

Planview Transfer Impact Assessment

Planview Services

Last updated: 8 October 2026

Overview

A Transfer Impact Assessment (TIA) is required when assessing the effectiveness of appropriate safeguards for transfers of personal data from the European Union (EU) or the European Economic Area (EEA) to a third country. Transfers of personal data from other countries may also require an assessment under the applicable privacy and data protection laws. As such, this TIA covers transfers to the destinations assessed below from the EU/EEA and other countries, including transfers into the EU/EEA, where relevant to the provision of Planview's services.

The subject matter of this TIA is to ensure conformity with the legal obligations Planview is subject to when such transfers are performed, namely to provide our customers with the appropriate information so that they can demonstrate compliance with their privacy and data protection obligations. This TIA aims at providing clear information on Planview's data transfers, and to serve as a tool for Planview customers when performing their own legally required TIAs of personal data shared with Planview in the context of the use of Planview's SaaS platform and related 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](#) (the 'Recommendations') and illustrates different scenarios where customer data is transferred to and from Planview. These steps also provide a structure for considering transfers from other countries, without replacing the requirements of the laws applicable to those transfers.

As data controllers/exporters, Planview customers are required and responsible for performing their own assessments, where required by applicable law, based on the information provided in this document and the circumstances of their transfers. This document is for 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 not suffice as an addition or alteration to any of them.

Step 1: Know your transfers

When providing our SaaS 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 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 to provide the contracted services. These transfers can be either internal, if performed within the Planview group, or external, when the data is transferred to one of Planview's sub-processors that support and facilitate the services.

A. Internal Transfers

Planview's SaaS services 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 support services to our customers.

The various Planview group entities provide requested support services to customers. Occasionally, these services may comprise international transfers of personal data occurring by means of written or verbal communication with our support team and/or access to personal data of data subjects (i.e. *users* of our services) located in the EU/EEA or other countries from one of our entities in another country. Such accesses are only triggered by an explicit request by the data controller and/or users submitting a request ticket, and solely for the purpose of providing the requested support services. Planview does not transfer personal data internationally without a direct instruction or authorization from our customers and/or users.

Information about the Planview group entities involved in the provision of support services, as well as their locations, is available on [Planview's Sub-Processor website](#).

B. 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 personal data on behalf of Planview to perform a range of activities, including but not limited to: providing security and monitoring of use in order for the services to function and to protect the information therein; providing incident detection and response services; providing on-demand cloud computing platforms, storage, data centers and data backups; authenticating users when accessing the services; enabling communication with and between the users; collecting data on application usage for analytics purposes so that Planview may improve and better tailor our services and features; and supporting AI-powered features, such as large language models (LLMs).

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 to a vendor privacy risk assessment as required by the applicable privacy and data protection regulations. Planview has written data processing agreements (DPAs) in place with all sub-processors requiring them to adhere to equivalent obligations as those required by Planview's customers (where Planview is a data processor), including security and privacy specific requirements that are not only legally but also contractually required.

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 relevant security controls to verify their compliance with the obligations set forth in the DPAs.

Sub-processors are listed on [Planview's Sub-Processor website](#). Notices of changes of sub-processors will be announced on the [Planview Status website](#) which can be subscribed to for updates.

Step 2: Identify the transfer tools you are relying on

- When customers provide personal data from within the EU/EEA to a Planview entity within the EU/EEA, no transfer of personal data to a third country occurs and no transfer mechanism under Chapter V of the GDPR applies as no personal data leaves the EU/EEA. In the event customers and/or users submit a support ticket, assistance may be required by support of other Planview group entities that may be located outside the EU/EEA. Planview uses the EU Standard Contractual Model Clauses (EU SCCs)¹ as an internal transfer mechanism to provide appropriate safeguards for the transfer when Planview EU/EEA entities transfer such data to any of the group's third country- based entities.
- If customers make a transfer of personal data subject to Chapter V of the GDPR to a Planview entity outside the EU/EEA, an applicable transfer mechanism is required. Where the transfer is not covered by an applicable adequacy decision, customers should sign the EU SCCs as an Annex to the Planview DPA, where applicable. This may be relevant when a third country-based customer offers any Planview services to its employees based in the EU, depending on the applicability of the GDPR and the circumstances of the transfer.

