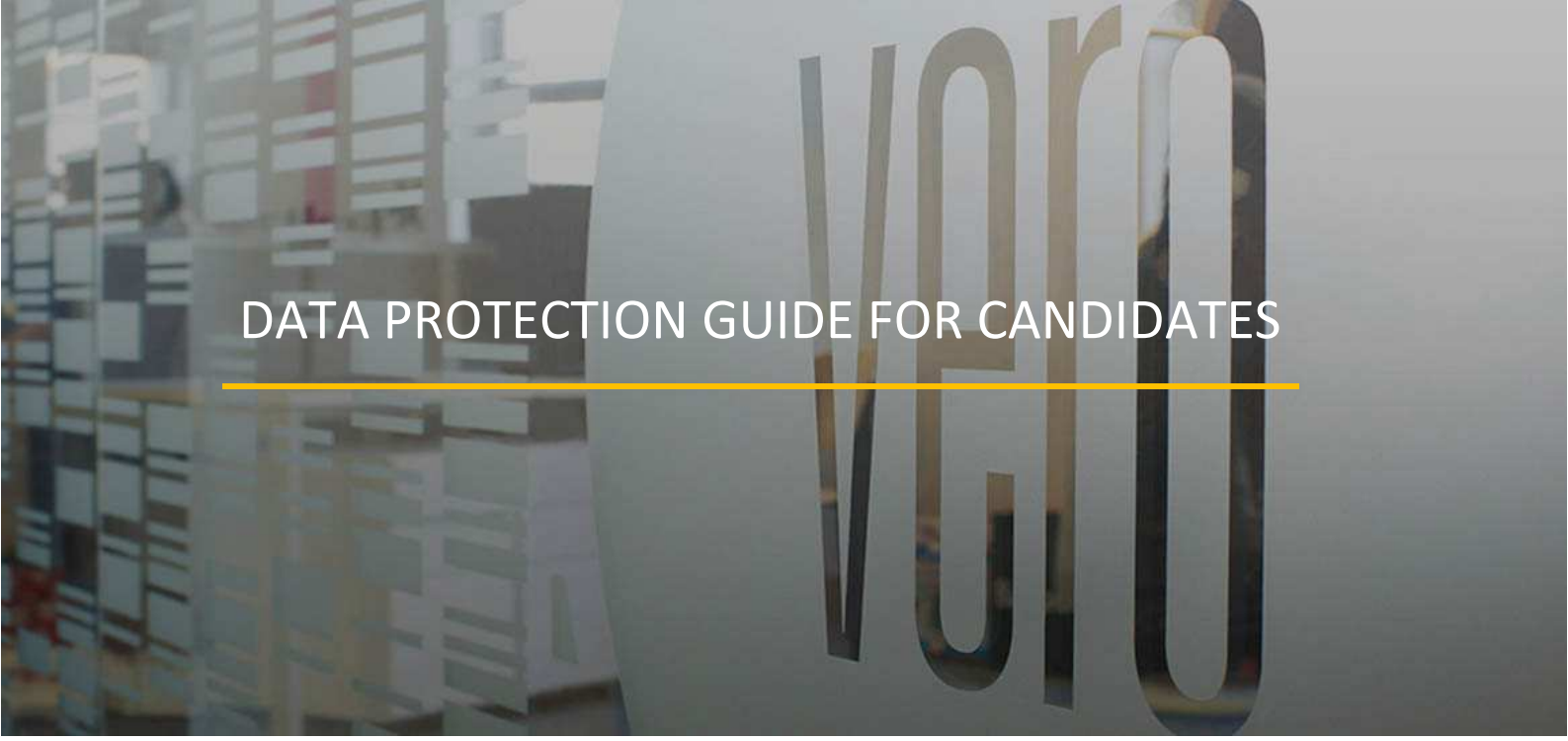

DATA PROTECTION GUIDE FOR CANDIDATES

Vero are conducting your employment screening checks at the instruction of your prospective or existing employer. Any personal data you provide to us in relation to your employment screening will be used solely for this purpose

Data processor vs controller

In connection with your employment screening, Vero Screening (Vero) is the data processor and your prospective or existing employer (our Client) is the data controller. This is in accordance with the terms and definitions of the General Data Protection Regulation (GDPR) and supporting UK data protection legislation.

