# Planview Transfer Impact Assessment

# Planview Services

## Overview

A Transfer Impact Assessment (TIA) is mandatory for any business that transfers personal data from EU to a third country. The subject matter of this TIA is to ensure conformity to the legal obligations Planview is subject to when such transfers are performed. This TIA aims at providing clear and exhaustive information of Planview's data transfers, and to serve as a tool for Planview customers when performing their own legally required TIA's of personal data shared with Planview in the context of the use of Planview's SaaS Products and Services

This document structure follows the steps established by the European Data Protection Board (EDPB) as defined in the *Recommendations (01/2020 ) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* and illustrate different scenarios where customer data is transferred to and from Planview.

*As data controllers/exporters, Planview customers are required and responsible for performing their own assessments based on the information provided in this document. This document has information purposes only and should not be interpreted as an obligation or commitment from Planview or any of its affiliates or suppliers. The services and products described in this document may be subject to changes without notice. Planview is exclusively bound by the terms and conditions as defined in agreements with customers and this document should suffice as an addition or alteration to any of them.*

---

## Step 1: Know your transfers

When providing our SaaS solution services Planview acts as a data processor, processing personal data on behalf of our customers and according to their direct instructions. Planview services are built up on an infrastructure with the highest quality and security standards in order to meet our customers' requirements and expectations of data protection. Planview relies on international data transfers of such data. These transfers can be either internal within the Planview Group, or external, when the data is transferred to one of Planview's sub-processors that support and facilitate the service.

### Internal Transfers

Planview SaaS products are used by customers in multiple geographical locations around the globe, encompassing different time zones. Accordingly, we understand that providing our

services with a high standard of quality globally requires a global presence to ensure 24/7 supportservices to our customers.

The various Planview offices provide requested support services to customers. Occasionally, these services may comprise international transfer occurring by means of access to personal dataof data subjects (i.e. *users* of our services) located in the EU from one of our offices outside EU. Such accesses are only triggered by an explicit request by the data controller and/or users submitting a request ticket. Planview does not process personal data without a direct instructionfrom its customers and/or users.

Planview support services are performed from the following locations:

| Planview SaaS Product | Planview Location |
|---|---|
| **ProjectPlace** | Sweden<br>USA<br>India |
| **Portfolios** | Germany<br>UK<br>USA<br>India |
| **Enterprise Architecture** | Germany<br>UK<br>USA<br>India |
| **PPM Pro** | Sweden<br>USA<br>India |
| **AgilePlace** | Sweden<br>USA<br>India |
| **IdeaPlace** | Sweden<br>USA<br>India |
| **Daptiv** | France<br>USA<br>India |
| **ChangePoint** | France<br>USA<br>India |
| **Barometer** | USA |
| **AdaptiveWork** | USA |

| | |
|---|---|
| | Israel<br>India |
| **Tasktop Hub** | UK<br>USA<br>Australia<br>Canada |
| **Tasktop Viz** | UK<br>USA<br>Australia<br>Canada |
| **Advisor** | USA |

**External Transfers**

A SaaS solution is built upon an infrastructure of several components. Planview's services are supported by infrastructure facilitators (i.e., sub-processors) which are disposed globally. These sub-processors process PII on behalf of Planview to provide security and monitoring of use in order for the services to function and protect the information therein.

At Planview, every sub-processor is thoroughly evaluated based on high security and privacy standards before engagement. At the initial stages of the onboarding the vendor is also submitted through a Data Protection Impact Assessment as required by the applicable privacy and data protection regulation. Planview requires its sub-processors to adhere to equivalent obligations as those required from Planview's customers (where Planview is a Processor), including security and privacy specific requirements that are not only legally but also contractually required for specific reasons.

After being onboarded, the sub-processors are constantly monitored for quality, privacy and security controls. At least once a year, our sub-processors are also audited against the agreements signed.

Sub-processors are listed on Planview's Customer Success Center website. Notices of changes ofsub-processors will be announced on the Planview Status website which can be subscribed to forupdates.

**Step 2: Identify the transfer tools you are relying on**

- When customers provide personal data originating from the European Economic Area (EEA) to a Planview entity within the European Union (EU), no transfer occurs and no transfer mechanism applies as no personal data leaves the Union. In the event customersand/or users submit a support ticket, assistance may be required by support

of other Planview Group entities that may be located outside the EU. Planview uses the EU Standard Contractual Model Clauses (SCC) the transfer mechanism to provide appropriatesafeguards to the transfer when Planview transfer such data to any of its third country- based entities.

- If customers transfer personal data originating from the European Economic Area (EEA) to a Planview entity outside the EEA, we highly encourage customers to sign SCCs as an Annex to the Planview DPA. This may be the case when a third country-based customer offers any Planview services to its employees based in EU.

**Step 3: Assess the effectiveness of your transfer tool in light of the law and practice in the thirdcountry**

Laws that may impinge on the effectiveness of the transfer tools (SCCs) in the **US Laws** that may impinge on the effectiveness of the transfer tools (SCCs) in the **US**

In Schrems II, the Court of Justice of the European Union (CJEU) identified two laws that may impinge on the effectiveness of the appropriate safeguards:

1. **Foreign Intelligence Surveillance Act (15 U.S.C § 1681) ('FISA'):** *establishes the standardsand procedures for conducting electronic surveillance for foreign intelligence purposes in the USA.*

2. **Executive Order 12333 (E.O. 1233):** *is a general organizing directive that (1) assigns different U.S. intelligence agencies responsibility for different types of overt and clandestine intelligence collection and counterintelligence activities, and (2) places restrictions on certain agencies' activities.*

The CJEU's decision on Schrems II focused on assessing the validity of the Decision 2016/1250 (Privacy Shield) based on the existence of these two laws. The scope was not to assess *any* personal data transfer to a third country. The conclusion by the CJEU was that appropriate safeguards remain as lawful data transfer mechanism under EU law *provided* that additional necessary assessments and measures are put into place. This outcome is reinforced by the Recommendations from the EDPB which clarify the necessity to assess the legal framework of the third country and to apply supplementary measures if needed.