¹ [Commission Implementing Decision \(EU\) 2021/914 of 4 June 2021](#) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

- If Planview needs to transfer the customer users' personal data subject to Chapter V of the GDPR to sub-processors located outside the EU/EEA, we shall rely on one of the following transfer mechanisms, as applicable: an adequacy decision adopted by the European Commission (as in the case of Canada for commercial organizations, Israel, the UK, or the US for commercial organizations participating in the EU-U.S. Data Privacy Framework); or, if such a decision is not yet in place, the EU SCCs signed between Planview and that sub-processor.
- For transfers from countries outside the EU/EEA to a Planview entity or sub-processor in any of the destinations covered by this TIA, including the EU/EEA, the applicable source-country law determines the required transfer mechanism. Depending on that law, this may be recognition of adequate protection, approved contractual safeguards, or another permitted basis. Where required, the relevant safeguards may include the EU SCCs, the UK International Data Transfer Agreement or UK Addendum to the EU SCCs, the EU SCCs with the adaptations required under Swiss law, or safeguards required by other applicable laws. When the EU SCCs and/or other abovementioned transfer mechanisms do not, by themselves, satisfy the transfer requirements of the source-country, Planview partners with the customer or sub-processor, as applicable, to ensure compliance with the local localization requirements, regulatory approvals and restrictions on onward transfers.

Notices of changes to the transfer tools that we rely on will be announced on the [Planview Status website](#) which can be subscribed to for updates.

According to the [Recommendations](#), for transfers of personal data subject to Chapter V of the GDPR, if the European Commission has already declared the country, region or sector to which the personal data is transferred as adequate through one of its adequacy decisions under Article 45 GDPR or under the previous Directive 95/46 (as long as the decision is still in force), no additional Chapter V transfer safeguards or assessment of the effectiveness of such safeguards are required for a transfer within the scope of that decision. As such, and because the corresponding adequacy decisions are still in force, the following third countries to which Planview may transfer personal data will not be further analyzed in this TIA for transfers covered by those decisions: Canada ([Commission Decision 2002/2/EC](#)), Israel ([Commission Decision 2011/61/EU](#)), and the United Kingdom ([Commission Implementing Decision \(EU\) 2021/1772](#)). These European Commission decisions do not, by themselves, establish the lawfulness of transfers from other countries to those destinations; the applicable source-country requirements are assessed separately. Nonetheless, certain countries recognize destinations covered by European Commission adequacy decisions as adequate under their own laws, or take those decisions into account when assessing the level of protection afforded by a destination, which may facilitate transfers subject to the scope and conditions of the applicable source-country rules.

Step 3: Assess the effectiveness of your transfer tool in light of the law and practice in the destination country

The following sections consider the laws and practices in the destination countries that may affect the protection of personal data received from the EU/EEA or other countries. References to EU SCCs, the Recommendations and EU law address the EU/EEA transfer requirements and should be read together with Step 2 for transfers subject to other laws.

A. United States of America (US)

Laws that may impinge on the effectiveness of the transfer tools (including EU SCCs, where applicable and where the transfer is not covered by the EU-U.S. Data Privacy Framework) 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 implemented in the context of transfers of personal data to the US:

1. [Foreign Intelligence Surveillance Act \(15 U.S.C § 1681\) \('FISA'\)](#): *establishes the standards and procedures for conducting electronic surveillance for foreign intelligence purposes in the USA.*
2. [Executive Order 12333 \(E.O. 12333\)](#): *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 Commission Implementing Decision (EU) 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 transfers to the US subject to appropriate safeguards, such as the EU SCCs, remain lawful under EU law *provided* that additional necessary assessments and measures are put into place to ensure that data subjects whose personal data are transferred are afforded a level of protection essentially equivalent to that guaranteed within the EU. This outcome is reinforced by the [Recommendations](#) which clarify the necessity to assess the legal framework of the third country and to apply supplementary measures if needed.

