

# UC Analytics

GDPR Compliance Statement

May 2018

## Code Software GDPR Compliance Statement

### Introduction

The **EU General Data Protection Regulation ("GDPR")** comes into force across the European Union on 25<sup>th</sup> May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21<sup>st</sup> Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

### Our Commitment

**Code Software** are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

**Code Software** are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new policies, procedures, controls and measures to ensure maximum and ongoing compliance.

### How We are Preparing for the GDPR

**Code Software** already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by 25<sup>th</sup> May 2018:-

- **Information Audit** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- **Policies & Procedures** - Implementing data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
  - **Data Protection** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
  - **Data Retention & Erasure** – we have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and

that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

- **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- **International Data Transfers & Third-Party Disclosures** – where **Code Software** stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- **Subject Access Request (SAR)** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- **Legal Basis for Processing** – where relevant we are implementing processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- **Privacy Notice/Policy** – where relevant we are implementing Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining Consent** – where relevant we are revising our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- **Direct Marketing** – **Code Software** do not and will not use any personal information for direct marketing purpose
- **Data Protection Impact Assessments (DPIA)** – **Code Software** does not process personal information that is considered high risk or includes special category/criminal conviction data.

- **Processor Agreements** – We do not use any third-parties to process personal information on our behalf
- **Special Categories Data** - We do not obtain or process any special category information.

### **Data Subject Rights**

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we can provide information of an individual's right to access any personal information that **Code Software** processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

### **Information Security & Technical and Organisational Measures**

Code Software takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Access controls;
- Password policy;
- Encrypted data transfer over SSL channels;

### **GDPR Roles and Employees**

Code Software understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans.

If you have any questions about our preparation for the GDPR, please contact Mark Armstrong who is Code Software's appointed GDPR person / DPO.

## ABOUT US

Formed in 2013, Code is a technology company focusing on analytics, reporting, recording and management solutions for Unified Communications.

As a company our goal is to assist organisation in optimizing their investment in UC, we also strive with our global network of partners to become a trusted and valued part of their eco-system.

We have installations in 5 continents ranging from SME's to multi-national global enterprises.

### UK OFFICE

Queen Ann House  
66 Cricklade Street  
Cirencester  
GL7 1JN  
Glos

**t** +44 (0)1285 657787  
**e** [info@codesoftware.net](mailto:info@codesoftware.net)

### US OFFICE

4500 140th Avenue North  
Suite 101  
Clearwater  
FL 33762  
United States

**t** +1 (774) 763-2278  
**e** [info\\_us@codesoftware.net](mailto:info_us@codesoftware.net)

### ROMANIA OFFICE

Chronos Business Center  
Saulescu nr. 29  
Iasi  
Romania

**t** +403322110035