

Brevo AB
Stadsgården 6, 6 tr.
116 45 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – Brevo AB

Datainspektionens beslut

- Datainspektionen konstaterar följande:
 1. Brevo AB är personuppgiftsansvarigt för de personuppgifter som Brevo AB behandlar i sitt mottagarregister. Detta gäller även om personuppgiftsbehandlingen utförs av personuppgiftsbiträden för Brevo AB:s räkning.
 2. Samtliga bolag som behandlar eller kan komma att behandla personuppgifter för Brevo AB:s räkning är personuppgiftsbiträden till Brevo AB.
 3. Brevo AB lever inte upp till kraven i 30 § andra stycket och 31 § andra stycket personuppgiftslagen, eftersom Brevo AB inte har kunskap om vilka bolag som behandlar personuppgifterna för dess räkning.
- Datainspektionen förelägger Brevo AB att upprätta personuppgiftsbiträdesavtal som lever upp till kraven i personuppgiftslagen.
- Datainspektionen förelägger Brevo AB att se till att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av de personuppgifter som behandlas inom Brevo AB eller för Brevo AB:s räkning hos Microsoft.

Datainspektionen avser att följa upp beslutet.

Redogörelse för tillsynsärendet

I januari 2011 påbörjade Datainspektionen ett tillsynsprojekt för att undersöka olika personuppgiftsansvarigas användning av molntjänster. Syftet med projektet har varit att kontrollera om personuppgiftslagens bestämmelser följs då molntjänster används för att behandla personuppgifter och att sprida kunskap

om personuppgiftslagen och dess krav. I projektet har tre inspektioner genomförts, däribland en inspektion hos Brevo AB (fortsättningsvis Brevo).

Inspektionen av Brevo genomfördes den 9 maj 2011. Protokoll över inspektionen har upprättats och översänts till Brevo. Vidare har Brevo inkommit med svar på kompletterande frågor samt med yttrande över protokollet.

Allmänt om tjänsten

Brevo är en digital brevlåda som företag och myndigheter kan använda för att distribuera brev. För att brev ska kunna skickas via Brevo krävs det att både avsändare och mottagare har avtal med/har skapat ett konto hos Brevo. Brevo använder Windows Azure som *plattform as a service* för denna tjänst.

De personuppgifter som Brevo samlar in från och lagrar om privatpersoner (*mottagare*) som använder tjänsten är personnummer, för- och efternamn, e-postadress och, om kunden önskar, mobiltelefonnummer.

Brevo har ansetts sig vara personuppgiftsansvarigt för de personuppgifter som samlas in från mottagare i samband med registrering av tjänsten. Brevo anser sig vara personuppgiftsbiträde åt de *kunder* som använder tjänsten för att distribuera brev, exempelvis UC AB, i de fall tillgänglighöret av brev innebär att personuppgifter behandlas.

Mottagaruppgifterna behandlas i Windows Azure, en av Microsofts molntjänster. Uppgifterna speglas också ner i "Satellite" en server som ligger utanför Microsoft molntjänst.

Kunden som skickar brev med Brevo kan lägga på en "tag" så att mottagaren ombedes att använda e-legitimation för att kunna öppna brevet.

Brevlådan ser ut som en "vanlig inkorg" där det syns vilka brev som är öppnade respektive olästa och där det framgår vem som är avsändare och om det finns bilagor. Mottagaren kan fritt välja att spara eller ta bort inkommen post.

IT-säkerhet

Aktivering av tjänsten

En privatperson som vill bli mottagare av elektroniska brev och använda Brevo kan starta ett konto antingen med en aktiveringskod eller med e-legitimation. Mottagaren kan när som helst avaktivera funktionen för de avsändare som den önskar och därmed återgå till att få fysisk post från avsändaren istället.

Inloggning för användarna i Brevo

När en privatperson loggar in görs detta med användarnamn, personnummer och lösenord. Mottagaren kan själv välja användarnamn och lösenord. Mottagarna måste inte byta lösenord. Den som gör misslyckade inloggningsförsök blir uteläst efter ett visst antal inloggningsförsök.

Brevo möjliggör inte för mottagarna att spara inloggningsuppgifter, utan mottagarna måste logga in varje gång. Detta utesluter inte att det finns sådana inställningar som enskilda kan göra i sina egna browsers. Ny inloggning krävs också efter inaktivitet under viss tid.

