VerseOne Group (“VerseOne”) Data Protection Policy

Table of Contents

1. About this document

This Data Protection Policy lays out how VerseOne complies with the principles of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) so that we as a company address data protection in a consistent and demonstrably accountable manner.

This policy sets out our approach to data protection, as well as the responsibilities for implementing the policy and monitoring compliance with it. It details the policy framework and information governance strategy in place at VerseOne Group to support a positive data protection and security culture.

This policy has been approved by the management of VerseOne Group and published and communicated to all staff. The policy is reviewed and updated annually or when needed to ensure continuing relevance to legislation and regulation.

2. Data Protection Officer (DPO) and management responsibility

VerseOne has a nominated Data Protection Officer (DPO) who is responsible for data protection compliance. The DPO is a member of the board of directors, ensuring the highest levels of accountability within our organisation and on-going resourcing sufficient to meet our data protection obligations.

In general, the DPO's responsibilities are as follows:

- inform and advise the company and its employees about its data protection obligations;
- monitor the company's compliance with data protection laws and regulations, including data management activities, documentation, and training;
- act as the first point of contact for supervisory authorities and individuals whose data is processed or held by the company;
- regularly update the Board about matters arising from and relating to data protection compliance.

VerseOne's board and management, who are collectively responsible for the company's activities and decision-making, are fully aware of the obligations of the company and its staff under current data protection legislation and regulation. The board and management are dedicated to leadership by example, demonstrating accountability for compliance with data protection principles and promoting a positive internal culture around data protection. The board and management take the lead when assessing data processing activities and at all times encourage and promote a "privacy and data protection by design" approach to working. Together with the DPO, the board and management work to drive awareness amongst all staff and stakeholders of the importance of good data protection practices.

VerseOne is registered with the Information Commissioner's Office under the Data Protection Act. Our registration number is Z2003770.

3. Privacy and data protection by design

VerseOne recognises the company's obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our data processing activities. Privacy and data protection are built into all of VerseOne's activities by design and by default, helping us to comply at all times with data protection principles. Data protection is built in to every documented corporate process and procedure, typically as part of our ISO 9001 and ISO 27001 documentation, and regularly assessed both internally and externally for compliance.

VerseOne as a company continually looks to minimise the amount and type of data we collect, process, and store, and undertakes regular data audits across appropriate areas of the business. Where appropriate, personally identifiable information fields within a data record are replaced by one or more artificial identifiers or pseudonyms to render our records less identifying and thereby reduce risk around data sharing and data retention. We regularly undertake reviews of all of our public-facing documents, policies, and privacy notices to ensure they meet the renewed transparency requirements under GDPR. On an on-going basis, we work to review and improve our data security procedures, tools, and controls, and we ensure any new business activities are undertaken in compliance with GDPR and individuals' rights therein.

4. Data protection training for all staff

VerseOne trains all staff about their data protection responsibilities. While not all staff handle sensitive data, every member of staff is briefed and educated as part of our overall commitment to good data protection and records management practice.

Data protection training is provided as part of the on-boarding process of every new staff member, and is given regularly to all staff as a group or as teams or functions to ensure that learning is targeted at the specific data-handling responsibilities of different job roles. This includes training on records management policy and responding to individuals' and Data Controllers' requests for data updating, erasure, and provision under subject access requests.

Data protection principles and updates are covered regularly in team and company meetings and points or articles of interest regularly shared through VerseOne's internal communications channels.

5. VerseOne Group as Data Processor

VerseOne Group (VerseOne) stands as a Data Processor in relation to the personal identifiable information (PII) of VerseOne clients' staff, customers, and service users.

We hold that it is the responsibility of the Data Controller to ensure that data they control has appropriate risk management and impact assessment measures and procedures in place, even where these interact with products and services supplied by VerseOne. VerseOne works closely with all Data Controllers to ensure any information risks identified are fed back on a regular basis, and as part of our project initiation procedures, we provide guidance for data and risk management and privacy impact assessments as they relate to VerseOne projects, where the circumstances indicate these should be undertaken.

