Data Processing Policy

May 2018

W:\CrmOpps\000292\GDPR and T&Cs May2018\Data Processing Policy - Rev 1_1.docx

1. Introduction and Requirements

This document has been prepared to formalise its procedures and handling of data relating to its external parties.

1.1 Definitions

Affiliate: means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with another entity, from time to time.

Agreement: means the agreement under which Logma has agreed to provide Products to the Client, of which these Data Processing Policy form part.

Control: the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the general management of the company (whether direct or indirect), and controls, controlled and the expression change shall be construed accordingly.

Client: this includes customers which are party to the Agreement in relation to the supply by Logma Products and other parties involved in business negotiations and relationships with Logma.

Logma: means Logma Systems Design Ltd (Company Number 02321865) and it's Affiliates

Products: means the hardware, software, software as a service and services (or any one or more of them) supplied or agreed to be supplied by Logma to the Client.

Removable Media: means any type of storage device that can be removed form a computer while the system is running. Examples include the following media, although this is not an exhaustive list: USB Pendrive, Portable Hard Disk, Memory Card, Floppy Disk, Magnetic Tape, CDs, DVDs, Blu-Ray disks, Zip Disk

1.2 Contact Details

Logma does not require the appointment of a DPO. Contact details for the Company

Logma Systems Design Limited
Logic Centre
Cunliffe Street
Chorley
Lancashire
PR7 2BA

Tel: 01257 233123
Email: info@logma.co.uk
Company Registration Number: 02321865

2. Classifications of Data

2.1 Business Data

Logma collects business data from its clients during normal business activities.

Data at pre-sales stage is usually obtained by reference from a third party or by direct contact initiated by the client. Additional business data may be obtained during the sales cycle direct from the client.

Data at post-sales stage is only obtained directly from the client under the provision of Products such as sales or support.

The information of Clients contacts and data may be used during the provision of our Products but is not used for any other activity and not shared with any external parties.

We share information with approved suppliers for the provision of our Products only when that information is required to provide said Products.

2.2 Personal Data

Any personal information relating to an individual's name, Email address or mobile number is only obtained under the heading of Business Data. No personal data is directly acquired and is only provided by the Client.

2.3 Sensitive Personal Data

Logma collects no such data for any external parties. The only medical data relates to current staff where necessary.

2.4 Children's Personal Data

Logma collects no such data

2.5 Legitimate Interest

The use of data held and which has been gathered with the consent of the Client will only be used by Logma for general Marketing when specific permission has been granted for this purpose.

Contact details and data we hold may be used for Marketing that is considered for legitimate reasons. Clients may be informed of changes and potential benefits that we believe may be of interest and which we feel we have a duty to deliver as part of our Products.

Marketing of a general nature may take place to Clients which have provided email contact details on web sites that do not hold any personal or personally traceable information.

3. Confidentiality

Any individual directly employed by Logma agrees to the following within their Terms of Employment

3.1 Staff Confidentiality

Logma staff acknowledge that in the ordinary course of their employment they will or may have access to confidential information, and that from time to time they will or may be informed that certain information with which they have access is confidential.

They agree that they will not, either directly or indirectly, and whether during the course of their employment or after its termination (Without limit in time) either for their purposes of for that of any other party, and for any reason including but not limited to financial gain, use or divulge or communicate to any person, firm, Company or organisation any information that they know or ought reasonably to have known to be confidential, including information that they are told is confidential, concerning the business or affairs of the Company or any of its or their customers, clients or suppliers.

For the purposes of this clause, "confidential information" means any information identifying a customer, trade secrets, customer lists, designs, information regarding product development, marketing plans, sales plans, projected acquisitions or disposals or properties, operating policies or manuals, business plans, purchasing agreements, financial records or other financial, commercial, business or technical information relating to the Company or information designated as confidential or proprietary that the Company may receive belonging to suppliers, customers or others who do business with the Company.

3.2 Code of Practice

Our staff are trained to ensure they understand the importance of any data that is presented within Logma via email, post or verbal advice from the Client with the authority to present such data. A Client must provide written notice regarding the data to be provided. The use of the data in a hard copy form will be limited to an immediate requirement for handling that data and on completion of the exercise that Logma is required to perform is so completed the hard copy will be shredded. Staff data may be required to be kept in hard copy format for the purposes of Payroll and HR Management purposes and when this is the case it will be in a secured and locked filing system.

All data that may refer to external company, external personal or internal staff details or data will be transferred to electronic storage when the purpose of the data requires to be held legitimately for the fulfillment of legal, processing and for reference for the required period of time. Staff data will be kept for the purposes of Payroll and HR Management purposes.

