Information Security

Nothing in this document is intended to provide you with,
or should be used as a substitute for, legal advice

02 January 2018

Introduction

The following document provides an introduction to our approach to information security and, in particular, our preparation for the EU General Data Protection Regulation (GDPR).

This document should be read in conjunction with the following documents (also contained in this folder):

Document 1: "Abintegro_Security Overview" [this document]

Document 2: "Abintegro_Statement of Applicability (ISO 27001) & GDPR Compliance" spreadsheet

Document 3: "Abintegro_Technical Architecture" pdf

Document 4: "Abintegro_End User_Privacy Policy" pdf

Document 5: "Abintegro_End User_Terms of Use" pdf

Document 6: "Abintegro_End User_Mobile App Terms" pdf

Document 7: "Abintegro_Client Terms of Use_Data Protection (clause 16) extract" pdf

Document 8: "Abintegro_Obtaining User Consent" pdf

Approach - Secure By Design

Every line of code in the Abintegro platform has been written with your security in mind. We use the very latest framework releases, reuse tried and tested modules, and apply fundamental security considerations to every aspect of software design and development. We also frequently review, and externally test, our platform to keep it ahead of emerging threats.

We're continuously improving our internal processes and security measures to ensure complete platform assurance, Abintegro maintains information security policies that are defined, approved by senior management, used and shared internally. Policies are informed by and aligned to the ISO27001 standard, and we are also pursuing certification for ISO27001.

Furthermore, everyone who works at Abintegro has been security vetted and accepted our confidentiality agreement. We make sure there are several layers of controls that individuals must go through to access user data.

We are committed to maintaining the highest possible data protection standards and ensuring we are, at all times, compliant with relevant legislation. In preparation for the European Union's (EU) General Data Protection Regulation (GDPR) replacing the 1995 Data Protection Act on 25 May 2018, we have undertaken a specific GDPR compliance review exercise (in June 2017), with our specialist GDPR readiness and data protection advisor, to ensure we take any additional legal and operational steps necessary in advance of May 2018. We are also committed to helping our customers with their GDPR compliance journey by providing robust privacy and security protections built into our services and contracts.

Security Measures - Examples

The following are examples of our security measures. Full details of all measures are provided in our Statement of Applicability.

PATCHING: We have automated systems in place that monitor the Abintegro platform for vulnerabilities.

ENCRYPTION AT REST: Our database has automatic encryption at rest.

HTTP STRICT TRANSPORT SECURITY: Our platform forces all requests over HTTPS, ensuring all traffic is secured in transit with TLS and protecting against protocol downgrade attacks.

REGULAR EXTERNAL PEN TESTS: We test our own product regularly by hiring specialist security organisations to attack us from the outside and in.

SECURITY CHECKS ON BUILD: We have automated safeguards in place to check our code for potential issues before anything goes live.

PASSWORD SALTING AND HASHING: We use the most secure cryptographic libraries throughout the platform. Passwords are salted and hashed together using HMACSHA1 and never stored in the clear.

HIGH AVAILABILITY: We've designed the platform to ensure high availability. We have a suite of contingency mechanisms to ensure 24/7 application availability.

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE: We put security at the heart of all our feature design and builds to ensure we are always maintaining our standards at 100%.

CUSTOMER DATA REGULATION: We never move user data out of the secured production environment for testing or any other reason.

Data Protection Overview

We follow the 8 principles of the Data Protection Act (1998), and we're prepared for the General Data Protection Regulation (GDPR). We have a designated Data Protection Officer, and accountability and privacy are principles that are designed into both our software and policies.

In order to use the Abintegro platform, users must be authorised by you (our client). Your users' data is always accessible in easily extracted csv. files from within the platform. We are also registered with the Information Commissioner's Office, with registration number Z1394547.

We regularly review how we can most securely store user data. We protect it in 3 key ways:

1. WHAT WE'RE STORING:

We store only necessary information, as provided by you and your users. Abintegro processes user personal data only in accordance with your instructions.

2. HOW WE'RE STORING IT:

We encrypt user data both at rest and in transit, and our site and storage processes are architected for security. See Security Measures for specific details.

3. WHO CAN ACCESS IT:

We have extensive internal access controls and regulations for the Abintegro team, who only have access to data under limited conditions, and have all been security checked.

Full details are provided in our Statement of Applicability which summarises the objectives and controls that are relevant and applicable to the Abintegro Information Security Management System (ISMS) in accordance with the requirements of ISO 27001:2013 (Information Security).

Data Protection - GDPR compliance

On 25 May 2018, the most significant piece of European data protection legislation to be introduced in 20 years will come into force. The EU General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive. The GDPR strengthens the rights that individuals have regarding personal data relating to them and seeks to unify data protection laws across Europe, regardless of where that data is processed.

Our commitment to GDPR

We are working hard to prepare for the EU's General Data Protection Regulation (GDPR). Keeping users' information safe and secure is one of our top priorities. We are committed to complying with the new legislation and will collaborate with our clients and partners throughout this process.