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

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 likelihood of information being targeted 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. 12333)

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 FISA 702) and target specific persons or identifiers. Additionally, the White Paper also clarifies that bulk collection of information (which was Schrems II’s 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 Planview Data Privacy Officer on a case-by-case basis. If the request contradicts the legal obligations Planview as a data processor is subject to and is not legally binding, it will be rejected (and subject to an appeal by the requestor if it insists to proceed). Planview’s Data Privacy Officer will inform the customer in the event a request is made (unless prohibited by law or a legally binding order of such body or agency, in which case Planview will use commercially reasonable efforts to obtain a waiver of such prohibition), and seek additional guidance as providing access to customer data needs additional instructions from the customer (being the data controller).

The EU-U.S. Data Privacy Framework (DPF)

On July 10, 2023, the European Commission adopted its adequacy decision for the EU-U.S. DPF, concluding that the US ensures an adequate level of protection (compared to that of the EU) for personal data transferred from the EU to US companies participating in the EU-U.S. DPF. The adequacy decision followed the US' signature of an [Executive Order](#) on 'Enhancing Safeguards for United States Signals Intelligence Activities', which introduced new binding safeguards to address the points raised by the CJEU in its Schrems II decision.

The US-based entities within the Planview Group are certified under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, meaning that transfers within the scope of the respective certifications from the EU/EEA, the UK or Switzerland may rely on the applicable framework without additional transfer safeguards being necessary. While these frameworks do not provide a general transfer basis for data originating from all other countries, the changes implemented in this context remain relevant to assess the effectiveness of appropriate safeguards for transfers of personal data from those other countries to the US, as mentioned below. Additionally, a significant amount of Planview's sub-processors is also currently certified under the EU-U.S. DPF.

In any case, even if some of Planview's internal or external transfers of personal data to the US do not rely on the European Commission's adequacy decision under the EU-U.S. DPF or on the corresponding decisions for the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF (instead using another transfer mechanism such as the EU SCCs), all the safeguards that have been put in place by the US Government in the area of national security and which led to the adoption of those decisions still apply to all data transfers to the US, therefore increasing the overall level of protection for the data subjects whose personal data are transferred. Notably, the limitations and safeguards provided for in the [Executive Order](#) signed by President Biden on October 2022:

- ensure that data can be accessed by US intelligence agencies only to the extent of what is necessary and proportionate to protect national security;
- enhance oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and
- establish an independent and impartial redress mechanism, which includes a new Data Protection Review Court, to handle and resolve complaints from Europeans concerning the collection of their data by US national security authorities for national security purposes.

B. India

Laws that may impinge on the effectiveness of the transfer tools (including EU SCCs, where applicable) in India

1. **Telecommunications Act, 2023**: establishes the government's power to take possession of telecommunication services or telecommunication networks and to directly intercept or disclose messages in case of public emergencies or in the interest of public safety. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, as amended in 2025, establish the relevant procedural safeguards.
2. **Information Technology (IT) Act, 2000**: establishes that government agencies may intercept, monitor, or decrypt electronic information, as well as monitor and collect traffic data or information that is exchanged through a computer resource. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009, issued under the IT Act, establish procedural rules to carry out this interception and monitoring.
3. **Sensitive Personal Data or Information (SPDI) Rules, 2011**: regulates the handling of specified sensitive personal data (e.g., passwords, financial data, health and medical-related data, biometrics, and sexual orientation). Where applicable, Rule 6 permits disclosure of this information to government agencies mandated by law for specified purposes, subject to its conditions.

Based on the assessment of the abovementioned third country laws, Planview has taken the following actions in determining the lawfulness of its transfers to India:

Do these laws apply to Planview?

1. Telecommunications Act, 2023

Planview considers to be outside the scope of this Act, since it regulates entities that provide telecommunications services or operate telecommunications networks, which involve the transmission of messages via electromagnetic systems. As a SaaS service provider, Planview offers application-layer services that run over existing internet infrastructure and do not themselves transmit messages or operate transmission networks.

2. Information Technology (IT) Act, 2000

When providing its services in India, Planview could be subject to Sections 69 and 69B of the IT Act governing the interception, monitoring or decryption of information and the monitoring and collection of traffic data for cybersecurity purposes, respectively. These provisions apply broadly to any 'intermediary' (person or organization receiving, storing or transmitting electronic records or providing services with respect to those records) or person in-charge of a computer resource (including data and software). However, Planview considers that the legal framework for the exercise of these governmental powers provides reasonable certainty of the low likelihood that we would be the subject of a direction for interception, monitor or decryption, given that the law states that such directions may only be issued by competent authorities when the required information cannot be obtained by any other reasonable means, and provides procedural safeguards such as authorization, duration limits and review. Since Planview provides enterprise SaaS solutions for project and portfolio management, it is highly unlikely that our systems would contain information relevant to the legitimate grounds admissible for such directions to be issued (such as national security, public order, or criminal investigations).

