VERIPH

# Veriphy compliance document:

# information security
# terms & conditions
# data privacy

*version 3.21 28/10/2023*



Registered in England and Wales. Company No. 05066478

Veriphy Ltd
5th Floor, 20 Gracechurch Street, London EC3V 0BG
E: support@veriphy.co.uk W: www.veriphy.com

## Contents

## Veriphy Ltd

**Registered address:**

5th Floor, 20 Gracechurch Street, London EC3V 0BG

Registered in England and Wales.

Company No. 05066478

Veriphy Ltd is a member of the Davies Group of companies, the parent of which is Davies Group Limited (Company Number 6479822)

**Website address:**

support@veriphy.co.uk

www.veriphy.com

**Operational Contact:**

Account Director:

Richard Devine

richard.devine@davies-group.com

**Data Protection:**

ICO Registration number: Z9851928

Data Protection Officer:

Yousif Ashaa

compliance@davies-group.com

0344 856 2424

# Information security

## Data Storage

All data is stored in MS Azure UK South data centre (London) with UK West (Cardiff) used for DR.

Data is encrypted with 256 bit AES encryption at rest.

Further detail is at: https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/

We have in place rolling 12 month irreversible data deletion.

## Patch Management Process

Automated patching on website/api via Azure App Service.

Automated patching on SQL Server via Azure agents.

## Penetration Testing

An external company - Security Metrics – (https://www.securitymetrics.com) performs audits/penetration testing against our infrastructure.

## Data Security

Role based security with username/password. There is one way, irreversible encryption of credentials. 5 incorrect password attempts results in lockout.

Antivirus/malware services are utilised on all server and management endpoints. Antivirus protection is provided by Symantec Endpoint Protection.

Cyber Essentials certification is in place.

All data is sent over https/TLS 1.2/PFS. Data is encrypted with 256 bit AES encryption in transit.

## Physical Security

In place are CCTV, access control, security guards, perimeter fencing, biometric ID screening, full body metal detection screening.

Data Centre access requires two-factor authentication with biometrics, full body metal detection screening, limited access request and approval with time limitation.

Data Centre Standards are: ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

## Data Disposal

Data can be instantly, securely erased on demand. Alternatively, data including backups and anonymized

Telemetry data are retained for a maximum of 90 days before deletion. EOL destruction after 3 years, defective equipment is wiped if possible before return to OEM or destroyed onsite if appropriate.

Data/devices are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

## Operational Security

System updates/changes will be deployed at regular scheduled intervals. Customers will be notified about the impact of the changes via email with notice of any required downtime or system availability issues.

Contingency plans will be in place in event of partial or total system failure. Antivirus/malware services are utilised on all server and management endpoints. Monitoring is provided by Azure Security Monitor and Automation.

## Disaster Recovery

There is a 99.9% uptime Microsoft SLA

Geo-redundancy to facilitate disaster recovery and maintain uptime:

Our primary region is UK South (London) with the secondary backup region of UK West (Cardiff).

The front-end website and API are hosted in the Azure App Service. This is a load balanced, managed environment with multiple instances and autoscaling for high availability and performance.

The database is powered by SQL Server 2016. SQL AlwaysOn technology is used to provide resilience for the data tier.

All data is located in the UK with locally redundant storage at both the primary and secondary sites.

Automatic failover to secondary (UK West) from primary region (UK South). In the unlikely event of an entire region failing a manual restore to the North or West Europe regions could be performed.

Point in time restore of all databases is available. Daily website file backups to locally redundant storage are performed.

All virtual machines are protected by Azure Recovery Vault.

The Azure business continuity strategy is listed here https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions.

We automate backup and encrypt databases, data and sites to locally redundant storage at both locations.  Recovery services is used for point of time restore of our hosted VMs which are also encrypted on locally redundant storage at both regions.

**Azure customer data protection**

Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies. The access-control requirements are established by the following Azure Security Policy:

- No access to customer data, by default.
- No user or administrator accounts on customer virtual machines (VMs).
- Grant the least privilege that's required to complete task; audit and log access requests.

Azure support personnel are assigned unique corporate Active Directory accounts by Microsoft. Azure relies on Microsoft corporate Active Directory, managed by Microsoft Information Technology (MSIT), to control access to key information systems. Multi-factor authentication is required, and access is granted only from secure consoles.

All access attempts are monitored and can be displayed via a basic set of reports.

