Crimson Tide & mpro5 GDPR overview

25th May 2018

CONTENTS

Crimson Tide and GDPR

At Crimson Tide Plc, we have been looking after client data for over 20 years and pride ourselves on our ability to secure and protect your data. In May 2018, the new EU GDPR legislation comes into effect and we want to assure our clients that we are ready. Working with Microsoft, our cloud hosting partner, we have put in place the steps required to not only ensure we, the data processors, are compliant but that we enable our clients, the data controllers, to demonstrate their compliance as well.

More detailed, line by line summary information, on the responsibilities applying as a result on the GDPR regulation and how we ensure compliance will be published before the deadline of the 25th of May and tools to help you manage the data you control will be implemented within our web-portal for your use in searching, deleting and anonymising personal data. Our service team will also be available as usual to help with more complex requests.

As an added safeguard, in addition to the security guarantees offered as part of the Azure service we use, Microsoft has also offered the following statement and guarantee:

Microsoft GDPR Statement and Guarantee

Trust is central to Microsoft's mission to empower every person and every organization on the planet to achieve more. So that you can trust the Microsoft products and services you use, we take a principled approach with strong commitments to privacy, security, compliance and transparency. This approach includes helping you on your journey to meet the requirements of the European Union's General Data Protection regulation (GDPR), a privacy regulation which goes into effect on May 25, 2018.

If your organization collects, hosts or analyzes personal data of EU residents, GDPR provisions require you to use third-party data processors who guarantee their ability to implement the technical and organizational requirements of the GDPR. To further earn your trust, we are making contractual commitments available to you that provide key GDPR-related assurances about our services. Our contractual commitments guarantee that you can:

- Respond to requests to correct, amend or delete personal data.
- Detect and report personal data breaches.
- Demonstrate your compliance with the GDPR.

Microsoft is the first global cloud services provider to publicly offer you these contractual commitments. We believe privacy is a fundamental right. The GDPR is an important step forward to further clarify and enable individual privacy rights and look forward to sharing additional updates how we can help you comply with this new regulation and, in the process, advance personal privacy protections. This statement is available directly from the Microsoft website here

Awareness

mpro5 acts as a data processor for each of our customers. We treat the security and privacy of our customers' data with the utmost respect and do not share any data with third-party organisations. Staff at all levels of the organisation are educated towards the key principles of GDPR and secure operating procedures, with controls in place to monitor and enforce adherence.

Information that mpro5 holds

mpro5 only stores personal data where it is required to provide the mpro5 service in accordance with our terms and conditions. For ease of understanding, the personal data register below assesses the type of data that is stored, where it came from, and its purpose.

Personal Data Register

System	Data Point	Source	Shared with	Notes
Internal CRM	Lead Name, Lead Email, Lead Phone Number	Conferences and Shows	None	Opted-in from meetings at shows and conference, or inbound email
Internal CRM	Customer Name, Address, Email	Existing Customers	None	Opted-in from contract
Internal CRM	Contact Name, Address, Email, Telephone Number	Existing Customers	None	Opted-in from contract
Customer Support	Contact Name and Email	Existing Users	None	Opted-in from web form, inbound email, or telephone call
Internal Document Management	Employee Name, Address, Phone Number, Email, National Insurance Number, Payroll Number, Date of Birth	Staff	Payroll Provider	
Customer Installation of mpro5	Customer Name, Address, Email, Phone	Existing Users	None	Corporate contact
Customer Installation of mpro5	Site Name, Address, Email, Phone	Existing Users	None	Corporate contact
Customer Installation of mpro5	Contract Name, Address, Email, Phone	Existing Users	None	Corporate contact
Customer Installation of mpro5	Location Name	Existing Users	None	Corporate contact
Customer Installation of mpro5	Mobile User Name and User Email	Existing Users	None	Corporate - email required for password reset not marketing
Customer Installation of mpro5	Web User Name and User Email	Existing Users	None	Corporate - email required for password reset not marketing
Customer Installation of mpro5	Names of signatories	Existing Users and their customers	None	Required by customers for processing of customers' contracts

How mpro5 communicates privacy information

What we expect of our customers

As a Data Processor for our customers, we expect a duty of care from our customers to ensure that affected people are made aware of the data being held and its purpose.

What our customers can expect of us

Our GDPR statement

Our standard terms and conditions can be found:

1. On any mpro5 contractual agreement
2. On the mpro5 mobile client
3. By logging a GDPR request via our helpdesk

Subject Access Request

At any time, a GDPR request can be submitted via our mpro5 helpdesk. For every subject access request submitted individuals will need to provide:

1. An email address of the associated individual
2. The type of data required
3. The reason for the request

For every subject access request submitted we will:

1. Acknowledge receipt
2. Comply or refuse within 30 days
3. If a refusal is made, we will provide a reason

Our lawful basis for processing personal data

mpro5 processes personal data in accordance with Article 6(1)(b) whereby "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

In simple terms this means that we store and process personal data in the following scenarios:

1. There is a pre-existing contract with the party and we need to process personal data to comply with our obligations under the contract
2. There isn't a pre-existing contract with the party but we have received a request for information relating to our services, for example to provide a quote or a demonstration

mpro5 does not engage in user-profiling activity, or share your data with any third parties for any purpose.

Data Breaches

The mpro5 GDPR framework for processing of data breaches consists of the following stages:

1. Detection
2. Assessment
3. Notification
4. Root Cause Analysis
5. Rectification

Detection

mpro5 includes real-time threat detection from a software perspective. Our teams receive notifications in real-time as to any attempted or successful intrusions within the mpro5 platform. However, in the event of a manual report of a breach from a party, the same process applies.

Assessment

The classification of the personal data held within mpro5 as highlighted in the Personal Data Register means it is highly unlikely to result in discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage to the subject.

That being said, each report is assessed by our technical team and our customers would be notified should breach of any of the above conditions occur.

Notification

Should a breach to the conditions outlined within the assessment criteria occur, mpro5 will:

1. Notify the ICO immediately outlining:
    a. The type of personal data breached
    b. The number of affected subjects
2. Notify each affected subject by email

In the event of large scale breaches affecting multiple customers, social media channels will also be used to broadcast a generic notification pertaining to the breach.

Root Cause Analysis

Once assessment is completed and notifications delivered where required, the mpro5 technical team will analyse how the breach occurred and make recommendations to the management team so as to avoid a future breach.

Rectification

mpro5 will implement where reasonable, all measures suggested from Root Cause Analysis to mitigate a breach of a similar type occurring in the future.

Once rectification has been implemented, notification will occur in the same manner as outlined previously for the successful closure of the breach.

Crimson Tide mpro limited Oakhurst House
77 Mt. Ephraim, Tunbridge
Wells Kent, TN4 8BS

info@crimsontide.co.uk

www.mpro5.com