Based on CJEU's conclusion, Planview has taken the following actions in determining the lawfulness of its transfers.

Do these laws apply to Planview?

1. **Foreign Intelligence Surveillance Act Section 702 ('FISA 702')**

   When providing its services from the US, Planview could be subject to FISA 702 as Planview may be considered a "remote computing service provider". Nonetheless, Planview considers that both practice and reported precedents show that the probabilities of public authorities seeking to access data held or transferred by Planview are significantly low. The Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II White Paper (White Paper) clarifies the low unlikelihood of information being target by US authorities by stating that companies whose transfers merely consist of "(…) *ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S.intelligence agencies would seek to collect that data*.". Accordingly, and having in mind the nature of the processing activities linked with Planview SaaS services, it is fair to conclude that this data is not likely to be of interest to US intelligence authorities.

2. **Executive Order 12333 (E.O. 1233)**

   The previously mentioned White Paper also clarified that this Executive Order by itself does not allow the U.S. government to require any company or person to disclose data. Any requests by a U.S government would have to be authorized by statute (such as FISA702) and target specific persons or identifiers. Additionally, the White Paper also clarifiesthat bulk collection of information (which was Schrems II main concern) is expressly prohibited.

   **Additional measures subject to a U.S government request**

   A request from a U.S law enforcement government agency would be vetted by the Data Privacy Officer on a case-by-case basis. If the request contradicts the legal obligations Planview as a data processor is subject to, it will be rejected (and subject to an appeal bythe requestor if it insists to proceed). Planview's Data Privacy Officer will inform the customer in the event a request is made, and seek additional guidance as providing accessneeds additional instructions from the customer (being the data controller).

Laws that may impinge on the effectiveness of the transfer tools (SCCs) in the **India Laws** that may impinge on the effectiveness of the transfer tools (SCCs) in **India**

The right to privacy has been recognized by the Supreme Court of India as a fundamental right under the Constitution of India. The Court also stated that this right is not limited to Indian citizens, giving EU residences the access to judicial remedies in case of infringing actions of Indian authorities. Additionally, any interception of electronic data (such as Section 69 of the IT Act 2000) is based on clear, precise, and accessible rules which respect the necessity and proportionality safeguards required by the EDPB.

Do these laws apply to Planview?

Notwithstanding, Planview does not host EU customer data in India. The transfers of EU customer data to India are exclusively limited to the access to the information necessary perform support services upon a customer request. Hence, Planview believes that the safeguards established in the Indian legal framework together with Planview's technical and organizational measures provide the appropriate safeguards necessary to protect customer data and ensure a lawful transfer under EU law.

**Step 4: Adopt supplementary measures**

Planview is committed to protect its customer's data to the highest degree and hence, despite the technically low likelihood of a law impinging on the effectiveness of the transfer tools applied,Planview has implemented several additional technical and organizational measures, as

- ISO 27001 and 27701 (PIMS) certifications
- SOC 2 reports
- Annual Pen-tests
- Encryption
- Security and privacy e-learnings and seminars (frequently, depending on the authorization)
- Internal policies and instructions to employees (annually updated and more often if needed)
- Internal authorization for access to data

- Incident Management Response Plan

- Planview requires its sub-processors to adhere to equivalent obligations as those requiredfrom Planview's customers (where Planview is a Processor), including security and privacy specific requirements that are not only legally but also contractually required for specificreasons

Data Protection enablement:

**Confidentiality**

- Hardware located in secure facilities meeting rigorous industry standards such as ISO27001 and 27701 / SOC 2
- Access to production systems limited to authorized personnel utilizing multi-factor authentication
- Standard encryption methods (TLS for data in transit / AES for data at rest) to ensure datasafety.

**Integrity**

- Data backups performed regularly and available for restoral should corruption occur.
- Write access to data strictly administered.
- Data / input validation to ensure complete, accurate data

**Availability and Resilience**

Suitable measures to ensure that personal data is protected from accidental destruction or loss.This is accomplished by:

- Redundant service infrastructure within data centers.
- Secure data centers that provide highest physical security, redundant power and infrastructure redundancy.

**Procedures for regular testing, assessment and evaluation**

- Third party penetration testing performed at regular intervals.
- Business continuity exercises performed at regular intervals.
- Protection by Design and Default.
- Ongoing evaluations to identify and remediate vulnerabilities.

**Step 5: Take any required formal steps**

Considering Planview relies on supplementary measures in addition to SCCs, there is no need to request authorization from the competent Supervisory Authority. Nonetheless, any competent Supervisory Authority is legally permitted and have the power to review the supplementary measures applied where required.

**Step 6: Re-evaluate at appropriate intervals**

Planview has implemented a Privacy Management Program (PMP) to ensure compliance with applicable privacy and data protection regulations. The PMP is managed by the Data Privacy Officer who is supported by Planview's Privacy Team. Among the focuses of the PMP is the constant monitoring of the developments in third countries' legal frameworks and their potentialimpact on the effectiveness of the applied transfer tools.

Furthermore, the PMP implementation is audited annually against ISO 27701 (PIMS) controls both internally and externally, to ensure Planview's ISO 27701 certification remains unaltered. Customers have access to the ISO certifications and Statements of Applicability through the Planview Customer Success Center.

---

*Last updated: 10/02/23*