The electronic receipt and transfer of data to and from Logma's care will be undertaken in a secure manner when Encryption will be used for any transfers to internal storage or to external data storage facilities or to authorised Client sites as necessary within the terms of performing our supply of Products. We may also request access to data other than our own company data and where this or the receipt of data is necessary to carry out our work this will be done within our Code of Practice.

All data and contact details provided by our clients or by businesses with which we are conducting negotiations or general business will be stored with the consent of the authorised business representative or the person whose details are being provided. These will be stored, processed and controlled as outlined in these policies.

4. Technical

This section details our standard methods and policies for handling data. Any queries will be brought to the attention of line manager or at Director level.

In the instance that a client has different requirements then these will be considered and measured against our standards with suitable recommendations to the client.

4.1 Remote Access

Where VPN connections are configured and employed these will use encryption to ensure security of data being transmitted.

4.2 Hosted Desktop Services

Only Logma approved providers will be used to provide Hosted Desktop facilities to Logma Clients. Those providers will comply with ISO27001 to ensure security of the environment and any such data contained therein. Data within the hosted environment will be treated securely (see item 4.5)

4.3 Offsite Backups

Where backup media is taken offsite any backup data will be stored with encryption and only be taken offsite by authored personnel. Any such backup media will be stored securely and not left in vehicles overnight.

Where automatic offsite backups are employed any data will be encrypted prior to transmission. Any such providers for Offsite Backups will be approved by Logma.

4.4 Removable Media

Any data that is recorded onto Removable Media that relates to Logma, Clients or Affiliates will be stored safely and not provided to unauthorized parties. Data will be encrypted unless that removable media is stored in a secure area such as a safe or vault.

4.5 Access to Data

Where an Application is made available to any user that contains business or personal data then said Application will employ password protection as a minimum to ensure authorised access to data.

Data stored within SQL Databases will only be accessed by authorised personnel and for activities that relate to carrying out their job functions.

4.6 Passwords

Where VPN connections are configured and employed these will use encryption in line with Logma's standard procedures and policies. Passwords will not be shared unless authority is given.

Where a password reset is requested or necessary it shall only be carried out by an authorised member of Logma personnel or Affiliate. A record of this event will be documented within the internal call logging system used by Logma. Where a Client has requested the password reset then verbal authorisation is acceptable if it is for that individual, if it is on behalf of another individual then an Email should be sent by an approved manager to support@logma.co.uk confirming the request – that Email will then be recorded on our call logging system.

4.7 Email

Where Hosted Exchange is used then Logma approved providers will be used. Any such provider will comply with ISO27001 to ensure security of the environment and any such data contained therein.

Strong passwords will be employed for all mail services including Hosted Exchange, POP3 and SMTP.

The standard Company Disclaimer will be used by all staff when communicating with external parties. Care will be taken with all content within Email (including message subject, body and attachments) and the intended recipients. Any attachments that contain Business or Personal data backups will be encrypted.

Any Email shots will use a suitable trusted platform such as MailChimp and always provide an Opt Out option.

4.8 System Administration Changes

Where a System Administration change is requested or necessary it shall only be carried out by an authorised member of Logma personnel or Affiliate. This covers configuration changes at Operating System level and within Business applications such as OneFit that affect the operation of said environment.

A record of this event will be documented within the internal call logging system used by Logma. A clients request should be made by an approved manager by email and sent to support@logma.co.uk t – the Email will then be recorded on our call logging system.

4.9 Communication with Any External Party

Care and consideration will be given to any Business or Personal data that is received or given to any external party. Data will only be transferred when there is a legitimate business requirement either on behalf of Logma, the Client or Logma Affiliates.

Where this information may cause a data breach then it will be reported to Director level. (see item 4.12)

4.10 Website Policies

Any websites associated to Logma will carry the following documentation which will also cover any external services that are used.

Privacy Policy

Cookie Policy

Registered address

Contact Us or Feedback pages will have Consent options

Optional Newsletter sign up will use a double opt-in method.

4.11 Documentation Controller

Logma has carried out an internal audit of data that is used within the organisation which covers both internal and external processes. This information has been documented within our 'Documentation Controller' document.

4.13 Data Breach

Where a Data Breach has been identified or reported then a full investigation will be initiated and be reported to Director level. A record of this event will be documented within the internal call logging system used by Logma. Any parties relevant to that this information will be notified of the initial report within 72 hours. We will allow up to 30 days to reach a conclusion and then report our findings to all parties concerned.