3. Sensitive Personal Data or Information (SPDI) Rules, 2011

The applicability of the SPDI Rules to Planview must take into consideration the Indian [Government's clarification of 24 August 2011](#), according to which bodies corporate handling sensitive information under contractual obligations with legal entities (within or outside of India) are not subject to Rules 5 and 6, while services provided under a direct contractual relationship with the data subject who shares the sensitive information remain subject to those Rules. Since Planview operates in the B2B industry and only processes customer and user personal data under agreements with legal entities, it is fair to conclude that Planview is not subject to Rule 6 of the SPDI Rules as a basis for government disclosure of sensitive information. At any rate, it also bears mentioning that Planview does not have access to any sensitive personal data from customers or users, as defined in the Rules, other than the passwords used to login in our SaaS services. Moreover, even if Rule 6 was applicable, government agencies may only require this information for the purposes of verification of identity, or for the prevention, detection, investigation, prosecution and punishment of offences – purposes for which the password to Planview's SaaS services is significantly unlikely to prove useful or relevant.

Indian data protection legal framework and additional measures

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 non-citizens from other countries 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 Recommendations.

India's data protection regime is now primarily governed by the Digital Personal Data Protection Act, 2023 (DPDPA), supported by the Digital Personal Data Protection Rules, 2025. When the core DPDPA processing obligations, individual rights and remaining substantive provisions enter into force on May 2027, they will replace the limited provisions of the IT Act 2000 and of the SPDI Rules with a comprehensive framework focused on individual rights and responsible data processing. The DPDPA strengthens data protection safeguards by introducing principles such as accuracy, lawfulness, data minimization, and storage limitation, while granting individuals rights to access, correct and erase their personal data, and to have access to an effective redress mechanism. It also establishes the Data Protection Board of India (DPBI) to oversee compliance and enforce accountability, reinforcing privacy protections in line with constitutional standards and global best practices.

Notwithstanding, Planview does not use data centers in India as a primary data host location for our customers' data. The transfers of customer data to India are limited to the access to the information necessary to 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 applicable laws.

C. Australia

Laws that may impinge on the effectiveness of the transfer tools (including EU SCCs, where applicable) in Australia

1. **Telecommunications (Interception and Access) Act, 1979 (TIA Act)**: *permits access to telecommunications content and data by Australian law enforcement and security agencies for national security or law enforcement purposes.*
2. **Part 15 of the Telecommunications Act, 1997**: *allows law enforcement and national security agencies to seek assistance from designated communications providers (DCPs) to address technical obstacles to investigations into serious crime and national security threats.*

3. [Surveillance Devices Act, 2004 \(SD Act\)](#): contains exceptions to the prohibition on the use of surveillance devices or the access and altering of data held in computers, allowing authorized law enforcement agencies to apply for warrants and seek authorizations to use tracking and surveillance devices, access data held in a computer, disrupt data held in a computer, and obtain information about criminal networks.

The current electronic surveillance laws in Australia are undergoing reform following the Government's response to the Comprehensive Review of the Legal Framework of the National Intelligence Community. As of the date of this TIA's last update, while the existing framework remains in force, it has been recognized as complex and outdated, and the Australian Government continues to develop draft legislation for a consolidated framework that will repeal and replace the powers currently divided between the TIA Act and the SD Act. Nonetheless, this TIA reflects the current legal framework as it stands today, and will be updated accordingly as further developments and legislative changes are introduced.

As such, based on the assessment of the abovementioned existing third country laws, Planview has taken the following actions in determining the lawfulness of its transfers to Australia:

Do these laws apply to Planview?

