Privacy Notice – Matthew James Consulting – Reviewed June 2023

Introduction

This policy sets out the different areas in relation to user privacy at Matthew James Consulting. Matthew James Consulting is a data processor in which they carry out background checks on employees and potential employees of the data controller. Furthermore, the way Matthew James Consulting processes, stores and protects user data and information will also be detailed within this policy.

As Matthew James Consulting is asked to carry out background checks you may be required to provide personal information; which will be used accordant to GDPR fair processing. We will ensure that all personal information supplied is held securely in accordance with GDPR.

Responsibilities:

Everyone who works for/with Matthew James Consulting has some responsibility for ensuring data is collected, stored and handled appropriately.

Each worker that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally
- Matthew James Consulting will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep data secure, by taking sensible precautions and following the guidelines below
- Strong passwords must be used and they should never be shared; these should also be changed regularly
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date, if it is no longer required – it should be deleted and disposed of securely.
- Employees should request help from their manager if they are unsure about any aspect of data protection.

What information is being collected?

Personal data is collected by Matthew James Consulting (the data processor) as requested by the potential employer/current employer (the data controller).

Personal data will be collected to correlate to the required screening/background checks.

Personal data can include, but not be limited to; Name, Gender, Date of Birth, Contact Details, Proof of Address, Photo ID, Employment History/Status, CV, Name Changes, Marriage Status, National Insurance Number, Credit History, Criminal History (accordant with law), Right to work, Directorship.

Who is collecting it?

Matthew James Consulting will collect personal data as required to complete a request from the data controller (employer/potential employer)

How is it collected?

Data will be collected via email, post & telephone communications. In some circumstances data will be received directly from the controller.

Data is also collected from third parties when carrying out certain background checks e.g. credit, criminal, references, qualification verifications.

Why is it being collected?

Data is collected to perform background checks for employment purposes as requested by the data controller.

Matthew James Consulting

How will it be used?

Data will be used to carry out background checks including but not limited to; Employment referencing, education referencing, credit checks, criminal records checks, qualification checks, identity checks, right to work, sanctions, FCA, NI, Directorship

What is the legal basis for collecting and processing the information?

For data subjects, we use legitimate interest as the legal basis for collecting and processing the information. We have carried out a Legitimate Interest Assessment (LIA) to ensure our processing is lawful. Following the LIA, we concluded that the legitimate interests (carrying out background screening on behalf of the data controller – our clients) outweigh any risks to the data subject. Please note, that as we rely on Legitimate Interests, the right to data portability does not apply.

How will it be stored & its safety?

Paper Data:
Data printed on paper is kept to a minimum. It is locked in a secure location where unauthorised people cannot access it. At Matthew James Consulting these files are locked in a secure unmovable cabinet and the building consists of 3 locked doors and a motion sensor alarm for access.
When paper documents have been printed out employees should make sure that they are not left where unauthorised people can see them. Once these documents are no longer needed they should be shredded and disposed of securely.
Electronic Data:
It must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

Our data is stored on a Cloud, administered by Venom IT www.venomit.com. Venom IT is certified ISO 9001 (organisational) and ISO 27001 (technical) and independently audited on ISO 27017 code of standards for cloud providers. Our IT provider is also Cyber Essentials certified and have been approved to supply their Cloud Hosting, Cloud Software and Cloud Support solutions through the latest iteration of the United Kingdom government's G-Cloud framework.
Data security is of paramount concern and they have therefore implemented the following systems & certifications at their Data Centres:

- They have 3 data centres, 2 of which are replicant data centres located in London and Manchester to ensure Integrity and Continuity.
- All their data centres are ISO 27001 certified (the main component for GDPR Technical compliance), with IL4-level security
- IP Ban – their unique, proprietary software – blocks repetitive login attempts and blacklists the attacking IP address across their entire network (prevention of unauthorised access)
- 2048-bit encryption (considered fit for banking, encryption is also part of GDPR requirements)
- Auto-failover & rollback (preservation of data Integrity & prevention of data loss)
- UPS with 7-day battery backup (Continuity)
- Fire protection using VESDA systems and FM200 gas suppression (physical security)
- Secure gated access, with 24-hour security control (physical security)
- All their data centres are UK-based

Data is backed up every 2 hours.

Access can only be gained by authorised individuals who have 2 passwords which are not shared and are changed regularly.

Data is never saved directly to laptops or other mobile devices.

Data is never stored on removable media.

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended

Matthew James Consulting

Personal data should not be shared informally

Data must be encrypted before transferring electronically – Matthew James Consulting uses TLS (Transport layer security) SMTP (Simple Mail Transfer Protocol) on all emails being sent.

Employees should not save copies of personal data of their own computers

Who will it be shared with?

Certain data will be shared with 3rd party organisations to apply for credit, civil & criminal checks with recognised agencies UCheck, Experian & Owens Online.

Name, Date of Birth, NI & Name changes will be shared with referees and/or educational facilities which can include other EU countries & Non-EU countries.

What will be the effect of this on the individuals concerned?

There will be no effect of this on the individual's records from the processes that Matthew James Consulting carry out.

Is the intended use likely to cause individuals to object or complain?

The data is processed for the individual's employment/potential employment therefore Matthew James Consulting would see no reason for the individual to object or complain.

How long will it be stored?

Data will be kept for a retention period of 3 months from the date of invoicing unless stated otherwise by the data subject. After this retention period has elapsed paper and electronic data will be securely destroyed.

Subject Access Requests:

All individuals who are the subject of personal data held by Matthew James Consulting are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed of how to keep it up to date
- Be informed how the company is meeting its data protection obligations

Subject access requests should be made by email, addressed to the data controller at jcarpenter@mj-consulting.co.uk.
The data controller will provide the relevant data within 30 days.
The data controller will always verify the identity of anyone making a subject access request before handing over any information

All individuals have the right to erasure & right to be forgotten, please also contact jcarpenter@mj-consulting.co.uk regarding this matter.

How to complain?

Please write to The Director, The Old Bank, 257 New Church Road, Hove, BN3 4EE. More information can be found on https://ico.org.uk/for-the-public/raising-concerns/

Disclosure of Information:
Section 29 of the DPA provides an exemption to data processing rules for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders. The GDPR does not cover the processing of personal data for law enforcement purposes. The UK will implement The Data Protection Law Enforcement Directive into UK law allowing data processing for the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."
Under these circumstances, Matthew James Consulting will comply with its legal obligations. However the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisors if necessary.

Matthew James Consulting