NAVEX WhistleB

Datasheet

Schrems II: Customer assurance guide and its impact on NAVEX WhistleB's whistleblowing system

In this article we answer a number of key questions relating to Schrems II, with a specific focus on whistleblowing and NAVEX's continued commitment to guarantee data privacy and security.

What is Schrems II?

Schrems II is a ruling issued in July, 2020 by the Court of Justice of the European Union (CJEU) that cancelled the EU-US agreement which means that the EU-US Privacy Shield Framework is no longer applicable as an adequate method to transfer personal data from the EU to the US, on the basis that the protections it afforded did not meet EU standards.

How is this issue related to whistleblowing?

Depending on their location, structure and choice of the whistleblowing solution vendor, certain organisations may need to transfer whistleblowing personal data between the EU and the US.

What areas of the US and EU legislation are relevant?

The EU GDPR restricts transfers of personal data outside of the EU to countries which cannot guarantee adequate protection unless an exception applies or an alternative approved transfer mechanism is in place. Until now, Standard Contractual Clauses (SCC) and Privacy Shield (for transfers to the US) have been the most common mechanisms used to protect the personal data transferred. In its determination that US laws do not guarantee an essentially equivalent level of protection, the court cited the breadth of US surveillance programmes (particularly Section 702 of FISA and Executive Order 12333).

What is NAVEX's viewpoint?

As an EU provider of cloud services, NAVEX is subject to and complies with both the EU and UK GDPR. Privacy and security have always been at the heart of everything we do to protect both whistleblowers and our customers' data. We have purposefully designed market-leading security into the NAVEX WhistleB system and selected the most secure IT providers. Data security and compliance with all applicable laws are and will remain focus points of the NAVEX WhistleB whistleblowing system. Find out more about this at our Trust Centre.

How and where is data stored for the NAVEX WhistleB system?

NAVEX has selected market-leading Microsoft Azure as its supplier of secure data hosting services for customer data. Microsoft Azure is an industry leader in terms of information security, IT security and data protection. All customer data stored and processed via Microsoft Azure is in the EU, with the primary data centre in Ireland and the secondary data centre in the Netherlands. However, as the parent company of Microsoft Azure is Microsoft Corporation, and the NAVEX WhistleB system is provided by NAVEX, both US owned companies, we understand the decisions by the CJEU raise questions for our customers.

How does the NAVEX WhistleB system affect the GDPR and Schrems II compliance?

Customer data is protected against any disclosure through strong encryption technology in the whistleblowing system. This encryption technology ensures that whistleblower report data is accessible by the customer only, not by NAVEX, its employees or any of its affiliates (including its US entity), any supplier, any authority nor any other third party. A NAVEX WhistleB customer has full and sole control of the encryption key. Only the customer can decrypt and authorise anyone access to their data. Outside of very narrow circumstances for certain optional services, no whistleblower report data processed by the NAVEX WhistleB system is transferred outside of the EU. For such optional services, the NAVEX WhistleB system relies on compliant sub-processors that process all data strictly in accordance with the GDPR and the Standard Contractual Clauses.

Further, in NAVEX's reasonable opinion upon internal and outside counsel review, it does not find US surveillance laws, including Section 702 FISA and Executive Order 12333, applicable to the NAVEX WhistleB system. A key factor organisations should be assessing are the circumstances surrounding personal data transfers, including the scope and application of US surveillance programmes on a US based data importer. They may consider the industry sector, for example (some industries may rarely be the subject of US government surveillance and therefore pose a minimal risk). To these points, neither Microsoft Corporation or NAVEX US is involved as a data importer, NAVEX has never received a FISA or EO 12.333 request with respect to the NAVEX WhistleB system or for any services NAVEX provides, and as noted above, the whistleblower report data is encrypted in a manner that allows only the customer access to this data.

Additionally, the collection practices at issue are communications data collection. It is extremely unlikely NAVEX, for any of the services it provides, will ever be subject to a FISA request or EO 12.333 order or request, as NAVEX does not process the type of data at issue. Such collection almost exclusively occurs at larger e-mail and social media companies, and the information to be collected must be foreign intelligence information.

In addition to it being very unlikely for NAVEX to be in scope of such programmes, NAVEX being under US based ownership makes it a US person under US law. This means NAVEX is provided greater protections from the surveillance laws at issue than non-US owned companies. FISA 702 prohibits the government from targeting NAVEX communications (including its communications containing third-party records), since NAVEX is a US person. EU owned companies not considered US persons or otherwise not communicating with US persons are not prohibited from being targeted under FISA in the same way NAVEX is. Under EO 12.333, the laws protecting US persons (e.g., Fourth Amendment and Privacy Act) still apply, meaning that the US government cannot target communications of NAVEX, since it is a U.S. person, without following special, specific procedures. Such limits do not apply to EU based companies who are not US persons.

Further, while NAVEX takes the approach that problematic US legislation does not apply to the NAVEX WhistleB system to begin with, as NAVEX does not have access to the whistleblower report data, it would not be able to provide such data if it ever did received such a public authority request, which is extremely unlikely to occur.

What's next?

Data privacy and security and compliance with all applicable laws are and will remain focus points of the NAVEX WhistleB whistleblowing system. We will therefore continue to monitor the current situation and the lack of agreement between the EU and the US very closely.