1. Telecommunications (Interception and Access) Act, 1979 (TIA Act)

Under the TIA Act, telecommunications data retention obligations, as well as the obligation to have the capability to intercept a communication passing over their system, applies only to telecommunications service providers, such as carriers, carriage service providers, and internet service providers. As a SaaS service provider, Planview offers application-layer services that run over existing internet infrastructure: we do not ourselves provide telecommunication services as defined in the TIA Act, own or operate telecommunications infrastructure, or supply telecommunications services to the public. Consequently, Planview considers to be outside the scope of the TIA Act.

2. Part 15 of the Telecommunications Act, 1997

When providing services used or likely to be used in Australia, Planview could be considered a "designated communication provider (DCP)", thus being under the obligation to assist Australian law enforcement and national security agencies in addressing technical obstacles to investigations. This is supported by the [Australian Department of Home Affairs 'Industry assistance under Part 15 of the Telecommunications Act 1997 – FAQ'](#) (the 'FAQ'), which references cloud service providers under the examples of types of industry assistance that can be required.

This industry assistance framework features a graduated approach for agencies to request assistance from DCPs, spanning from requests for voluntary assistance if the DCP is willing, to notices which compel the DCP to build a technical capability to assist the agencies, the latter being issued by the Attorney-General with the approval of the Minister for Communications. However, there are no standing assistance obligations on DCPs under this framework; providers are only required to take action when an agency serves a formal request or notice. According to the FAQ, *“practically speaking, the majority of companies who meet the definition of designated communications provider will not need to engage with the industry assistance framework.”* Moreover, even if we were served such a notice, the law establishes requirements concerning reasonableness, proportionality, practicability and technical feasibility, as well as clear limits and restrictions that Planview could leverage to contest the request and ensure the protection and confidentiality of customer data – namely, requests must not require a DCP to build or implement a systemic weakness or vulnerability (e.g., agencies cannot request ‘backdoors’ to be built or implemented into Planview’s SaaS services), to inadvertently weaken the information security of other persons, to build a decryption capability or make our encrypted systems less effective, to not fix a security flaw in our products, or to build an interception or data retention capability. Agencies must also obtain a warrant or authorization to allow for communication interception or access to data.

3. Surveillance Devices Act, 2004 (SD Act)

The SD Act establishes procedures for Australian agencies to obtain warranties and authorizations for the use and installation of surveillance and tracking devices, or for the access, retrieval or disruption of data held in computers. It also contains assistance provisions, which may impose obligations on private organizations subject to the applicable statutory conditions. Since Planview does not store customer data on workstations or removable devices, and the data centers used for storage and computing of customer data are managed by our third-party hosting and collocation service providers, there is a considerably low likelihood that even if Planview were subject to such a warrant, any customer data would be accessed or disrupted as a result.

Moreover, the law provides for adequate restrictions, oversight and accountability mechanisms to ensure that electronic surveillance powers are used by Australian agencies in a targeted and proportionate way, in line with the safeguards required by the Recommendations – including the limitation of these surveillance activities to certain types of serious offences, requirements for the secure storage and destruction of records, record-keeping and reporting obligations for the agencies, and oversight and inspection by the Commonwealth Ombudsman or the Inspector General of Intelligence and Security.

Australian data protection legal framework and additional measures

Australia regulates data privacy and protection through a combination of federal, state, and territory laws. At the federal level, the Privacy Act 1988 (Cth), of which the Australian Privacy Principles (APPs) are a cornerstone, is the main data protection legislation and applies to private sector entities with an annual turnover of at least AU\$3 million with an Australian link. Where the relevant Planview entity is subject to the APPs, they regulate how personal information is collected, used, disclosed, and stored by private sector entities, ensuring transparency, lawfulness, purpose limitation, data minimization, storage limitation, accuracy, and security. Individuals have the rights to access and correct their data, as well as to receive information about the processing of such data.

