Wellbeing Software Group

GDPR Statement

Introduction

The European Union's General Data Protection Regulation (GDPR) comes into effect on 25th May 2018 bringing with it wide ranging changes and new responsibilities for organisations that process personal data. These changes will affect all organisations which hold or process personal data, including the Wellbeing Software Group (hereafter referred to as Wellbeing).

This document outlines the anticipated impact on Wellbeing and our approach to ensuring our compliance with the new legislation.

Are we a data controller or a data processor?

A 'data controller' is an entity that controls how and why personal data is processed and a 'data processor' uses, handles or works with the data under the instruction of the controller. Therefore, Wellbeing is a data processor for the purpose of existing data privacy legislation and GDPR. Wellbeing is also a data controller in that we store and manage data about our customers, suppliers and staff.

How does the GDPR affect us?

The GDPR affects Wellbeing in its capacity as a data controller for the information we store and manage about our customers, suppliers and staff. However, our core business is providing software solutions, technical support, and in some cases hosting, to our customers. In this respect we process data under the instruction of a data controller and therefore we are a data processor.

Consequently, we must take heed and be compliant with the requirements for both data controllers and processors.

How are we becoming compliant?

Wellbeing has always taken its responsibility for information security and data protection seriously owing to our position as a market leader in the development and maintenance of innovative information systems to the UK healthcare sector. Consequently, we have always operated high standards of information security and data protection and we are committed to maintaining those high standards.

Wellbeing has two main areas of focus in preparing for GDPR:

1. Ensuring our own compliance.
2. Assisting the users of our software applications with their compliance.

Our compliance

Prior to the GDPR, Wellbeing implemented company-wide information security and data protection controls through its ISO 27001-certified Information Security management System (ISMS).

Wellbeing has undertaken an external, independent gap analysis of our existing controls against the GDPR's requirements to understand where they need to be augmented or where additional controls need to be introduced.

Wellbeing has used the output from this gap analysis to inform and establish a GDPR compliance programme which includes the following key activities:

- A review of all data processing activities including confirmation of our lawful bases and purposes for processing data, where data resides, how data is secured and who can access or change data.
- Refreshing our staff Data Privacy Awareness Training
- Updates to our internal security processes to meet GDPR requirements including processes associated with data subject rights, personal data breach response, privacy by design and third party compliance
- Updates to internal policies, procedures and privacy notices.
- A review of the contractual terms between Wellbeing and our customers and suppliers

Wellbeing has also appointed a Data Protection Officer (DPO) with responsibility for advising and monitoring our compliance with all applicable data protection laws.

Our customer's compliance

Wellbeing is acutely aware that customers trust us and our software solutions to protect their sensitive data. We therefore commit to ensuring that the security of our customer's data continues to be at the forefront of everything we do and demonstrating this commitment by continuing to submit our ISMS for external validation against ISO 27001 and other industry standards.

Similarly, customers will need to be confident that Wellbeing can assist them in meeting their GDPR obligations. As such, we are committed to applying the principles of privacy by design and default to our products. This includes providing features within our software that customers can leverage for their own compliance, particularly in relation to data subject rights and data protection impact assessments (DPIAs). We will inform our customers when new features become available.

Wellbeing understands the importance of informing our customers of any incidents or breaches that affect their data. Wellbeing is confident that our technical and organisational measures significantly reduce the risk of data breaches however, in the unfortunate event that a breach does occur, we are prepared to provide timely notification to customers and also to assist with any ensuing investigation.

Will our contracts change?

GDPR contains a legal requirement obliging organisations to update existing contracts that deal with data protection to a more detailed standard.

To comply with this requirement Wellbeing is amending our standard terms which sets out each party's obligations in relation to data protection. In incorporating these updates, the document sets out in more detail, each party's responsibilities in relation to how and for what reason either party is collecting, using or handling personal data.

Further questions

If you have any further questions, please contact us at [which email address]