Angling Trust/Fish Legal

PD16a – Data Privacy Policy (for Internal Employees)

CONTENTS

1. INTRODUCTION

Angling Trust and Fish Legal are committed to safeguarding the privacy and security of all personal, sensitive, and confidential data. This Privacy Policy provides internal employees, contractors, and volunteers with high-level guidance on their responsibilities when handling data, in accordance with the **UK GDPR** and the **Data Protection Act 2018**.

This Policy complements the **Data Protection Policy**, which outlines detailed internal procedures, and the **Data Privacy Statement**, which informs external stakeholders about how their data is processed. Employees are expected to familiarise themselves with all three documents to ensure compliance.

2. SCOPE

This Policy applies to:

- All employees, contractors, and volunteers of Angling Trust and Fish Legal.
- Personal, sensitive, and confidential data handled during operations.
- Data in all formats, including physical documents, digital files, emails, and verbal communications.

This document should be read alongside the **Data Protection Policy**, which provides comprehensive operational details, and the **Data Privacy Statement**, which outlines our external commitments to data subjects.

3. KEY PRINCIPLES FOR HANDLING DATA

3.1. Lawfulness, Fairness, and Transparency

- Ensure all data processing complies with legal requirements and aligns with the commitments outlined in the **Data Privacy Statement**.
- Only collect and process data for legitimate business purposes.

3.2. Confidentiality

- Keep all personal, sensitive, and confidential data secure and private.
- Refer to the **Data Protection Policy** for procedures on handling and sharing data securely.

3.3. Data Minimisation

- Collect only the minimum data necessary to fulfil specific tasks or responsibilities. Please refer to the **Data Minimisation Policy** for more information

3.4. Accuracy

- Regularly review and update data to ensure its accuracy.
- Follow the procedures in the **Data Protection Policy** to correct or report inaccurate data.

3.5. Data Security

- Protect data using strong passwords, secure storage methods, and encryption where necessary.
- Avoid storing data on personal devices or sharing through unauthorised channels.

3.6. Storage Limitation

- Retain data only for as long as specified in the **Data Retention Schedule**, which is part of the **Data Protection Policy**.

4. HANDLING SENSITIVE AND CONFIDENTIAL DATA

4.1. Special Category Data

Special category data (e.g., health, ethnicity, or disability status) requires extra care:

- Ensure explicit consent is obtained before processing such data.
- Limit access to only authorised personnel.

4.2. Employee and Member Data

- Use employee and member data solely for legitimate HR or operational purposes.
- Any sharing or disclosure must comply with the procedures outlined in the **Data Protection Policy**.

5. REPORTING DATA BREACHES

All employees must report suspected or confirmed data breaches immediately to the **Data Protection Officer (DPO)**.

- Examples of breaches include unauthorised access, accidental sharing, or loss of devices containing data.
- Breaches are handled according to the **Data Protection Policy** to mitigate risks and ensure compliance.

6. EMPLOYEE RESPONSIBILITIES

Employees are required to:

- Understand and adhere to this Privacy Policy, the **Data Protection Policy**, and the **Data Privacy Statement**.
- Complete mandatory training on data protection.
- Handle data responsibly, securely, and in compliance with organisational guidelines.
- Please see Appendix 1 for more information on the role of data custodians.

Failure to comply may result in disciplinary action, up to and including termination of employment.

7. MONITORING AND COMPLIANCE

Angling Trust conducts regular audits and monitoring activities to ensure compliance with this Policy. Employees are expected to cooperate fully during these reviews.

8. ACCESSING RELATED DOCUMENTS

This Policy should be read in conjunction with:

1. **Data Protection Policy**: A detailed document outlining internal data handling procedures, available on the internal intranet.
2. **Data Privacy Statement**: An external-facing document explaining our commitments to data subjects, available on the Angling Trust website.

Employees should refer to these documents for further clarification on specific topics.

9. CONTACT FOR GUIDANCE

For questions, concerns, or additional support, contact the **Data Protection Officer (DPO)**:

Address: Management Suite 1, The Oasis Meadowhall Centre, Sheffield, S9 1EP
Phone: 0114 400 0021
Email: anglingdpo@samuraisecurity.co.uk

This Policy will be reviewed annually and updated as needed to reflect changes in laws or organisational practices.

Effective Date: **Per Issue Date**

Version Control	
Issue Date	Sep 25
Version number	2.0
Document Owner	Paul Gant

APPENDIX 1 - UNDERSTANDING THE ROLE OF A DATA CUSTODIAN

1. INTRODUCTION

In data management and information security, **Data Custodians** and **Data Owners** play essential roles in safeguarding and effectively managing data assets. This document provides an overview of what a data custodian and data owner do, their responsibilities, and how individuals within an organisation can determine if they hold one or both roles.

---

2. WHAT IS A DATA CUSTODIAN?

A **Data Custodian** is an individual or team responsible for the safe and secure storage, maintenance, and handling of data within an organisation. Unlike data owners, who have decision-making authority over data usage and access, data custodians ensure the operational aspects of data protection and maintenance. Data custodians handle the "how" of data management, while data owners focus on the "what" and "why."

Key Responsibilities of a Data Custodian:

- **Data Protection and Security**: Implementing safeguards to protect data from unauthorized access, corruption, and loss.
- **Data Storage**: Ensuring that data is stored in secure and accessible environments.
- **Data Maintenance**: Regularly updating and validating data to keep it accurate and current.
- **Compliance with Policies**: Adhering to organisational and regulatory data privacy and security policies.
- **Access Control**: Implementing and managing access controls to ensure only authorized personnel can access sensitive data.

