workfront®

Customer privacy faq

What is the GDPR? What are the key changes that have impacted Workfront? How does Workfront collect, use, share, store and transfer personal data with? What other Privacy Regulations does Workfront conform to? Here are the most Frequently Asked Questions from our customers around data protection and how Workfront has implemented privacy best practices within our organisation.

What is the General Data Protection Regulation (GDPR)?

Enforced on 25th May 2018, the EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The new GDPR compliance requirements affect the way you capture data, how you use data and how you store data, for further information on Workfront's GDPR compliance, please visit our Privacy Policy webpage.

What are the key GDPR changes that have impacted Workfront?

- **Consent.** The conditions for obtaining a valid agreement by a person to use his/her personal data are more rigorous.
- **DPO.** Most companies are required to appoint a Data Protection Officer to serve an an internal resource and external point of contact for privacy compliance at companies.
- **Individuals' Rights.** People have the right to ask an organization for access to their data, to correct it, move it or erase it.
- **Transparency.** People must receive detailed information about how their data will be collected, used, shared, transferred and retained.
- **Privacy by Design.** Companies must embed privacy into the design of their products and services throughout the whole product development lifecycle.
- **Accountability.** Companies must document their data processing activities, data flows and compliance as well as their risk and impact assessments.
- **Processors and Sub-Processors.** Data processors have direct obligations and liabilities under the GDPR, and must be authorized by the data controller to use sub-processors.
- **Data Transfers.** Companies must implement a valid data transfer mechanism to transfer personal data outside of the EEA.
- **Contracts.** Contracts must include mandatory provisions and clarify roles and responsibilities of each party handling personal data.
- **Data breach.** Data controllers are required to notify data breaches to supervisory authorities within 72 hours of awareness and, in some cases, to affected people.
- **Sanctions.** If companies don't meet the obligations of the GDPR, they may face fines of up to 4% of their global annual turnover or EUR 20 million whichever is higher.

What other privacy regulations does Workfront conform to?

California Consumer Privacy Act (CCPA)

California passed the GDPR-esque California Consumer Privacy Act (CCPA) June 28 2018, which will be enforced Jan. 1, 2020. Workfront already has stringent controls in place by continuing to strengthen our security readiness for data protection and privacy of California State residents to ensure that we are well within compliance before the enforcement date.

If you are a resident of California, under the age of 18 and have registered for an account with us, you may ask us to remove content or information that you have posted to our websites. Please visit our website and submit a request via our privacy request portal.

Personal Information Protection and Electronic Documents Act (PIPEDA)

The federal privacy law sets out the ground rules for how private-sector organizations collect, use or disclose personal information in the course of commercial activities across Canada. On November 1, 2018 important changes came into force addressing breach notification rules and processes. Workfront ensures that when processing information of Canadian data subjects, steps have been assessed and addressed in complying with the new rules and regulations into an already robust Data Breach Response Program.

What Certifications does Workfront hold?

Does Workfront have any formal accreditation for data protection standards?

Workfront is **ISO 27001:2013, 27017, and 27018** certified. A copy of the certificate is attainable on our website.

Workfront plans to obtain a **SOC 2 Type II report** mid year in 2019 which will be made available to potential customers at their request.

What customer personal data does Workfront collect?

What personal data does Workfront collect from its customers?

- First Name
- Last Name
- Work Email Address
- Job Role

What personal data does Workfront collect from potential customers?

- First Name
- Last Name
- IP Address
- Company information, including title and contact information for each user

Does Workfront process any Special Categories of Data for its customers?

Workfront does not process Special Categories of Data for the performance of services. No special categories of data will be transferred unless expressly stated in Data Processing agreement (DPA) by the customer. Customers may submit special categories of data into the Workfront platform, to the extent of which is determined and controlled by the customer in its sole discretion except as limited by the DPA.

How does Workfront protect customer data?

Where does Workfront store customer data?

All US customer accounts are stored by AWS in either the US West or US East region, with the US West Region being the primary storage location. EU customer Data is stored in Dublin, Ireland as the primary region and Frankfurt, Germany as the secondary. Workfront has two co-located data centers in Sterling, Virginia and Santa Clara, California.

Does Workfront have an up to date Data Processing Agreement (DPA)?

Workfront's Data Processing Agreement is accessible via our website for customer review. Alternatively, if customers have a DPA that they'd like Workfront to sign, they can do so by sending a copy of their DPA to privacy@workfront.com.

What is Workfront's data retention period for customer data?

Customer data, including backups, are deleted within 60 days of the termination of a customer contract, or within 30 days of receiving a validated request from a customer.

