Bisnode Kredit AB
169 93 Solna

Tillsyn enligt personuppgiftslagen (1998:204) – Autentisering av användare som medges åtkomst till personuppgifter i kredit-upplysningsregister

Datainspektionens beslut

Datainspektionen konstaterar att Bisnode Kredit AB behandlar personuppgifter i strid med 31 § personuppgiftslagen (1998:204) genom att Bisnode Kredit AB saknar nödvändig kontroll över vem som står bakom registrering av den mobila enhet som registreras för användning av autentiseringsmetoden Bisnode Secure App.

Datainspektionen förelägger Bisnode Kredit AB att vidta sådana åtgärder att registreringsförfarandet innebär att Bisnode Secure App endast kan knytas till en behörig användare eller upphöra med att medge åtkomst till kopiepliktig kreditupplysningsinformation via en webbplats efter autentisering med autentiseringsmetoden Bisnode Secure App.

Datainspektionen konstaterar att Bisnode Kredit AB vid användning av autentiseringsmetoderna SMS med kod och SMS med länk behandlar personuppgifter i strid med 31 § personuppgiftslagen genom att Bisnode Kredit AB saknar nödvändig kontroll över vem som står bakom registrering av ett telefonnummer till ett BisnodeID.

Datainspektionen förelägger Bisnode Kredit AB att vidta sådana åtgärder vid registreringen så att ett BisnodeID endast kan kopplas till ett av Bisnode Kredit AB i förväg känt telefonnummer eller upphöra med att medge åtkomst till kopiepliktig kreditupplysningsinformation via en webbplats efter autentisering med autentiseringsmetoderna SMS med kod och SMS med länk.

Datainspektionen konstaterar att Bisnode Kredit AB behandlar personuppgifter i strid med 31 § personuppgiftslagen (1998:204) genom att Bisnode Kredit AB genom att medge åtkomst till kopiepliktig kreditupplysningsinformation via en webbplats efter autentisering med användarnamn och lösenord som kompletterats med tillgången till en webblänk som skickats via oskyddad e-post.

Datainspektionen förelägger Bisnode Kredit AB att upphöra att medge åtkomst till kopiepliktig kreditupplysningsinformation via en webbplats efter autentisering med användarnamn och lösenord som kompletterats med tillgången till en webblänk som skickats via oskyddad e-post.

Datainspektionen avslutar ärendet med de rekommendationer som finns på sidan nio.

Redogörelse för tillsynsärendet

Datainspektionen har inlett tillsyn mot Bisnode Kredit AB (härefter Bisnode) i syfte att följa upp Datainspektionens beslut i ärende dnr 1823-2010. Bisnode har i ärendet svarat på skriftliga frågor om och förevisat fyra autentiseringsmetoder som Bisnode använder för att säkerställa identiteten hos användare innan Bisnode medger dem åtkomst till personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt 11 § kreditupplysningslagen (1974:1173). De fyra autentiseringsmetoderna är Bisnode Secure App, SMS med kod, SMS med länk och e-post med länk.

Tillsynsfrågan rör om Bisnode med dessa metoder vidtar lämpliga åtgärder för att uppnå en lämplig säkerhetsnivå enligt 31 § personuppgiftslagen (1998:204) till skydd för personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt 11 § kreditupplysningslagen när Bisnode medger användare åtkomst till sådana personuppgifter via Internet.

Skäl för beslutet

Tillämpliga bestämmelser

Den personuppgiftsansvarige, här Bisnode, ska enligt 31 § personuppgiftslagen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna, och hur pass känsliga de behandlade personuppgifterna är.

Bestämmelsen ska enligt förarbetena till personuppgiftslagen (prop. 1997/98:44, sid. 135) ha samma innebörd som artikel 17.1 och 17.2 i dataskyddsdirektivet (95/46/EG) som förtydligar att åtgärderna ska skydda personuppgifterna från bland annat otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk.

Allmänna utgångspunkter för Datainspektionens bedömningar

Autentisering är en åtgärd för att verifiera en uppgiven identitet. Åtgärden vidtas som ett led i att tillse att endast behöriga användare får åtkomst till personuppgifter. Eftersom det här är fråga om åtkomst till integritetskänsliga personuppgifter (kreditupplysningsinformation) över öppet nät (Internet) räcker inte autentisering med endast användarnamn och lösenord som autentiseringshjälpmedel för att uppnå en lämplig säkerhetsnivå, se beslut i Datainspektionens tidigare ärende dnr 1823-2010.