Inloggning för administratörer i Brevo

Vid inloggning för administratörer används Live-id. Det är samma sorts id som används för inlogg till MSN och Hotmail. Det finns interna krav på hur lösenordet, som den anställde själv väljer, ska se ut, men det finns inga tekniska funktioner för kontroll av lösenordet. Alla har dock programvaran Keypass, som innehåller bl.a. en lösenordsgenerator, och ska använda den.

Åtkomst med databasverktyg till databaser i Windows Azure begränsas genom Windows Azures brandvägg, till Brevos kontors internetanslutning.

Kommunikation och skydd av uppgifter

Kommunikation mellan Satellite och Windows Azure sker genom webbservice via ett webbgränssnitt som skyddas med SSL. Varje dokument i en fil krypteras med en ny nyckel och nycklarna lagras logiskt separerade från varandra i Microsofts moln.

Enligt avtal har Microsoft aldrig rätt att ta del av Brevos data utan lov från Brevo.

Behörigheter

Brevo använder sig av fyra olika miljöer: utveckling, acceptans, produktion och demo. Användarna har olika användar-id för de olika miljöerna. Produktionsdelen nås av fyra utvecklare. Hittills har samma person beslutat om och administrerat behörigheter, men detta kommer att ändras. Brevo har ännu inga skriftliga rutiner för behörighetstilldelning.

Loggning

Microsoft loggar all inloggning till Azure men delar inte med sig av loggarna. Sådan inloggning är upp till Brevo att logga själva. Idag för Brevo inga sådana loggar.

Back up

All data i produktionsmiljön lagras redundant i tre instanser. Brevo har egna säkerhetskopior för att kunna återställa efter egna misstag. Även dessa finns i molnet. Säkerhetskopiorna lagras krypterat.

Utplåning

Gallringsrutin finns. För att undvika att någon som valt att avregistrera sig inte genast får en ny inbjudan sparas personnumret. Planen är dock att ge användaren möjlighet att välja. Ett konto som deaktiveras ligger vilande i 60 dagar. Under den tiden kan användaren välja att aktivera sitt konto igen. Därefter plockas all data och alla dokument bort.

Personuppgiftsbiträdesavtal och andra avtal

Brevo har tecknat ett Enterprise Agreement med Microsoft. Brevo har granskat avtalen med Microsoft och ansett att säkerheten är tillräcklig. Microsoft följer standarden för ledningssystem för informationssäkerhet, ISO 27001, och har oberoende granskare som en till två gånger om året genomför granskningar enligt revisionsstandard SAS 70 typ I och II. Brevo får del av dokumentationen från granskningarna. Brevo anser att Microsoft kan erbjuda större säkerhet än om Brevo själv skulle stå för säkerheten.

Det finns ett personuppgiftsbiträdesavtal i en bilaga till avtalet med Microsoft. I detta finns bl.a. följande avsnitt

4. Scope and purpose of data processing. The scope and purpose of processing of the Customer Data that Customer provides to Microsoft through the use of the Online Services is described in the Agreement. Microsoft will only process such customer data for the purpose of providing the Online Services and performing its obligations in accordance with the agreement.

5. Technical and organizational security measures. Microsoft will take technical and organizational measures to help protect Customer Data from unauthorized access, use, or disclosure. Specifically, with respect to its Windows Azure platform

- a) Microsoft will take technical and organizational measures to help:
 - i. Restrict access to and portability of data processing equipment employed to process or use Customer Data
 - ii. Restrict access to the use of data-processing systems
 - iii. Ensure that parties authorized to use data-processing system have access only to data covered by their access privileges
 - iv. Ensure that unauthorized parties cannot read, copy, change or remove Customer Data during processing and use or after storage.

- v. Ensure that unauthorized parties cannot read, copy, change or remove Customer Data during transmission or storage on media;
 - vi. Ensure that it may be ascertained where exactly Customer Data is intended to be transmitted using data-transmission equipment;
 - vii. Ensure that it may be verified after the fact whether and by whom Customer Data has been inputted into, changed in or removed from data-processing system;
 - viii. Ensure that Customer Data to be processed as part of a contract may be processed only in accordance with the instructions of the data owner; and
 - ix. Ensure that Customer Data is protected against incidental destruction or loss.
- b) If Microsoft discovers unauthorized use or disclosure of Customer Data we process on your behalf, Microsoft will make commercially reasonable efforts to notify you.
 - c) More information on the technical and organizational measures we take to help protect Customer Data can be found in The Technical Overview of the Security Features in Windows Azure Platform. We regularly reassess these measures and reserve our right to update them without notice.
 - d) (...)

