VeroPoint

Data Protection Guide for Candidates

17 November 2021 I Reading time 6 minutes (approx.)

We'll take good care of your personal data. This guidance document offers advice and guidance on data protection during the screening process.

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.

Any personal data you provide to us will be used solely for your employment screening

We employ strict technical and organisational measures to safeguard 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 [EU & UK].

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

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 EU & UK General Data Protection Regulation [GDPR] and supporting UK data protection legislation.

Data Minimisation

Our Candidate Portal [online screening form] has been designed to collect the minimum amount of information necessary, to enable the checks and verifications required by your prospective or existing employer. In some instances, you may be asked to provide supporting documentation to evidence the information you provided in your questionnaire, or to complete an element of the screening. In such instances you're encouraged to redact non-relevant or particularly sensitive

information which isn't required as part of the screening process. An example of this might be a bank statement, requested to evidence a period of employment which can't be confirmed at source. In this instance, sensitive information [eg account number, sort code, outgoing payments etc] isn't relevant to the screening process and should be redacted. The only information Vero need to confirm is your identity, your incoming salary payments and the date of these payments.

Your Vero contact will be able to advise you on what information you can redact.

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

If you want to exercise any of the above data subject rights, you'll 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'll pass your request promptly to our Client, so they can assist. As the data processor, we'll provide reasonable assistance, to enable our Client to fulfil their obligations under the GDPR and respond to your request. We'll act solely on their instruction.

Candidate Export-Import

We're conscious you might be asked to go through a screening process with Vero more than once – either for the same Client or for a different Client. So we want to make the 'repeat screen' process as easy as possible for you. With this in mind, we've built an 'export-import' interface into the Candidate Portal [your online screening form]. This functionality means you can keep a local copy of the information you provide to Vero. And if you happen to be screened by Vero again in the future, you can simply re-import this data and use it to populate your new screening form. Look out for the 'Export data' prompt when you complete your online form.

Result Data

Although 'export-import' gives you the option to locally store re-submit the data you provide to Vero, it's important to know the results of your screening [eg reference responses or criminal record checks] can't be automatically carried across from one screening to another. There are two reasons for this. Firstly, it's possible these results may no longer be up to date [this is particularly the case with 'dynamic' checks such as criminal record or financial integrity checks]. As such they can't be re-used. Secondly, if your repeat screening is being conducted on behalf of a different data controller [Client], Vero will need to seek permission from the original data controller before releasing any information either directly to you, or to your new employer [with your permission].

Screening Report Copy

If you want to access the results of a previous screening exercise we conducted on you – perhaps to share with a third party - you'll need to do this by making a GDPR 'Right of Access' request direct to the data controller [Vero's Client]. Alternatively, you can make the request to Vero; however, please be aware we'll be required to forward your request to the data controller on your behalf. They will then respond and release copies of the result data directly to you. You can then share this with your chosen third party, if required. Please do bear in mind that Vero only keep copies of your screening report for a limited about of time [see 'Destruction of Data' below].

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 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've 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.

Security Standards

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

Input Controls

All system actions are audited [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 subject to employment screening, prior to joining our business. They're also required to complete data protection and information security training courses on their first day, and they repeat this training annually thereafter. Our employee contracts also 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've lived, worked or studied outside of the UK or 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 our Privacy notice for Candidates 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'll be happy to help: +44 (0)1273 840 800 or dpo@veroscreening.com