## Data protection

Azure provides customers with strong data security, both by default and as customer options.

**Data segregation**: Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.

**At-rest data protection**: Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.

**In-transit data protection**: Microsoft provides a number of options that can be utilized by customers for securing data in transit internally within the Azure network and externally across the Internet to the end user. These include communication through Virtual Private Networks (utilizing IPsec/IKE encryption), Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway or Azure Front Door), protocols directly on the Azure virtual machines (such as Windows IPsec or SMB), and more.

Additionally, "encryption by default" using MACsec (an IEEE standard at the data-link layer) is enabled for all Azure traffic travelling between Azure datacenters to ensure confidentiality and integrity of customer data.

**Data redundancy**: Microsoft helps ensure that data is protected if there is a cyberattack or physical damage to a datacenter. Customers may opt for:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.

Data can be replicated within a selected geographic area for redundancy but cannot be transmitted outside it. Customers have multiple options for replicating data, including the number of copies and the number and location of replication datacenters.

**Data destruction**: When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

# Veriphy Terms

## VERIPHY GENERAL CONDITIONS

Veriphy is a software platform, accessible via the internet, which allows customers to perform various anti-money laundering, other know-your-customer checks and other checking and verification services. By agreeing to these General Conditions, which incorporate the Third Party Conditions, an **agreement** is formed between the Customer and Veriphy and the Customer agrees to be bound by the General Conditions and Third Party Conditions.

Please note that the Customer may not begin using some or all of the Services until Veriphy has successfully verified the Customer's identity and business sector.

## AGREED TERMS

### 1. INTERPRETATION

1.1 The definitions and rules of interpretation in this clause apply in these General Conditions.

**agreement:** the agreement made between the Customer and Veriphy, incorporating these General Conditions and the Third Party Conditions.

**Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

**Confidential Information:** information that is proprietary or confidential and is either clearly labelled as such or identified as Confidential Information in clause 10.5 or clause 10.6.

**Controller**, **processor**, **data subject**, **personal data**, **personal data breach, processing and appropriate technical and organisational measures**: as defined in the Data Protection Legislation.

**Data:** means the information and data which is stored on and/or accessed through the Services, including relating to individuals or businesses and/or the original source materials containing such data.

**Data Processing Terms**: the terms appearing at the end of these General Conditions which apply where Veriphy is processing the Customer's personal data as a processor.

**Data Protection Legislation:** the UK Data Protection Legislation and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the relevant data protection or supervisory authority and applicable to a party.

**Documentation:** the user guides made available to the Customer by Veriphy online via the help section of www.veriphy.com or such other web address notified by

Veriphy to the Customer from time to time which sets out the user instructions for the Services.

**Effective Date:** the date the agreement is entered into.

**Fees:** the fees for the Services payable by the Customer to Veriphy for the Services, as set out on the Website or as otherwise agreed in writing between Veriphy and the Customer.

**Laws:** means laws, regulations and rules, treaties, legal and regulatory requirements and codes of conduct which govern the use of the Services and Data.

**Reports:** means all Data, scores, reports, documents and other output and information provided by Veriphy or its Third Party Suppliers as part of the Services**.**

**Security Event**: means any incident where a user ID and/or password for access to the Services or the Data, or any information related thereto, is or has been lost, stolen, compromised, misused or used, disclosed, accessed or acquired in an unauthorised manner or by any unauthorised person, or for any purpose contrary to the terms of the agreement.

**Services:** means the products and/or services which are provided to the Customer by Veriphy to include, where applicable, provision of access to Data and Reports

**Software:** the online software applications provided by Veriphy as part of the Services.

**Third Party Conditions:** the terms and conditions (as amended from time to time) applicable to that part of the Services or Data which are supplied by a Third Party Supplier.

**Third Party Supplier:** means any third party which provides Data, Reports or services which are incorporated into the Services by Veriphy from time to time

**UK Data Protection Legislation**: all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

**Users:** those employees, agents and independent contractors of the Customer who are authorised by the Customer to use the Documentation and Services and to access the Data and Reports.

**Virus:** any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or

data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

**Website:** means Veriphy's website located at www.veriphy.com.

1.2 Clause, schedule and paragraph headings shall not affect the interpretation of these General Conditions.

1.3 A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.6 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.7 A reference to a statute or statutory provision is a reference to it as it is in force as at the date of the agreement.

