Prepared By: Krisztina Shutt
On: 25.05.2018
Signature: Krisztina Shutt

Approved By: Leon Reed
On: 03.11.2021
Signature: Leon Reed

OBJECTIVES

To establish and maintain a clear policy and the procedures for implementing this policy relating to Privacy and Data Protection and to ensure that the company is compliant with the requirements of the General Data Protection Regulation (GDPR).

SCOPE

This is a core procedure and applies to all parts of the company and all staff.

RESPONSIBILITY

Senior management is responsible for the implementation of these procedures.

Senior Management – This refers to either the Chief Executive Officer (CEO) or Chief Technical Officer (CTO) who manage the entire process and must make sure that all other staff are doing their job at the right time and to the required quality.

General Manager – This refers to the Manager in charge of running the company's operations on a day-to-day basis which includes job bookings, scheduling, invoicing, and accounting.

Supply Chain Program Manager - This refers to the Manager in charge of running the supply chain programs for retailers, this job also includes building online questionnaires and audits on the Company's bespoke, cloud-based system.

Salesperson – This is the person who visits the prospect or customer and tries to get business or set up an audit program for the company. The salesperson may be anyone other than auditors in the company but mainly will be senior management at the moment.

Auditor (Lead, Senior or Assessor) - The person who visits the site, performs the audit and is solely responsible for delivering a professional and accurate audit report by the required time.

Coordinator – This person is fully responsible for the entire process of receiving a client booking, checking all the information is correct and chasing anything that is missing, preparing, and sending out invoices, final approval of the audit report and sending to the client. Another description for this role is **Customer Service**. All entries in Optimus related to his/her client are his/her responsibility.

Scheduler – This person is responsible for scheduling the audits with the right auditor and ensuring that the logistics work and all auditors have a high level of utilisation per week/month.

Report Checker – This person is responsible for checking all audit reports 100% for accuracy and following up with auditors on matters that need to be clarified. He/ She is also responsible for gathering statistics on auditor's accuracy and on-time performance.

For detailed information on the qualifications and exact job descriptions referenced positions please refer to the documents *VQM-002 Verisio Org Chart and VQM-003 Job Descriptions.*

DEFINITIONS

The names of documents used in this process are in *Italic*. Blank forms to be completed in the process are <u>underlined</u>. Key terms highlighted in **bold**. Forms and documents referred to are all listed in the Appendix at the end of the procedure. Abbreviations will be placed in brackets after the full descriptions, the first time they are used.

The font used for this procedure is **Monserrat 10 Black**

All references to He/ She are interchangeable.

The words **Customer** and **Client** are interchangeable.

A **Supplier** can be an agent, trader, middleman or the actual production site. A **factory** is the actual production site where the goods are made, or final assembly is done. A factory may also be a farm for food clients. If the factory has several sites that need to be visited then the expression **plant** may be used to define these further. A factory is the production **site** that is to be audited. Sometimes an office location may be audited on instruction from the customer. A factory may be 2 people or 50,000 people. A factory may be a farm or any other type of production line.

A **Job** is a request to audit a factory or inspect products in a factory. One set of audit or inspections reports will be issued per job.

Optimus refers to the Compliance Management Software system that Verisio uses to book, schedule, invoice, track and file all audit and inspection job requests from customers. For further information relevant Optimus Training documents which are to be found in the Library folder of Optimus available to all employees.

Xero is the cloud-based invoicing system used by Verisio to issue invoices and manage accounting.

Data Controller has a specific meaning within the General Data Protection Regulation. It means a person, organisation or body that determines the purposes for which, and the way, any Personal

Data is processed.

Data Processor means any person, organisation or body that processes personal data on behalf of and on the instruction of the company. Data processors have a duty to protect the information they process by following the Data Protection Rules.

Data Subject means a living individual about whom the company processes Personal Data and who can be identified from the Personal Data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their Personal Data and the information that the company holds about them.

Personal Data means any information relating to a living individual who can be identified from that information or in conjunction with other information, which is in, or is likely to come into, the company's possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g., a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

Processing means any activity that involves use of Personal Data. It includes obtaining, recording, or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

Special Categories of Personal Data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the data subject.

