparande och skulder samt försäkringsinnehav utgjort integritetskänsliga uppgifter för vilket kravet på stark autentisering gäller (se Datainspektionens beslut dnr 634-2012, 653-2012 och 654-2012) enligt 31 § personuppgiftslagen. Liksaså har Datainspektionen i sin tidigare praxis ansett att uppgifter som omfattas av sekretess är integritetskänsliga och krävt stark autentisering vid utlämnande över öppet nät (se Datainspektionens beslut dnr 401-2013).

Av 28 kap. 5 § offentlighets- och sekretesslagen (2009:400) framgår att sekretess gäller för uppgift om hur premiepensionsmedel har placerats för en enskilds räkning hos Pensionsmyndigheten om det inte står klart att uppgiften kan röjas utan att den enskilde lider men. Det råder alltså

[1] Se prop 2003/04:40 s. 33

presumtion för sekretess. I samband med att aktuell sekretessbestämmelse infördes framfördes att vissa personer skulle uppleva det som ett allvarligt intrång i deras personliga integritet om uppgifter om hur premiepensionsmedel har placerats skulle lämnas ut (SOU 1997:131, s. 124 f.). Det framfördes att vissa personer skulle kanske till och med påverkas i sitt val av fonder om de visste att uppgifterna kunde lämnas ut.

För uppgifter om en persons tillgodohavande på pensionskontot samt storlek på pensionen kom utredningen dock fram till att det inte fanns tillräckligt vägande skäl för att föreslå en annan ordning än den som då rådde, nämligen sekretess med rakt skaderekvisit. För uppgift om vad en pensionssparare bestämt om efterlevandeskyddet i premiepensionen råder absolut sekretess. På Dina Pensionssidor visas information om den registrerade har ett så kallat efterlevandekonto. Information om vad en person bestämt om efterlevandeskyddet där det råder stark sekretess är dock inte tillgängligt via Dina Pensionssidor.

I 111 kap. 6 § socialförsäkringsbalken anges att om någon annan metod för identifiering eller skydd mot förvanskning av uppgifter finns och den är tillräcklig säker med hänsyn till risken för integritetsintrång eller annan skada får den användas.

Pensionsmyndigheten har med stöd av förordning (2009:1175) med vissa bemyndiganden för Pensionsmyndigheten föreskrivit att det för att få tillgång till personuppgifter krävs användande av personlig kod som utgetts av Pensionsmyndigheten eller användning av e-legitimation (PFS 2013:2).

Vilket krav på säkerhet ska ställas på Pensionsmyndighetens tillhandahållande av personuppgifter via Dina Pensionssidor?

Pensionsmyndigheten har hänvisat till ett JK-beslut där frågan var huruvida det var en kränkning av den enskildes personliga integritet att skicka information om hur pensionsmedel placerats i ett fysiskt brev som inte varit förslutet (2003-02-21, dnr 1980-02-42). Känsligheten hos uppgifterna i JK-ärendet kan jämföras med de uppgifter som är föremål för prövning i aktuell tillsyn. Tillgängliggörande av uppgifter i tjänsten Dina Pensionssidor innefattar dock automatiserad behandling av personuppgifter via Internet. När uppgifter behandlas digitalt ökar möjligheterna att sammanställa, kartlägga och sprida uppgifter om enskildas personliga förhållanden. Det medför i sin tur ökade risker för intrång i enskildas personliga integritet.

Skyddet mot integritetskränkningar vid automatiserad behandling av personuppgifter har på grund av de risker som finns inom EU ansetts kräva särskild reglering vilket åstadkoms genom EU:s dataskyddsdirektiv. JK:s beslut avseende en försändelse, i ett kuvert kan inte appliceras på den digitala hantering som är aktuell i detta ärende.

Pensionsmyndigheten har genom bemyndigande föreskrivit att det för att få tillgång till personuppgifter krävs användande av personlig kod som utgetts av Pensionsmyndigheten eller användning av e-legitimation. Föreskrifterna är meddelade i behörig ordning. I förarbetena till bestämmelserna i socialförsäkringsbalken uttalar lagstiftaren att andra enklare former för identitetskontroll, såsom pinkod, är godtagbar i de fall risken för skada vid obehörigt intrång eller andra förfaranden är liten.