1.8 A reference to a statute or statutory provision shall include all subordinate legislation made as at the date of the agreement under that statute or statutory provision.

1.9 A reference to writing or written includes e-mail.

1.10 References to clauses and schedule are to the clauses and schedule of these General Conditions; references to paragraphs are to paragraphs of the relevant schedule to these General Conditions.

## 2. SERVICES

2.1 In consideration for the payment of the Fees by the Customer to Veriphy and for the duration of the agreement, Veriphy shall:

(a) at the Customer's request, provide the Services and make available the Data and the Documentation to the Customer; and

(b) grant to the Customer and its Users a non-exclusive, non-transferable licence to access and use the Services and the Data (including any Reports) solely for the Customer's internal business purposes.

2.2 The Customer acknowledges that the Services are constantly being updated and added to and therefore will change from time to time without notice.

2.3 Not all of the Services may be available immediately after the agreement is entered into as some parts of the Services are subject to external verification prior to them being available.

## 3. USE OF THE SERVICE

3.1 The Customer shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the Services that:

(a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

(b) facilitates illegal activity;

(c) depicts sexually explicit images;

(d) promotes unlawful violence;

(e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

(f) is otherwise illegal or causes damage or injury to any person or property;

and Veriphy reserves the right, without liability or prejudice to its other rights to the Customer,

to disable the Customer's access to any material that breaches the provisions of this clause.

3.2 The Customer shall not:

(a) except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under the agreement:

(i) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software and/or Documentation (as applicable) in any form or media or by any means; or

(ii) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or

(b) access all or any part of the Services, Data, Reports or Documentation in order to build a product or service which competes with the Services and/or the Documentation; or

(c) use the Services, Data, Reports and/or Documentation to provide services to third parties; or

(d) subject to clause 20.1, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services, Data, Reports and/or Documentation available to any third party except the Users, or

(e) attempt to obtain, or assist third parties in obtaining, access to the Services, Data, Reports and/or Documentation, other than as provided under this clause **Error! Reference source not found.**; or

(f) introduce or permit the introduction of, any Virus into Veriphy's network and information systems.

3.3 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services, Data, Reports and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify Veriphy.

3.4 Each User shall keep a secure password for their use of the Services, that such password shall be changed no less frequently than every 6 months and that each User shall keep his password confidential.

3.5 The rights provided under this clause **Error! Reference source not found.** are granted to the Customer only, and shall not be considered granted to any subsidiary or holding company of the Customer.

## 4. DATA PROTECTION

4.1 Each Party shall comply with its respective obligations under the Data Protection Legislation in respect of any personal data processed in relation to the agreement.

4.2 The Customer represents and warrants that it has the right to collect, process, and use personal data for the purpose(s) for which it is accessing the Services, the Data and the Reports and that it has complied with all other obligations under applicable Laws that relate to its access to and use of the Services, including, without limitation, that before it provides any personal data to Veriphy, it shall:

(a) make due notification to any relevant regulator including its use and processing of the personal data and comply at all times with the Data Protection Legislation;

(b) ensure it is not subject to any prohibition or restriction which would: (i) prevent or restrict it from disclosing or transferring the personal data to Veriphy, as required under the agreement; or (ii) prevent or restrict either Party from processing the personal data as envisaged under the agreement;

(c) ensure that all required notices have been given and, as applicable, all required authorisations or consents have been obtained, and are sufficient in scope to enable each Party to process the personal data as required in order to obtain the benefit of its rights, and to fulfil its obligations, under the agreement in accordance with the Data Protection Legislation, including the transfer of such personal data to and by Veriphy and Veriphy’s third party service providers in any jurisdiction.

4.3 To the extent that Veriphy act as a processor of personal data on behalf of the Customer under the agreement, the Parties shall process such personal data in accordance with the Data Processing Terms which appear at the end of these General Conditions

4.4 The Customer agrees that it shall not permit any of its Users, group companies, operations, businesses, employees, agents or representatives located outside the European Economic Area to access the Services and/or to use the Data unless it has entered into European Commission-approved Standard Contractual Clauses or other appropriate safeguards as described in the Data Protection Legislation.

