NAVEX WhistleB

Datasheet

Schrems II: Guide d'assurance client et son incidence sur le dispositif d'alerte professionnelle NAVEX WhistleB

Dans cet article, nous répondons à un certain nombre de questions clés relatives à Schrems II, en mettant l'accent sur les signalements et l'engagement continu de NAVEX à garantir la confidentialité et la sécurité des données.

Qu'est-ce que Schrems II ?

Schrems II est une décision rendue en juillet 2020 par la Cour de justice de l'Union européenne (CJUE) qui a annulé l'accord UE-États-Unis selon lequel le cadre du bouclier de protection des données UE-États-Unis n'est plus applicable comme méthode adéquate pour transférer des données à caractère personnel de l'UE vers les États-Unis, sur la base du fait que les protections qu'il offrait ne satisfaisaient pas aux normes de l'UE.

Quel est le lien entre ce sujet et les alertes professionnelles ?

En fonction de leur localisation, de leur structure et du choix du fournisseur de la solution d'alertes professionnelles, certaines organisations peuvent transférer des données personnelles liées à des alertes professionnelles entre l'UE et les États-Unis.

Quels sont les domaines de la législation américaine et européenne concernés ?

Le RGPD de l'UE limite les transferts de données à caractère personnel en dehors de l'UE aux pays qui ne peuvent pas garantir une protection adéquate, à moins qu'une exception ne s'applique ou qu'un autre mécanisme de transfert agréé ne soit mis en place.

Jusqu'à présent, les clauses contractuelles types (SCC) et le bouclier de protection des données (pour les transferts vers les États-Unis) ont été les mécanismes les plus courants pour protéger les données à caractère personnel transférées.

Dans sa détermination que les lois américaines ne garantissent pas un niveau de protection essentiellement équivalent, le tribunal a cité l'ampleur des programmes de surveillance américains (en particulier la Section 702 de la FISA et l'Ordonnance exécutive 12333).

Quel est le point de vue de NAVEX ?

En tant que fournisseur de services cloud de l'UE, NAVEX est soumis au RGPD de l'UE et du Royaume-Uni et s'y conforme.

La confidentialité et la sécurité ont toujours été au cœur

de tout ce que nous faisons pour protéger à la fois les lanceurs d'alertes et les données de nos clients. Nous avons délibérément conçu une sécurité à la pointe du marché dans le dispositif NAVEX WhistleB et nous avons sélectionné les fournisseurs de services informatiques les plus sûrs.

La sécurité des données et le respect de toutes les lois applicables sont et resteront les points forts du dispositif d'alerte professionnelle NAVEX WhistleB. Pour en savoir plus à ce sujet, consultez notre Centre de confiance.

Comment et où les données sont-elles stockées pour le dispositif NAVEX WhistleB ?

NAVEX a choisi Microsoft Azure, leader du marché, comme fournisseur de services d'hébergement de données sécurisées pour les données des clients. Microsoft Azure est un leader du secteur en termes de sécurité de l'information, de sécurité informatique et de protection des données.

Toutes les données des clients sont stockées et traitées via Microsoft Azure dans l'UE, le centre de données principal étant situé en Irlande et un centre de données secondaire aux Pays-Bas. Cependant, étant donné que la société mère de Microsoft Azure est Microsoft Corporation et que le dispositif NAVEX WhistleB est fourni par NAVEX, deux sociétés américaines, nous comprenons que les décisions de la CJUE soulèvent des questions pour nos clients.

Quel est l'effet du dispositif NAVEX WhistleB sur la conformité au RGPD et à Schrems II ?

