iBase Media Services Ltd GDPR statement

Updated 21/03/2018

Contents

1 What we do

iBase Media Services Ltd are specialists in the field of digital asset management*, with a client base spanning Europe, America and Australasia. We work both in the public and private sectors, taking in art galleries, museums, universities, libraries, local councils, charities, commercial picture and video libraries, marketing companies, research organisations, architects, pharmaceutical companies, and many more.

> * Digital asset management is a catch all term for software systems used for a variety of requirements and applications, including picture libraries; video libraries; photo archives; internal digital asset control and management; e-commerce for selling digital assets including images, video and audio files; management of all other files types including documents, spreadsheets, PDFs, etc…; marketing asset management; museums and art galleries; academic, science and technology; sport and culture.

In addition to providing software solutions, iBase also provide consultancy and expertise in a variety of associated disciplines, including digital preservation, collections management integration and e-commerce.

For more information see https://www.ibase.com

2 U.K. Information Commissioner's Office registration

Registration reference: ZA257115

Nature of work description:

Nature of work - Software Development

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information:

We process personal information to enable us to provide a service in which we design, test, sell and support software; promote our services; maintain our accounts and records and manage our staff.

Type/classes of information processed:

We process information relevant to the above reasons/purposes. This may include:

- personal details.
- information necessary for the development and test of software.

Who the information is processed about:

We process personal information about our clients, employees, suppliers and individuals necessary for software development.

Who the information may be shared with:

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection

Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- suppliers and service providers
- professional advisers and consultants
- financial organisations
- employment and recruitment agencies
- central government

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

3 Employee awareness

All iBase Media Services employees have been made aware of this document and its meaning and have freely available access to it.

4 Definition of personal information

See GDPR Article 4 item 1 at https://gdpr-info.eu/art-4-gdpr/

5 Personal information permanently held

a) Employees - name, address, telephone number, date of birth, NI number, bank sort code and account number, remuneration.

b) Clients, including self-service clients – names, email addresses and telephone numbers.

c) Sales prospects - names, email addresses and telephone numbers.

6 Personal information occasionally and temporarily held

a) Temporary copies of a client’s database are occasionally held with the permission of the client for carrying out necessary development or support work.

7 Personal information not held but which might be accessed and processed per occasion

Personal information held by clients in their iBase database, whether in the clients’ I.T. environment or in the iBase Amazon AWS hosting environment, might be occasionally accessed to carry out necessary development or support work.

8 Records of processing activities

As detailed in the GDPR, iBase Media Services are not obliged to keep a record of processing activities.

Article 30 of the GDPR (https://gdpr-info.eu/art-30-gdpr/) about “Records of processing activities” paragraph (5) of the GDPR states that “*The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes* *special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.”*

Recital 13 of the GDPR (https://gdpr-info.eu/recitals/no-13/) also refers to “Taking account of micro, small and medium-sized enterprises” and derogation with regard to record-keeping for organisations with fewer than 250 employees.

However; a record of all processing requests from clients and the action taken for them is automatically created in our support management system.

9 Delegated processors

9.1 Amazon AWS

iBase systems hosted by iBase as a service to our clients are deployed in the Amazon AWS cloud service. For Amazon AWS GDPR compliance see https://aws.amazon.com/compliance/gdpr-center/

9.2 Accountant

A firm of accountants prepare the company accounts and process the company payroll. An agreement is in place with them for the secure transmission and storage of personal information.

10 Consent

10.1 Employees

All employees have given consent to the personal data being held that is necessary for their employment and remuneration.

10.2 Clients

The iBase Media Services support and hosting agreements state that a client’s acceptance of them means that they consent to their data being modified in accordance with their instructions, and a temporary copy occasionally being held by iBase Media Services as required for that purpose.

10.3 Self-service clients

Clients are able to create an iBase system by clicking a link on the iBase website. In doing so they will voluntarily provide their name and email address.

10.4 Sales prospects

Personal information voluntarily provided to iBase generally includes name and email address.

11 Security of data held or temporarily held

a) Access to the iBase Media Service office is only by keyholders.

b) No laptops and no portable devices containing personal information are used by iBase, except for a backup drive which is kept at a secret offsite location. Data on the backup drive is encrypted.

c) All filing cabinets containing personal information are kept locked, and no keys are left in the office.

d) Each employee has their own unique and secure password to computers, the internal network and to the Amazon AWS hosting environment. The passwords are regularly changed.

e) All incoming emails are checked and cleared by a spam and virus protection portal before delivery to the iBase Exchange Server. Emails failing acceptance criteria are not delivered but are reported to the addressee for review and subsequently deleted in the spam and virus protection portal.

f) Employees will make a report to an iBase director if they think that a security incident has occurred.

12 Changes to a client's iBase database

a) iBase Media Services Ltd will not make any changes to clients' data or digital assets except with their express written instruction, and it is on this legal basis that iBase operates as a data processor.

b) iBase Media Services Ltd will not view client data or digital assets except as necessary on a need to know basis in the course of development or support.

13 Non-disclosure of information

No personal data is shared with anyone - except iBase employees on a need to know basis - without explicit written authority from the subject, or the appropriate data controller organisation, or a recognised law enforcement agency.

14 Authorised disclosure of information

Authorised requests for disclosure of information will be complied with at least within one calendar month.

15 Destruction of information

a) Information in digital form will be deleted, and in hard copy shredded, within five working days of a request from either the subject of the information, or from the data controller of the information.

b) Temporary copies of a client's database which are no longer required for development or support purposes are deleted.

16 Audit of temporarily held client databases

Once every month a list of all temporary client databases which contain personal information is reviewed and updated as required. Any databases no longer required are permanently deleted.

17 Ownership of information held in a client's iBase database

For the avoidance of doubt, wherever an iBase system is deployed, including in an iBase Media Services owned environment:

a) The client owns and has full ownership and responsibility in all respects for the content of the data and digital assets on their iBase system, and iBase Media Services Ltd accept no responsibility in any respect for the content and legality of their data and digital assets.

18 For iBase clients - system security

18.1 Secure Environment

iBase hosted within Amazon's AWS cloud environment is tested to ensure that no-one can gain unauthorised access to client files or data. We periodically carry out penetration checks to make sure that our software meets the latest relevant PCI guidelines. We can also restrict access to a system to a range of IP addresses or domains if required.

18.2 Permissions and Roles

The iBase security model allows clients to set up the different levels of access that are required to assets and associated metadata, allowing specification of exactly who can upload, view, edit, download or share different assets, who can see or edit which metadata fields, who can carry out editorial or workflow-based functions or who can access the various administration functions of the system.

18.3 External Applications

Any authorised external application (such as a website or content management system) can also be granted the same variety of access to assets and metadata as can be granted to human users. By using these permissions in combination with different folders, control can be dynamically applied to which applications can see or download which files.

18.4 Audit Log and Reporting

iBase systems includes comprehensive auditing of every action that is carried out, including details of the user, date & time, IP address, asset and success or failure of the action. This extends to uploading, downloading, searching and editing, and can be easily viewed either with the inbuilt reporting system, or by using a third-party application.

END