As part of our relationship as a Data Processor, the Customer Solutions Director and Chief Technical Officer have responsibility for managing information risks, coordinating procedures to mitigate risk, and for logging and risk assessing information assets. Where VerseOne identifies non-tolerated information risks, we take appropriate mitigating action ourselves or agree an action plan with the affected Data Controller, as outlined in our Critical Issue Process (available upon request).

VerseOne's contractual obligations arising from the General Data Protection Regulation are laid out in the Master Customer Solutions Agreement (VO-ISO-MCSA) clauses 15.1-3 and the Master Product Licence and Maintenance Agreement (VO-ISO-PLMA) clauses 3.10-12. Data Controllers should ensure they have a copy of their agreements with VerseOne when assessing compliance with data protection regulations.

5.1. Information flow

VerseOne has conducted an audit to map the data that we process and how it flows into, through, and out of our business. This information flow includes notes of any transfers of information from one location to another, including between VerseOne and its suppliers.

Personal data of clients' staff, customers, and service users may be entered into the VerseOne software solution or collected during the course of interacting with VerseOne in the following forms.

Staff members nominated as procurement or project team members for purposes of communication with VerseOne:

This information is usually provided to VerseOne as part of the procurement and project delivery process for the purposes of contact information and as records, minutes, and notes relating to the project itself. This information is stored indefinitely for legitimate purposes relating to account continuity and financial audits. VerseOne holds this information in the following locations:

- Hard copy of organisation's customer file, maintained in lockable secure filing areas.
- Soft copy of organisation's customer file, maintained in VerseOne's hosted customer relationship management and finance software.
- Soft copy of organisation's project records maintained in VerseOne's hosted project management software and locally-hosted file storage area;
- VerseOne staff email archives.

Staff members nominated as users of the VerseOne software:

This information is usually provided to VerseOne as part of the project delivery process in the training stages, as well as input into the VerseOne software directly by authorised representatives of the organisation. Staff information may also be included in the solution for Single Sign-On (SSO) and contact directory purposes. This information is stored in the software database and can be accessed by:

- Any other user of the VerseOne software who has the requisite in-system privileges to manage user accounts;
- VerseOne staff providing solution support per their official job description.

The Data Controller is responsible for management and deletion of this data from the software solution, with the assistance of VerseOne where any system-based impediments to deletion may occur. Any data deleted from the VerseOne software is immediately irretrievable by the software users, and after the expiry of the most recent backup of the software solution (which is dependent on the hosting location of the solution).

The organisation's customers and/or service users who are invited to become users of the VerseOne software:

This information is usually provided to VerseOne as part of the project delivery process, as well as input into the VerseOne software directly or through secure data transfer methods by authorised representatives of the organisation. Some data transfer methods (e.g. some application programming interfaces (APIs)) may bypass the VerseOne software database to deliver information on-screen, and where this is the case some of the points below may not apply. This information is stored in the software database, and

may be stored in an associated secure file storage area such as FTPS/SFTP, and can be accessed by:

- Any other user of the VerseOne software who has the requisite in-system privileges to manage user accounts;
- VerseOne staff providing solution support per their official job description.

The Data Controller is responsible for management and deletion of this data from the software solution and any associated secure file storage area, with the assistance of VerseOne where any system-based impediments to deletion may occur. Any data deleted from the VerseOne software is immediately irretrievable by the software users, and after the expiry of the most recent backup of the software solution (which is dependent on the hosting location of the solution).

Members of the public who are invited to become users of the VerseOne software.

This information is usually provided directly by the member of the public via voluntary registration for access to a private area of the VerseOne solution or completion of an online form. This information is stored in the software database and can be accessed by:

- Any other user of the VerseOne software who has the requisite in-system privileges to manage user accounts;
- VerseOne staff providing solution support per their official job description.

The Data Controller is responsible for management and deletion of this data from the software solution, with the assistance of VerseOne where any system-based impediments to deletion may occur. Any data deleted from the

VerseOne software is immediately irretrievable by the software users, and after the expiry of the most recent backup of the software solution (which is dependent on the hosting location of the solution).

Third-party software systems or hosting environments used by VerseOne where PII may be stored or referenced are covered by our suppliers' policies standing in relation to our company as Data Processors. No information that VerseOne holds in these systems is or should be accessed by these third-party suppliers. VerseOne never provides PII to third parties for their own use of any kind.