4.5 The Customer acknowledges that in the event of a Security Event, the Customer shall notify Veriphy immediately, shall cooperate fully with any action Veriphy and/or the Customer is obliged by law to take in respect of such Security Event or independently fulfil its own obligations that may result in Veriphy's reasonable discretion. The Customer agrees that unless required by law or the relevant regulatory authority, any notification of a Security Event to the data subject or to a regulatory body shall not reference Veriphy or the Services through which the Data was provided, nor shall Veriphy be otherwise identified or referenced in connection with the Security Event, without Veriphy's express written consent.

4.6 The Customer shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law and all fines and costs relating to a Security Event other than where such Security Event is a direct result of Veriphy's negligence and/or breach of the agreement.

## 5. THIRD PARTY SUPPLIERS

5.1 To the extent that the Services, Data or Reports derives from a Third Party Supplier, the Third Party Conditions shall apply. The Customer acknowledges that Veriphy has discretion to determine which Third Party Supplier is used in the provision of Services, Data and Reports at any given time. In the event of a conflict between the Third Party Conditions (as applicable) and these General Conditions, the Third Party Conditions shall apply.

## 6. VERIPHY'S OBLIGATIONS

6.1 Veriphy undertakes to provide the Services with reasonable skill and care.

6.2 Veriphy:

(a) does not warrant that:

(i) the Customer's use of the Services or the Data or Reports will be uninterrupted or error-free; or

(ii) that the Services will be available for access all the time or at any time on a continuous uninterrupted basis;

(iii) that the Services, Data, Reports and Documentation will meet the Customer's requirements.

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services, Data, Reports and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

6.3 The Customer acknowledges and agrees that the Data is sourced from selected public records and other sources. Veriphy, or its Third Party Suppliers, do not take any steps to verify the accuracy or completeness of the Data and Veriphy does not make any warranty, representation of the Data or that it is up to date. The Data is

therefore provided to the Customer "as is" and with no undertaking as to the accuracy, completeness of Data or that the Data is up to date. The Services are not the source of the Data, nor are they a comprehensive compilation of the Data. The Customer acknowledges that Data supplied by Veriphy to the Customer are not intended to be used as the sole basis for any decision significantly affecting a data subject and that Customer is responsible for any decisions or actions it takes.

6.4 The agreement shall not prevent Veriphy from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under the agreement.

6.5 Veriphy warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under the agreement.

## 7. CUSTOMER'S OBLIGATIONS

7.1 The Customer shall:

(a) Only use the Services and the Data for its own internal business purposes subject to any restrictions set out in these General Conditions or the Third Party Conditions.

(b) provide Veriphy with:

(i) all necessary co-operation in relation to the agreement; and

(ii) all necessary access to such information as may be required by Veriphy;

in order to provide the Services, including but not limited to security access information and configuration services;

(c) without affecting its other obligations under the agreement, comply with all applicable laws and regulations with respect to its activities under the agreement including its use of the Services, Data and the Reports;

(d) keep all Data and Reports accessed using the Services confidential and secure;

(e) carry out all other Customer responsibilities set out in the agreement in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the parties, Veriphy may adjust any agreed timetable or delivery schedule as reasonably necessary;

(f) ensure that the Users use the Services, the Data and the Reports in accordance with the terms and conditions of the agreement and shall be responsible for any Authorised User's breach of the agreement;

(g) obtain and shall maintain all necessary licences, consents, and permissions necessary for Veriphy, its contractors and agents to perform their obligations under the agreement, including without limitation the Services;

(h) ensure that its network and systems comply with the relevant specifications provided by Veriphy from time to time; and

(i) be, to the extent permitted by law and except as otherwise expressly provided in the agreement, solely responsible for procuring, maintaining and securing its network connections and telecommunications links from its systems to Veriphy's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

## 8. FEES AND PAYMENT

8.1 The Customer shall pay Fees to Veriphy for the Services in accordance with this clause 8. Unless otherwise agreed in writing, the Fees for the Services are set out on the Website and are subject to change from time to time. The Fees are on a pay-per-use basis as described on the Website.

8.2 The Customer shall be responsible for any access or attempted access to the Services made using the Customer's account and shall be responsible for any usage, whether or not such usage was authorised by it.

8.3 Veriphy shall invoice the Customer for the Fees monthly until termination of the agreement and the Customer shall pay each invoice within 30 days after the date of such invoice.

