23. Data Protection, Retention And Destruction

Reviewed By: Melissa Munnich

Review Date: 30th October 2024

23.1 Introduction

Woodhurst Consulting Limited ("Woodhurst") is committed to protecting the confidentiality, integrity, and accessibility of our customers', suppliers', partners', and employees' data, including personal data. This policy outlines Woodhurst's approach to data protection and compliance with applicable data protection legislation, including the General Data Protection Regulation (GDPR), the UK Data Protection Act 2018, and anticipated UK Data Protection Reform.

Woodhurst operates as a data controller and data processor for specific data processing activities, described in this policy. To ensure data protection practices align with applicable regulations, **Woodhurst has appointed its Head of Operations, Alex Bywater (alex.bywater@woodhurst.com), as both the Data Protection Officer (DPO) and Information Security Officer (ISO).** Alex Bywater is responsible for overseeing data protection compliance and information security within the organisation.

23.2 Definitions within Policy

Client Engagement: An engagement entered into by Woodhurst and a customer with a signed contract.

Contract: The contract between Woodhurst and the Customer comprising a series of terms and conditions.

Customer: The organisation purchasing services from Woodhurst.

Order: The customer's order for services, comprising a signed acceptance of Woodhurst's proposal.

Proposal: The description or specification of the Services provided by Woodhurst to the customer.

Services: The services, including the deliverables, supplied by Woodhurst to the Customer as set out in the proposal.

23.3 Data Protection Roles

23.3.1 Data Protection Officer (DPO) and Information Security Officer (ISO)

The Head of Operations, Alex Bywater (alex.bywater@woodhurst.com), has been appointed as the Data Protection Officer (DPO) and Information Security Officer (ISO) for Woodhurst. Alex Bywater is responsible for overseeing Woodhurst's data protection strategy, information security measures, and ensuring compliance with data protection legislation. As the DPO and ISO, Alex is also the primary point of contact for regulatory authorities and data subjects with enquiries regarding data protection practices.

23.3.2 Data Controller

When Woodhurst determines the purposes and means of processing personal data, it acts as a data controller. This includes activities related to customer and supplier relationship management, marketing, event administration, and employee data management.

23.3.3 Data Processor

For personal data processed in connection with consulting services provided to customers, Woodhurst acts as a data processor, following customer instructions and the terms of a data processing agreement.

23.4 Data Processing Activities

You can read more on the categories of personal data that we process for which purposes and on which legal grounds in the table below:

Data Controller	Purpose	Data Subjects	Category of Personal Data	Legal Basis	Source	Retention Period	Disclosure to Third Parties
The company which has entered into a contract or an engagement letter with the client.	Management of customer relations, including financial and contract administration.	Clients and customers, including their employees.	Non- sensitive personal data, i.e. name, position, contact details.	Processing of personal data is necessary for the performance of contracts with the customer, cf. GDPR, Article 6(1)(b). Processing is also necessary in order for Woodhurst to pursue its legitimate interests in being able to manage contracts, invoice and evaluate the customer relationship, manage and maintain IT systems, administer and manage our website, systems and applications, statistics and business development, cf. GDPR, Article 6(1)(f).	The data subjects.	Five years after the latest project for the customer has been completed.	Personal data may also de disclosed to subcontracto who are directly involved in th project for the customer.
Woodhurst Consulting Limited (Company No.: 11803336)	Marketing activities, including customer relationship management (CRM) system.	Customers and potential customer, including their employees	Non- sensitive personal data, i.e. name, position, contact details.	Processing is necessary in order for Woodhurst to pursue its legitimate interests in being able to manage and strengthen customer relations, developing our business and services (e.g. identifying customer needs and	Customers including customers' employees and public sources such as linkedin.com	As long as data is relevant to Woodhurst from a commercial perspective or until the data subject requests a deletion of the data.	Data will not b disclosed to third parties.

				improvements in service delivery) cf. GDPR, Article 6(1)(f).			
The company which has entered into a contract with the supplier or business partner.	Management of suppliers and business partners.	Suppliers and business partners, including their employees.	Non- sensitive personal data, i.e. name, position, contact details.	Processing of personal data is necessary for the performance of contracts with the supplier, or business partner, cf. GDPR, Article 6(1)(b). Processing is also necessary in order for Woodhurst to pursue its legitimate interests in being able to evaluate the business relationship, cf. GDPR, Article 6(1)(f).	The data subjects	As long as data are relevant to Woodhurst from a commercial perspective or until the data subjects requests deletion of the data.	Data may als de disclosed subcontracto who are directly involved in th project for the customer.
The company which organises the event.	Administration of events.	Participants in events.	Non- sensitive personal data, i.e. name, position, contact details	Processing of personal data is necessary for the performance of contracts with participants, cf. GDPR, Article 6(1)(b). Processing is also necessary in order for Woodhurst to pursue its legitimate interests in being able to evaluate event, cf. GDPR, Article 6(1)(f).	The data subjects	As long as data are relevant to Woodhurst from a commercial perspective or until the data subjects requests deletion of the data.	Data may als de disclosed subcontracto who are directly involved in th event.
The company to which the data subject has consented to receiving newsletters from.	Administration of newsletters.	Subscribers to newsletters.	Non- sensitive personal data, i.e. name, position, contact details.	Processing of personal data is necessary for the performance of contracts with participants, cf. GDPR, Article	The data subjects	Until the data subjects terminate the subscription.	Data will not b disclosed to third parties.

