AFM Solutions – Talent Mgt - DATA PRIVACY & PROTECTION POLICY

1. Introduction

Asset Finance & Management Ltd (with registered company number 01725456 and registered company address at 155 – 157 High Street, Aldershot, Hampshire GU11 1TT) ("**AFM**") from time to time collects, uses and stores personal information about individuals with whom we come into contact as part of our business-to-business activity and with whom we consider we may retain some form of contact in order to deliver improvements and enhancements to our finance and HR-related services. This information needs to be collected and dealt with appropriately whether collected or stored digitally in a database or in paper form, and whether processed or not in any other way.

NOTE: AFM does not hold or process data relating to employees or any individual connected to our customers, suppliers or business associates other than in respect of those employees who represent such organisations in their contractual dealings with AFM and are authorised to deal with us in connection with our finance, HR services or other business-2-business contracts ("Contract Subjects").

This Policy sets out to ensure that we process Personal Data properly under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018, which supplements GDPR in the UK. "Personal Data" means any information relating to you, or from which you may be identified or identifiable.

AFM regards the lawful and correct treatment of Personal Data as very important to its business and to maintaining the confidence of those with whom we deal. We intend to ensure that Personal Data is treated lawfully and correctly, and we will adhere to the Principles of Data Protection and to the 6 "Pillars" of GDPR (see attached Appendices).

2. Data Controller & Data Processor

AFM is:

- Data Controller in respect of Personal Data relating to our Contract Subjects ("**Contact Data**"); and
- Data Controller in respect of Personal Data submitted to us via our website ("**Website Data**").

3. Purpose of Processing as Data Controller

- We process Contact Data on the grounds of our legitimate interests and fulfilment of our contract with the organisation you represent to ensure we are able to provide services to or receive services from that organisation.
- We process Website Data on the grounds of our legitimate interests in responding to any queries or comments you submit.

4. Disclosure

- We may share Contact Data and Website Data with our underwriting banks for the purposes of our finance business. The underwriting banks will undertake credit reference checks and search other relevant registers for anti-money laundering purposes. If such transfer is to take place, we will discuss this in more detail with you.
- We may also share Contact Data and Website Data:

(i) to the extent we are legally required to disclose it; and/or

(ii) to third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this policy.

5. Data Storage

- Contact Data: We will process your Contact Data for the period in which we provide services to or receive services from your organisation and a further period of 7 years from the date on which our contract with your organisation expires or is terminated. We process Contact Data for this period in case any issues arise in respect of the services we provide or receive. If we become aware during the 7 year period that your Contact Data is no longer accurate we will either rectify or delete it.

- Website Data: We retain no data other than for analytics purposes - this is all anonymised on Google Analytics and Squarespace analytics. Contract Form data is emailed through to AFM and is deleted shortly after use (within 7 days). We will process Pure Chat webchat enquiries in line with the terms set out at https://www.purechat.com/privacy.

IBM Kenexa and Qualtrics data: IBM are the data processors for assessments, Brassring and other Kenexa products and services; Qualtrics processes data for any survey business that we become involved in (see IBM and Qualtrics GDPR terms). Any employee Personal Data will be held and processed under contracts between these service providers and employers. AFM has its own Kenexa assessment account and uses this for demos and trials and occasional "Pay as you go" services, but (a) the data is held on secure IBM servers; and (b) any personal data we receive through our mail will be processed strictly in accordance with the employer's instructions and will be not be stored and will be deleted immediately after use.

6. Data Transfer

Our data is stored in Lotus Notes and ACT for Notes, both applications being hosted on Prominic.net. Prominic have data breach response plans and are audited annually under SSAE-16 . Systems and facilities are under 24/7 monitoring for network vulnerability the latest cyber security threats. Prominic.Net, Inc is located in the US and is a registered member of Privacy Shield. We are in the process of reviewing the safeguards upon which Personal Data is available to Prominic.Net, Inc following the recent decision which invalidated Privacy Shield. We will update our privacy policy as soon as possible.

7. Your rights

You benefit from a number of rights in respect of the Personal Data we hold about you, in particular: (a) access to your data (b) rectification of your data (c) right to be forgotten (d) right to restrict processing (e) data portability (f) right to object. More information is available from the Information Commissioner's Office website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/). These rights apply for the period in which we process your Personal Data.

In addition, AFM will ensure that we have nominated an individual to have specific responsibility for ensuring compliance with Data Protection and that:

i everyone processing Personal Data understands that they are contractually responsible for following good data protection practice;

ii everyone processing Personal Data is appropriately trained to do so;

iii guidance is always available to those handling Personal Data;

iv we deal promptly and courteously with any enquiries about Personal Data;

v we describe clearly how we handle Personal Data;

vi we regularly review and audit the ways we hold, manage and use Personal Data;

vii we regularly assess and evaluate our methods and performance in relation to handling Personal Data; and

viii all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

If you think we have processed your Personal Data unlawfully or that we have not complied with GDPR, you can report your concerns to the supervisory authority in your jurisdiction. The supervisory authority in the UK is the Information Commissioner's Office ("ICO"). You can call the ICO on 0303 123 1113 or get in touch via other means, as set out on the ICO website - https://ico.org.uk/concerns/.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with the General Data Protection Regulation 2016. In case of any queries or questions in relation to this policy please contact mbaker@afmgroup-solutions.co.uk/

Appendix I - 6 pillars of General Data Protection Regulation

The 6 Pillars of GDPR are:

1) Lawfulness, fairness and transparency: data should be gathered and used in a way that is legal, fair and understandable. The public have the right to know what is being gathered and have this corrected or removed.

2) Purpose limitation: use of data must be for a legitimate purpose specified at the time of collection and should not be shared with third parties without permission.

3) Data minimization: any data collected must be limited only to what is needed for the purpose agreed with the Data Subject.

4) Accuracy: data must be accurate, up to date, and, if no longer accurate, rectified or erased.

5) Storage limitation: data must be stored only for as long as is necessary. Any archived data must be held securely and if used for research purposes in the future, anonymised.

6) Integrity and confidentiality: data must be held in a safe and secure way and all reasonable steps taken to ensure the security of this information and avoid accidental loss, misuse or destruction.