8.4 If Veriphy has not received payment within 7 days after the due date, and without prejudice to any other rights and remedies of Veriphy:

(a) Veriphy may, without liability to the Customer, disable the Customer's password, account and access to all or part of the Services and Veriphy shall be under no obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid; and

(b) the Customer shall pay interest on the overdue sum from the due date until payment of the overdue sum, whether before or after judgment. Interest under this Clause 8.4 will accrue each day at 4% a year above the Bank of England's base rate from time to time, but at 4% a year for any period when that base rate is below 0%.

8.5 All amounts and fees stated or referred to in the agreement:

(a) shall be payable in pounds sterling;

(b) are non-cancellable and non-refundable;

(c) are exclusive of value added tax, which shall be added to Veriphy's invoice(s) at the appropriate rate.

## 9. PROPRIETARY RIGHTS

9.1 The Customer acknowledges and agrees that Veriphy and/or its licensors own all intellectual property rights in the Services, the Data, the Reports and the Documentation. Except as expressly stated herein, the agreement does not grant the Customer any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trademarks (whether registered or unregistered), or any other

rights or licences in respect of the Services, the Data, the Reports or the Documentation.

9.2 Veriphy confirms that it has all the rights in relation to the Services, the Data, the Reports and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of the agreement.

## 10. CONFIDENTIALITY

10.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under the agreement. A party's Confidential Information shall not be deemed to include information that:

(a) is or becomes publicly known other than through any act or omission of the receiving party;

(b) was in the other party's lawful possession before the disclosure;

(c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or

(d) is independently developed by the receiving party, which independent development can be shown by written evidence.

10.2 Subject to clause 10.4, each party shall hold the other's Confidential Information in confidence and not make the other's Confidential Information available to any third party, or use the other's Confidential Information for any purpose other than the implementation of the agreement.

10.3 Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of the agreement.

10.4 A party may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause 10.4, it takes into account the reasonable requests of the other party in relation to the content of such disclosure.

10.5 The Customer acknowledges that details of the Services, and the results of any performance tests of the Services, constitute Veriphy's Confidential Information.

10.6 No party shall make, or permit any person to make, any public announcement concerning the agreement without the prior written consent of the other parties (such consent not to be unreasonably withheld or delayed), except as required by law, any governmental or regulatory authority (including, without limitation, any relevant securities exchange), any court or other authority of competent jurisdiction.

10.7 The above provisions of this clause 10 shall survive termination of the agreement, however arising.

## 11. INDEMNIFICATION AND LIMITATION OF LIABLITY

11.1 Veriphy will use reasonable efforts to deliver the Services and Data requested by the Customer however the Customer acknowledges that Data and Reports are provided on an “as is” and “as available” basis. The Customer acknowledges that the Services involve conveying information provided to Veriphy and its Third Party Suppliers by other sources, Veriphy cannot and will not, for the fee charged for the Services, be an insurer or guarantor of the accuracy or reliability of the Services, the Data or the Reports. Accordingly, Veriphy does not guarantee, warrant or represent the accuracy, timeliness, completeness, validity, currentness, merchantability or fitness for a particular purpose of the Services, the Data or the Reports and subject to clause 11.4, Veriphy shall not be liable to the Customer or any third parties for any loss or injury arising out of or caused in whole or in part by Veriphy’s acts or omissions, whether negligent or otherwise, in procuring, compiling, collecting, interpreting, reporting, communicating or delivering the Services, Data or Reports.

11.2 The Customer will indemnify, defend, and hold Veriphy and the Third Party Suppliers (and their affiliates) harmless from and against any and all liabilities, damages, losses, claims, costs and expenses, including reasonable legal fees, which may be asserted against or incurred by Veriphy or the Third Party Suppliers, arising out of or resulting from the use, disclosure, sale or transfer of the Services, Data and/or the Reports (or information therein) by the Customer, or for the Customer’s breach of the agreement. The Customer warrants not to sue or maintain any cause of action, claim, demand, cross claim, third party action or other form of litigation or arbitration against Veriphy, the Third Party Suppliers or their officers, directors, employees, contractors, agents, affiliated bureaus or subscribers arising out of or relating in any way to the Services, the Data or the Reports (or information therein) being blocked by the Third Party Suppliers or not being accurate, timely, complete or current. The Customer agrees that the Third Party Suppliers and their data suppliers are entitled to enforce the data security, use, legal compliance and indemnification provisions of the agreement directly against the Customer.