In accordance with VerseOne's size, we maintain an Information Asset Register documenting what types of personal data we hold, where it came from, and what we do with it. Any processing activities we do that are out of the ordinary course of business activities, or that are likely to result in a high risk to the rights and freedoms of natural persons, are recorded in specific Data Protection Impact Assessments (DPIAs).

5.2. Sub-processors

VerseOne will only engage a sub-processor where the project indicates it is necessary, and then only with the specific authorisation of the Data Controller. Sub-processors will be engaged under a written Contract which outlines the data protection arrangements and expectations the sub-processor must have in place.

VerseOne will ensure that any data is shared securely with the sub-processor and that we obtain the relevant assurances that the sub-processor has implemented appropriate technical and organisational measures to ensure the security of the personal data they are processing on our behalf. If there are to be any changes in the written Agreement, VerseOne will undertake to seek additional authorisation from the Data Controller before any changes are made.

5.3. Operational base

VerseOne does not currently operate outside of the European Union. VerseOne's named Data Protection Officer operates inside of the European Union. We ensure robust levels of protection are in place relating to personal data that may be entered into software systems in use within the company which are hosted outside of the European Union (for example in support tickets or project management software), e.g. through ensuring that the relevant suppliers are registered with Privacy Shield[1], the US-EU-Swiss mutual recognition framework for data protection.

[1] https://www.privacyshield.gov

5.4 Breach notification

VerseOne recognises its duty to inform Data Controllers of any personal data breach without undue delay after becoming aware of it, and accordingly has internal and external breach identification and reporting procedures in place, as found in our Critical Issue Process (available upon request).

Staff are trained in recognising a personal data breach and the company has procedures in place to ensure that we can assist Data Controllers in their responsibilities to act when a data breach occurs.

The Customer Solutions Director and Chief Technical Officer are responsible for monitoring the type, volume, and cost of incidents to identify trends and help prevent recurrences.

5.5 Right of access and right to rectification and data quality

VerseOne has a documented procedure in place to respond to Data Controllers' request for information or the updating of information following an individual's request to access their personal data. The Customer Solutions Director and Chief Technical Officer are responsible for ensuring VerseOne deals with these types of requests in a timely manner and that requested information is provided in commonly used and accessible formats.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

5.6 Right to erasure, including retention and disposal

VerseOne has written documentation in place covering erasure, data retention, and data disposal to ensure we know when to dispose of various categories of data in a planned and secure manner.

This information is held in the Information Asset Register (VO-GDPR-REG) and can be provided upon request.

VerseOne recognises that individuals have the right to be forgotten. This includes that VerseOne as Data Processor erases their data when it is no longer necessary, the individual objects to the processing or withdraws consent, it was unlawfully obtained or must be erased to comply with a legal obligation, or is in relation to a child.

Where the request for erasure relates to a VerseOne customer's member of staff whose information is held in conjunction with contractual or financial documentation, VerseOne claims an overriding lawful basis in retaining this data in order to comply with contractual and legal obligations.

5.7 Right to restrict processing

VerseOne has documented procedures for responding to a Data Controller's request to suppress the processing of specific personal data.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

5.8 Right of data portability

VerseOne recognises the right of individuals to obtain and reuse their personal data for their own purposes across different services. VerseOne has a documented procedure in place to respond to Data Controllers' request for information or the updating of information following an individual's request to access their personal data. The Customer Solutions Director and Chief Technical Officer are responsible for ensuring VerseOne deals with these types of requests in a timely manner and that requested information is provided in commonly used and accessible formats.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

5.9 Information security

VerseOne recognises the risks involved in processing personal data within its information technology systems and takes appropriate technical measures to secure this data. This includes, but is not limited to, consideration for the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Our Information Security policy (confidential) details our approach to information security as well as the technical and organisational measures we implement and the roles and responsibilities staff have in relation to keeping information secure. Our information security processes and procedures are documented as part of our work to achieve ISO 27001 certification.

VerseOne's Information Security policy sets out the standards for network and physical security, access controls, secure configuration, patch management, internet use, data storage and maintenance, and incident management within the company. The company institutes regular checks of compliance with the policy to give assurances that security controls are operational and effective, and carries out regular staff training on all areas detailed within the policy.