In response to the Privacy Act Review Report 2022, the Australian government has initiated a thorough reform of the Privacy Act which will in principle address some of the concerns raised in 2001 when Australia was last assessed for an adequacy decision by the European Commission, including the existence of a small business exception. The first tranche of these privacy reforms – the Privacy and Other Legislation Amendment Act 2024 (Cth) – was already passed in late 2024, introducing measures to enhance the privacy of individuals (e.g., new tiers of civil penalties and increased transparency requirements for automated decision-making), a new statutory tort for serious invasions of privacy, and new offences to specifically criminalize 'doxing'. At the end of August 2026, the Australian Government further released an exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 for public consultation. This Bill is meant to bolster privacy protections for Australians and help tackle emerging risks from new technologies, including artificial intelligence and wearable devices

Planview hosts customer data in Australia only for customers in APAC and the Middle East (excluding Israel), and not for customers in other regions, in order to respect applicable regional requirements. For customers in these other regions, transfers of customer data to Australia are exclusively limited to the access to the information necessary to perform support services upon a customer request. Planview believes that the safeguards established in the Australian 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 applicable laws.

D. European Union / European Economic Area (EU/EEA)

Laws that may impinge on the effectiveness of the transfer tools in the EU/EEA

1. **General Data Protection Regulation (GDPR)**: *establishes a comprehensive framework for the lawful processing of personal data in the EU/EEA. Article 23 permits the restriction of the obligations and rights provided for in this Regulation under certain conditions. Article 48, in turn, states that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if based on an international agreement in force between the requesting third country and the EU or a Member State.*
2. **Law Enforcement Directive (Directive (EU) 2016/680)**, implemented nationally: *establishes the data-protection requirements governing competent authorities' processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It does not itself establish a general power to compel private entities to disclose personal data; Such underlying power to demand records, conduct searches or intercept communications must be grounded in a separate applicable Union or national law.*
3. **National laws governing law enforcement, intelligence and surveillance**: *may permit public authorities in EU/EEA countries to require disclosure of or obtain access to personal data. The applicable powers and safeguards depend on the country and the purpose of access. Examples of these laws in the countries where Planview may host customer data include the Article 10 Act (G10), the Federal Intelligence Service Act (BNDG) and the Code of Criminal Procedure, in Germany; the Internal Security Code, Book VIII (including L851–L853) and the Code of Criminal Procedure, in France; the Act (2008:717) on Signals Intelligence in Defence Intelligence Activities and the Code of Judicial Procedure, Chapter 27, in Sweden; and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and Criminal Justice Act 2011, section 15, in Ireland.*
4. **ePrivacy Directive (Directive 2002/58/EC)**, implemented nationally: *Article 15(1) of this Directive permits Member States to adopt legislation restricting specified protections (including communications confidentiality and rules on traffic and location data) to enable surveillance, retention, access or disclosure for national security, defense, public security, criminal investigations or prevention of unauthorized use of electronic communications systems, but only where the restriction is necessary, appropriate and proportionate in a democratic society.*

Based on the assessment of the abovementioned laws, Planview has taken the following actions in determining the lawfulness of its transfers to the EU/EEA:

Do these laws apply to Planview?

1. General Data Protection Regulation (GDPR)

When processing personal data in the context of the activities of its EU/EEA establishments, Planview is subject to the GDPR, regardless of whether the data originates from the EU/EEA or another country. Indeed, the protections enshrined in this Regulation are not limited to individuals who are EU/EEA citizens or residents; they apply to any individual whose personal data is processed by a data controller or data processor established in the EU, regardless of where that individual is located.

With regards to Article 23, while it creates a prerogative for the EU or its Member States to restrict GDPR obligations and rights, and thus does not apply directly to Planview, it is possible that Planview becomes indirectly subject to an obligation to respect such a restriction when enshrined in Union or Member State law. However, this Article sets out strong and extensive safeguards for the restriction of GDPR obligations and rights: it must be made only through a legislative measure, respect the essence of fundamental rights and freedoms, be necessary and proportionate in a democratic society, and be limited to important objectives of general public interest (e.g., national and public security, prevention, investigation, detection or prosecution of criminal offences, protection of judicial independence).

2. Law Enforcement Directive (Directive (EU) 2016/680)

Since this Directive applies only to competent public authorities (or other bodies or entities entrusted by Member State law to exercise public authority and public powers) for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, it is not directly applicable to Planview. However, it is worth noting that the Law Enforcement Directive and its national implementing legislation requires strict safeguards to prevent arbitrary or disproportionate processing of personal data by competent authorities in this context, including the need for lawful and necessary processing, specified purposes, proportionate further use, non-excessive collection, data quality, retention controls and appropriate security. These requirements are supported by logging, independent supervision by oversight bodies with meaningful enforcement powers, individual rights and judicial remedies.