11.3 The Customer acknowledges that Veriphy and/or its Third Party Suppliers maintains a database, updated on a periodic basis, from which the Customer obtains the Services, Data and Reports, and that Veriphy or its Third Party Suppliers do not undertake a separate investigation for each enquiry or request for Services made by the Customer. The Customer also acknowledges that the prices Veriphy charges the Customer for the Services are based upon Veriphy’s expectation that the risk of any loss or injury that may be incurred by use of the Services will be borne by the Customer and not Veriphy. The Customer therefore agrees that it is responsible for determining that the Services are in accordance with Veriphy’s obligations under the agreement. If the Customer reasonably determines that the Services (including the Data or Reports) do not meet Veriphy’s obligations under the agreement, the Customer shall so notify Veriphy in writing within ten (10) days after receipt of the Services in question. The Customer’s failure to notify Veriphy within the specified period of time herein, shall mean the Customer accepts the Services as is, and Veriphy will be discharged of any liability for non-performance of the Services. If Customer so notifies Veriphy within ten (10) days after receipt of the Services, then, unless Veriphy disputes the Customer’s claim, Veriphy will, at its option, either re-perform the Services in question or issue the Customer a credit for the amount the

Customer paid to Veriphy for the nonconforming Services. The Customer agrees that the credit for nonconforming Services shall be Veriphy's aggregate liability for every kind of liability arising under or in connection with the agreement including liability in contract, tort (including negligence), misrepresentation, restriction of otherwise in connection with the non-conforming Services. Unless the Customer notifies Veriphy that it intends to make a claim in respect of an event within the notice period given in this clause 11.3, Veriphy shall have no liability for that event.

11.4 Nothing in the agreement excludes the liability of Veriphy:

(a) for death or personal injury caused by Veriphy's negligence; or

(b) for fraud or fraudulent misrepresentation.

11.5 Veriphy has given commitments as to the quality of the Services. In view of these commitments, the terms implied by sections 3, 4 and 5 of the Supply of Goods and Services Act 1982 are, to the fullest extent permitted by law, excluded from the agreement.

11.6 Subject to clause 11.4, Veriphy shall not be liable whether in tort (including negligence), contract, misrepresentation, restitution or otherwise for any of the following howsoever arising under the agreement:

(a) loss of profits or loss of earnings.

(b) loss of sales or business.

(c) loss of agreements or contracts.

(d) loss of anticipated savings.

(e) Increase in bad debt or failure to reduce bad debt.

(f) loss of use or corruption of software, data or information.

(g) loss of or damage to goodwill; and

(h) indirect or consequential loss.

11.7 Subject to clause 11.3, clause 11.4 and clause 11.6, Veriphy's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of the agreement shall be limited to the total Fees paid during the 3 months immediately preceding the date on which the claim arose. This cap on liability shall be reduced by any credits awarded in accordance with clause 11.3

## 12. AUDIT

12.1 The Customer agrees that, subject to the Customer being given reasonable prior written notice, it shall permit Veriphy and its authorised independent auditors to have reasonable access during the Customer's normal business hours to the Customer's relevant premises, operations, records and systems for the sole purpose of ensuring that the Customer is complying with its obligations under the agreement.

12.2 In the event of Veriphy exercising its rights under clause 12.1 Veriphy shall at all times comply with the Customer's reasonable safety and security rules and regulations in place from time to time.

## 13. SUSPENSION AND TERMINATION

13.1 The agreement shall, unless otherwise terminated as provided in this clause 12, commence on the date it is entered into and shall continue indefinitely unless either party gives to the other written notice to terminate in which case the agreement shall terminate with immediate effect.

13.2 If the Customer breaches any of the terms of the agreement, Veriphy shall be entitled to suspend the Services (or any part of them) with immediate effect.

13.3 Without affecting any other right or remedy available to it, either party may terminate the agreement with immediate effect by giving written notice to the other party if:

(a) the other party commits a material breach of any term of the agreement and (if such a breach is remediable) fails to remedy that breach within 14 days of that party being notified in writing to do so;

(b) the other party takes any step or action in connection with its entering administration, provisional liquidation or any composition or arrangement with its creditors (other than in relation to a solvent restructuring), obtaining a moratorium, being wound up (whether voluntarily or by order of the court, unless for the purpose of a solvent restructuring), having a receiver appointed to any of its assets or ceasing to carry on business or, if the step or action is taken in another jurisdiction, in connection with any analogous procedure in the relevant jurisdiction;

(c) the other party suspends, or threatens to suspend, or ceases or threatens to cease to carry on all or a substantial part of its business; or

(d) the other party's financial position deteriorates so far as to reasonably justify the opinion that its ability to give effect to the terms of the agreement is in jeopardy.