Your responsibilities as a client

Abintegro clients normally act as the data controller for any personal data they (or their users) provide to Abintegro in connection with their use of Abintegro's services. The data controller determines the purposes and means of processing personal data, while the data processor processes data on behalf of the data controller. Abintegro is a data processor and processes personal data on behalf of the data controller when the controller (and their users) use the Abintegro platform.

Data controllers are responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that any data processing is performed in compliance with the GDPR. Controllers' obligations relate to principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, and accuracy, as well as fulfilling data subjects' rights with respect to their data.

Data Protection - GDPR compliance

Abintegro's obligations under the GDPR: high level overview

Under the GDPR, processors have certain primary obligations in relation to any personal data they process on behalf of a data controller.

As a processor of personal data (e.g. on behalf of clients), Abintegro must:

- immediately inform the controller if in its opinion the controller's instructions infringe the GDPR or other European or national data protection provisions.
- notify the controller without undue delay after becoming aware of a personal data breach.
- assist the controller, where necessary and upon request, in carrying out data protection impact assessments.
- not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- not process those data except on instructions from the controller, unless required to do so by European or national law.

To understand how Abintegro complies with its responsibilities under the GDPR please review the following document: "Abintegro_Statement of Applicability (ISO 27001) & GDPR Compliance".

Data Protection - GDPR compliance

The following summarise the key steps we are taking in conjunction with our clients:

Updated terms

We have updated our client and user terms of use and privacy policy to reflect the obligations of controllers and processors - specifically where we act as a processor of personal data on behalf of our clients. We have also updated our approach to data protection indemnities and liability. These terms of use are being rolled out, in consultation with our clients, in time for May 2018.

Review the following document(s):

Document 4: “Abintegro_End User_Privacy Policy” pdf
Document 5: “Abintegro_End User_Terms of Use” pdf
Document 6: “Abintegro_End User_Mobile App Terms” pdf
Document 7: “Abintegro_Client Terms of Use_Data Protection (clause 16) extract” pdf

Privacy notices

Our privacy policy has been updated to reflect GDPR requirements including: explaining the legal basis for processing the data, data retention periods, individuals right to complain and that the information be provided in concise, easy to understand and clear language.

Review the following document(s):

Document 4: “Abintegro_End User_Privacy Policy” pdf

Data Protection - GDPR compliance

Robust safeguards

We are well placed to meet the security requirements of the GDPR. Our services are backed by robust, technical and organisational safeguards. Full details are available in our Statement of Applicability which summarises the objectives and controls that are relevant and applicable to the Abintegro Information Security Management System (ISMS) in accordance with the requirements of ISO 27001:2013 (Information Security).

Review the following document(s):

Document 2: “Abintegro_Statement of Applicability (ISO 27001) & GDPR Compliance” spreadsheet
Document 3: “Abintegro_Technical Architecture” pdf

Incident response

We will continue to promptly inform our clients of incidents involving customer data in line with the data protection commitments in our terms of use and we will help you identify and respond to security or privacy events (and any personal data breaches under the GDPR) without delay and with all available information.

Review the following document(s):

Document 2: “Abintegro_Statement of Applicability (ISO 27001) & GDPR Compliance” spreadsheet

Data Protection - GDPR compliance

User transparency

We will continue to enhance transparency about how data is used in our services. We provide detailed explanations on how we use data in our privacy policy which is available to you and your users on every page of the Career Centre.

Review the following document(s):

Document 4: “Abintegro_End User_Privacy Policy” pdf

Privacy practices

We already have processes to build privacy into our products from the very earliest stages, and we are further evolving our practices, including Data Protection Impact Assessments, to meet the GDPR’s requirements around Privacy by Design and Privacy by Default.

Review the following document(s):

Document 2: “Abintegro_Statement of Applicability (ISO 27001) & GDPR Compliance” spreadsheet

International transfers

Our client terms of use and privacy policy make it clear that we do not transfer personal data outside the EEA or the EU.

Review the following document(s):

Document 4: “Abintegro_End User_Privacy Policy” pdf

Data Protection - GDPR compliance

User consent

To assist with our clients' responsibility as data controller for ensuring appropriate consents are obtained from users, we are implementing a facility in the Career Centre to present users with necessary consent forms (separate from other terms and conditions) and acceptance buttons. All user consents are maintained on the Career Centre so that we can track these on behalf of our clients. Our privacy policy sets out the process for users withdrawing consent.

Review the following document(s):

Document 8: "Abintegro_Obtaining User Consent" pdf

Further guidance

Existing guidance

- ICO's overview of the GDPR (available here).
- The ICO's updated Privacy Notices code of practice (available here).
- The ICO's Draft guidance on consent under the GDPR (available here).
- The ICO's Draft guidance on contracts and liability (available here).
- The ICO's GDPR checklist for data controllers (available here).
- The ICO's GDPR checklist for data processors (available here).