8. Subcontractors; Transfers. Microsoft may hire other companies to provide limited services on its behalf, such as providing customer support. Any such subcontractors are prohibited from using personal data for any purpose other than to deliver the services Microsoft has retained them to provide. Microsoft is responsible for its subcontractors' compliance with the obligations of this amendment. Any subcontractors to whom Microsoft transfers personal data will first enter into written agreements requiring that the subcontractor provide at least the same level of privacy protection with respect to personal data it receives from Microsoft as is required by the relevant Safe Harbor principles as set forth by the U.S. Department of Commerce regarding the collection, use and retention of data from the European Economic Area, and Switzerland. Customer consents to Microsoft's transfer of Customer Data to subcontractors as described herein. Except as set forth above, as agreed by Microsoft and Customer, or as required by law, Microsoft will not transfer to any third party (not even for storage purposes) personal data that Customer provides to Microsoft through the use of online Services.

Överföring till tredjeland

Vid inspektionen visades det administrativa gränssnittet för Windows Azure upp där det framgick att Brevo lagrar data i "North Europe", vilket enligt Brevo betyder att data lagras på Irland och i Holland. Vidare uppgavs vid inspektionen att personuppgifter aldrig överförs till tredje land. Inte heller har någon i tredje land tillgång till personuppgifterna. Detta framgår enligt Brevo av avtalen med Microsoft.

Skäl för beslutet

Personuppgiftsansvar

Enligt 3 § personuppgiftslagen är den personuppgiftsansvarige den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Vidare är, enligt samma bestämmelse, den som behandlar personuppgifter för den personuppgiftsansvariges räkning personuppgiftsbiträde. Personuppgiftslagen riktar sig till den personuppgiftsansvarige, det vill säga den som bestämmer ändamålet med och medlen för en viss behandling.

Företag och myndigheter kan använda Brevo för att distribuera brev elektroniskt. Enskilda personer kan välja att registrera sig hos Brevo för att kunna bli mottagare av brev elektroniskt. För att brev ska kunna skickas via Brevo krävs det att både avsändare och mottagare har avtal med/har skapat ett konto hos Brevo. Brevo har anlitat Microsoft och deras molntjänst Windows Azure för lagring av uppgifter om avsändare och mottagare. Datainspektionen konstaterar att Brevo är personuppgiftsansvarigt för mottagares personuppgifter i sitt register. De kunder som anlitar Brevo för att distribuera brev är personuppgiftsansvariga för personuppgifter i de dokument som de skickar med Brevo och Brevo är personuppgiftsbiträde för behandlingen.

Av ingivet avtal till Datainspektionen framgår att Brevos personuppgiftsbiträde Microsoft kan anlita andra företag. Det har i ärendet inte framkommit att Brevo har kunskap om vilka dessa företag är.

Datainspektionen konstaterar att samtliga bolag som behandlar eller kan komma att behandla personuppgifter för Brevos räkning är personuppgiftsbiträden till Brevo.

Personuppgiftslagen och användningen av molntjänster

Dagens dataskyddslagstiftning är i vissa avseenden svår att förena med det som vi idag kallar för molntjänster. Personuppgiftslagen, och dataskyddsdirektivet som lagen bygger på, utgår från att det är den personuppgiftsansvarige som är den starka, bestämmande aktören som faktiskt kan instruera och kontrollera vad dennes personuppgiftsbiträden gör. Den i ärendet granskade molntjänstanvändningen visar att verkligheten ser annorlunda ut. Det är personuppgiftsbiträdet som erbjuder en tjänst och som i standardavtal och policyer anger vad som gäller vid tillhandahållande av tjänsten.

Möjligheterna för den personuppgiftsansvarige att formulera egna instruktioner och precisera vilka säkerhetsåtgärder som bör vidtas tycks ytterst begränsade. Istället för att formulera egna instruktioner och villkor för personuppgiftsbehandlingen måste den personuppgiftsansvarige granska de avtalsvillkor

och riktlinjer som molntjänstleverantören erbjuder. Utifrån dessa måste den personuppgiftsansvarige kunna bedöma om den personuppgiftsbehandling som den personuppgiftsansvarige vill låta molntjänstleverantören utföra kommer att vara tillåten och tillräckligt säker. Den bedömningen måste göras med beaktande av personuppgiftslagens bestämmelser, om bl.a. ändamålen med behandlingen, tredjelandsoverföring och säkerhetsåtgärder samt slutsatserna av den personuppgiftsansvariges egen risk och sårbarhetsanalys. Otydliga avtal och skrivningar som möjliggör för molnleverantören att ensidigt förändra villkoren för behandlingen medför stora risker eftersom den personuppgiftsansvarige då inte kan veta om den, genom anlitaandet av molntjänstleverantören, uppfyller personuppgiftslagens krav. Möjligheterna för den personuppgiftsansvarige att kontrollera behandlingen försvåras också när molntjänstleverantören låter flera juridiska personer, som också kan finnas i flera olika länder, behandla personuppgifterna.