13.4 On termination of the agreement for any reason:

(a) all licences granted under the agreement shall immediately terminate and the Customer shall immediately cease all use of the Services, Data, Reports and/or the Documentation;

(b) each party shall return and make no further use of any equipment, property, Documentation and other items (and all copies of them) belonging to the other party;

(c) any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination shall not be affected or prejudiced.

## 14. FORCE MAJEURE

Veriphy shall have no liability to the Customer under the agreement if it is prevented from or delayed in performing its obligations under the agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of Veriphy or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that the Customer is notified of such an event and its expected duration.

## 15. VARIATION

No variation of the agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives) provided always that the General Conditions and Third Party Conditions may be amended from time to time by Veriphy with the applicable version being published on the Website.

## 16. WAIVER

No failure or delay by a party to exercise any right or remedy provided under the agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

## 17. RIGHTS AND REMEDIES

Except as expressly provided in the agreement, the rights and remedies provided under the agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

## 18. SEVERANCE

18.1 If any provision or part-provision of the agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the agreement.

18.2 If any provision or part-provision of the agreement is deemed deleted under clause 18.1 the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

## 19. ENTIRE AGREEMENT

19.1 The agreement, incorporating the General Conditions and Third Party Conditions, constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties,

representations and understandings between them, whether written or oral, relating to its subject matter.

19.2 Each party acknowledges that in entering into the agreement it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the agreement.

19.3 Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the agreement.

19.4 Nothing in this clause shall limit or exclude any liability for fraud.

## 20. ASSIGNMENT

20.1 The Customer shall not, without the prior written consent of Veriphy, assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under the agreement.

20.2 Veriphy may at any time assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under the agreement.

## 21. NO PARTNERSHIP OR AGENCY

Nothing in the agreement is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

## 22. THIRD PARTY RIGHTS

The agreement does not confer any rights on any person or party (other than the parties to the agreement and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

## 23. NOTICES

23.1 Any notice required to be given under the agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its address set out in the agreement, or such other address as may have been notified by that party for such purposes, or sent by fax to the other party's fax number as set out in the agreement.

23.2 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. A notice sent by fax shall be

deemed to have been received at the time of transmission (as shown by the timed printout obtained by the sender).

## 24. GOVERNING LAW

The agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.

## 25. JURISDICTION

Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the agreement or its subject matter or formation (including non-contractual disputes or claims).

## Schedule – Data Processing Terms

1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This Schedule is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation. In this Schedule, **Applicable Law** means (for so long as and to the extent that they apply to Veriphy) the law of the European Union, the law of any member state of the European Union and/or Domestic UK Law; and **Domestic UK Law** means the UK Data Protection Legislation and any other law that applies in the UK.

1.2 The parties acknowledge that this Schedule shall only apply where the Customer is the controller and Veriphy is the processor.

1.3 Without prejudice to the generality of clause 1.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to Veriphy and/or lawful collection of the personal data by Veriphy on behalf of the Customer for the duration and purposes of this agreement.

1.4 Without prejudice to the generality of clause 1.1, Veriphy shall, in relation to any personal data processed in connection with the performance by Veriphy of its obligations under this agreement:

(a) process that personal data only on the documented written instructions of the Customer unless Veriphy is required by Applicable Laws to otherwise process that personal data. Where Veriphy is relying on Applicable Laws as the basis for processing personal data, Veriphy shall promptly notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit Veriphy from so notifying the Customer;

(b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential; and

(d) not transfer any personal data outside of the European Economic Area unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(i) the Customer or Veriphy has provided appropriate safeguards in relation to the transfer;

(ii) the data subject has enforceable rights and effective legal remedies;

(iii) Veriphy complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any personal data that is transferred; and

(iv) Veriphy complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the personal data;

(v) assist the Customer, at the Customer's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(vi) notify the Customer without undue delay on becoming aware of a personal data breach;

(vii) at the written direction of the Customer, delete or return personal data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the personal data; and

(viii) maintain complete and accurate records and information to demonstrate its compliance with Schedule and allow for audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of Veriphy, an instruction infringes the Data Protection Legislation.

