INFORMATION SECURITY STATEMENT

Introduction

On 25th May 2018, the General Data Protection Regulation (GDPR) became law in all European member states, even though the UK is due to exit the EU, the GDPR will still be applicable to the UK through equivalent domestic law or single market membership.

The new Regulation will replace the current Data Protection Act 1998 (DPA) which was developed at a time when most data processing was still paper-based. There was also a limited understanding of the impact that technology would have on the way we process data.

The GDPR is designed to offer effective legislation for 21st Century Data Processing, the core principles are largely the same as the existing Data Protection Act, however there have been key changes and enhancements that are important to understand if you want to remain compliant with the new law.

In this document, we, Telstar Mobile Media Limited, (TMM) will take you through some of the key points of the GDPR and how we implement them as a Processor of your Data. Please note that this document only details how TMM handles your data as a Data Processor. For the avoidance of doubt, this is the data you transfer to us for the purpose transmitting communications. This data will be referred to in this document as "end-user data", it is the data that you control and that you contract with us to process on your behalf. If you would like information on how we process your data as a Data Controller, you can view our Privacy Policy on our website.

Consent

One of the lawful basis' for processing data and under the Data Protection Act, probably the most common grounds for processing. Under the GDPR, the requirements for using consent as your lawful basis have been set higher than ever before. Consent needs to be gained, recorded and managed in a much more comprehensive manner than under the Data Protection Act, a draft document providing guidance to the changes around consent requirements under the GDPR has been produced by the ICO, which is expected to be finalised in the first half of April 2018.

The service that we provide to you means that TMM is the Data Processor of the information that you share with us for the purpose of transmitting communications and you are the Data Controller.

TMM act solely on your instructions and process your data to send communications to your end users. TMM does not obtain, record or manage consent from data subjects on your behalf. It is your responsibility as the Data Controller to ensure that you have and can demonstrate where necessary, records of consent from data subjects needed for us to transmit communications using the information you provide. We do not directly interact with your end users as TMM, all communications are sent on your instructions as if they come from you directly and we are "transparent" in the communications delivery process.

Data Retention

TMM understands that excessive data retention is not compliant with both the old and new Data Protection rules. Accordingly, TMM retains your messaging data for no longer than two years from

the date that you sent the communication - unless instructed otherwise – for example, where a zero-day retention service has been applied to the account.

Any fields containing Personally Identifiable Data (PID) are redacted after the retention period, before being permanently deleted. Messaging data is limited to the mobile number and the content of the message.

Storage of PID is in secure, access controlled environments, segregated from all other TMM networks. Hardware within those secure environments is owned by TMM.

'Sent Items Download' data stored in AWS Dublin is retained for 13 months after which data is deleted within the AWS instance.

Data transmitted via our Messaging Studio application will have copies stored in Microsoft Azure in the UK. The retention period for reporting data/analytical data is defined by you, the customer. Operational data is also stored in Azure, this is in line with standard TMM messaging retention periods (two years).

Data transmitted via our outbound voice channels is retained for two years.

Data Protection Measures

Data protection measures taken by TMM are based on the ISO27001 Information Security standard. This standard is applied to all areas of the business; both our office and production environments are certified on an annual basis by an accredited external auditor.

A customer facing version of our Information Security Management System (ISMS) Manual detailing these measures is available to customers on request. The manual provides statements on how we implement the ISO 27001 controls at TMM.

As an illustrative, high level overview, TMM has taken the following measures, among others:

Access Control

- Access to all systems by employees is controlled by a username and unique password. TMM has a Password Policy which sets minimum complexity requirements and procedures to ensure passwords are changed on a regular basis by all staff
- All access at TMM is on the basis of least privilege, as such employees only have access to the minimum amount of data that they need to do their job
- Access to customer data is heavily restricted as a result of our "least privilege" policy, all access is frequently reviewed to ensure that new starter, and movers and leavers procedures are being adhered to by all relevant teams.

Firewalls

- We use firewalls on all internet facing elements of our infrastructure to protect data and control traffic into and out of the business. Firewalls are also enabled on all employee endpoints at all times
- IDS and IPS are enabled on our production environment firewalls.

Antivirus

- All our equipment and servers are protected using appropriate real-time anti-virus, anti-spyware and anti-malware software
- An Anti-Malware policy is in place to ensure that staff are fully aware of their obligations and do not obstruct the operation of the application.