EXECUTIVE SUMMARY

Key facts of the policy

In line with the requirements of the new General Data Protection Regulation (GDPR) that has just come into effect, Verisio has developed policy and procedures to address the challenges relating to our industry. The salient features in practical terms are as follows:

- Verisio takes data protection seriously and has robust processes in place.
- In the course of auditing, we gather confidential information on companies and individuals which must be stored and processed with great diligence. This confidentiality has always been at the heart of good social compliance auditing. If any confidential interviews have been recorded, the copy of the recording will be transferred onto a hard drive and locked in a safe in our Head Office. Only Senior Management and Office Manager will have keys to the safe. This information will not be added to our cloud-based system, and it has to be removed from the auditors telephone or computer.
- All data we gather is stored in our cloud-based Optimus system housed in a typhoon- and earthquake-proof data centre. This data is protected by security that exceeds the Advanced Encryption Standard (AES). No stand- alone personal data is permitted to be kept on individual computers.
- Every access by any user is recorded by the system using IP addresses and date stamps. Master and Individual passwords are changed on a regular basis and must exceed 12 mixed and random characters.
- During the audit, data subjects are requested to give consent to the use of their data as part of their contractual commitment to the master client. Their data can only be viewed by the controller, the processor, the subject, and the master client.
- All data is collected and processed in a lawful, fair, and transparent manner.
- Verisio has appointed an Internal Data Protection Officer.
- Any data subject may have full view of all the data held on them by requesting a log-in to the Optimus system. Commonly any data will have already been shared in the form of a hard or soft-copy audit report.
- Data may be shared with law enforcement or intelligence where the standards of vital, public, and legitimate interests are met. This may apply in the case of vulnerable workers or children being under immediate threat.
- Verisio may contact companies with relevant information to any audit or services but will ask consent for any direct mailings.
- As part of the contractual arrangement within auditing, data must be kept for an indefinite period of time, as agreed between the master client and the data subject. However, if all parties are in agreement, data may be erased permanently from the system.

Introduction and background

Verisio is a **Data Controller** and consequently must process all **Personal Data** (including Special Categories of Personal Data) about Data Subjects in accordance with the General Data Protection Regulation (the "GDPR") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "**Data Protection Rules**"). For the avoidance of doubt, Verisio remains the sole Data Controller, even where processing is carried out by affiliated offices or sub-contractors.

Verisio will collect, store, use and otherwise process Personal Data about the companies and people with whom it interacts, who are the **Data Subjects**. This may include clients, workers, employees, contractors, suppliers and other third parties.

Verisio processes Personal Data so that it can comply with its statutory obligations and achieve its objective of advancing and maintaining the good corporate social compliance and the fight against Modern Slavery.

Every Data Subject has several rights in relation to how Verisio processes their Personal Data. Verisio is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieving and maintaining the trust and confidence of Data Subjects. Therefore, Verisio will regularly review its procedures, to ensure that they are adequate and up to date, not less than once a year.

Data protection principles

Verisio as the Data Controller is required to comply with the six data protection principles set out in the GDPR, which provide that Personal Data must be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
5. Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a way that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational security measures.

There is also an overarching principle: the Data Controller must be able to demonstrate compliance with the six principles. Accountability is vital.

The Data Protection Officer (DPO)

Senior Management has overall responsibility for compliance with the Data Protection Rules. However, **Data Protection Officer** (the **"DPO")** shall be responsible for ensuring day-to-day compliance with this Policy and the Data Protection Rules.
Senior Management will provide the DPO with sufficient resources and support to carry out his responsibilities. The DPO will perform and annual review (usually in December of all procedures) to ensure they are fit for purpose and the policy is being met.

The DPO is designated as the **Head of Training** - privacy@verisio.global

The General Manager, assisted by her team of Coordinators have overall responsibility for ensuring our compliance with Data Protection legislation within the company. She will ensure that:

- The Data Protection Policy is implemented and communicated effectively.
- A data protection culture of continuous improvement is created, and progress monitored
- Suitable and sufficient funds, people, materials, and equipment are provided to meet all data protection requirements.
- There is regular communication and consultation with employees and clients on data protection issues.
- Data protection incidents are recorded, investigated, and reported to the DPO.

This Policy applies to all Personal Data processed by the company in whatever format (e.g. paper, electronic, film) and regardless of how it is stored (e.g. electronically or in filing cabinets). It also includes information that is in paper form but is intended to be put into electronic form and to any recordings made such as telephone recordings and CCTV.

How we will comply?