6. VerseOne as Data Controller

VerseOne stands as a Data Controller in relation to the personal identifiable information (PII) of VerseOne clients, staff, suppliers, and stakeholders.

Where VerseOne uses a Data Processor, the relationship is governed by a written Contract outlining both parties' responsibilities and liabilities. VerseOne recognises its liability for Data Processors' compliance with data protection regulations and only appoints Data Processors who can provide sufficient guarantees that all regulatory requirements will be met and the rights of individuals protected. Data Processors only act on documented instructions provided by VerseOne, except where compliance is required by a higher authority. VerseOne maintains a Data Sharing Log as part of the Information Asset Register (VO-GDPR-REG) recording what data has been shared, the purpose of sharing, whom the data has been shared with, and for how long and under what restrictions or rules. This log is reviewed on a regular basis to ensure well-founded and compliant decision-making.

6.1. Information flow

As Data Controller, VerseOne regularly conducts information audits across our business in order to identify the data that we hold and use and how it flows through the business. We recognise our responsibility to comply with accountability principles in the General Data Protection Regulation, which require the company to show how we comply with its requirements.

Information flow is documented in our Information Asset Register (VO-GDPR-REG), which details:

- The nature of the information;
- The purpose of holding and/or processing the information;
- The location where the information is held;
- The area of the business responsible for the integrity of the information;
- The approximate volume of information records of each asset type;
- Whether or not the information is shared outside of the company and with whom;
- The format in which the information is held;
- The retention period for the asset type;
- Any backup regimes in place for the asset type;
- The method of disposal for the asset type;
- The risks and impact associated with holding or using the information.

Summaries of this information can be made available upon request.

Any processing activities we do that are out of the ordinary course of business activities, or that are likely to result in a high risk to the rights and freedoms of natural persons, are recorded in specific Data Protection Impact Assessments (DPIAs).

6.2. Lawful bases and consent

VerseOne regularly reviews the purposes of our data processing activities to ensure the most appropriate lawful basis for each activity. The company assesses whether the processing is necessary for the relevant purpose, and that we are satisfied that there is no other reasonable way to achieve that purpose. The lawful basis for processing each information asset type is recorded in the Information Asset Register (VO-GDPR-REG).

Most of the data VerseOne holds and uses is held under the following lawful bases:

- **Contract**—Necessary as part of contractual obligations the company has entered into, or plans to enter into (such as quote provision, contracts and order forms, project documentation, and support requests);
- **Legal obligation**—Necessary in order to comply with common law and/or statutory obligations (such as VAT inspections and other government revenue audits);
- **Legitimate interests**—Necessary as part of a wider legitimate interest for the business where processing cannot be separated from the business activity and constitutes minimal risk for the individual's interests (such as holding IP addresses of devices accessing our web servers as part of our log file analysis and audits).

Where information is requested by the company for reasons other than the lawful bases listed above, separate consent requests requiring a positive opt-in are in use, offering specific options and levels of consent, details of how the data will be used, and how to withdraw consent at any point.

As part of its on-going relationship with individuals, VerseOne continually reviews consent provided and seeks it afresh if intending to hold or use data in a way different from that originally consented to.

VerseOne does not offer any services to, or intentionally collect or process any data from, persons under the age of 18. We may hold IP addresses of website visitors under the age of 18 who visit the websites of VerseOne or our clients, but these are never identified or used for identifying purposes.

6.3 Data Protection Impact Assessments (DPIA)

VerseOne recognises that effective Data Protection Impact Assessments allow us to identify and fix potential problems at an early stage, reducing risks, costs, and damage to the business and to individuals whose data we process. VerseOne carries out DPIAs where indicated in the regulation according to the following framework:

- describing the processing operations and purposes for the data collection and usage, as well as any relevant legitimate interests;
- assessing the necessity and proportionality of the processing in relation to the purpose;
- assessing the risks to individuals;
- plans for controlling risks, particularly around information security;
- consultation with the DPO, processors, contractors, stakeholders, and other groups of affected persons.