Secure Equipment Including Laptops and Mobile Phones

- All company laptops and mobile phones are full disk encrypted and are individually password protected. All TMM created documentation must be stored in secure online storage, never on employee endpoints
- Customer data is only stored within TMM production environments, TMM employees do not store customer data on their endpoints or process data outside of our secured production environments. Due to the majority of staff using laptops, removable storage is not generally needed. If used, the removable storage is subject to the same controls as our mobile device policy
- Employees are made aware of the risks of taking company equipment out of the office and the importance of protecting their own equipment.

Data in Transit / Encryption

- All transfers of customer end user information from TMM owned and controlled hardware and networks is by way of VPN connections, this is how your data is transmitted to Network Operators for communications delivery
- Connections from you to our systems are secured depending on the method used:
- If you connect to us using our web applications, the connection is encrypted and authenticated using TLS 1.2
- If you use an SFTP automation to transfer files to TMM, it is secured via SSH
- If you connect to us using one of our APIs - the security of the connection will be dependent on your integration, we strongly recommend that you use HTTPS in your integration to us, rather than HTTP.

Backup, Disaster Recovery and Business Continuity

We schedule and conduct regular backups to ensure that all data is stored safely, securely and remains available for the purpose of restoration in a disaster recovery situation.

- Full system backups of servers and databases are taken daily
- Transaction log backups are taken every 15 minutes
- Backups are stored in our Disaster Recovery Data Centre location
- We have Business Continuity and Disaster Recovery plans to ensure that we can minimise business damage from a major issue affecting staff, office and data centre locations & equipment.

Monitoring

- Our platform is continuously monitored by our operations team, TMM has a dedicated on-call team that ensure that all platforms are monitored 24/7/365, any issues are raised with stakeholders and will be subject to our robust incident management procedures to ensure our estate remains secure and error free
- We subscribe to industry vulnerability reporting mediums and review all industry known vulnerabilities on a regular basis, with new threats being assessed on a daily basis. Where we discover that we are using a potentially vulnerable component, this risk is assessed in the context our business operations and environment and if appropriate, we will patch the issue as soon as possible
- We have processes in place to ensure that all data storing equipment is physically and securely destroyed at end of life, we do not recycle media and maintain copies of media destruction certificates from our trusted and certified supplier
- We conduct penetration tests on an annual basis using a certified third party supplier. In addition to this, we undertake external and internal vulnerability scans using Authorised Scanning Vendors and vulnerability assessment applications.

Employee Training and Education

All employees:

- Are subject to strict pre-employment vetting in line with our Hiring Policy, they must successfully complete aptitude testing and have a number of checks carried out prior to a full offer of employment being made. These checks include: education, employment, right to work and criminal record checks. Additional checks are required for certain roles i.e. finance related;
- They are trained on the importance of data security at TMM and learn of the measures they must take to protect personal, company and customer data as part of their induction process and each month as part of our ongoing e-learning initiative;
- All staff have confidentiality obligations clearly set out as part of their contract of employment.

Policies and Procedures

In addition to the above, we maintain, enforce and support policies to ISO27001 standard for:

- physical premises security;
- security of data held on site;
- the secure storage, deletion and disposal of customer data;
- prohibition on the use of personal devices and accounts for work purposes;
- acceptable use of TMM owned equipment.

All of these measures and the entire ISO systems are audited internally by the compliance team and externally by our third party accreditation body on an annual basis, the compliance team also conduct security sweeps on an ad-hoc basis to ensure that certain policies are being adhered to by all staff.

Risks

TMM continuously assesses all risks. Risk assessments detail treatment plans that act as recommendations to help the business reduce the impact and/or probability of the identified risk. Risks and treatment plans are regularly reviewed, we assess risks related to our systems, staff, assets and operational activities. TMM has identified this as an area that, whilst compliant with requirements such as ISO 27001, we adhere to the principle of continual improvement.

We use enterprise risk management software to support and enhance our approach to risk management. We identify dependencies as risks to our business and security objectives through risk registers, with activities arising to treat those risks effectively.

Breach Notifications

TMM takes all of the above measures to secure your data as part of our Data Processing activities. In the event of a data breach, we will inform you within 24 hours of us becoming aware of any security issue has led to a data breach including any customer data.

We have also:

- Implemented security measures into our IT systems, networks, and general business practices to detect and respond to security issues in an effective manner
- Developed an Incident Response Procedure to respond to all incidents and trained all staff in how to respond when an incident happens
- Defined customer communications in the event of any incident.