				6(1)(b). Processing is also necessary in order for Woodhurst to pursue its legitimate interests in being able to send the newsletter to the subscriber, cf. GDPR, Article 6(1)(f).			

23.5 Data Protection for Client Engagements

Both parties will (and will procure that any of their respective directors, officers, employees, permitted agents, licensees and contractors will) comply with all applicable requirements of the Data Protection Legislation. These Terms are in addition to, and do not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

In respect of Personal Data, the Customer is the controller and Woodhurst is a processor acting on behalf of the Customer. The processing of Personal Data by Woodhurst permitted under these

Terms shall be as follows:

- Duration: the duration of the Contract;
- Subject matter and purpose: the provision of the Services;
- Nature: as set out in the Order; and
- Types of personal data and categories of data subject: as set out in the Order

The Customer shall:

- Ensure that it has in place all necessary appropriate legal bases, consents (if required), notices and policies to enable the lawful transfer of Personal Data to Woodhurst
- Not instruct Woodhurst to undertake any processing activity that does not comply with, or which would result in either party breaching its obligations under, the Data Protection Legislation;
- Ensure that all Personal Data transferred to Woodhurst by or on behalf of the Customer shall be accurate and up-to-date;
- Not knowingly or negligently do or omit to do anything which places Woodhurst in breach of its obligations under the Data Protection Legislation.

Woodhurst shall:

- Process Personal Data only on the written instructions of the Customer save where otherwise required by law (in which case Woodhurst will notify the Customer of such requirement prior to such processing, unless prohibited from doing so by such law).
- Transfer Personal Data outside the EEA only where the European Commission has adopted a decision that the recipient country ensures an adequate level of protection, where Woodhurst provides appropriate safeguards and ensures the availability for data subjects of enforceable data subject rights and effective legal remedies (in accordance with the requirements of the Data Protection Legislation) or otherwise where the transfer is permitted under the Data Protection Legislation (including where the transfer falls within the specific derogations set out in Article 49 GDPR).
- Obtain a commitment of confidentiality from any person it allows to process Personal Data. and engage third parties to process Personal Data on its behalf only with contractual terms no less restrictive than described in this policy.

- Implement appropriate technical and organisational measures to (a) ensure an appropriate level of security of Personal Data; and (b) assist the Customer to respond to requests for exercising data subjects' rights.
- Assist the Customer to comply with its obligations in respect of any Personal Data breach (including notification of the same to the supervisory authority and/or data subjects).
- Make available to the Customer all information reasonably necessary to demonstrate compliance with data protection, retention and destruction.

On termination or expiry of the Contract (however caused), at the Customer's choice and cost, delete or return to the Customer all Personal Data and copies thereof that it has within its power, ownership or control.

Each party shall indemnify the other party (to the fullest extent permitted by law) against any claim, loss, damage, expense or fine incurred by the other party arising under or in connection with the Data Protection Legislation and caused by any action or omission of the first party (or its directors, officers, employees, permitted agents, licensees and contractors) unless such action or omission is specifically requested by the other party.

23.6 Automated Decision-Making and Profiling

In line with GDPR Article 22 and in preparation for the EU Digital Services Act and UK Data Protection Reform, Woodhurst does not currently utilise automated decision-making processes or profiling that significantly affects individuals. Should automated decision-making become relevant, Woodhurst will ensure that data subjects are informed of the logic involved, as well as the significance and consequences of such processing.

23.7 Data Breach Management

In the event of a data breach, Woodhurst will:

1. Detect and Report: Employees are required to report breaches immediately to the DPO, ideally within 24 hours of detection.
2. Contain and Recover: The DPO leads containment efforts, which may include IT support, credential resets, or external expertise.
3. Risk Assessment: The DPO evaluates potential risks and impacts on data subjects.
4. Notify: Regulatory authorities and data subjects will be notified where required within the legally mandated 72-hour timeframe.
5. Investigate and Document: All breaches are documented, with corrective actions noted.
6. Record-Keeping of Breaches: Woodhurst maintains comprehensive records of all data breaches, including minor incidents, as required by the EU Digital Services Act for ensuring transparency and risk mitigation.

23.8 Data Disposal

Upon expiry of the data retention period or when a data subject requests erasure, data will be securely deleted:

- Electronic Data: Deleted securely using relevant electronic deletion methods.
- Hardcopy Data: Shredded securely.
- Data Disposal Audits: Periodic audits will verify that data disposal aligns with legal and policy requirements.

23.9 Data Retention

As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed).