3. National laws governing law enforcement, intelligence and surveillance

Planview may be subject to legally binding requests for customer data under the laws of the EU/EEA country concerned. Such powers are, however, subject to the applicable national safeguards and oversight, the European Convention on Human Rights, and, where EU law applies, the EU Charter of Fundamental Rights and the case law of the CJEU. In particular, the German, French, Swedish and Irish surveillance and disclosure regimes share safeguards requiring government access to have a statutory basis and either judicial approval or ministerial authorization with independent supervision or review, pursue specified legitimate purposes, and satisfy applicable necessity and proportionality requirements. Depending on the power concerned, these safeguards include defined thresholds for authorizing access, limits on the scope and duration of surveillance, controls on the use, retention, disclosure and destruction of information, and oversight through courts or specialist independent bodies. The regimes also provide avenues for complaints or legal challenges.

4. ePrivacy Directive (Directive 2002/58/EC)

The national laws transposing this Directive or implementing the prerogative conferred in Article 15(1) primarily impose the obligations to retain specified data, disclose it or facilitate authorized interception in this context on providers of publicly available electronic communications services and public communications networks (such as telecommunications operators, internet access providers and other communications providers falling within the relevant definitions). Since Planview is a SaaS service provider, and does not operate publicly available electronic communications services or public communications networks, Planview considers that it is outside the scope of these obligations.

EU/EEA data protection legal framework and additional measures

In the EU/EEA, privacy and data protection are primarily regulated through the GDPR, which applies throughout the EEA, together with applicable national legislation. The GDPR establishes requirements for lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, security and accountability. Processing in the context of the activities of an EU/EEA establishment is subject to the GDPR within its material scope, regardless of the nationality or residence of the individuals concerned or whether the personal data originates from outside the EU/EEA. As a data processor, Planview is required to comply with the applicable processor obligations, including processing on documented instructions from our customers, ensuring confidentiality, implementing appropriate technical and organizational measures, imposing applicable obligations on sub-processors, and notifying customers without undue delay after becoming aware of a personal data breach. Compliance is overseen by independent supervisory authorities with investigative and corrective powers,

including the power to order restrictions on processing and impose administrative fines, and individuals may exercise their rights with the data controllers, lodge complaints, seek judicial remedies and claim compensation where the legal conditions are met.

The EU/EEA data protection framework is widely recognized as an international benchmark for the protection of personal data. This recognition is reflected in other countries' own adequacy determinations or equivalent transfer provisions. For example, the UK recognizes the EEA under [Schedule 21 of the Data Protection Act 2018](#); Switzerland lists EU/EEA countries in [Annex 1 of its Data Protection Ordinance](#); Uruguay recognizes EU/EEA countries under [Resolution 23/021](#); Argentina recognizes EU Member States under [Disposition 60-E/2016](#); and the Dubai International Financial Centre (DIFC) also recognizes all EU/EEA countries as providing an adequate level of protection under its [Data Export & Sharing](#) framework. These are recognitions under the respective source-country laws, rather than adequacy decisions issued by the European Commission.

Planview hosts customer data in the EU/EEA only for customers in Europe, Africa and Israel, and not for customers in other regions, in order to respect applicable regional requirements. For customers in these other regions, transfers of customer data to the EU/EEA are exclusively limited to the access to the information necessary to perform support services upon a customer request. Planview considers that the EU/EEA legal framework together with Planview's technical and organizational measures provides a high level of protection for customer data transferred to the EU/EEA, ensuring a lawful transfer under applicable laws.

Step 4: Adopt supplementary measures

Planview is committed to protecting our customers' 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, such as those stated in the '[Technical and Organizational Measures](#)' document available on Planview's Trust website.

Step 5: Take any required formal steps

For transfers subject to the GDPR, the use of supplementary measures in addition to the EU SCCs does not, in itself, require authorization from the competent supervisory authority. For transfers subject to other laws, any applicable notification, authorization or other formal requirements are assessed and fulfilled in partnership with the customer or sub-processor, as applicable. Nonetheless, any competent supervisory authority is legally permitted and has 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 the legal frameworks of the source and destination countries and their potential impact 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 Trust website](#).

Last updated: 08/10/26