Dataskyddsbestämmelserna är inte bara en nationell fråga. Bestämmelserna finns för att skydda en grundläggande mänsklig rättighet. Denna rättighet har EU skyddat genom reglering i dataskyddsdirektivet 95/46/EG. I direktivet finns krav på att medlemsstaterna ska förskriva att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter. Medlemstaterna kan inte förskriva en lägre nivå av säkerhet för personuppgifterna än vad som stadgas i dataskyddsdirektivet. I förarbetena till socialförsäkringsbalken uppges att bestämmelserna i 111 kap 5 och 6 §§ socialförsäkringsbalken är en precisering av 31 § personuppgiftslagen vilket får som konsekvens att Pensionsmyndighetens säkerhetsåtgärder måste uppfylla såväl kraven i socialförsäkringsbalken som personuppgiftslagen. Mot den bakgrunden prövar Datainspektionen om Pensionsmyndighetens vidtagna säkerhetsåtgärder är tillräckliga.

I dataskyddsdirektivet 95/46/EG utrycks att överföring av uppgifter i ett nätverk (läs Internet) som en särskild risk i sig. Datainspektionen konstaterar att autentisering med enbart lösenord (i det här fallet personlig kod) medför en högre risk för dataintrång än om man utöver lösenord använder sig av något ytterligare autentiseringshjälpmedel.

Datainspektionen konstaterar att uppgifter om enskildas personliga ekonomi är tillgängliga i Pensionsmyndighetens tjänst Dina pensionssidor med inloggning enbart med pinkod. Av dessa uppgifter omfattas vissa uppgifter av stark sekretess, såsom uppgift om fondval. Datainspektionen konstaterar att

uppgifter som rör den enskildes personliga förhållanden och som omfattas av stark sekretess utgör så pass integritetskänsliga uppgifter att det krävs stark autentisering om uppgifterna är tillgängliga över öppet nät.

Vidare är det möjligt att genom Dina Pensionssidor få tillgång till en pensionsprognos gjord av minpension.se som omfattar en persons hela pension, det vill säga personens allmänna pension, tjänstepension och privata pension. I denna samlade bild inkluderas personuppgifter från banker som omfattas av banksekretess. Uppgifter kan även komma från andra aktörer där som regel avtalsförhållande mellan den enskilde och den aktuella aktören hindrar ett utlämnande av personuppgifter om den enskilde spararen till någon annan än spararen själv.

Datainspektionens bedömning är att även de uppgifter som hämtas genom minpension.se som omfattar en samlad bild av en enskilds hela pension utgör så pass integritetskänsliga uppgifter att autentisering med enbart personlig kod inte är tillräcklig.

Datainspektionen förelägger Pensionsmyndigheten enligt 45 § första stycket personuppgiftslagen att vidta åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter om fondval i tjänsten samt uppgifter som ger en samlad bild av en enskilds hela pension, det vill säga personens allmänna pension, tjänstepension och privata pension i tjänsten Dina Pensionssidor, genom att införa stark autentisering.

Även övriga uppgifter som behandlas i Pensionsmyndighetens tjänst Dina Pensionssidor som avser uppgifter om enskildas personliga ekonomiska förhållanden kan omfattas av sekretess, vilket indikerar att uppgifterna har en integritetskänslighet som kräver en högre säkerhetsnivå än autentisering med enbart personlig kod. Pensionsmyndigheten har anfört att det är väsentligt att de här uppgifterna är lättåtkomliga för många. Vid bedömningen av vilken säkerhetsnivå som är lämplig ska emellertid Pensionsmyndigheten utgå från känsligheten på de olika uppgifterna, riskerna med behandlingen, de tekniska möjligheter som finns samt kostnaderna för att genomföra de olika säkerhetsåtgärderna. Datainspektionen förutsätter att Pensionsmyndigheten gör en bedömning av vilka säkerhetsåtgärder som bör vidtas för att skydda övriga personuppgifter utifrån ovanstående kriterier. Särskild hänsyn bör tas till de risker som finns vid tillgängliggörande av personuppgifter via Internet.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av juristen Ulrika Bergström.

Katarina Tullstedt

Ulrika Bergström