When establishing and/or reviewing retention periods, the following shall be taken into account:

The objectives and requirements of the Company.

The type of personal data in question.

The purpose(s) for which the data in question is collected, held, and processed.

The Company's legal basis for collecting, holding, and processing that data.

The category or categories of data subject to whom the data relates.

Professional Indemnity Insurance; Ability to carry out consultancy services; HMRC.

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

23.9.1 Vulnerability Remediation Timelines

Woodhurst maintains a documented process for identifying, assessing, and remediating vulnerabilities across its systems and infrastructure. Vulnerability scans are conducted periodically, and results are risk-ranked using industry-standard criteria. The remediation timelines are as follows:

- **Critical vulnerabilities** are addressed within **48 hours** of identification.
- **High-risk vulnerabilities** are remediated within **5 business days**.
- **Medium-risk vulnerabilities** are resolved within **15 business days**.
- **Low-risk vulnerabilities** are addressed as part of scheduled maintenance within **30 business days** or as otherwise prioritised.

Exceptions to these timelines must be formally documented and approved by the Information Security Officer, with justification and an interim risk mitigation plan where required

23.10 Subject Access and Data Subject Rights

Woodhurst respects the following rights of data subjects under GDPR:

- **Right to Access**: Data subjects may request access to their personal data.
- **Right to Rectification**: Data subjects can correct inaccuracies in their data.
- **Right to Erasure**: Data subjects may request deletion where data is no longer needed.
- **Right to Restrict Processing, Portability, and Object**: Data subjects have the right to restrict, transfer, or object to processing under GDPR.

23.11 Data Protection by Design and Default

Woodhurst incorporates data protection into the initial stages of project development, ensuring compliance by implementing data minimisation, pseudonymisation, and secure storage practices.

23.11.1 Data Protection Impact Assessments (DPIAs)

For high-risk processing activities, **Data Protection Impact Assessments (DPIAs)** will be conducted, documented, and reviewed to evaluate and mitigate risks to data subjects, as mandated by GDPR and the anticipated **UK Data Protection Reform**.

23.12 Record of Processing Activities (ROPA)

Woodhurst maintains a **Record of Processing Activities (ROPA)**, documenting categories of personal data processed, purposes, retention periods, and security measures. This aligns with GDPR Article 30 requirements and future obligations under the **EU Digital Services Act**.

23.13 Use of Internet of Things (IoT) Devices

Woodhurst does not store or process client data using Internet of Things (IoT) devices. As IoT technology does not form part of our operational or technical architecture, baseline IoT security documentation is not applicable. Should any future business activities involve IoT components, appropriate security controls will be developed and implemented in alignment with recognised UK information security standards.

23.14 Threat Intelligence and Monitoring

Woodhurst leverages reputable sources of cyber threat intelligence, including alerts and advisories issued by the UK National Cyber Security Centre (NCSC) and Microsoft Defender for Endpoint, to ensure our information security posture is regularly updated in line with evolving threats. These sources inform both strategic policy decisions and tactical defensive measures.

Regular management information reports on key cyber risks, system alerts, and patching status are reviewed by the Chief Operating Officer and Information Security Officer on at least a quarterly basis.

23.15 Training and Compliance

Woodhurst conducts annual data protection training to maintain awareness and compliance with data protection laws across the organisation. Training programmes are reviewed and updated regularly to incorporate changes under the **UK Data Protection Reform**. All employees receive mandatory cyber security training that includes specific modules on phishing, social engineering, and safe digital behaviours. All phishing attempts are reported publicly to the Woodhurst team as part of our internal process to improve vigilance and awareness.

23.16 Device Access and Remote Security Controls

Woodhurst only issues company-managed laptops for all work-related activities. These devices are enrolled in Microsoft Intune and governed by corporate security policies that enforce disk encryption, endpoint protection, and secure authentication.

MFA, conditional access, and device compliance checks are standard across all access points. While we do not monitor the real-time geographic location of devices, Microsoft Defender alerts us to suspicious login behaviour, including anomalous access attempts.

Local and personal printer connections are disabled by default to reduce the risk of unauthorised data exposure.

23.17 Asset Management

Woodhurst maintains a centralised asset register that records all company-issued laptops and related hardware. Devices are tracked through endpoint management tooling, and all client data access occurs only on approved and monitored devices.

Off-site use of devices is governed by strict access controls and audit logging to ensure traceability and data protection.

23.18 Cyber Audit and Assurance

Cyber security policies and practices are reviewed regularly by senior management and the Information Security Officer. Microsoft 365 and Defender tools provide audit logging, behavioural monitoring, and actionable alerts.

Audit results and control checks are reviewed internally, with documented remediation plans implemented for any identified risks. Relevant documentation and summary reports can be provided to clients upon request to support due diligence

reviews.

23.19 Review and Updates

This policy will be reviewed annually or upon significant legal or regulatory changes to ensure compliance with **GDPR**, **anticipated UK Data Protection Reform**, and **EU Digital Services Act** obligations.