1.5 The Customer consents to Veriphy appointing third-party processors of personal data under this agreement. Veriphy confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement substantially on that third party's standard terms of business and Veriphy confirms reflect and will continue to reflect the requirements of the Data Protection Legislation. As between the Customer and Veriphy, Veriphy shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this paragraph 1.5.

1.6 Veriphy may, at any time on not less than 30 days' notice, revise this Schedule by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to the agreement).

# Privacy Policy

## Veriphy Privacy

## Policy Information

## Usage

Veriphy Ltd. ("we") are committed to safeguarding your privacy online. The information we collect from you is only that required by us and/or any third party vendor or organisation associated with us in order for us to provide you with the information you have requested.

We handle all information provided in a secure manner and treat it as completely confidential.

We will not supply your personal information to any other person unless you have expressly authorised us to do so.

## Data Protection Act

We are registered under the Information Commissioner's Office Data Protection Register, Registration Number Z9851928. http://www.ico.gov.uk

Your data is protected in the UK by the Data Protection Act 2018 and the GDPR. The data subject has the right to see what is held about them and correct any inaccuracies. They can also request that data held about them is removed or transferred to an authorised (By the ICO) firm. Firms however do have a legal and regulatory right to retain their data indefinitely dependent upon their status. The data subject may be charged a fee if there are multiple requests.. This will be waived if any of the information which we hold is incorrect.

If you have any queries about the information we hold on you, please contact our Data Protection Officer:

Yousif Ashaaf

**e:**compliance@davies-group.com
**t:** 0207 8705901

## Veriphy GDPR Policy

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), identity checks, and Criminal Record checks in line with their legal obligations to comply with the AML and related regulations.

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.

.
As the conducting of AML Checks is a legal obligation, as is completion of Criminal Record checks, we have a lawful basis for the processing of this data.

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.

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.

We have implemented a rolling disposal system to permanently erase all data that is older than12 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.

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 web service through which all data is processed is secured using SSL provided by industry leaders SecureSign, Trustwave and Security Metrics.

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.

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

Our servers are UK based.

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.

Veriphy Ltd's Data Protection number is Z9851928.

**Cookies**

This site does not use cookies except for the opt-in only facility for remembering log-in details.

Our uses of data

We use the data we collect to operate our business and provide the products we offer. The information we collect may be used for the provision of only the services we offer in the normal trading of the business. 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.
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.

Sharing Your data

Your personal information may be shared with and processed by a number of third parties which include but are not limited to regulatory, dispute resolution or law enforcement bodies or with prospective buyers or purchasers in the event we wish to sell all or part of our business.
Your data may be disclosed when we believe in good faith that the disclosure is required by law; necessary to protect the safety of our employees or the public; required to comply with a judicial proceeding, court order or legal process; or for the prevention or detection of crime (including fraud).

We will only share your information in compliance with data protection laws.

Data Retention

We will only keep data for as long as it is necessary to continue providing our products and services to you and/or to fulfil our legal and regulatory obligations in line with our data retention policy.

We have implemented a rolling disposal system to permanently erase all data that is older than12 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.

Data Subject Rights

Subjects have a number of rights in relation to the information we hold about them. These include: the right to object to the use of your personal information to the right to ask for a copy of the personal information We hold about you, subject to certain exemptions; the right to ask us to update or correct your personal information to keep it accurate; the right to withdraw any permission you have previously provided; the right to ask us to delete your personal information from our records if it is no longer needed for the original purpose; the right to ask us to restrict the use of your personal information in certain circumstances; and the right to complain about how we handle your data.

We will consider your request and either comply with it or explain why we are not able to. Please note, we may request evidence of your identity to process your request.

If you are not happy with any aspect of how we handle your data, we encourage you to come to us in the first instance but you are entitled to complain to the Information Commissioner's Office (ICO):

Who to contact:

If you wish to exercise any of your rights or have any queries about how we use your personal information, please contact our Compliance Officer by email: compliance@davies-group.com, by telephone to 0207 8705901 or by post to Veriphy Limited, 71 Grey Street, Newcastle upon Tyne NE1 6EF

Writing: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113 (local rate) 01625 545 745 (National Rate)

Website: https://ico.org.uk/concerns

Registered in England and Wales. Company No. 05066478

**Veriphy Ltd**

5th Floor, 20 Gracechurch Street, London EC3V 0BG

**E:** support@veriphy.co.uk

**W: www.veriphy.com**