How does Workfront delete customer data?

Workfront deletes customer personal data at the request of the customer or after termination of Workfront's service agreement. The Enterprise Security Office works in collaboration with the Infrastructure team to ensure customer data are deleted using industry-standard data destruction techniques including mechanical media destruction and forensically-sound erasure. Data subject requests for deletion are managed using the DSAR portal (See below).

Does Workfront maintain a Disaster Recovery Plan?

Workfront's provides a high-level overview of the plans maintained by the company in a Security or Emergency event. The Business Continuity Plan (BCP) focuses on sustaining Workfront's business processes during and after a disruption. A copy is made available to customers upon request.

Does Workfront ensure third parties and/or sub processors are bound by a Data Processing Agreement?

Workfront maintains a fully compliant data processing agreement (DPA) and Standard Contractual Clauses (SCC) to ensure requirements are met and bound by third parties and sub processors.

Where can I obtain a copy of Workfront GDPR documents and/or contracts?

A DPA is downloadable off our website.

Any other document must be approved under a Non-Disclosure Agreement (NDA) by our legal team. Contact privacy@workfront.com.

Who are Workfront's Sub-processors?

Workfront's maintains a current list of sub-processors authorized to process personal data for Workfront's services on our Privacy Policy webpage.

How does Workfront comply with Data Subject Rights?

Does Workfront manage Data Subject Access Requests (DSAR)?

Workfront maintains a DSAR portal hosted by OneTrust. Any data subject can submit a data subject request for personal data whereby Workfront is the Controller entity. For more information and enquiries into rectification, erasure, portability, access, objection, restriction or a general privacy inquiry or complaint, access the DSAR portal link on Workfront's Privacy Policy webpage.

How does Workfront fulfil the rights of Data Subjects?

Workfront's DSAR portal specifies the request type being requested, the entity is must then be verified as a data subject of Workfront as a Controller (not processor) and then identification is verified for approval of request. Depending on the request type, subsequent subtasks are completed and applicable teams are notified. Workfront's Privacy Office takes the necessary steps to ensure the DSAR is met within the Regulatory time frame of 30 days.

Does Workfront's provide consent notification and Cookie preferences?

Workfront has a Cookie banner whereby consent notification is given and preference settings can be amended. Implemented by OneTrust, a third party vendor tool manages cookie consent maintained on our external webpage. Please refer to Workfront's Cookie Policy.

Where does Workfront transfer Data?

Does Workfront transfer Data outside the area of origin?

In order to provide the Services and depending on customer location, Workfront and its Subprocessors may transfer Personal Data to (i) countries in the EEA; (ii) countries formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries"); and (iii) the United States and other non-Adequate Countries provided a valid transfer mechanism is in place (see below).

Workfront also performs cross border data transfers to provide a "Follow the Sun" support model, granting 24 hour support and defect resolution services provided by Workfront employees in Yerevan, Armenia to all of our customers.

Does Workfront have safeguards in place for International Data Transfers?

Workfront is certified with the EU-US and SWISS-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Workfront has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/ or our website.

What Privacy practices does Workfront have in place?

Does Workfront deploy employee Privacy trainings?

Workfront administers additional measures to ensure job-specific privacy training provided to all employees so they are proficient in protecting customer data and the laws that are impacted by behavior that endangers data security and privacy.

How is the training completion measured?

Workfront uses a 3rd party training platform that is kept current with changes to the privacy regulatory environment. The 3rd party training platform maintains records of employee completion of the training. GDPR training is required on an annual basis and is part of the New Hire Orientation.

How does Workfront notify its customers in the occurrence of a Data Breach?

Workfront has a defined Data Breach Response Program and will notify impacted customer(s), prior to notifying the appropriate Data Processing Authority. We take the partnership with our customers as a foundational guide based on trust and open communication; and as such, we will communicate any instances of compromised personal data to our customers prior to other sources. Workfront will notify impacted customers via existing communication channels or as documented in contract.

Does Workfront have an up to date Privacy Policy?

See the Privacy section on our website.

Does Workfront have an assigned Data Protection Officer?

Workfront
Attn: Data Protection Officer
3301 Thanksgiving Way, Suite 100 Lehi, Utah 84043, USA
Email: privacy@workfront.com

More Information

Workfront maintains public facing information on its Privacy Policy webpage. On this page, a link is provided to Workfront's Privacy Portal which will allows customers or employees to submit inquiries to the Workfront Privacy Office. There are additional GDPR materials available on our website including our Data Processing Agreement or alternatively you can contact the Privacy Office at privacy@workfront.com.