



Customer Data Privacy Notice

May 2018

Customer Data Privacy Notice

Overview

EPM Limited ("EPM", "we" or "us") holds personal data on its Customers, and their staff, to provide its services. This Customer Data Privacy Notice details the personal data EPM may retain, process and share with third parties relating to your organisation and its staff. EPM is committed to ensuring that your information is secure, accurate and relevant. To prevent unauthorised access or disclosure, we have implemented suitable physical, electronic, and managerial procedures to safeguard and secure personal data we hold.

This policy will be subject to periodic review and it is recommended that you review this document from time to time to ensure that you are aware of any amendments applicable to the retention, processing and sharing of personal data.

A current copy can be found on www.epm.co.uk or via request from the Data Protection Officer.

Review History

Date	Version	Amendments/Comments	Reviewer(s)
Jan 18	1.0	Initial draft	M Eastwood
May 18	2.0	Final Version	R O'Driscoll

Contents

Customer Data Privacy Notice	1
Customer Data Privacy Notice	1
Overview	1
Review History	1
Introduction	1
Types of personal information we collect	1
Purposes for processing personal information	2
Employment or work-related purposes	2
Contractual purposes	2
Legal purposes	2
Legitimate interest	2
Who we share personal information with	3
Transfers to other group companies	3
Transfers to third-party service providers	3
Transfers to other third parties	3
Legal basis for processing personal information	3
Transfer of personal information abroad	4
Data retention periods	4
Data privacy rights	4
Updates to this Notice	5
Contact details	5
Annex A – Third-party processors	6
Key third-party processors	6
Additional third-party processors	6

Introduction

Education Personnel Management Limited ("EPM", "we" or "us") holds personal data on its Customers, and their staff, to provide its services. This Customer Data Privacy Notice details the personal data EPM may retain, process and share with third parties relating to your organisation and its staff. EPM is committed to ensuring that your information is secure, accurate and relevant. To prevent unauthorised access or disclosure, we have implemented suitable physical, electronic, and managerial procedures to safeguard and secure personal data we hold.

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. This Notice sets out the personal information that we collect and process as a data processor, the purposes of the processing and the rights connected with it.

If you are in any doubt regarding the applicable standards, or have any comments or questions about this Notice, please contact the Data Protection Officer.

Types of personal information we collect

During your engagement with EPM, or during negotiations with EPM, we may process personal information about you, your staff and other individuals whose personal information has been provided to us. The data we process will depend on the services we provide your organisation.

The types of personal information we may process may include, and is not limited to:

- Identification data – such as name, gender, photograph, date of birth, National Insurance Number.
- Contact details – such as home and business address, telephone/email addresses.
- Employment details – such as job title/position, office location, employment contract, performance and disciplinary records, grievance procedures, sickness/holiday records.
- Background information – such as academic/professional qualifications, education, CV, criminal records data (for vetting purposes, where permissible and in accordance with applicable law).
- Marital status.
- Financial information – such as banking details, tax information, withholdings, salary, benefits, expenses, company allowances.
- IT information – information required to provide access to EPM systems and networks such as IP addresses, log files and login information.
- Sensitive personal information (special categories under the General Data Protection Regulation) includes any information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, trade union membership, or information about your health/sex life ("**Sensitive Personal Information**"). Generally, we try not to collect or process any Sensitive Personal Information about Customers and their staff, unless authorised by law or where necessary to comply with applicable laws. However, in some circumstances, we may need to collect, or request on a voluntary disclosure basis, some Sensitive Personal Information for legitimate employment-related purposes: for example, information about

racial/ethnic origin, gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; or information about physical or mental health conditions for provision of work-related accommodations or for managing absences from work.

Purposes for processing personal information

Employment or work-related purposes

We collect and use this personal information for the purpose of supporting and managing the employment or working relationship between our Customers and their staff – for example, employment records and contract information and bank account and salary details.

We primarily process this personal information through a global human resources system ("**ERP System**") called Microsoft Dynamics Navision, which is a tool that helps us to administer HR, Payroll and Pensions.

We retain a cloud-based backup of our ERP System and all emails sent and received externally. This is held within the EU. All emails are securely stored and retained for at least a period of 7 years – this data is retained for EPM's legitimate interest to ensure that all advice given is preserved and fully auditable to meet legal obligations.

Contractual purposes

We use this personal information when it is necessary for the provision of our services, in line with the purposes agreed upon between our Customer and EPM.

