# OneTrust Employee Rights Automation

Automate Employee Privacy Rights Requests from Intake through Fulfillment

Data privacy continues to be a growing concern for individuals around the world and as more people learn they have the right to issue a Privacy Rights Request (DSAR), the more they are exercising this right. Initially, employees were only given rights under General Data Protection Regulation (GDPR) and excluded from other privacy laws like the California Consumer Privacy Act (CCPA), which focused heavily on consumers. However, California's newest evolution of their privacy law, the California Privacy Rights Act (CPRA), extends those rights originally limited to consumers to employees as well. This expands the scope of Privacy Rights Requests for many organizations as these rights are now extended to more individuals and employee requests pose unique challenges to the organizations that must fulfill them.
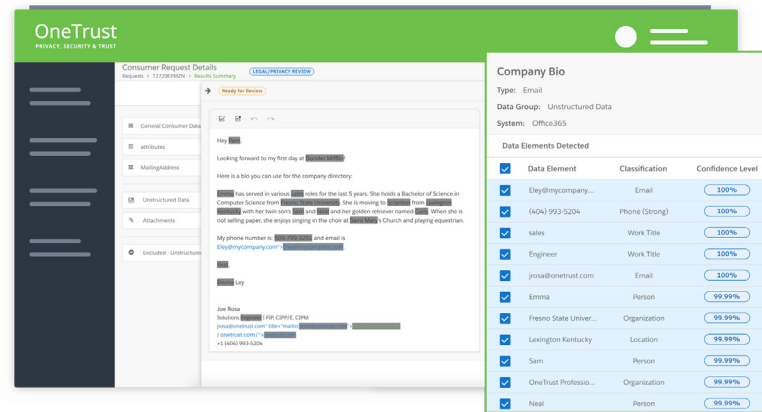
Employee vs Consumer DSARs

Regardless of whether the request is made by a consumer or employee, organizations must find, aggregate, and review data to fulfill a rights request. However, employee requests are generally more challenging than consumer requests for a few reasons. When fulfilling employee DSARs, the amount of data that organizations must comb through to fulfill the requests becomes significantly larger, as most organizations hold more data on their employees than their consumers. Additionally, employee data is much more unstructured in formats such as emails, PDFs, Word documents, and images. Because of the unstructured nature of the data, it is much more likely to contain sensitive information not related to the requestor like others' personal data or confidential company information. These complexities make automation even more critical for employee requests, especially when it comes to the discovery and aggregation of the individual's data and the ability to remove or redact sensitive information that should not be shared with the requestor.

How OneTrust Helps

OneTrust Employee DSAR Automation streamlines the request intake process, automates data discovery, identifies and removes sensitive data from files, strengthens team collaboration and workflows, and allows for a secure delivery of final documents back to the requester. Focused employee workflows and capabilities enable you to:

INTAKE REQUESTS THROUGH EXISTING EMPLOYEE PORTALS

Leverage pre-built integrations and configurable web forms to embed employee request intake into existing HRIS, recruiting, or other employee-facing tools.

SCALE DATA DISCOVERY ACROSS LARGER DATA SETS

Employee data means larger volumes of data and more unstructured data. OneTrust helps scale data discovery & classification across these large data sets and both structured & unstructured data.

ENSURE EMPLOYEE PRIVACY WITH AUTOMATED DATA REDACTION

Unstructured employee data often houses sensitive company data, as well as others' personal data. Leverage AI-driven data redaction to remove sensitive data before responding to the requestor.

OneTrust

PRIVACY, SECURITY & GOVERNANCE

Streamline the Intake Process with Templates & Customization

- Make use of pre-built intake templates or create customized, dynamic forms to embed directly into employee portals
- Easily validate the requester's identity through existing HR systems or single sign-on capabilities
- Utilize information collected through intake forms to quickly route requests and streamline the fulfillment process

Simplify & Automate Workflows

- Easily assign tasks and collaborate with multiple teams within the organization to save time
- Utilize various workflows and easily determine which teams need to be involved in the fulfillment process (i.e. Legal, HR, Privacy, IT)
- Create manual review steps that can be inserted prior to responding to the requestor

Automate Data Discovery

- Automatically discover, classify, and inventory employee data across your IT ecosystem
- Support for cloud, on-premises, and legacy systems and structured and unstructured data
- When a request is received, execute a targeted search of each employee system for data associated with the requestor
- Aggregate, update, flag for deletion, and take other automated actions against the data through robotic process automation

Redact Sensitive Data that Should Not be Shared

- Replace manual tasks with fully automated capabilities for finding and redacting sensitive data that is comingled with the requester's information, such as others' personal data or proprietary company information
- Leverage the latest technology across AI, Machine Learning, Natural Language Processing (NLP), and Optical Character Recognition (OCR) to automate redaction across several file types including documents, PDFs, images, spreadsheets, and emails.

Maintain Secure Communication & Reporting

- Communicate with the requestor through the secure messaging portal during the process – from aiding in clarifying the scope of the request to providing the final data file in the case of an access request
- Access historical data about requests to keep up with benchmarking and regulatory requirements
- Toggle on automated retention rules to purge data associated with a request after a set time period

START A FREE TRIAL OR REQUEST A DEMO AT **ONETRUST.COM**

OneTrust
PRIVACY, SECURITY & GOVERNANCE