BrightArrow's General Data Protection Regulation (GDPR) Compliance Statement

Published: May 8, 2018

Privacy Commitment

The EU General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive (European Directive 95/46/EC), strengthening the rights that EU individuals have over their data, and creating a uniform data protection law across Europe.

BrightArrow ensures compliance with applicable GDPR regulations as a **data processor**. We also will assist our customers, the **data controllers**, to ensure complete control of their private data to empower them to meet their GDPR obligations.

Specifically, we have addressed GDPR data protection requirements that are applicable to data processors.

Data processing

Our ability to fulfill our commitments as a data processor to our customers, the data controllers, is a part of our compliance with GDPR where data controllers are using BrightArrow to process personal data. Because of this requirement, BrightArrow will continue to ensure we're doing the maximum to protect data and improve our processes and procedures where we identify the opportunity.

Controls

We regularly review our Information Security Policy to ensure that we take into account all requirements, confirming we're fulfilling our obligations to GDPR as a data processor.

Our customers depend on us to manage and protect their environments. A strictly limited number of BrightArrow employees are authorized to access customer environments and then only when necessary, according to strict guidelines. Those few employees are required to sign strict confidentiality agreements to ensure full compliance with the privacy requirements. We comply with information security best practices including data encryption.

Data Protection

BrightArrow commits to conforming to information security best practices. In line with GDPR, appropriate measures are assessed in terms of a variety of factors including the sensitivity of the data, the risks to individuals associated with any security breach, state of the art technologies, and the nature of the processing. Regular testing of the effectiveness of all security measures is a continuous process.

In accordance with the GDPR, our policy remains consistent in that we will only ever use personal data which we process on our customers' behalf in accordance with our customers' instructions. We will also promise to implement industry standard security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information.

Third-Party Processors

BrightArrow's hosts its system within the Rackspace™ environment, and Rackspace™ themselves are (amongst other certifications) ISO27001 accredited.

Customer Guidance for *Data Subject Request (SAR)* Responsiveness

An important part of the GDPR requirements is the ability of our Customers to response to their constituents (notably parents') queries and requests regarding GDPR Data Subject Rights. Please note that BrightArrow's Customers prepare their procedures and processes to conform with SARs as they, as Data Controllers, are solely responsible for the handling of and response to SARs.

Requests and Responses

Here are the rights of the Customers' constituents, and the actions the Customer can take to ensure the correct and appropriate action to each such request.

Right to information

Constituents have the right to know what personal information you have and what you do with it.

Action:
Within the List Details and Reports pages, an administrator can find and review all data for a contact.

Right to access
Constituents have the right to receive a copy of their personal data.

Action:
The data can be exported from the List Details and Reports pages and the contact's personal information can be retrieved from the resultant Excel spreadsheet.

Right to rectification
Constituents have the right to request modification of the data.

Action:
Since the BrightArrow data is synchronized with the Student Information System (SIS), any requested modification of the data should be accomplished within the SIS – such data is then automatically transferred to the BrightArrow system.

Right to object to automated decision making
Constituents have the right to request human intervention, as an alternative to the automated process.

Action:
If a constituent requests that they not receive notifications, BrightArrow provides a Do Not Contact page. If they request that their contact information not be transferred at all into the BrightArrow system, BrightArrow has some mechanisms to fulfill that request and the Customer should make that request directly to BrightArrow.

Right of restriction
Constituents can request a block of personal data processing.

Action:
Upon request by Customer, BrightArrow will promptly remove all current and past records of a contact. It will also block subsequent receipt of any data associated with that contact.

Right to portability
Right to receive data back for reuse, in usable electronic form.

Action:
Any and all data associated with a contact can be exported from the List Details and Reports pages and provided by the Customer to the contact in Excel or PDF formats.

Right to erasure
Deletion of the subject's personal data.

Action:
Upon request by Customer, BrightArrow will promptly remove all current and past records of a contact.