Personal Data Protection Tools in Priority

Version 18.2

May 2018

Table of Contents

The purpose of this document is to ensure all Priority Software customers that using Priority ERP will enhance their ability to comply with the GDPR.

All current versions of the Priority ERP system already allow customers to fully comply with the GDPR. In some cases, however, compliance may require a manual operational procedure. In order facilitate the process and make it easier for our customers, Priority has developed additional automated tools to support GDPR. These tools are detailed herein and will be supported from Priority V 18.2.

1. Overview

In May 2016, the European Union (EU) adopted a law entitled the **General Data Protection Regulation (GDPR)** which lays down a set of rules relating to the protection of personal data belonging to individuals or “natural persons”. As of 25 May 2018, the GDPR will be a directly applicable law in all member states within the EU.

Additional countries are also in the process of setting down similar laws and regulations. As these laws come into effect, the compliance requirements of companies controlling and processing personal data is increased.

As would be expected, Priority is committed to assisting its customers in complying with any data protection and privacy laws. To that end, Priority Version 18.2 includes a set of tools designed to assist our customers in meeting their compliance requirements with regard to the GDPR. This document describes these new tools.

2. Ensuring the Rights of Individuals: Access, Erasure & Portability

In many cases, Priority will contain data about individuals such as Contact Persons or Candidates who are not necessarily users of the system. Under the new rules, these individuals have the right to obtain this data and/or to request that it be erased.

Since these individuals are not necessarily administrative users within Priority, the course of action available to them is to contact the organization's DPO (Data Protection Officer) with their request to obtain or erase their data.

The tools described herein are designed to assist the DPO to respond to these requests quickly and efficiently. The process works as follows: Priority introduces a new Direct Activation called "Show/Erase Privacy Data" for each of the following Priority Entities:

- Contact Person
- Lead
- Candidate
- Employee

When running the activation in "Display" mode, it will generate a spreadsheet displaying the contents of any fields containing data which might be considered personal information. This realizes the dual rights of Access & Portability. When running in "Erase" mode, the procedure will anonymize the contents of any field considered to be personal. In addition, the status of the entity will be changed to "Erased under Privacy request".

Notes:

- The list of fields considered to contain personal information is determined by a screen-level interface entity. The system will include a default set of fields. Adding or removing fields in this interface is possible through this interface definition.
- It is certainly possible that a customer/s has added custom entities that record data which may be considered personal. In this case, it is the responsibility of the customer/partner to add a similar Activation and Interface, using the standard interfaces supplied by Priority as a template.
- The existence of personal information within Multiline Texts and Document attachments must be managed separately by the customer.
- It remains the responsibility of the DPO to be in contact with the individual who requested the data with regards to the fulfillment of the request.

3. Obtaining and Managing Consent

In addition to ensuring the rights to obtain and/or forget personal data, Priority will include a tool for managing the **consent** of any individual to have his or her data recorded by the organization, regardless of whether this data is recorded in Priority or elsewhere.

To this end, we introduce a new screen in Priority – the **Consents** screen. It enables fine-grained obtainment and management of consent by defining a set of agreements for which the organization requires affirmation or consent. Each set of agreements is bundled as a Consent Edition, with separate agreements for each of the entities listed in the previous section. Once the Consent Edition for an entity is updated, any previous editions are invalidated and the individual will be required to grant consent to the updated set of agreements.

In addition, a new sub-screen for these entities will describe the list of editions to which the individual granted their consent, including the edition number and the timestamp of when the consent was recorded. The main screen for the entity will also include a “Consent Required” flag if the individual has not given their consent for the latest edition of the agreement set.

4. Obtaining Consent from Priority Users

Since candidates, leads and contact persons do not typically log into the organizational Priority system, consent needs to be obtained by a comparable means of manual communication. In contrast, consent can be obtained directly from employees who log into the system.

When a user logs into Priority, the system will check if the user has consented to the latest edition of the Consent agreement as defined in the Consents screen described above. If this is not the case, the system will present this agreement to the user as part of the login process. The user will be blocked from accessing the system if consent is not given.

As described in the previous section, a new sub-screen will be added to the Employees screen which will detail the editions to which the user has granted consent.

5. System Security

Priority includes a wide range of tools designed to ensure the security, confidentiality, integrity, availability and resilience of the data stored within the system. Since these requirements are generally a requirement of privacy laws, this section details some of the tools available within the system that enable them:

- **Privilege Explorer:** This tool is used in order to assign privileges on a per company basis for the system's menus, forms, form columns, programs, reports and warning messages. Users can be restricted from updating certain forms, or running individual programs or reports. You can also restrict access to the contents of a specific form column, to prevent it from being changed or deleted, or even viewed.
- **Priority Web Client**: When using this client, all client-server data communication is encrypted using the same algorithms used by banks in order to secure their websites. In addition, access to attachments is available only to users who have access to the entity containing the attachment.
- **3rd-party Authentication:** Priority includes support for delegating user authentication to 3rd parties, leveraging their authentication methods, such as multi-factor authentication and biometrics.

We invite all Priority Software customers to contact us with any and all questions and concerns regarding GDPR compliance.

Please contact us at info@priority-software.com and we will promptly reply.