# Q&A: Paylocity & the General Data Protection Regulation (GDPR)

In anticipation of the May 25, 2018, enforcement date of the European Union's General Data Protection Regulation (GDPR), Paylocity is hard at work implementing a comprehensive compliance program. To learn more about the newest change in data privacy regulation and what it means for our clients please read below.

## What role does Paylocity play in data collection?

Paylocity usually acts as a "Processor" to its customers who are "Controllers" of "Personal Data" of people in the European Union (EU), as these terms are defined under the GDPR. As a provider of cloud-based payroll and human capital management solutions, we process personal data on behalf of our clients that may have employees all over the world. Our clients are the controllers of data. They instruct us regarding the personal data that we process.

## What are the Rights to Personal Data under the GDPR?

The GDPR ensures greater protection of personal data for EU individuals. It includes a comprehensive definition of "personal data" as any information that can be used to identify someone. Further, the GDPR empowers EU consumers by giving them rights to, and control of, their data, and by requiring anyone processing this personal data to better protect it. Some of the fundamental rights of these EU individuals include the right of access to their personal data, the right to rectification of this data, the right to be forgotten (erasure), the right to restrict processing, the right to data portability (and to receive copies of the data) and the right to object. If you want to know more about the tools we have available at Paylocity that allow you (as a data controller) to meet the data subject rights under GDPR please contact us at privacy@paylocity.com.

## What is Paylocity's GDPR Addendum?

To facilitate our customers' compliance with requirements for contracts between entities involved in processing personal data, Paylocity is providing all customers a GDPR Addendum to their subscription services agreement with Paylocity. The GDPR Addendum contains all the terms and commitments required by the GDPR for compliant contracts between Controllers and Processors or Processors and Subprocessors. It is specifically tailored to Paylocity's platform, applications, and architecture, and, when executed, modifies your subscription services agreement to align with the GDPR.

## What about the security of cross-border data transfers?

Paylocity takes privacy very seriously. We treat the data that our customers collect and use on our platform with the utmost sensitivity and employ strict policies and protections to help ensure the privacy of that information. As such, Paylocity is certified under both the EU-US Privacy Shield and the Swiss-US Privacy Shield Frameworks -- which complement the GDPR. The EU-US and Swiss-US Privacy Shield Frameworks are mechanisms composed of data protection principles agreed upon by the US Department of Commerce with both the European Commission (EC) and the Swiss Federal Data Protection and Information Commissioner to facilitate data transfers between the European Economic Area (EEA) and the US and Switzerland and the US.

 

## What are other mechanisms Paylocity has put in place to facilitate compliance with GDPR?

- Data protection – Paylocity has put in place physical, technical, and administrative controls to safeguard client employee data. More information about those controls can be found here: https://www.paylocity.com/security
- Breach notification – Paylocity will inform you – at the contact information you provided to us – of a data breach within 36 hours of discovery so that you can notify your Supervisory Authority within 72 hours of discovery.
- Data Protection Officer – We have voluntarily appointed at DPO. Bradley Schaufenbuel is Paylocity's Data Protection Officer and he can be reached by sending an e-mail message to privacy@paylocity.com or by calling +1-224-857-5159.
- Data Protection Impact Assessments – Paylocity conducts Data Protection Impact Assessments when specific risks occur to the rights of data subjects. For more information, please contact us at privacy@paylocity.com.

## Who needs to execute Paylocity's GDPR Addendum?

***For any question involving the interpretation or applicability of the GDPR, you should consult with your legal counsel.*** In general, customers should execute the GDPR Addendum if it:

- Has an establishment in the European Union, European Economic Area, or Switzerland, regardless of whether the processing takes place in the EU/EEA/Switzerland or not;
- Offers goods or services, irrespective of whether payment is required, to data subjects in the EU/EEA/Switzerland;
- Monitors the behavior of data subjects that takes place within the EU/EEA/Switzerland.

A customer does not need to execute the GDPR Addendum if it does not process any personal data from Europe through its Paylocity services.

## How is data protected going forward?

These are the things that you (as data controller) are responsible for:

- Collecting information about data subjects.
- Obtaining consent from data subjects to collect and use their data for payroll and HCM purposes.
- Ensuring that only the minimal data needed about an employee for payroll and HCM purposes is collected and placed within Paylocity applications.
- Ensuring that the data placed within Paylocity applications is accurate.
- Sign the GDPR Addendum.

## What if you have additional questions?

Please keep in mind that this page does not cover every aspect of EU data privacy, **nor should you consider it legal advice.** This is meant to provide background information and help you better understand Paylocity's strategy to comply with the GDPR. Should you have questions about the GDPR Addendum, please contact us at privacy@paylocity.com. Should you have questions about the GDPR in general, please contact your legal counsel.

 