Revised: May 2018

PDS and European Union General Data Protection Regulation (GDPR)

General Data Protection Regulations, otherwise known as GDPR, is a set of data protection rules that strengthen and unify data protection for individuals across the EU. It's intended to "protect the fundamental rights and freedoms of natural persons and their right to the protection of their personal data". These regulations which are an update to the EU's previously existing data protection rules were approved and adopted by the EU Parliament in April 2016 and go into effect May 25, 2018.

PDS® as your software provider has certain responsibilities under GDPR. Depending on whether you are hosting your PDS Vista® software on premises (on-premise) or PDS is hosting your Vista software on its computers (PDS hosted), the responsibilities vary. When PDS hosts your Vista software for you, PDS has contractual obligations based on the contract with each organization.

PDS is SOC 1 Type 2 (Service Organization Control) compliant. Our SOC report is available upon request. In addition, PDS has an EU-U.S. Privacy Shield certification which is described in its Privacy Policy. If you have any questions on GDPR and PDS, please email privacy@pdssoftware.com.

Below are key practices under GDPR and the rights and freedoms of the natural persons including employees, applicants, etc. ("employees") that are relevant to the PDS Vista® solution.

Processing Employee Personal Data Based on "Consent" vs. "Legitimate Interests"

Employee personal data may also be lawfully processed on the "legitimate interests" of the employer. Examples of "legitimate interests" may include (i) in order to fulfill the employment contract, (ii) to pay the employee, and (iii) payment of various taxes by the

employer, etc. Employers will want to ensure they have clearly captured why personal data is captured from employees and the reasons for each instance in which it is used.

Right of Access

Employees can request to be informed on what you are doing with their data and a record of that data. The right of access includes information about the processing purposes, the processing category of personal data, the receiver or categories of receivers, the planned duration of storage, information about the rights of those impacted such as correction, erasure or restrictions to processing, and the right to object to this processing

Secure Access to Data Based on Need

Vista security provides a means to include or exclude individuals or groups from seeing certain data. This can be configured by the Vista system administrators.

For customers hosted by PDS, PDS provides the appropriate access to its personnel based on need. More on this can be found in PDS' SOC report.

Right to Rectification

GDPR allows the employees to correct and data that they deem incorrect. This would be done in Vista upon request to the customer.

Right to Erasure ("right to be forgotten")

Employees have to the right to request erasure of any and all data that is not deemed necessary for the purpose that it was collected or if consent is withdrawn. Vista provides for the capability for the employer to erase the appropriate data, and in some cases, this can be done by the employee themselves.

For PDS hosted customers, upon termination of the mutual contract, all customer information is removed per the contractual obligations.

Activity Logging

Vista provides detailed activity reports that allow the user to search on specific data sets including but not limited to employee information. Vista Analytics can also be used to give a “real-time” window into the activity.

Breach Notification

For PDS hosted customers, in the event of a data breach, PDS will promptly notify its customers affected on the circumstances surrounding the data breach.

Cross-Border Data Movement

PDS has an EU-U.S. Privacy Shield certification, described in its Privacy Policy, which outlines its policy on data movement.