Data protection principles

As an organisation which processes large volumes of personal data, we take seriously our responsibility to protect the personal data in our custody. We employ strict technical and organisational measures to safe guard the secure collection, processing, use and storage of your personal data and our employment screening services are conducted in a manner which is compliant with the principles set down in Article 5 of the GDPR.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Security standards

Our commitment to the security of the personal data in our care is highlighted by our ISO 27001 and Cyber Essentials accreditations.

Data subject rights

As a data subject the GDPR provides you with the following rights:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing

- the right to data portability
- the right to object

Should you wish to exercise any of the above data subject rights, you will need to direct your request to your prospective or existing employer, in their capacity as the data controller. If you contact us regarding your data subject rights, we will pass your request promptly to our Client, in order that they can assist.

As the data processor, we will provide reasonable assistance to our Client, to enable them to fulfil their obligations under the GDPR and respond to your request. We will act solely on their instruction.

Data Minimisation

Our Candidate portal has been designed to collect the minimum amount of information necessary, to enable the checks and verifications required by your prospective or existing employer to be conducted.

In some instances, you may be asked to provide supporting documentation to evidence the information you have provided in your questionnaire, or to complete an element of the screening. In such instances you are encouraged to redact non-relevant or particularly sensitive information which is not required as part of the screening process.

An example of this might be a bank statement, requested to evidence a period of employment which cannot be confirmed at source. In this instance, sensitive information such as account number, sort code, outgoing payments etc is not relevant to the screening process and can therefore be redacted. The only information Vero need to confirm is your identity, your incoming salary payments and the date of these payments.

Please contact the Vero employee coordinating your screening, to confirm what information you can redact.

Destruction of data

Regarding the destruction of your personal data, all papers and information collated during the screening process remain the property of your prospective or existing employer, our Client. All originating hard copy papers and electronic records will be securely stored in accordance with the retention schedule prescribed by our Client.

Once the agreed retention period is met, all such records will be deleted from Vero's systems or destroyed by secure on-site shredding.

Screening platform

Our online screening platform captures and reports screening data and results to our Clients. This platform has been specifically designed to offer a secure method of conducting background screening.

We have put in place specific controls to ensure the confidentiality, integrity and security of your personal data is maintained. These controls apply to both the back-office production interface and the client-side platform.

Input controls

All actions within our systems are audited with date, time and employee identification to ensure traceability.

Access control

To protect against unauthorised access to IT systems, access is by username and encrypted password only and all our screens and computers are locked when not attended.

In addition, the processing of data is restricted by job role on a need-to-know basis, with strict

system access controls meaning only certain personnel can copy, delete or modify data.

Availability controls

To ensure your data is protected against accidental destruction or loss, our primary database server is mirrored within our data centres. All data is backed up off-site by a licensed data recovery supplier and appropriate anti-virus / firewall systems are in place.

Access to premises

Entry to our Head Office is controlled via two separate entry fobs and an alarm system in place. All entry and exit of the building is recorded and CCTV covers all internal doors.

Key holder and alarm system access is restricted and entry to Vero's secure server room is by key fob and a physical key. CCTV is present within the server room recording all entry.

Personnel training and controls

All our employees are themselves subject to employment screening, prior to joining our business. They are also required to complete data protection and information security training courses on their first day of employment.

Employee data protection training is repeated by annually thereafter and our employee contracts include strict obligations regarding the handling of personal data and confidential information.

Supplier management

To deliver our services we work with a network of trusted third-party service providers. If you have lived, worked or studied outside of the EEA, it may be necessary for us to share your data with these third parties, to verify the information you provide, or conduct the checks required by your prospective or existing employer.

These third parties are subject to our formal supplier management policies and procedures which ensure the personal data we share with them is adequately protected, in line with EU and UK law. Our supplier management policies and procedures cover contractual agreements, site security audits, annual information security questionnaires and supplier screening.

Privacy policy

Prior to sharing your personal information with us, we recommend you read the content of our **Privacy notice for Candidates** on our website https://www.veroscreening.com/privacy-policy/ This privacy notice provides full details regarding the personal data we collect, why we collect it and who we share it with.

Contact us

For any queries regarding the handling of your personal data by Vero, please contact our Data Protection Officer who will be happy to help: +44 (0)1273 840 800 or dpo@veroscreening.com

Version control

Issue	Description	Approval	Date of Issue
2.0	First issue	P Hutchinson	21.08.2015
2.1	Document rewrite to include GDPR provisions	P Hutchinson	08.05.2018