Personuppgiftslagens krav på säkerhet vid behandling av personuppgifter

Enligt 31 § första stycket personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Med organisatoriska åtgärder avses säkerhetsarbetets organisation och rutiner, instruktioner och policyer. Ju känsligare personuppgifter som behandlas, desto högre blir kraven på säkerhetsåtgärderna. Åtgärderna ska nämligen 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.

Den säkerhetsnivå som bedöms tillräcklig för en viss personuppgiftsbehandling måste givetvis upprätthållas i alla lägen – även om den personuppgiftsansvarige anlitar någon annan för att utföra personuppgiftsbehandlingen åt sig. För att integritetsskyddet inte ska försämrats om den personuppgiftsansvarige anlitar någon annan måste, enligt 31 § andra stycket, den som anlitar ett personuppgiftsbiträde för behandling av personuppgifter förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

För att integritetsskyddet ska upprätthållas krävs också, enligt 30 § andra stycket personuppgiftslagen, att den personuppgiftsansvarige måste ha ingått ett skriftligt avtal med personuppgiftsbiträdet, i vilket det framgår att personuppgiftsbiträdet bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.

Kravet på skriftligt personuppgiftsbiträdesavtal, 30 § personuppgiftslagen

I avtal som Brevo har givit in vid inspektionen framkommer att personuppgifter kan komma att behandlas av andra företag än Microsoft. I enlighet med vad som ovan konstaterats är alla bolag som behandlar personuppgifter för Brevos räkning att betrakta som personuppgiftsbiträden till Brevo.

Krav på personuppgiftsbiträdesavtal med underleverantörer

Datainspektionen har tidigare ansett att det krävs att den personuppgiftsansvarige själv ingår avtal med varje personuppgiftsbiträde/underbiträde för att uppfylla kravet i 30 § andra stycket personuppgiftslagen. Kravet på personuppgiftsbiträdesavtal kan enligt Datainspektionen dock uppfyllas även genom att den personuppgiftsansvarige ger ett personuppgiftsbiträde mandat att ingå avtal med underbiträden. Detta gäller under förutsättning att det föreskrivs att underbiträdena är skyldiga att följa den personuppgiftsansvariges instruktioner och att varje personuppgiftsbiträde också föreskrivs vara skyldigt att uppfylla de säkerhetskrav som den personuppgiftsansvarige ska uppfylla enligt 31 § personuppgiftslagen. Dessutom måste den personuppgiftsansvarige säkerställa att den har kännedom om vilka personuppgiftsbiträden som kan komma att behandla dennes personuppgifter.

Brevo har i sitt personuppgiftsbiträdesavtal med Microsoft gett Microsoft mandat att anlita andra företag. I avtalet föreskrivs att underbiträdena inte får behandla personuppgifter för andra syften än vad som bestämts enligt avtalet och att de ska vara skyldiga att ha minst samma skydd som Microsoft ska ha enligt avtalet. Avtalet säkerställer dock inte att Brevo har kännedom om vilka personuppgiftsbiträden som kan komma att behandla Brevos personuppgifter.

Datainspektionen bedömer att Brevo måste säkerställa att de har kännedom om vilka personuppgiftsbiträden som kan komma att behandla Brevos personuppgifter för att leva upp till kravet i 30 § andra stycket personuppgiftslagen.

Datainspektionen rekommenderar vidare att personuppgiftsbiträdesavtalet säkerställer att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande. När avtalet upphör saknar personuppgiftsbiträdet normalt grund för att fortsätta behandla personuppgifterna.

Kravet på kontroll av personuppgiftsbiträden

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde måste denne, enligt personuppgiftslagen 31 § andra stycket, förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna. När det är

fråga om s.k. molntjänster kan det på grund av den teknik som används vara svårt att svara på var data lagras eller bearbetas rent fysiskt och därmed även geografiskt. Om en molnleverantör utan användarens vetskap kan flytta data inte bara mellan olika underleverantörer men också mellan olika länder, minskar den personuppgiftsansvariges möjligheter att följa upp och försäkra sig om att personuppgiftsbiträden verkligen vidtagit de åtgärder som de åtagit sig. En grundläggande förutsättning för att kunna uppfylla säkerhetskraven i 31 § personuppgiftslagen och kravet på kontroll av personuppgiftsbiträden är att den personuppgiftsansvarige har kännedom om vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning.

