

Privacy at Paylocity



September 2024





Paylocity and the Data Privacy Landscape

At Paylocity, we take our responsibility towards data privacy seriously. We are committed to safeguarding the privacy and protecting the personal information of everyone we interact with, including our colleagues, contractors and job applicants, client employees and contractors, and business contacts such as clients, prospects, vendors, and website users.

In keeping with this responsibility, we are committed to complying with applicable privacy and data protection laws and regulations. As a leading provider of payroll and human capital management (HCM) software solutions, Paylocity's services are designed to assist our clients in meeting their own compliance requirements and safeguarding their data.

We provide this informative material to help our clients understand our privacy practices and how they fit with Paylocity's products and services. This also includes information regarding the privacy policies, processes, and controls established by Paylocity.

Please note that the information in this document on legal or technical subject matters is for general awareness only and does not constitute legal or professional advice or warranty of compliance with applicable laws. The content of this document may be subject to change.

Our Privacy Program

Paylocity has a robust global privacy program led by our Chief of Privacy and staffed with a team of professionals with deep expertise in data privacy and data governance. The program has support and oversight from our regulatory compliance and enterprise risk committees, which have representation from all functions of the organization.

The privacy program comprises multiple domains, including governance and accountability, training and awareness, and privacy-by-design, to ensure that personal information is properly handled and protected through the data lifecycle.

Our privacy program is designed to implement the following set of privacy principles. These principles form the bedrock of our global privacy program, ensuring that every interaction and transaction is conducted with the utmost respect for privacy rights and protections:



Governance and Accountability



Transparency and Notice



Purpose Limitation



Data Minimization



Data Retention



Data Quality and Accuracy



Data Security



Protection of Data Subject Rights



Safeguards of Data Transfers

For more information about our approach to privacy, visit our [Privacy Center](#).

How Our Services Fit with Privacy and Data Protection Laws

Whether personal information is subject to the General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), or other US or international privacy or data protection laws, our commitment to privacy is unwavering and reflected in our daily actions and focus on privacy.

We process personal information on behalf of our clients as a data processor. Our service agreement includes a data protection addendum (DPA) that aligns with the requirements and provides the appropriate level of protection for complying with applicable privacy laws, including the GDPR and CCPA.

We also act as a data controller for certain personal information, such as business contact information, when we provide services. This is necessary for us to comply with applicable laws, to manage our operations, including billing, and to improve our services to our clients.

For more information on how we comply with privacy laws around the world, please visit our Privacy Center.



Transparency

We value the trust our clients place in us, thus we've implemented adequate measures to process and protect your personal information appropriately. As such, we have established our Privacy Center to provide visibility into how we handle personal information for the different types of relationships we have.

In our Privacy Center, you can find more information about how we handle information we collect via our products, mobile applications, websites, or otherwise interactions with us.

Data Transfers

The Paylocity group of entities, through our clients, collects and processes personal information of employees across the globe.

Paylocity participates in and certifies compliance with the Data Privacy Framework. Paylocity is committed to comply with applicable data protection laws on the transfer of personal information from other jurisdictions, including:



European Economic Area (EEA)



United Kingdom (UK)



Switzerland



Any country that has implemented data transfer restrictions

Additionally, we've put other measures in place to ensure data transfers are conducted in compliance with applicable data protection laws. For example, when transferring personal information out of the EEA, UK, and Switzerland, we also rely on the applicable EU Standard Contractual Clauses (SCCs).

Subprocessors

We rely on subprocessors to provide some of our services. We have an established process to inform our clients whenever we add new subprocessors. For more information, please visit our Trust Center:

We require our subprocessors to sign a data protection addendum (DPA) that is equally protective as those we enter into with our clients. This DPA covers transferring personal information out of the EEA, UK, and Switzerland, including through SCCs or other approved mechanisms.

Data Subject Rights

Under applicable privacy and data protection laws, individuals have rights with respect to their personal information. These rights include the right to access personal information, the right to correct inaccurate data, and the right to data deletion.

Generally, it is the responsibility of our clients, as data controllers, to respond to data subject requests. To the extent that data subject requests relate to information processed within our products, Paylocity will provide reasonable assistance to ensure our clients can comply with their responsibilities. Note: If a data subject request is made directly to Paylocity, we will promptly direct the data subject to contact their current or former employer, as our clients are the data controllers.

For assistance with responding to data subject requests, our clients can contact the Privacy Office directly at privacy@paylocity.com. Our clients can also work with their account managers to submit requests for assistance.

Data Protection Impact Assessments

We've established processes to evaluate the risks related to processing activities, including privacy impact assessments (PIAs)/Data Protection Impact Assessments (DPIAs).

To the extent that we perform certain processing activities in relation to our services, we provide necessary information to our clients in conducting their PIAs or DPIAs. Paylocity will also assist clients as part of the their consultations with data protection authorities as required.

Privacy Incidents and Data Breaches

While we have implemented robust measures to safeguard personal information, no measure is 100% effective. As such, Paylocity has established processes to identify, contain, mitigate, and remediate any privacy incident that may impact the confidentiality, integrity, or availability of the personal information we process as part of our services.

Additionally, our processes are designed to ensure we can notify our clients without undue delay of privacy incidents they should be made aware of and to assist our clients in managing any adverse impact from any incident caused by Paylocity.



Security is a MUST at Paylocity

We have implemented administrative, technical, and physical security measures to ensure the confidentiality and integrity of the personal information we process. This includes measures that protect against unauthorized or unlawful processing, accidental loss, destruction, or damage.

Paylocity has invested in implementing the highest standards of security as evidenced by the list of our certifications available at our Trust Centers:

Contact Us



More Resources