Olika autentiseringsmetoder har olika egenskaper som i sin tur är förknippade med olika risker. Den personuppgiftsansvarige ska beakta sådana risker vid en lämplighetsbedömning enligt 31 § personuppgiftslagen. Det gäller särskilt risken för att en obehörig användare identifierar sig som en behörig användare och sedan felaktigt blir verifierad som en behörig användare så att den personuppgiftsansvarige därför medger den obehörige användaren åtkomst till personuppgifter. Det gäller även sådana risker som ligger utanför den personuppgiftsansvariges kontroll.

Oavsett vilken säkerhetsnivå en autentiseringsmetod kan ge får de organisatoriska åtgärderna kring metoden, till exempel registreringen av

användare och användaruppgifter, inte utgöra en svag länk eftersom det kan få till följd att en lämplig säkerhetsnivå inte uppnås.

Uppnår Bisnode en lämplig säkerhetsnivå med Bisnode Secure App?

Bisnode har i huvudsak uppgett följande om autentiseringsmetoden Bisnode Secure App.

För åtkomst till Bisnodes webbtjänster krävs först och främst att användaren har ett så kallat BisnodeID. Ett BisnodeID består av användarens användarnamn (som utgörs av en e-postadress) och ett tillhörande lösenord. Det finns krav på hur lösenordet ska vara utformat. Användaren väljer själv ett lösenord som uppfyller dessa krav.

För att Bisnode i ett andra steg, efter användarens inloggning till webbplatsen med sitt BisnodeID, ska medge användaren åtkomst till personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt 11 § kreditupplysningslagen kräver Bisnode en ytterligare autentisering av användaren med någon av de i ärendet förevisade fyra autentiseringsmetoderna. Användaren kan då välja att registrera sig för användning av autentiseringsmetoden Bisnode Secure App.

För att en användare ska kunna använda sig av den ytterligare autentiseringsmetoden Bisnode Secure App behöver användaren ladda ner appen till en mobil enhet som han eller hon själv väljer och registrera den till sitt BisnodeID. Registreringsförfarandet inleds med att ett e-postmeddelande skickas till den e-postadress som utgör användarens användarnamn i dennes BisnodeID. E-postmeddelandet innehåller en webblänk som användaren ska aktivera (klicka på) inom en viss tid. Användaren kan välja att registrera flera mobila enheter för användning av Bisnode Secure App.

Registreringsförfarandet innebär att appen på den mobila enheten förses med en identifierande kod avsedd att identifiera den mobila enheten samt en särskild kod (seed) från en säkerhetsserver. Den särskilda koden lagras, krypterat med en tillfällig nyckel som säkerhetsservern tillhandahåller, på en särskild, skyddad del av den mobila enhetens lagringsminne. Den tillfälliga nyckeln lagras inte på den mobila enheten. Användaren måste också välja en PIN-kod för användning av appen. Om den mobila enheten stödjer användning av fingeravtryck kan användaren använda det istället fin en PIN-kod.

Vid autentisering med Bisnode Secure App skickar säkerhetsservern den tillfälliga nyckel som behövs för att dekryptera den särskilda koden till den mobila enheten. Den särskilda koden dekrypteras och används tillsammans med användarens valda PIN-kod (eller fingeravtryck) för att generera en autentiseringsnyckel. Användarens PIN-kod (eller fingeravtryck) lagras varken på den mobila enheten eller på säkerhetsservern. Autentiseringsnyckeln finns sedan registreringsförfarandet lagrad på säkerhetsservern.
Autentiseringen sker genom ett så kallat handskakningsprotokoll (challenge-response) mellan appen i användarens mobila enhet och säkerhetsservern. Appen använder autentiseringsnyckeln för att kryptera en förfrågan (challenge) från servern. Appen skickar sedan tillbaka ett svar (response) till säkerhetsservern som består av resultatet av krypteringen. Servern dekrypterar sedan svaret med hjälp av den där, sedan registreringsförfarandet, lagrade autentiseringsnyckeln. Om svaret från den mobila enheten är det förväntade, det vill säga att den på säkerhetsservern lagrade autentiseringsnyckeln kan användas för att korrekt dekryptera svaret från appen, anser Bisnode den ytterligare autentiseringen framgångsrikt genomförd.

