NAVEX WhistleB

Datasheet

Schrems II:Leitfaden zur Kundensicherung und seine Auswirkungen auf das Whistleblowing-System NAVEX WhistleB

In diesem Artikel beantworten wir eine Reihe von wichtigen Fragen zu Schrems II. Wir konzentrieren uns dabei insbesondere auf Whistleblowing und das fortwährende starke Engagement von NAVEX für Datenschutz und Datensicherheit.

Was ist Schrems II?

Schrems II ist ein Urteil des Gerichtshofs der Europäischen Union (EuGH) vom Juli 2020, mit dem das Abkommen zwischen der EU und den USA aufgehoben wurde, was bedeutet, dass der EU-US-Datenschutzschild-Rahmen nicht mehr als angemessene Methode zur Übermittlung personenbezogener Daten aus der EU in die USA gilt. Der Grund ist, dass die von ihm gewährten Schutzmechanismen nicht den EU-Standards entsprachen.

Wieso wirkt sich dieses Urteil auf das Whistleblowing aus?

Je nach Standort, Struktur und ausgewähltem Dienstleister für Hinweisgebersysteme müssen gewisse Organisationen möglicherweise personenbezogene Daten des Hinweisgebers zwischen der EU und den USA übertragen.

Welche Teile der US- und EU-Gesetze sind relevant?

Die DSGVO der EU schränkt die Übermittlung personenbezogener Daten in Länder außerhalb der EU ein, die keinen angemessenen Schutz garantieren können, es sei denn, es gibt eine Ausnahme oder einen alternativen anerkannten Übermittlungsmechanismus.

Bisher waren Standardvertragsklauseln (SVK) und der Datenschutzschild (für den Transfer in die USA) die üblichsten angewendeten Schutzmechanismen bei der Übertragung personenbezogener Daten.

In seiner Feststellung, dass die US-Gesetze kein im Wesentlichen gleichwertiges Schutzniveau garantieren, verwies das Gericht auf den Umfang der US-Überwachungsprogramme (insbesondere Abschnitt 702 der FISA und der Exekutivverordnung 12333).

Welchen Standpunkt vertritt NAVEX?

Als EU-Anbieter von Cloud-Diensten unterliegt NAVEX der DSGVO der EU und des Vereinigten Königreichs und hält diese ein.

Datenschutz und Sicherheit stehen schon seit unserer Gründung im Zentrum all unserer Aktivitäten – wir schützen sowohl die Daten von Hinweisgebenden als auch die unserer Kundschaft. Von Beginn an haben wir unsere marktführenden Sicherheitsstandards bewusst in das NAVEX WhistleB-System integriert und die sichersten IT-Anbieter ausgewählt.

Datensicherheit und die Konformität mit allen anwendbaren Gesetzen stehen beim Hinweisgebersystem von NAVEX WhistleB im Mittelpunkt und werden auch weiterhin der Schwerpunkt bleiben. Erfahren Sie in unserem Trust Centre mehr dazu.

Wie und wo werden Daten für das NAVEX WhistleB-System gespeichert?

NAVEX hat das marktführende System Microsoft Azure als sicheren Datenhosting-Service für Kundendaten ausgewählt. Microsoft Azure ist in der Branche der führende Dienst für Informationssicherheit, IT-Sicherheit und Datenschutz.

Alle Kundendaten werden über Microsoft Azure in der EU gespeichert und verarbeitet. Das Hauptrechenzentrum be indet sich in Irland und ein weiteres in den Niederlanden.

Da jedoch die Muttergesellschaft von Microsoft Azure die Microsoft Corporation ist und das NAVEX WhistleB-System von NAVEX bereitgestellt wird, beides US-Unternehmen, verstehen wir, dass die Entscheidungen des EuGH Fragen für unsere Kunden aufwerfen.

Wie wirkt sich das NAVEX WhistleB-System auf die Einhaltung der DSGVO und Schrems II aus?