6.4 Right to be informed

VerseOne provides individuals with the following privacy information when requesting or collecting personal data:

- Details about VerseOne Group, including our DPO;
- The purpose and lawful basis for processing data requested and source of it (where obtained externally);
- The categories of personal data requested;
- Details of all recipients of the data, including any third parties or locations outside of the European Union;
- Retention periods of the personal data requested;
- The rights available to individuals providing the personal data and how to exercise these;
- Any statutory or contractual obligations relating to providing the data;
- Any automated decision-making, including profiling.

This information is provided at the time that personal data is requested or collected in a concise, transparent, intelligible, accessible, and clear way.

We regularly review and update our privacy notices and information.

6.5 Right of access and right to rectification and data quality

VerseOne has a documented procedure in place to respond to individuals' request for information or the updating of information. The Customer Solutions Director and Chief Technical Officer are responsible for ensuring VerseOne deals with these types of requests in a timely manner and that requested information is provided in commonly used and accessible formats.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

A Records Management policy (VO-GDPR-RMP) is in place to ensure regular review of the information VerseOne processes and stores, as well as detailing rules for creating and keeping information records. The policy also provides for regular data quality checks to provide assurances about the accuracy of the data input and maintained by members of VerseOne staff.

6.6 Right to erasure, including retention and disposal

VerseOne has written documentation covering erasure, data retention, and data disposal to ensure we know when to dispose of various categories of data and help plan for its secure disposal.

This information is held in the Information Asset Register (VO-GDPR-REG) and can be provided upon request.

VerseOne recognises that individuals have the right to be forgotten, and this includes that VerseOne as Data Controller erase their data when it is no longer necessary, the individual objects to the processing or withdraws consent, it was unlawfully obtained or must be erased to comply with a legal obligation, or is in relation to a child.

VerseOne recognises its responsibility to ensure the erasure request has been complied with where any Data Processors have been shared the information in question.

6.7 Right to restrict processing

VerseOne has documented procedures for responding to individuals' request to suppress the processing of specific personal data.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

6.8 Right of data portability

VerseOne recognises the right of individuals to obtain and reuse their personal data for their own purposes across different services. VerseOne has a documented procedure in place to respond to individuals' request for information or the updating of information. The Customer Solutions Director and Chief Technical Officer are responsible for ensuring VerseOne deals with these types of requests in a timely manner and that requested information is provided in commonly used and accessible formats.

A copy of this procedure is available upon general request and is provided to any data owner making a request of this nature.

6.9 Right to object

VerseOne recognises that individuals have the right to object to the processing of their personal data based on their situation with regard to the criteria laid out in the General Data Protection Regulation. VerseOne's privacy notices inform individuals of their right to object, and where possible VerseOne has systems in place to allow individuals to discontinue our processing of their data without making a formal request.

The Customer Solutions Director and Chief Technical Officer are responsible for ensuring that where an individual objects to the processing of their data and it meets the criteria above, that processing is stopped immediately.

6.10 Rights related to automated decision-making including profiling

VerseOne does not undertake any processing operations that constitute automated decision-making as defined by the General Data Protection Regulation.

6.11 Information security

VerseOne recognises the risks involved in processing personal data within our information technology systems and takes appropriate technical measures to secure this data. This includes, but is not limited to, consideration for the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Our Information Security policy (confidential) details the approach taken to information security as well as the technical and organisational measures we implement and the roles and responsibilities staff have in relation to keeping information secure. Our information security processes and procedures are documented as part of our work to achieve ISO 27001 certification.

VerseOne's Information Security policy sets out the standards for network and physical security, access controls, secure configuration, patch management, internet use, data storage and maintenance, and incident management within the company. The company institutes regular checks of compliance with the policy to give assurances that security controls are operational and effective, and carries out regular staff training on all areas detailed within the policy.

6.12 Breach notification

VerseOne recognises its duty to inform the individual and the Information Commissioner's Office (ICO) of any personal data breach likely to result in a high risk to the rights and freedoms of individuals without undue delay after becoming aware of it, or within 72 hours in the case of the ICO. Accordingly, the company has internal and external breach identification and reporting procedures in place, as found in our Critical Issue Process (available upon request).

Staff are trained in recognising a personal data breach and the company has procedures in place to ensure robust breach detection, investigation, and reporting.

The Customer Solutions Director and Chief Technical Officer are responsible for monitoring the type, volume, and cost of incidents to identify trends and help prevent recurrences. Any relevant findings are promptly reported to the Board.