Les données des clients sont protégées contre toute révélation grâce à une technologie de cryptage renforcé qui est intégrée au dispositif d'alerte professionnelle. Cette technologie de cryptage garantit que les données des signalements sont accessibles uniquement par le client, et non par NAVEX, ses employés ou l'une de ses filiales (y compris son entité américaine), tout fournisseur, toute autorité ou tout autre tiers. Un client de NAVEX WhistleB a le contrôle total et exclusif de la clé de chiffrement. Seuls les clients peuvent déchiffrer et autoriser l'accès à leurs données à d'autres personnes. En dehors de circonstances très limitées pour certains services optionnels, aucune donnée de signalement des lanceurs d'alerte traitée par le dispositif NAVEX WhistleB n'est transférée en dehors de l'UE. Pour ces services optionnels, le dispositif NAVEX WhistleB s'appuie sur des sous-traitants conformes qui traitent toutes les données dans le strict respect du RGPD et des Clauses contractuelles types.

En outre, de l'avis raisonnable de NAVEX lors de l'examen par des conseillers internes et externes, elle ne trouve pas de lois américaines sur la surveillance, y compris la Section 702 de la FISA et l'Ordonnance exécutive 12.333, applicables au dispositif NAVEX WhistleB. Les organisations devraient évaluer les circonstances entourant les transferts de données à caractère personnel, y compris la portée et l'application des programmes de surveillance américains sur un importateur de données basé aux États-Unis. Elles peuvent envisager le secteur industriel, par exemple (certaines industries peuvent rarement faire l'objet d'une surveillance du gouvernement américain et donc présenter un risque

minimal). À ces points, ni Microsoft Corporation ni NAVEX US n'est impliquée en tant qu'importateur de données, NAVEX n'a jamais reçu de demande FISA ou EO 12.333 concernant le dispositif NAVEX WhistleB ou pour tout service fourni par NAVEX, et comme indiqué ci-dessus, les données du rapport de signalement sont chiffrées d'une manière qui permet uniquement au client d'accéder à ces données.

En outre, les pratiques de collecte en question sont la collecte de données de communication.

Il est extrêmement improbable que NAVEX, pour l'un des services qu'il fournit, fasse l'objet d'une demande FISA ou d'un ordre ou d'une demande EO 12.333, car NAVEX ne traite pas le type de données en question. Cette collecte se fait presque exclusivement dans les grandes entreprises de messagerie électronique et de réseaux sociaux, et les informations à collecter doivent être des informations de renseignement étrangères.

Outre le fait qu'il est très peu probable que NAVEX entre dans le champ d'application de ces programmes, NAVEX étant détenue aux États-Unis, elle est considérée comme une personne américaine selon le droit américain. Cela signifie que NAVEX bénéficie de plus de protections contre les lois de surveillance en question que les sociétés non détenues aux États-Unis.

La FISA 702 interdit au gouvernement de cibler les communi-cations NAVEX (y compris ses communications contenant des dossiers de tiers), car NAVEX est une personne américaine. Il n'est pas interdit aux sociétés détenues par l'UE qui ne sont pas considérées comme des ressortissants américains ou qui ne communiquent pas avec des ressortissants américains d'être ciblées en vertu de la FISA de la même manière que NAVEX. En vertu du décret présidentiel 12.333, les lois protégeant les ressortissants américains (p. ex., le Quatrième amendement et la loi sur la protection de la vie privée) s'appliquent toujours, ce qui signifie que le gouvernement américain ne peut pas cibler les communications de NAVEX, car il s'agit d'un ressortissant américain, sans suivre des procédures spéciales et spécifiques. Ces limites ne s'appliquent pas aux sociétés siégées dans l'UE qui ne sont pas des ressortissants américains.

En outre, bien que NAVEX a adopté l'approche selon laquelle la législation américaine problématique ne s'applique pas au dispositif NAVEX WhistleB dans un premier temps, car NAVEX n'a pas accès aux données de signalement des lanceurs d'alerte, elle ne serait pas en mesure de fournir ces données si elle avait déjà reçu une telle demande de l'autorité publique, ce qui est extrêmement peu probable.

Quelle est la prochaine étape ?

La confidentialité, la sécurité des données et le respect de toutes les lois applicables sont et resteront les points forts du dispositif d'alerte professionnelle NAVEX WhistleB. Nous continuerons donc à suivre de très près la situation actuelle et l'absence d'accord entre l'UE et les États-Unis.