Kundendaten sind durch eine starke Verschlüsselungstechnologie im Hinweisgebersystem

vor jeglicher Offenlegung geschützt. Diese Verschlüsselungstechnologie stellt sicher, dass die Daten der Hinweisgebermeldungen nur für den Kunden zugänglich sind, nicht aber für NAVEX, seine Mitarbeiter oder eine seiner Tochtergesellschaften (einschließlich der US-Einheit), einen Lieferanten, eine Behörde oder eine andere dritte Partei. WhistleBs Kundinnen und Kunden haben die volle und alleinige Kontrolle über den Verschlüsselungscode. Die Entschlüsselung von und der Zugriff auf Daten kann nur durch den jeweiligen Kunden oder die jeweilige Kundin durchgeführt oder ermöglicht werden. Außerhalb sehr enger Umstände für bestimmte optionale Dienste werden keine Daten zu Hinweisgebermeldungen, die vom NAVEX WhistleB-System verarbeitet werden, außerhalb der EU übermittelt. Für solche optionalen Dienste verlässt sich das NAVEX WhistleB-System auf konforme Unterauftragsverarbeiter, die alle Daten streng in Übereinstimmung mit der DSGVO und den Standardvertragsklauseln verarbeiten.

Darüber hinaus findet NAVEX nach vernünftiger Einschätzung von internen und externen Rechtsberatern keine für das NAVEX WhistleB-System geltenden US-Überwachungsgesetze, einschließlich Abschnitt 702 FISA und Executive Order 12333. Ein Schlüsselfaktor, den Unternehmen bewerten sollten, sind die Umstände im Zusammenhang mit der Übermittlung personenbezogener Daten, einschließlich des Umfangs und der Anwendung von US-Überwachungsprogrammen auf einen in den USA ansässigen Datenimporteur. Sie können zum Beispiel den Industriesektor in Betracht ziehen (einige Branchen sind selten Gegenstand der Überwachung durch die US-Regierung

und stellen daher ein minimales Risiko dar). Zu diesen Punkten ist anzumerken, dass weder die Microsoft Corporation noch NAVEX US als Datenimporteur beteiligt ist, dass NAVEX nie eine FISA- oder EO 12.333-Anfrage in Bezug auf das NAVEX WhistleB-System oder für die von NAVEX erbrachten Services erhalten hat, und dass, wie oben erwähnt, die Daten der Hinweisgebermeldungen so verschlüsselt sind, dass nur der Kunde Zugang zu diesen Daten hat.

Darüber hinaus geht es um die Erhebung von Kommunikationsdaten.

Es ist äußerst unwahrscheinlich, dass NAVEX mit einem der von ihm erbrachten Services jemals Gegenstand einer FISA-Anfrage oder einer EO 12.333-Anordnung oder -Anfrage sein wird, da NAVEX die fragliche Art von Daten nicht verarbeitet. Eine solche Erhebung findet ast ausschließlich bei größeren E-Mail- und Social-Media-Unternehmen statt, und die zu erhebenden Informationen müssen ausländische Geheimdienstinformationen sein.

Abgesehen davon, dass es sehr unwahrscheinlich ist, dass NAVEX in den Anwendungsbereich solcher Programme fällt, ist NAVEX als Unternehmen mit Sitz in den USA nach US-Recht eine US-Person. Das bedeutet, dass NAVEX einen größeren Schutz vor den betreffenden Überwachungsgesetzen genießt als Nicht-US-Unternehmen. FISA 702 verbietet es der Regierung, auf NAVEX-Kommunikation (einschließlich ihrer Kommunikation, die Aufzeichnungen Dritter enthält) zuzugreifen, da NAVEX eine US-Person ist. Für EU-Unternehmen, die nicht als US-Personen gelten oder nicht mit US-Personen kommunizieren, gilt – anders als für NAVEX – kein Schutz vor Maßnahmen im Rahmen von FISA. Gemäß EO 12.333 gelten weiterhin die Gesetze zum Schutz von US-Personen (z. B. Vierter Zusatzartikel zur Verfassung der Vereinigten Staaten und Datenschutzgesetz), was bedeutet, dass die US-Regierung, ohne spezielle, spezifische Verahren zu beolgen, nicht au die Kommunikation von NAVEX zugreifen kann, da es sich um eine US-Person handelt. Solche Beschränkungen gelten nicht für Unternehmen mit Sitz in der EU, die keine US-Personen sind.

Zum einen vertritt NAVEX den Standpunkt, dass die problematische US-Gesetzgebung nicht auf das NAVEX WhistleB-System anwendbar ist, andererseits hat NAVEX keinen Zugang zu den Daten der Hinweisgebermeldungen, d. h. NAVEX wäre nicht in der Lage, diese Daten zur Verfügung zu stellen, würde jemals eine derartige Anfrage einer Behörde eingehen, was zudem äußerst unwahrscheinlich ist.

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.