EINPRESSWIRE

SCHREMS II WEBINAR FAQ #3: Do Additional Safeguards enable Schrems II compliant EU employee data processing?

Yes. If you are already practicing Data Protection by Design and By Default.

BRUSSELS, BELGIUM, October 20, 2020 /EINPresswire.com/ -- Schrems II Webinar FAQ #3 of 25: Do Additional Safeguards enable Schrems II compliant EU employee data processing?

Yes. If you are already practicing Data Protection by Design and By Default, most employee-related processing involving EU personal data can continue using additional safeguards like GDPR-heightened Pseudonymisation.

NOTE: Answers to numerous questions related to the ability of Pseudonymisation and Data Protection by Design and by Default to enable EU employee-related processing - both in the context of Schrems II compliance purposes and generally - were combined in the following.

SCHREMS II FAQ # 03

Do Additional Safeguards enable Schrems II Compliant EU employee data processing?

Watch this video & read the answer at:

▶ SchremsII.com/FAQS

PLEASE share your comments below with the rest of the Linkedin Working Group community.

Schrems II Webinar FAQ 3 of 25: Do Additional Safeguards enable Schrems II compliant EU employee data processing?

Anonos: Maximizing Data Liquidity – Universal Protection & Unrivaled Utility

Limitations of Consent and Contract for EU Employee Data Processing

Unlike many other use cases, consent-based processing will rarely be an option for employee-related data (1). This is because of the imbalance of power between employers and employees; employees can only freely give consent in exceptional circumstances. It is extremely difficult for employers to rely on the lawful basis of consent to process employees' personal data (2).

With consent generally not available, attention naturally turns to contract-based processing. However, in that case processing is limited to what is strictly necessary for the performance of the contract (3). In the employment context, this might cover payroll and benefits administration, but cannot extend to secondary uses like Talent Analytics. Moreover, the use of contract does not constitute an additional safeguard that would enable international transfer of this data for processing outside the EU for the same reasons SCCs alone are now inadequate - government agencies that might surveill the data are not bound by the contract.

As discussed in the webinar, one of the consequences of the Data Protection by Design and by Default (DPbDD) obligations under Article 25 of the GDPR is that if processing can be done using de-identified data it must be. Note that this is true whether processing is done within the EU (localised), or outside the EU. Using GDPR pseudonymisation to de-identify data can be quite useful in establishing the grounds for processing based on legitimate interests.

Legitimate Interest Processing for EU Employee Data

Using a technical and organisation safeguard like GDPR heightened Pseudonymisation can "tip the balance in favour of the controller" so that employee data can be processed under legitimate interests grounds under the GDPR (4). And, if a Data Protection Impact Assessment is performed along these lines prior to export to a non-EU processor, with only the EU exporter retaining the ability to relink to employee identity, this can satisfy Schrems II requirements to allow processing to continue both inside and outside of the EU.

Schrems II Compliant Processing of EU Employee Data Using DPbDD

Many high value uses of EU employee data, like Talent Analytics, can be done in compliance with DPbDD obligations by using de-identified data. Where processing cannot be done using de-identified data, processing is likely to have to be localized, and limited to what can be performed pursuant to performance of a contract. This is because, in the case of international transfers, of the obvious inability to limit parties other than an EU exporter to identify the data subjects, and, in the case of localized processing, of the difficulty of meeting the requirements for legitimate interests processing on identifiable data.

As always, the practicality of DPbDD in a specific situation will be determined by non-privacy related legal requirements applicable to the situation (e.g., employment requirements) but this question provides a good opportunity to review some underlying principles of DPbDD.

Potential DPbDD Approaches

The following three DPbDD options, among others, may be available.

Option No 1:

The identity of the individual could be de-identified by replacing their name and other identifying information with a random pseudonym (we will refer to this pseudonym as “RP1” for Random Pseudonym One) that could be randomly assigned and not derived from the underlying data so that it would not be susceptible to re-identification if intercepted (see https://en.wikipedia.org/wiki/One-time_pad). RP1 could be used to refer to the individual rather than the identifying information. The EU Employer/Exporter could hold the GDPR Article 4(5) “additional information” that is necessary to attribute the RP1 pseudonym to the specific data subject. Care would need to be taken not to use the same RP1 pseudonym to the point that unauthorized third parties could infer, single out or link the RP1 pseudonym to the individual without requiring access to the additional information held separately by the EU Employer/Exporter. Different pseudonyms could be used at different times for different purposes, with the “additional information” necessary to attribute the different pseudonyms to the same individual held by the EU Employer/Exporter.

Option No. 2:

The employee information exported by the EU Employer/Exporter could be aggregated into a format that enables desired processing at a small cohort or “look-alike” group level; only the defined cohort values would be provided to the data importer for processing. Cohorts must be small enough to represent the distinct characteristics, attributes, preferences, activities, behaviours and even location of a real group of data subjects necessary to achieve business objectives from processing data, but large enough that they don’t enable singling out, linking to, or inferences about the identity of individual data subjects (5). This balance can be hard to strike without applying technical measures to reduce re-identification likelihood. Upon receipt of the results of processing by the data importer, the EU Employer/Exporter can then re-link the information to the appropriate employee data using the “additional information that they possess and maintain exclusively in the EU.

Option No. 3:

When there are insufficient numbers of EU employees to create the cohorts suggested in Option No 2 above, synthetic data can be added to the data provided to the data importer which represents fictitious employees while ensuring that the important statistical properties of the sample data are reflected in synthetic data.

Summary

Although consent may be an option in some cases for non-EU based processing of EU personal data, it is rarely available as a basis for processing employee data, and so is not relevant as a Schrems II solution. Contract has very narrow applicability to only specific types of administrative processing and does not address Schrems II requirements for additional safeguards that ensure protection against surveillance. However, where processing of employee data can be done in de-identified form, GDPR pseudonymisation has the three-fold benefit of:

Supporting DPbDD requirements;
Assisting in meeting the requirements for legitimate interests processing; and
Serving as an additional safeguard to help meet Schrems II requirements.

****
The Schrems II Webinar - Lawful Data Transfer - with NOYB, EDPS and industry experts was held on 8 October 2020. Over 2,300 registered and submitted over 900 questions. These 900+ questions were distilled down to the top 25 Frequently Asked Questions (FAQs). These FAQs are being posted to the LinkedIn Schrems II group for comments by the community and at SchremsII.com/FAQs. If you are not already a member of the Schrems II LinkedIn group, we encourage you to join to learn and participate in the discussion. A summary, transcript and replay of the webinar can be viewed at SchremsII.com/learn.

******
(1) See Section 3.1.1 in Guidelines on Consent under Regulation 2016/679 (wp259rev.01) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 at page 6.
(2) https://www.cooleygo.com/gdpr-a-guide-for-employers/
(3) See Section III.2.2 of Opinion 06/2014 on the Notion of Legitimate Interests https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf at page 16.
(4) See Section III.3 of Opinion 06/2014 on the Notion of Legitimate Interests https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf at page 23 - 43.
(5) For example, see https://www.anonos.com/variant-twin-value-proposition

Schrems II FAQs from
Anonos
email us here