This policy is intended to ensure that any processing of Personal Data is in accordance with the Data Protection Rules and the data protection principles. The company will therefore:

- Ensure that, when personal information is collected, the Data Subject is made aware of the Privacy Notice and informed of what data is being collected and for what legitimate purpose(s).
- Be transparent and fair in processing Personal Data.
- Take steps to ensure the accuracy of data at the point of collection and at regular intervals,

thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them.

- Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected.
- Share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures.
- Ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the European Economic Area (the "EEA").
- Ensure that data is processed in line with the Data Subject's rights, which include the right to:

  - request access to Personal Data held about them by the company.
  - have inaccurate Personal Data rectified.
  - have the processing of their Personal Data restricted in certain circumstances.
  - Have Personal Data erased in certain specified situations (in essence where the continued processing of it does not comply with the Data Protection Rules).
  - Prevent the processing of Personal Data for direct-marketing purposes.
  - Ask the company to prevent Processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual.
  - Prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on them.
  - Ensure that all employees are aware of and understand the company's data protection policies and procedures.
  - Adopt a Data Retention Policy which sets out the periods for which different categories of Personal Data will be kept.
  - Design projects, processes, and systems with privacy in mind at the outset

Through adherence to this Policy and related data protection policies, and through appropriate record-keeping, the company will seek to demonstrate compliance with each of the data protection principles.

Data Security & Responsibilities

The company must ensure that appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful processing or damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). In particular, wherever possible, all employees should endeavor to ensure that:

- The only individuals who have access to Personal Data and are able to process it are those who are authorised to do so.
- Personal Data is stored only on the **Optimus Compliance Management system** and not on individual PCs, portable electronic devices, or removable storage media, unless those devices have been encrypted.
- Passwords are kept confidential, are changed regularly, and are not shared between individuals. Passwords should be a minimum of 12 characters long, including capitals, numbers, and symbols.
- PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks.
- Offices, desks and filing cabinets/cupboards are kept locked if they contain Personal Data of any kind, whether in digital or electronic format or on paper.
- When destroying Personal Data, paper documents are securely shredded, and electronic data is securely deleted.
- Personal Data removed from an office is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public, using passwords/passcodes. Encrypting portable electronic devices and storing such devices securely (e.g. not left in the boot of a car overnight).

If any employee becomes aware that there has been a Data Breach, you must report this immediately to the DPO.

Privacy Notice & Consent Form

When any information is collected from an individual, they must be made aware of the prevailing approved **Privacy Notice**. The Privacy Notice provides information about what, why and how information is processed. All employees should make yourself aware of it.

The Consent Form, which is part of the Privacy Notice ensures that Data Subjects have clearly signed consent to the data being held on them as part of the auditing process.

When auditors visit a site to be audited, they may use Verisio's standard *F-ADMIN Privacy Notice & Consent Form* which must be signed by the parties whose data is being collected. When working on behalf of client's with their own documentation Verisio auditors will use whatever suitable Privacy Notice document has been provided as part of the scheme or client program.

Data Processors

The company may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g. a payroll provider, a third-party IT provider, delivery of mail shots). In such situations, the company will share necessary information with the Data Processor, but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

Personal Data will only be transferred to a third-party, a Data Processor, if the DPO is satisfied that the third party has in place adequate policies and procedures to ensure compliance with the Data Protection Rules. There should be a written contract in place between Verisio and the Data Processor as well, which

Third Party Requests

Verisio may from time to time receive requests from third parties for access to documents containing Personal Data. The company may disclose such documents to any third party where it is legally required or permitted to do so by law.

Such third parties may include the other audit organisations, health professionals, the Police and other law enforcement agencies, the GLAA, HMRC, the Security Services other regulators, immigration authorities, insurers, local authorities (e.g. Trading Standards) or Courts and Tribunals.
Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal operations must immediately contact the DPO.

Subject Access Requests (SARs)

Any Data Subject may exercise their rights as set out above (e.g. the right of access to the Personal Data which the company holds about them, or the right to have Personal Data erased). To be valid, a **Subject Access Request** must be made in writing and provide enough information to enable the company to identify the Data Subject and to comply with the request. This includes requests made via email or regular mail.

All Subject Access Requests will be dealt with by the DPO. Employees who receive a Subject Access Request must forward it to the DPO immediately in order that such requests can be replied to within the strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

The DPO will generally respond to the SAR by providing a log-in to the Data Subject to Optimus and they can view all data being kept there.