Brevo har uppgett att man granskat avtalet med Microsoft. Vidare följer Microsoft standarden ISO 27001 samt har oberoende granskare som en till två gånger om året genomför granskningar enligt SAS 70 typ I och II. Brevo får del av dokumentationen från dessa granskningar.

Att använda sig av tredjepartsrevision kan vara ett sätt att kontrollera att leverantören och tjänsten uppfyller vissa säkerhets- och kvalitetskrav. Det fråntar dock inte den personuppgiftsansvarige från ansvaret att kontrollera att personuppgiftsbiträden både kan och verkligen vidtar säkerhetsåtgärder i enlighet med 31 § personuppgiftslagen. Kan den personuppgiftsansvarige inte formulera egna instruktioner och villkor måste denne granska de avtalsvillkor och riktlinjer som molntjänstleverantören erbjuder och göra en bedömning utifrån dessa. Brevo är även skyldigt att säkerställa att det på lämpligt sätt har möjlighet att följa upp att dess personuppgiftsbiträden lever upp till villkoren i avtalet.

För att Brevo ska kunna uppfylla kraven på kontroll av dem som behandlar personuppgifter för dess räkning förutsätts att Brevo vet vilka det är skyldiga att kontrollera. Det gäller oavsett hur Brevo väljer att uppfylla kraven.

Datainspektionen konstaterar att Brevo inte lever upp till kraven i 31 § andra stycket personuppgiftslagen, eftersom Brevo inte har kunskap om vilka som behandlar personuppgifterna för bolagets räkning.

IT-säkerhet

Brevos personuppgiftsansvar innebär att det alltid är Brevo som ytterst har ansvaret för att dess personuppgifter skyddas även när personuppgiftsbiträden anlitas.

Ju större integritetsrisker en viss personuppgiftsbehandling innebär desto högre är kraven på säkerhetsåtgärder. Hur stora integritetsrisker som en viss behandling innebär beror bland annat på antalet personer som de behandlade

uppgifterna avser, mängden personuppgifter som behandlas om varje person och känsligheten hos de behandlade uppgifterna. Även möjligheten att strukturera personuppgifterna har i det här sammanhanget betydelse.

De uppgifter som Brevo är personuppgiftsansvarigt för, dvs. mottagares personuppgifter i Brevos kundregister, är inte sådana känsliga personuppgifter som avses i 13 § personuppgiftslagens eller så pass integritetskänsliga att det krävs starkare autentiseringslösning för att få åtkomst till uppgifterna än den lösning som Brevo redan använder sig av, nämligen användarnamn och lösenord.

Mot bakgrund, av den typ av uppgifter som Brevo har personuppgiftsansvar för, har Datainspektionen heller inte något att invända mot de åtgärder som vidtagits för att skydda de uppgifter som behandlas och kommunikation av dessa.

Datainspektionen konstaterar att Brevo inte har några åtkomstloggar, utan att loggar endast förs av Microsoft och att dessa inte lämnas ut till Brevo. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring, förlust, ändringar, otillåten spridning eller otillåten tillgång till uppgifterna. Det ställs högre krav på dessa åtgärder om behandlingen innefattar överföring av personuppgifter via öppna nät. Brevo måste därför säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av personuppgifter inom Brevo eller hos Microsoft.

Loggkontroll ska kunna ske på förekommen anledning. Därav följer att Brevo ansvarar för att se till att det finns loggar och att loggarna kan användas för att utreda obehörig åtkomst – oavsett om personen som haft åtkomst till uppgifterna befinner sig hos Brevo eller hos Microsoft.

Datainspektionen förelägger Brevo att tillse att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av de personuppgifter som behandlas inom Brevo eller för Brevos räkning hos Microsoft.

Brevo har inga skriftliga rutiner för behörighetstilldelning. Vid inspektionen framkom att det i organisationen pågick en förändring av hur tilldelningen av behörigheter går till i bolaget. Datainspektionen förutsätter att denna översyn innebär att bolaget skaffar sig rutiner för behörighetstilldelning.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. 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 Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Catharina Fernquist, IT-säkerhetsspecialisterna Adolf Slama samt juristerna Lena Carlsson och Ulrika Andersson, föredragande.

Göran Gräslund

Ulrika Andersson