Den tillfälliga nyckel som krypterar den särskilda koden för lagring i den mobila enheten byts ut vid varje autentiseringstillfälle.

Datainspektionens bedömning
Datainspektionen bedömer att det finns brister i det registreringsförfarande som föregår Bisnodes användning av Bisnode Secure App.

Registreringen av en mobil enhet för användning av Bisnode Secure App bygger på kännedom om en användares BisnodeID (användarnamn och lösenord) och åtkomst till den användarens e-postkonto. Åtkomst till ett e-postkonto omgärdas normalt sett inte av en hög nivå av säkerhet. Den idag helt dominerande autentiseringslösning som används för åtkomst till e-post är användarnamn och lösenord. Användarnamn och lösenord ger en låg nivå av säkerhet vilket innebär att Bisnode inte kan säkerställa att uppgifterna som lämnas vid registreringen av en mobil enhet lämnas av den behörige användaren. Genom att registreringen av en mobil enhet är möjlig utifrån kännedom om en användares användarnamn och lösenord uppnår Bisnode därmed inte den höga nivå av säkerhet som autentiseringsmetoden är avsedd

att uppnå. Detta i kombination med att Bisnode dels tillåter användarna att själva registrera vilka mobila enheter de vill utan att Bisnode vet att innehavaren av den mobila enheten verkligen är den behörige användaren och dels att de samtidigt kan vara registrerade för olika autentiseringsmetoder innebär enligt Datainspektionens uppfattning att risken för obehörig åtkomst ökar och att möjligheten att upptäcka och förebygga obehörig åtkomst minskar på ett sätt som innebär att Bisnode inte uppnår en lämplig säkerhetsnivå enligt 31 § personuppgiftslagen.

För att komma till rätta med bristen behöver Bisnode skaffa sig nödvändig kontroll över vem som står bakom registrering av den mobila enhet som registreras för användning av autentiseringsmetoden Bisnode Secure App.

Bisnode ska därför föreläggas att vidta sådana åtgärder vid registreringsförfarandet som innebär att Bisnode Secure App endast kan knytas till en behörig användare.

Det kan ske genom att ersätta e-postmeddelandet vid registreringsförfarandet med ett SMS till ett av Bisnode i förväg känt telefonnummer.

Uppnår Bisnode en lämplig säkerhetsnivå med SMS med kod eller SMS med länk?

Bisnode har i huvudsak uppgett följande om autentiseringsmetoderna SMS med kod och SMS med länk.

För åtkomst till Bisnodes webbtjänster krävs först och främst att användaren har ett BisnodeID.

För att Bisnode i ett andra steg, efter användarens inloggning till webbplatsen med sitt BisnodeID, ska medge användaren åtkomst till personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt 11 § kreditupplysningslagen kräver Bisnode en ytterligare autentisering av användaren. Annvändaren kan då välja att registrera sig för användning av autentiseringsmetoden SMS med kod eller SMS med länk.

För att en användare ska kunna använda sig av autentiseringsmetoden SMS med kod eller SMS med länk behöver användaren registrera ett telefonnummer till sitt BisnodeID. Registreringsförfarandet inleds med att ett e-postmeddelande skickas till den e-postadress som utgör användarens

användarnamn i hans eller hennes BisnodeID. E-postmeddelandet innehåller en webblänk som användaren ska aktivera (klicka på) inom en viss tid. Användaren uppger därefter ett telefonnummer på webbplatsen varpå ett SMS-meddelande med en aktiveringskod skickas till det telefonnumret. Användaren ska sedan skriva in aktiveringskoden på webbplatsen inom en viss tid och om aktiveringskoden stämmer överens med den som skickades via SMS registreras telefonnumret för användning av den valda autentiseringsmetoden till användarens BisnodeID.

Vid autentisering med autentiseringsmetoden via SMS med kod skickas ett SMS med en engångskod till det registrerade telefonnumret vid varje autentiseringstillfälle och om användaren manuellt skriver in engångskoden på webbplatsen inom en viss tid anser Bisnode den ytterligare autentiseringen framgångsrikt genomförd.

