NAVEX WhistleB

Datasheet

Schrems II: Kundgarantiguide och dess inverkan på visselblåsarsystem NAVEX WhistleB

I den här artikeln besvarar vi ett antal viktiga frågor om Schrems II, med särskilt fokus på visselblåsning och NAVEX fortsatta åtagande att garantera datasekretess och säkerhet.

Vad är Schrems II?

Schrems II är ett avgörande som utfärdades i juli 2020 av EU:s domstol (CJEU) och som upphävde avtalet mellan EU och USA, vilket innebär att EU:s och USA:s Privacy Shield-ramverk inte längre är tillämpligt som en adekvat metod för överföring av personuppgifter från EU till USA, på grundval av det skydd som det gav inte uppfyllde EU-standarderna.

Hur hänger denna fråga samman med visselblåsning?

Beroende på plats, struktur och val av leverantör för visselblåsarlösning kan vissa organisationer behöva överföra personuppgifter om visselblåsning mellan EU och USA.

Vilka delar av USA:s och EU:s lagstiftning är relevanta?

EU:s GDPR begränsar överföring av personuppgifter utanför EU till länder som inte kan garantera tillräckligt skydd om inte ett undantag gäller eller en alternativ godkänd överföringsmekanism finns på plats.

Hittills har Standard Contractual Clauses (SCC) och Privacy Shield (för överföringar till USA) varit de vanligaste mekanismerna för att skydda de överförda personuppgifterna.

I sitt fastställande att amerikansk lagstiftning inte garanterar en väsentligen likvärdig skyddsnivå åberopade domstolen bredden av amerikanska övervakningsprogram (särskilt avsnitt 702 i FISA och Executive Order 12333).

Vilken syn har NAVEX på frågan?

Som EU-leverantör av molntjänster är NAVEX föremål för och efterlever både EU:s och Storbritanniens GDPR.

Säkerhet har alltid varit kärnan i allt vi gör för att skydda både visselblåsare och våra kunders data. Vi integrerar målmedvetet marknadsledande säkerhet i vårt NAVEX WhistleB-system och väljer ut de säkraste IT-leverantörerna.

Datasäkerhet och efterlevnad av all gällande lagstiftning har, och kommer alltid att ha, högsta prioritet i visselblåsarsystemet NAVEX WhistleB. Läs mer om detta på Trust Centre.

Hur och var lagras data för NAVEX WhistleB-systemet?

NAVEX har valt marknadsledande Microsoft Azure som leverantör av säkra datavärdtjänster för kunddata. Microsoft Azure är branschledande när det gäller informationssäkerhet, IT-säkerhet och dataskydd.

All kunddata som lagras och behandlas via Microsoft Azure finns inom EU, med det primära datacentret i Irland och det sekundära datacentret i Nederländerna. Men eftersom moderföretaget för Microsoft Azure är Microsoft Corporation och NAVEX WhistleB-systemet tillhandahålls av NAVEX, båda USA-ägda företag, förstår vi att besluten från CJEU väcker frågor hos våra kunder.

Hur påverkar NAVEX WhistleB-systemet efterlevnaden av GDPR och Schrems II?

Kunddata skyddas av en avancerad krypteringsteknik i visselblåsarsystemet. Denna krypteringsteknik säkerställer att visselblåsarrapporter endast är tillgängliga för kunden, och inte för NAVEX, dess anställda eller något av dess dotterbolag (inklusive dess amerikanska enhet), någon leverantör, någon myndighet eller annan tredje part. NAVEX WhistleB-kunden har alltid ensam full kontroll över krypteringsnyckeln. Det är bara kunden som kan dekryptera och ge åtkomst till uppgifterna. Utanför de mycket snäva omständigheterna för vissa tilläggstjänster överförs inga uppgifter om visselblåsarrapporter som behandlas av NAVEX WhistleB-systemet utanför EU. För sådana tilläggstjänster förlitar sig NAVEX WhistleB-systemet på biträden som uppfyller kraven och behandlar alla uppgifter strikt i enlighet med GDPR och standardavtalsklausulerna.

