Supplier - Statement of GDPR Compliance

Introduction
Keeping our customer's IT systems, information and data safe and secure is a top priority for Cosmic. It is also a complex task that relies on technical knowledge as much as staff awareness and commitment.

Data is processed and controlled by Cosmic in order for us to carry out our Contracted Duties with customers. As a Data Processor to you, this document outlines our ability to fulfil our commitments as part of Article 28 of the Regulation. It is reviewed annually by the CEO (Operations) and signed off at Board Level.

We operate in line with ITIL standards and best practice and current information security best practice in developing processes and procedures. Full details of our Privacy Policy are listed on our website.

How Cosmic manages its systems

Management of Information Security

Ultimate responsibility for information security rests with the CEO (Operations) of Cosmic, but on a day-to-day basis the Technology Manager shall be responsible for managing and implementing the policy and related procedures.

Cosmic is obliged to abide by all relevant UK and European Union legislation. Cosmic complies with the following legislation and is registered with the Information Commissioner's Office:

General Data Protection Regulation 2018
Data Protection (Processing of Sensitive Personal Data) Order 2000.
Copyright, Designs and Patents Act (1988)
Computer Misuse Act (1990)

Data Asset review
Cosmic carries out regular reviews of it's own business assets, classifies and assesses risk and decides the best ways to mitigate risks. This is held in an Information Security Policy that is reviewed every year. All staff are trained on the policy and procedures.

Customer's data is reviewed and maintained by the principle of data minimisation. This means that we will only ever seek to keep the data necessary to enact our business activities. We review our Data assets once a year, or earlier if there is a termination, breach or incident.

Monitoring and Logging

Vulnerability scans are carried out annually and active Server Monitoring is in place for 24/7 scanning and server health.

Back-up policy

Cosmic backs up its data regularly. Our on-premise server is backed up on-premise and additional off-premise encrypted daily backup (stored off-site every other day). There is a disaster recovery plan in place to cover events of flooding, fire and theft.

Regular back ups of Cloud services are monitored and stored on EU-located servers and are encrypted end to end and at rest.

Archives are carried out every 6 months and are encrypted and stored safely.
Annual tests are carried out for recovery of data.

Cyber Threat awareness
Cosmic reviews threats as part of its daily activity. Current threats are listed in our Risk Register and updated regularly. We are members of the SW Cyber Security Cluster and CiSP and receive weekly updates on threats. These updates are disseminated throughout the IT and web departments.

Access Controls
Cosmic premises are physically secured with door entry access and the premises manned by a reception desk. Only pre-authorised appointments are allowed onto site.

Access to computer facilities is restricted to authorised users who have business need to use the facilities. Only staff members have access to the Cosmic network.

System access is restricted to staff and all staff permissions that are appropriate to their role. All staff have individual, complex username and passwords to log onto Cosmic networks and services.

Secure Setup, Configuration and Management

All Cosmic's software and hardware is setup and configured to provide the most effective protection for our customers data.

Cosmic runs annual penetration tests for it's own network that identifies any undiscovered issues and patch management is carried out regularly.

Our Technology Manager sets up and configures all software and hardware purchased for our use. We

- Remove unnecessary software and services from devices
- Encrypt mobile hardware
- Update all default passwords to complex passwords
- Restrict the number of unsuccessful attempts for login
- Set up anti-virus and malware protection
- Configure hardware and software to operate according to staff role
- Hardware and software is updated regularly by all members of staff

How Cosmic manages customer's data

Data storage and deletion

Cosmic only retains data that's needed to ensure we carry out the duty of our activity with Customers. Data is stored on our third party CRM, Customer Service software and our Cloud Storage provider. Due Diligence has been carried out on our Third Parties.

At the end of our provision of service, Cosmic acts under your request, and we will delete or return all personal data to you. If you do not specify, files are deleted from Cosmic records within a week of a customer exit, this includes all web records. However customer details and financial transactions are retained for HMRC purposes for the statutory time period.

Website data

Site build and Architecture

We design our sites by evaluating the risks that are presented, in particular from processing personal or sensitive data on your sites. We build sites with Privacy by Design principles that support data integrity and privacy of personal data.

We assess site design for risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data within the parameters of website design.

Patch and Exploit Management

Our websites are built using third party, Open Source code that requires software updates and patches. We monitor notices and take action on patches and updates. We have an exploit and patch management procedure.

How Cosmic manages hosting of client websites

Cosmic uses a third party hosting solution for web hosting. All hosting is located in the UK within robust, professional hosting solutions. Support is available 24/7/365, with a response time on average of 5 minutes. Back ups are contained with the same environment across multi-tenanted sites.

We have carried out due diligence with our hosting solution. Our hosting solution is ISO 27001 accredited with independent, expert verification that information security is managed in line with international best practice. The key components of ISO 27001 environment include:

- Assessment of Risk
- Organisation of information security
- Physical and environmental security
- Access control
- Information security incident management
- Compliance

If your site is not hosted by us, you will need to inform us of patch and exploits and provide us access to update if required.

How we manage domain registrations

We register domains with Nominet and Tucows. Nominet have issued interim guidelines on their GDPR compliance and they will update their policies on 22nd May. For more information visit https://registrars.nominet.uk/namespace/uk/gdpr-changes

Tech support data

Customer Cloud Backup solutions

Where third party cloud backup services are deployed for customer data, the third parties have issued third party GDPR statements for data storage location and data security.

Physical Access to Customer sites

Where Cosmic hold keys to customers premises, keys are stored in a locked safe and signed in and out.

Remote Access to Customer sites

We access your systems using a third party secure software. No access is gained to staff end-point devices without staff knowledge and permission. Access to servers is acknowledged through pre-authorised agreement as part of our service provision.

Removal of Customers Assets from site

Assets are removed with customer's permission from site and a hardware certificate is issued to the customer for the duration of the removal.

Disposal of Customers Assets from site

All assets are formatted and data erased before they are securely destroyed to military standards. A disposal certificate is sent out to the customer and a request to remove from the customer's asset register

Dealing with Access Rights Requests

Cosmic will assists you to fulfil your obligation to respond to requests for exercising the data subject's rights. If you have a request, please email web@cosmic.org.uk with the subject heading ACCESS RIGHTS REQUEST.

Notification of breaches

We take reasonable steps to mitigate against breaches of personal data. Cosmic maintains a record of breach incidents and has a full procedure in the event of a breach.

Cosmic will notify you, without delay, if your personal or sensitive data is breached.

Work with Forensic Investigators

Cosmic's forensic investigators have been appointed and when engaged, they will determine how the breach or exposure occurred, the types of data involved, the number of internal/external individuals and/or organisations impacted, and analyse the breach or exposure to determine the root cause.

Cooperation with Supervisory Authorities

We will not process the data you give us except on written instruction from you, unless we are required to by law. We will also co-operate with supervisory authorities such as the Information Commissioner's Office on request.

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0	1/3/2017	New version	Kate Doodson
v2.0	8/5/2018	Updates to notifications	Kate Doodson

For more information on the status of this document, please contact:	Kate Doodson E-mail: kate@cosmic.org.uk
Date of Issue	May 2018