Vid autentisering via SMS med länk skickas ett SMS med en webblänk till det registrerade telefonnumret och om användaren klickar på webblänken inom en viss tid anser Bisnode den ytterligare autentiseringen framgångsrikt genomförd.

Utgångspunkter för Datainspektionens bedömning
Den teoretiska utgångspunkten för att autentiseringslösningar som använder sig av SMS-meddelanden ska uppnå en högre nivå av säkerhet än användarnamn och lösenord är att användaren har ett fysiskt SIM-kort registrerat till sin person och att SMS-meddelandena, som utgör autentiseringshjälpmedlen, enbart kan läsas i den mobila enhet, till exempel en mobiltelefon, som SIM-kortet sitter i och det endast av den registrerade användaren.

Det finns ett flertal risker med autentiseringslösningar som använder sig av SMS-meddelanden som autentiseringshjälpmedel. SMS-meddelanden kan komma på avvägar av tekniska skäl, genom till exempel avlyssning eller omdirigering, eller genom att någon ser meddelandet på eller bereder sig tillgång till meddelandet i den registrerade mobila enheten. Många mobila enheter visar till exempel början av ett SMS utan att det behövs en PIN-kod för att låsa upp enheten. Det finns skadlig kod som kan läsa, vidarebefordra och använda SMS-meddelanden för att kringgå den här typen av autentiseringslösningars syfte. Det finns helt mjukvarubaserade telefonitjänster som alltså helt saknar den koppling till ett fysiskt SIM-kort

som autentiseringsmetoden bygger på. Det finns webbtjänster för att kunna ta emot och läsa SMS-meddelanden, även för telefonitjänster som tillhandahålls med SIM-kort. Sådana webbtjänster bygger företrädesvis på autentisering med enbart användarnamn och lösenord. På så sätt skulle ett autentiseringshjälpmedel som är tänkt att åstadkomma en högre nivå av säkerhet bli tillgängligt för en användare på ett sätt som motsvarar en lägre nivå av säkerhet. Det i sin tur är något som inte överensstämmer med syftet att åstadkomma en högre nivå av säkerhet kring frågan om användarens identitet.

Datainspektionens bedömning
Bisnodes användning av autentiseringsmetoderna som bygger på SMS för autentisering av användare innan Bisnode medger användarna åtkomst till personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt 11 § kreditupplysningslagen har enligt Datainspektionen följande brister.

Registreringen av ett telefonnummer för användning av någon av autentiseringsmetoderna som bygger på SMS utgår enbart ifrån kännedom om en användares BisnodeID (användarnamn och lösenord) och åtkomst till den användarens e-postkonto. Åtkomst till ett e-post-konto omgärdas normalt sett inte av en hög nivå av säkerhet. Den idag helt dominerande autentiseringslösning som används för åtkomst till e-postkonton är användarnamn och lösenord. En sådan lösning ger en låg nivå av säkerhet som innebär att Bisnode inte kan säkerställa att de uppgifter som lämnas vid registreringen av telefonnumret lämnas av den behörige användaren.

Genom användning av användarnamn och lösenord är det därmed möjligt att koppla telefonnummer till ett BisnodeID på ett sätt som motsvarar en lägre nivå av säkerhet än vad autentiseringsmetoderna är avsedda att uppnå.

Vidare tillåter Bisnode användarna att själva registrera vilka telefonnummer de vill. Det innebär att användarna kan välja att registrera telefonnummer som är kopplade till eller tillhandahålls genom tjänster som saknar koppling till ett fysiskt SIM-kort eller ger webbåtkomst till sms.

Detta innebär sammantaget enligt Datainspektionens uppfattning att risken för obehörig åtkomst ökar och att möjligheten att upptäcka och förebygga obehörig åtkomst minskar på ett sätt som innebär att Bisnode inte uppnår en lämplig säkerhetsnivå enligt 31 § personuppgiftslagen för de personuppgifter

som ska skyddas. Att användare kan vara registrerade för olika autentiseringsmetoder samtidigt förstärker denna brist ytterligare.