Legal purposes

We may use personal information where we consider it necessary for complying with laws and regulations, including collecting and disclosing staff member personal information as required by law (e.g. for tax, health and safety, anti-discrimination laws), under judicial authorization, or to exercise or defend the legal rights of EPM.

Legitimate interest

We may use personal information where we consider it necessary for EPM's legitimate interest, including:

- Marketing similar services to our Customers

Details on these activities can be found on [EPM's Website Privacy Notice](#).

Who we share personal information with

We take care to allow access to personal information only to those who require such access to perform their tasks and duties in relation to the provision of our services, and to third parties who have a legitimate purpose for accessing it to support these purposes. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the security and confidentiality of the information is maintained.

Transfers to other group companies

Personal data relating to account holders (the Customer) may be shared with other members of the Citation Group for other legitimate business purposes such as IT services/security, tax and accounting, and general business management and for marketing purposes.

Transfers to third-party service providers

In addition, we make certain personal information available to third parties who provide services to us. We do so on a "need to know basis" and in accordance with applicable data privacy law.

Transfers to other third parties

We may also disclose personal information to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant
- In response to lawful requests by public authorities (including for national security or law enforcement purposes)
- As necessary to establish, exercise or defend against potential, threatened or actual litigation
- Where necessary to protect the vital interests of our staff or another person
- In connection with the sale, assignment or other transfer of all or part of our business; or
- With your expressed consent

Legal basis for processing personal information

Our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you (i.e. provision of services), or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact EPM's Data Protection Officer.

Transfer of personal information abroad

We may need to transfer personal information to countries other than the ones in which the information was originally collected. When we export your personal information to a different country, we will take steps to ensure that such data exports comply with applicable laws. For example, if we transfer personal information from the European Economic Area to a country outside it, such as the United States, we will implement an appropriate data export solution such as entering into EU standard contractual clauses with the data importer or taking other measures to provide an adequate level of data protection under EU law.

Data retention periods

Personal information will be stored in accordance with applicable laws and kept for as long as needed to carry out the purposes described in this Notice or as otherwise required by applicable law. Generally, this means your personal information will be retained until the termination of employment, or relationship with EPM plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial or disciplinary actions) or to document the proper termination of employment or work relationship (e.g. to tax authorities or pension authorities). Please refer to our [Customer Data Retention Policy](#)

Data privacy rights

The account holder(s) may exercise the rights available under applicable data protection laws as follows:

- Access, correct, update or request deletion of personal information
- **Object to processing** of personal information, ask us to **restrict processing** of personal information or **request portability** of personal information.
- If we have collected and process personal information using a person's consent, then this can be **withdrawn** at any time. Withdrawing consent will not affect the lawfulness of any processing we conducted prior to withdrawal, nor will it affect processing of personal information conducted in reliance on lawful processing grounds other than consent.
- You have the **right to complain to a data protection authority** about our collection and use of personal information. For more information, please contact your local data protection authority. In the United Kingdom, the data protection authority is the Information Commissioner's Office whose website is <https://ico.org.uk/>

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. You can read more about these rights at: <https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/>

Updates to this Notice

This Notice may be updated periodically to reflect any necessary changes in our privacy practices. In such cases, we will inform you accordingly. We encourage you to check this notice periodically to be aware of the most recent version.

Contact details

Please address any questions or requests relating to this Notice to EPM's Data Protection Officer at DPO@epm.co.uk or write to:

Data Protection Officer

Education Personnel Management

St John's House

Spitfire Close

Ermine Business Park

PE29 6EP

Annex A – Third-party processors

Key third-party processors

The following are EPM's key third-party processors who will, during your employment, process your personal data.

Bottomline Technologies Ltd provide our BACS software. For more information, please see [Bottomline's Privacy Notice](#).

Atlantic Data Ltd provide disclosures.co.uk. For more information, please see [Atlantic Data Privacy Policy](#).

Additional third-party processors

Additionally, your data may be shared with several third-party processors to meet legal requirements, where EPM outsources aspects of its processes or when providing specific services relating to maintaining your employment or benefits. These companies may include, but are not limited to, the following:

We use a third-party software provider, Send in Blue, to deliver our advice notes and invitations for events. We gather statistics around email opening and clicks using industry standard technologies including clear gifs to help us monitor and improve our service. For more information, please see [SendinBlue's Privacy Notice](#).

In order to fulfil our Service Level Agreement with you we may be required to supply information to pension funds in order to meet your reporting obligations. The information provided will be limited to the specific requirements of that pension fund.

Where the above third-party processors transfer data overseas outside of the European Economic Area (EEA), appropriate safeguards are in place to protect the data transferred.