---

3. WHAT IS A DATA OWNER?

A **Data Owner** is responsible for defining and overseeing data's purpose, access, and compliance requirements. While data custodians handle the technical side of data security, data owners hold the authority to make decisions about how data is used within the organisation.

Key Responsibilities of a Data Owner:

- **Setting Data Usage Policies**: Defining how data should be used and accessed in line with business objectives.
- **Risk and Compliance Oversight**: Ensuring data use meets organisational and regulatory standards.
- **Access Authorization**: Determining who can access data based on its classification and purpose.

- **Data Value Assessment**: Evaluating data's importance to the organisation and guiding how it should be prioritized and protected.

---

4. DATA CUSTODIAN VS. DATA OWNER: THE DIFFERENCE

While a data owner makes decisions on data handling and usage, a data custodian is responsible for implementing these decisions practically. Here's a quick comparison:

Role	Data Owner	Data Custodian
Focus	Decides on data use, access, and value	Focuses on secure storage, processing, and access
Authority	Has decision-making power over data policies	Follows guidelines and policies to implement security
Responsibilities	Risk and value assessment, data categorization	Access management, storage, and infrastructure

Real-World Examples

1. **Healthcare Sector:**
    - **Data Owner**: The head of the medical records department is often the data owner for patient information. They decide who can access patient records, determine data-sharing policies, and ensure compliance with regulations like HIPAA.
    - **Data Custodian**: The IT team responsible for the hospital's electronic health record (EHR) system acts as the data custodian. They ensure patient data is stored securely, maintain access controls, and handle data backup.
2. **Financial Services:**
    - **Data Owner**: In a bank, the head of customer analytics might own the customer transaction data. They determine how it can be used for business insights and define who can access it for analytics.
    - **Data Custodian**: The bank's data operations team, tasked with managing the databases storing transaction data, acts as the custodian. They ensure data is backed up, encrypted, and accessible only to authorized users.

---

5. DETERMINING IF YOU ARE A DATA OWNER, CUSTODIAN, OR BOTH

Are You a Data Custodian?

You may function as a data custodian if you handle, store, or maintain data in any form. Here's a checklist to help you determine if you fit the role:

1. **Data Access and Control**:
    - Do you set or manage permissions for who can access specific data?
    - Are you responsible for implementing access restrictions to secure data?
2. **Data Storage and Security**:

- Do you oversee the environment where data is stored (e.g., databases, file servers)?
- Are you tasked with ensuring that data is protected from unauthorized access or loss?

3. **Policy and Compliance Implementation**:
   - Are you responsible for implementing compliance measures like encryption, backup protocols, or data retention policies?
   - Do you ensure data storage practices comply with organisational and regulatory standards?
4. **Data Backup and Recovery**:
   - Do you manage data backup processes to protect against data loss?
   - Are you responsible for restoring data in case of data loss or corruption?
5. **Data Integrity and Maintenance**:
   - Do you routinely verify and update data to maintain its accuracy and reliability?
   - Are you tasked with the regular upkeep of data storage systems?

Are You a Data Owner?

Data ownership involves making strategic decisions about data's use, value, and access. Here's a checklist to help you determine if you may be a data owner:

1. **Decision-Making Authority**:
   - Do you make decisions regarding the purpose and scope of data usage?
   - Are you responsible for classifying data and setting usage policies?
2. **Defining Data Access**:
   - Do you determine who is allowed to access data based on organisational needs?
   - Are you responsible for authorizing access levels according to data sensitivity?
3. **Regulatory Compliance**:
   - Are you accountable for ensuring data use complies with legal, regulatory, and organisational requirements?
   - Do you decide on the data's retention period and privacy guidelines?
4. **Risk Management**:
   - Do you assess the risks associated with data and make decisions to mitigate them?
   - Are you tasked with determining the data's value to the organisation and prioritizing its protection?

Note: Dual Role - Data Owner and Custodian

In some cases, you may act as both data owner and custodian, especially in smaller organisations. For example, a small business's head of marketing may both manage (own) and maintain (custodian) customer contact information, deciding how data can be used while also ensuring it is securely stored and compliant with data protection regulations.

---

6. HOW DATA OWNERS AND DATA CUSTODIANS WORK TOGETHER

Effective data management relies on collaboration between data owners and custodians. Here's how they complement each other:

1. **Data Access and Authorization**:
    - **Data Owner**: Sets access permissions based on data classification and business needs.
    - **Data Custodian**: Implements these permissions, maintaining access control systems.
2. **Compliance and Security**:
    - **Data Owner**: Establishes policies for data compliance and usage standards.
    - **Data Custodian**: Enforces these policies by setting up security measures like encryption, backups, and audit trails.
3. **Data Integrity and Maintenance**:
    - **Data Owner**: Defines standards for data accuracy and reliability.
    - **Data Custodian**: Ensures data is regularly updated, validated, and backed up to meet these standards.
4. **Risk Mitigation and Reporting**:
    - **Data Owner**: Assesses data-related risks and determines necessary protections.
    - **Data Custodian**: Executes protective measures and generates regular reports on data status, access logs, and incidents.

---

7. IMPORTANCE OF THE DATA CUSTODIAN AND DATA OWNER ROLES

Data owners and custodians are critical to an organisation's data governance framework. Each plays a role in protecting data integrity, enforcing access controls, and ensuring compliance. By working together, data owners and custodians provide a robust data management strategy that safeguards the organisation and the stakeholders whose data they manage.

---

8. CONCLUSION

Data custodianship and ownership are foundational roles in data governance and security. If your responsibilities align with those outlined in this document, it's essential to understand and embrace your role. Collaboration between data owners and custodians ensures effective, secure, and compliant data management.