No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to provide additional copies of information previously provided. Where the company considers a request to be manifestly unfounded, excessive or repetitive, the company may lawfully refuse to respond and, if so, the DPO will inform the Data Subject of this in writing within the one-month period.

Direct Marketing

Any use of Personal Data for marketing or mail-shot purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (the **"PECR"**) (and any replacement legislation) which relate to marketing by electronic means.

Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or mail- shot communications will be sent to them. The PECR requires that Verisio has the prior consent of recipients in certain circumstances before it sends any unsolicited electronic messages for the purpose of marketing activities (e.g. updates on services and legislation).

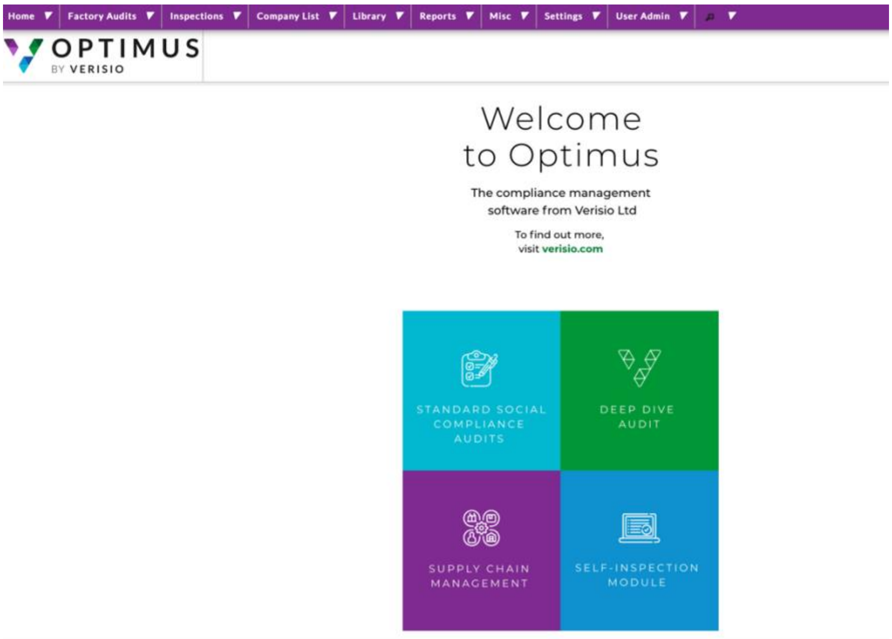
Any use of Personal Data for direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the DPO.

Optimus Compliance Management System

Optimus is a **cloud-based business management system designed in-house to control the entire process of running the company and delivering our services**. It comprises a Client Relationship Module (CRM), scheduling, invoicing and planning functionality as well as a module (**Gladius**) that allows Verisio to create client specific audit reports or Self- Assessment Questionnaires with appropriate Corrective Action Plan Reports (CAPR).

Optimus is a third-generation software tool designed for the auditing and quality control industry, written mainly in **Ruby on Rails 4.1**. Ruby is a server-side web application framework. Rails is a model-view-controller (MVC) framework, providing default structures for a database, a web service and web pages.

All the data is stored in a typhoon and earthquake proof data centre and is back up in real time continuously. This data is protected by security that exceeds the Advanced Encryption Standard (AES). Back-up and security protocols are based on those used in the banking industry. In the event of any data breach by unauthorised parties (hackers) the system would immediately respond. All activity from users is logged and can be traced by to IP addresses.



Data Retention

As part of the contractual arrangement within auditing, data must be kept for **an indefinite period of time**, as agreed between the master client and the data subject.

However, if all parties agree, data may be erased permanently from the system. This can be done within Optimus.

Data may not be erased permanently if there are legal proceedings going on.
As a matter of good housekeeping Verisio will review all data **relating to audits older than 5 years** and if considered obsolete by all parties who have an interest in this data then it can be erased permanently to free up electronic storage space.

Annual Review

This policy will be reviewed at least **every 12 months around December**, in accordance with the company's programme of document review and updates but may be subject to change at any time.

Any updates and changes will be noted in the Version Control table at the end of this document.

DOCUMENTS REFERENCED IN THIS PROCEDURE:

- *VQM-002 Verisio Org Chart*
- *VQM-003 Job Descriptions*

REVISION HISTORY

Version	Brief details of Revision	Revised by	Date
180525-4	New branding	Krisztina Shutt	23 Aug 2021