Datainspektionen anser att när SMS används som autentiseringshjälpmedel måste de överföras till användaren på ett sätt som inte komprometterar robustheten eller säkerheten i autentiseringsmetoden, det vill säga att överföringen av och åtkomsten till SMS inte utgör en svag länk som innebär att en lämplig säkerhetsnivå inte uppnås. Den personuppgiftsansvarige behöver därför vidta ytterligare lämpliga åtgärder enligt 31 § personuppgiftslagen för att säkerställa att varken registreringen, överföringen eller användningen av autentiseringsmetoderna utgör en sådan svag länk.

Ett exempel på en sådan åtgärd är att skilda kommunikationskanaler används för åtkomsten till kreditupplysningsuppgifterna respektive överföringen och användningen av SMS:en med autentiseringshjälpmedlen. En sådan åtgärd försvårar möjligheten för en eventuell angripare att komma över både BisnodeID-lösenordet och SMS:et genom att manipulera en enda fysisk enhet eller att avlyssna en enda kommunikationskanal.

Bisnode ska därför föreläggas att vidta sådana åtgärder vid registreringen så att ett Bisnode ID endast kan kopplas till ett av Bisnode i förväg känt telefonnummer.

Övrigt
Datainspektionen rekommenderar Bisnode att vidta åtgärder för att försvåra möjligheten för en eventuell angripare att komma över både BisnodeID-lösenordet och SMS:et genom att manipulera en enda fysisk enhet eller att avlyssna en enda kommunikationskanal.

Uppnår Bisnode en lämplig säkerhetsnivå med e-post med länk?

Bisnode har i huvudsak uppgett följande om autentiseringsmetoden e-post med länk.

För åtkomst till Bisnodes webbtjänster krävs först och främst att användaren har ett BisnodeID.

För att Bisnode i ett andra steg, efter användarens inloggning med sitt BisnodeID, ska medge användaren åtkomst till personuppgifter i kreditupplysningsregister som är kopiepliktiga enligt

11 § kreditupplysningslagen kräver Bisnode en ytterligare autentisering av användaren. Användaren kan då välja att använda sig av autentiseringsmetoden e-post med länk.

För att en användare ska kunna använda sig av autentiseringsmetoden behöver ingen ytterligare registreringsåtgärd vidtas. Vid autentisering med e-post med länk bekräftar användaren tillgång till den sedan tidigare registrerade e-postadressen. Det sker genom att aktivera (klicka på) en webblänk som i samband med autentiseringen skickas i ett e-postmeddelande till den e-postadressen. Om webblänken aktiveras inom en viss tid anser Bisnode den ytterligare autentiseringen farmgångsrikt genomförd.

Datainspektionens bedömning
När en användare väljer att använda metoden e-post med länk för att ta del av kreditupplysningsinformation verifieras användarens identitet genom att denne har kännedom om och kan använda användarens BisnodeID samt har tillgång till användarens registrerade e-postkonto.

Den idag helt dominerande autentiseringslösning som används för åtkomst till e-post är användarnamn och lösenord. Genom en sådan autentisering blir det autentiseringshjälpmedel (e-postmeddelandet med länken) som här är tänkt att åstadkomma en högre nivå av säkerhet än användarnamn och lösenord tillgängligt för användaren efter autentisering med användarnamn och löseord. Det innebär, enligt Datainspektionens mening, att Bisnode genom att tillåta användning av autentiseringsmetoden e-post med länk inte lever upp till kravet på en lämplig säkerhetsnivå enligt 31 § personuppgiftslagen för att skydda åtkomsten till kopiepliktig kreditupplysningsinformation.

Bisnode Kredit AB ska därför föreläggas att upphöra att medge åtkomst till kopiepliktig kreditupplysningsinformation via en webbplats efter autentisering med användarnamn och lösenord som kompletterats med tillgången till en webblänk som skickats via oskyddad e-post.

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 ni fick del av beslutet. 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 generaldirektören Kristina Svahn Starrsjö efter föredragning av avdelningsdirektören Hans Kärnlöf. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Catharina Fernquist och IT-säkerhetsspecialisten Magnus Bergström deltagit.

Kristina Svahn Starrsjö

Hans Kärnlöf

Kopia till: Personuppgiftsombudet, med e-post