Data Protection Officers

TMM has a dedicated compliance team that are responsible for all Data Protection questions, requests, issues and queries across the organisation. TMM is not currently required to appoint a Data Protection Officer (DPO) under the criteria set out in the GDPR, however this position will be regularly reviewed.

Any questions that you have in relation to Data Protection can be raised with your account manager, subject access requests are detailed in the section below.

The Rights of Data Subjects

As a Data Processor, TMM will not respond directly to any request raised by one of your customers whose data we have processed. We will contact you to make you aware of the request and assist you in meeting your obligations under the GDPR. Examples of where we may need to assist to meet the rights of a data subject include:

Subject Access Requests

A right that carries over from the Data Protection Act, this should be a familiar concept for most Data Controllers. Key changes under the GDPR are:

- Timeframe - Data Controllers now have one calendar month to respond to a Subject Access Request, this has been reduced from 40 calendar days
- Charges - Under the DPA, Controllers can charge a “reasonable fee” for any Subject Access Request, this has generally been accepted as £10. This has been changed in the GDPR and

the first copy of the data requested by a data subject must be given to them for free. Controllers can charge a reasonable fee for subsequent copies.

Data that you transferred to TMM can be made available for this purpose, providing it is still stored by us. Subject access requests can be raised with TMM via our Subject Access Request Form. There is a charge associated with requests of this nature - please contact your account manager for details. Subject Access Requests will be fulfilled within 30 days of us receiving the request from you.

Right to be Forgotten and Erasure

Much has been made of the enhancements to this right under the GDPR; it will give data subjects the right to ask for their information to be deleted if they object to processing, or withdraw their consent. In the UK, this right has been used to amend inaccurate information about data subjects, for example, in Google search results. Whilst the enhancements do not provide an absolute right to be forgotten, they will result in more deletion requests being received by Data Controllers.

Requests for specific data to be deleted can be raised with your account manager.

Records of Processing Activity

TMM is a Data Processor for all customer information. As such we only process your data on your instructions and for the purpose providing the communications service that is part of the performance of the contract between you and us. The sole purposes of our processing activities is the transmission and delivery of communications to your end users.

We keep a record of all the messages that we send on your behalf in line with our data retention policy. As detailed in in the Data Retention section, this is for no longer than two years from the date that the communication is sent.

Third Party Transfers

TMM passes your information to network operators for the purpose of delivering your communication to the End Users handset or Network Termination Equipment. This type of transfer is intrinsic to the provision of our products and services.

For SMS communication in the UK we only use our direct connections to the UK Mobile Networks to ensure that we can trace your data from our systems to the end user handset.

Data transmitted over our voice products is via a Session Initiation Protocol (SIP) stack hosted in our Derby Data Centre, Node 4. The Data Centre SIP Stack provides connections to network operators for communications delivery.

A feature of our service - Sent Items Download - is hosted within Amazon Web Services (AWS) Dublin.

Messaging Studio and Rich Content/Communications Service (RCS) data is hosted in Microsoft Azure (UK) for operational purposes.

For all third party networks that we use, we have conducted a due diligence audit to ensure that each supplier has taken adequate technical and organisational measures required to offer security standards that are materially similar to those described in this document for our own infrastructure.

We have also entered into (or are in the process of entering into) contracts with all third parties that solidify the data protection obligations of all parties and extend the minimum requirements detailed in any Data Processing Agreement between You and Us to our suppliers.

Data Processing Agreements

TMM has produced a Data Processing Agreement (DPA) that can be used by our customers to ensure that you are meeting your obligations as a data controller under the GDPR. Our DPA is available upon request from your account manager and form part of our updated terms and conditions that are available here.

Data Maps

As part of our privacy framework, TMM has conducted comprehensive data mapping of our systems to provide "Data Life Cycles" for all of the PID that we process and control. Customer facing versions of our data maps will be produced over the coming weeks and will be available upon request to help you meet your obligations under the accountability principle of the GDPR. Requests can be raised with your account manager, who will be able to share data maps specific to our products and services that you use.

Data Protection Impact Assessments (DPIA)

We understand that certain types of processing may require our customers to complete a DPIA to demonstrate that they have considered the rights and freedoms of data subjects before engaging in their proposed processing activities. TMM are a service provider for business communications and do not have visibility of the content you are sending through our platform. If your processing activities are considered high risk, or you are processing special categories of data, you may require our input into your DPIA. Please raise any requests of this nature with your account manager.