



veriphy.comTM
business intelligence

**people and company
information:**

**gdpr (the general data
protection regulation)**

The Information Commissioner's Office (ICO) has provided a checklist of questions that must be answered in order to show that an organisation is ready for, and compliant with, the introduction of **GDPR**.

Below are **Veriphy's responses** to those questions.

Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

Veriphy has audited the personal data that it holds and where it comes from. Data is provided by our clients for the purposes of carrying out Anti-Money Laundering checks (AML) in line with their legal obligations to comply with the 4th Anti-Money Laundering Directive.

The data is processed against various databases as outlined in our compliance document and the results delivered to our clients on our secure platform. Transmission of data is end to end encrypted.

Your business has identified your lawful basis for processing and documented them.

As the conducting of AML Checks is a legal obligation then we have a lawful basis for the processing of this data.

Your business has reviewed how you ask for and record consent.

The AML Regulations stipulate that consent is not required nor should it ever be sought when conducting AML Checks and it is unlawful to do so. Therefore, records are also not kept.

Consent to process children's personal data for online services

Veriphy does not process children's personal data.

Your business has a process to recognise and respond to individuals' requests to access their personal data.

The information we hold on individuals is subject to various items of legislation not least the Proceeds of Crime Act, which makes it a criminal offence for us to allow access to the results of an AML check, namely the offence of 'Tipping Off.

Where an individual believes that the information processed through our system is incorrect we would refer them to the organisation that gathered the information in the first place, i.e. the organisation which ran the AML check.

Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.

We have implemented a rolling disposal system to permanently erase all data that is older than 12 months. This cut off point has been determined to bring a balance between the needs of our clients to access checks that have been carried out and GDPR. Best practice guidance for AML compliance is checks should be carried out at least once a year making any checks older than this of little value. Where checks have been conducted for purposes other than AML compliance, the associated data will be deleted upon request, and otherwise after 12 months as above. Data is never shared beyond the process of checking or used for any other purpose.

Your business has procedures to respond to an individual's request to restrict the processing of their personal data.

The 4th AML Directive which came into force in the UK on the 26th of June 2017 clearly states that for Anti-Money Laundering purposes the data subject has no right to object to the check being carried out.

Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

Data related risks are taken very seriously. To this end, all transmission of data is end to end encrypted to the highest possible standard. Our webservice through which all data is processed is secured using SSL provided by industry leaders SecureSign, Trustwave and Security Metrics.

Your business understands when you must conduct Data Protection Impact Assessments (DPIA) and has processes in place to action this.

Our service is penetration tested on a monthly basis to ensure the highest level of protection against any developing security threats in line with DPIA best practice.

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

All key people within the organisation are fully aware and actively support the need for compliance with data protection legislation.

Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.

Our servers are UK based.

Your business has effective processes to identify, report, manage and resolve any personal data breaches.

We have designed systems to automatically identify and reports any data breaches and have a technical team available 24/7 to manage and resolve any such breaches.

Your business is currently registered with the Information Commissioner's Office.

Veriphy is a Data Controller under UK Data Protection law and is registered with the ICO with the registration number Z9851928. Our Data Protection Officer is George Ford, who you can contact via dpo@veriphy.com

Veriphy: excellent data at the touch of a button

→ Data sources:

We source our data from the best possible suppliers – BT, Royal Mail, HM Treasury, OFAC, Creditsafe, Equifax, Experian, Lawyer Checker and LexisNexis.

→ Payment methods:

We invoice monthly in arrears, by email. We accept payment by card, BACS, direct debit or cheque. Our system includes a full management and audit facility.

→ How we work:

We charge only for the checks that you undertake. We do not require pre-payment, and we not require a minimum level of checks. You have the freedom to choose. Set-up, subscription, support and the addition of new users are all free.

→ To join:

To become one of the thousands of Veriphy users please go to www.veriphy.com

Company details:

Veriphy Ltd

68 Jesmond Road West . Jesmond . Newcastle upon Tyne . NE2 4PQ

T: 0845 094 8931

E: support@veriphy.co.uk

W: www.veriphy.com

Registered in England and Wales.

Company No. 05066478

v. 1.03 09/02/2018

www.veriphy.com
support@veriphy.co.uk