Wie geht es jetzt weiter?

Datenschutz und Datensicherheit und die Konformität mit allen anwendbaren Gesetzen stehen beim Hinweisgebersystem von NAVEX WhistleB im Mittelpunkt und werden auch weiterhin der Schwerpunkt bleiben. Wir werden deshalb die Entwicklungen in diesem Bereich und zwischen der EU und den USA genauestens beobachten, da nun aufgrund des Schrems II-Urteils eine Vereinbarung fehlt.

Vidare finner NAVEX, enligt sin skäliga uppfattning vid intern och utomstående granskning, inte att amerikanska övervakningslagar, inklusive avsnitt 702 FISA och Executive Order 12333 är tillämpliga på NAVEX WhistleB-systemet. En viktig faktor som organisationer bör bedöma är omständigheterna kring överföring av personuppgifter, inklusive omfattningen och tillämpningen av amerikanska övervakningsprogram på en USA-baserad uppgiftsinförare. De kan till exempel gälla industrisektorn (vissa branscher är sällan föremål för amerikansk statlig övervakning och utgör därför en minimal risk). Till dessa punkter är varken Microsoft Corporation eller NAVEX US inblandade som dataimportör, NAVEX har aldrig mottagit en FISA- eller EO 12333-begäran avseende NAVEX WhistleB-systemet eller för någon av tjänsterna NAVEX tillhandahåller, och som nämnts ovan krypteras visselblåsarrapportens data på ett sätt som endast ger kunden åtkomst till dessa data.

Dessutom avser insamlingsmetoderna i fråga insamling av kommunikationsdata. Det är ytterst osannolikt att NAVEX, för någon av de tjänster NAVEX tillhandahåller, någonsin kommer att bli föremål för en FISA- eller EO 12333-begäran, eftersom NAVEX inte behandlar den typ av uppgifter som det gäller. Sådan insamling sker nästan uteslutande hos större e-post- och sociala medieföretag och informationen som ska samlas in ska vara utländsk underrättelseinformation.

Förutom att det är mycket osannolikt att NAVEX kommer att omfattas av sådana program, gör NAVEX under USA-baserat ägande det till en amerikansk person enligt amerikansk lag. Detta innebär att NAVEX ges större skydd mot de aktuella övervakningslagarna än företag som inte ägs i USA. FISA 702 förbjuder regeringen

att rikta in sig på NAVEX-kommunikation (inklusive kommunikation som innehåller tredjepartsposter), eftersom NAVEX är en amerikansk person. EU-ägda företag som inte betraktas som amerikanska personer eller på annat sätt inte kommunicerar med amerikanska personer är inte förbjudna att bli föremål för FISA på samma sätt som NAVEX är. Enligt EO 12333 gäller fortfarande de lagar som skyddar amerikanska personer (t.ex. Fourth Amendment and Privacy Act), vilket innebär att den amerikanska regeringen inte kan rikta in sig

på kommunikation med NAVEX, eftersom det är en amerikansk person, utan att följa särskilda, specifika procedurer. Sådana gränser gäller inte för EU-baserade företag som inte är amerikanska personer.

Även om NAVEX intar ståndpunkten att problematisk amerikansk lagstiftning inte gäller NAVEX WhistleB-systemet till att börja med, eftersom NAVEX inte har tillgång till visselblåsarrapporter, skulle det inte gå att tillhandahålla sådana uppgifter om en sådan begäran inkom från en offentlig myndighet, något som är mycket osannolikt.

Vad händer nu?

Datasäkerhet och efterlevnad av all gällande lagstiftning har, och kommer alltid att ha, högsta prioritet i visselblåsarsystemet NAVEX WhistleB. Vi kommer därför att fortsätta följa upp den nuvarande situationen och bristen på överenskommelse mellan EU och USA mycket noga.