OPTIX SOLUTIONS
Digital Excellence

CLIENT DATA HANDLING POLICY

Version 3 Date created 07/09/2020

Author: Rob Stevens, Operations Director

Data Protection Officer: Rob Stevens, Operations Director

Optix Solutions 1st Floor Alphin Brook House Alphin Brook Road Marsh Barton Exeter EX2 8RG

OPTIX SOLUTIONS
Digital Excellence

Client Data Policy Contents Page

1. Principles

Optix Solutions Limited shall comply with the principles of data protection (the Principles) enumerated in the General Data Protection Regulation (GDPR). We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent - Data collection must be fair, for a legal purpose and we must be open and transparent about how the data will be used.

2. Limited for its purpose - Data can only be collected for a specific purpose.

3. Data minimisation - Any data collected must be necessary and not excessive for its purpose.

4. Accurate - The data we hold must be accurate and kept up to date.

5. Retention - We will not store data longer than necessary.

6. Integrity and confidentiality - The data we hold must be kept safe and secure.

We must ensure accountability and transparency in all our use of personal data. We must be able to show how we comply with each Principle. You are responsible for keeping a written record of how all data processing activities which you undertake comply with each of the Principles. These records must be kept up to date and must be approved by the relevant Data Protection Officer (DPO).

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must be able to demonstrate compliance. Both you and we have a duty to understand and comply with our respective responsibilities, thus ensuring that we meet the following data protection obligations to:

- fully implement all appropriate technical and organisational measures,
- maintain up to date and relevant documentation on all processing activities,
- conduct Data Protection Impact Assessments, and
- implement measures to ensure privacy by design and default, including:
    - data minimisation
    - pseudonymisation
    - transparency
    - allowing individuals to monitor processing
    - creating and improving security and enhanced privacy procedures on an ongoing basis

2. Responsibilities

2a. Optix Solutions' Responsibilities:

● Analysing and documenting the type of personal data we hold

● Checking procedures to ensure they cover all the rights of the individual

● Identifying the lawful basis for processing data

● Ensuring consent procedures are lawful

● Implementing and reviewing procedures to detect, report and investigate personal data breaches

● Storing data in safe and secure ways

● Assessing the risk that could be posed to individual rights and freedoms should data be compromised

● Reviewing all data protection procedures and policies on a regular basis

● Arranging data protection training and advice for all staff members and those included in this policy

● Answering questions on data protection from staff, board members and other stakeholders

● Responding to individuals such as Clients and employees who wish to know the details of data being held on them by us

● Checking and approving with third parties that handle the company's data any contracts or agreements regarding data processing

● Ensuring that all systems, services, software and equipment meet acceptable security standards

● Checking and scanning security hardware and software regularly to ensure it is functioning properly

● Researching third-party services, such as cloud services which the company is considering using to store or process data

● Approving data protection statements attached to emails and other marketing copy

● Addressing data protection queries from Clients, target audiences or media outlets

● Coordinating activities internally with the Optix DPO to ensure that all marketing initiatives adhere to data protection laws and the Company's Data Protection Policy

2. Responsibilities (continued)

2b. Client's/Partner's Responsibilities:

● Fully understanding your data protection obligations

● Checking that any data processing activities with which you are dealing on our behalf comply with our Data Handling Policy and are justified

● Not using data in any unlawful way

● Not storing data incorrectly, being careless with data or otherwise causing us to breach data protection laws and/or our policies through your actions

● Complying with this policy at all times

● Raising any concerns, notifying us of any breaches or errors as soon as you become aware of them, and reporting to us anything suspicious or contradictory to this policy or our legal obligations without delay. NB Please note the importance of this responsibility as set out in greater detail in section 4)

3. Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Optix DPO.

3a. Data Security

Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Optix DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

3b. Storing Data Securely

● In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.

● Printed data will be shredded when it is no longer needed.

● Data stored on a computer will be protected by strong passwords that are changed regularly.

● We will always use a password manager to create and store passwords, and would recommend that Clients and Partners adopt the same policy.

● Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used.

● The Optix Operations Director (Rob Stevens) will approve any cloud service used to store data.

● Servers containing personal data will be kept in a secure location, away from general office space.

● Data will be regularly backed up in line with the Company's backup procedures.

● Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

● All servers containing sensitive data will be approved and protected by security software.

● All possible technical measures will be put in place to keep data secure.

3. Accuracy and Relevance (continued)

3c. Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, and determined in a manner consistent with GDPR data retention guidelines.

3d. Transferring Data Internationally

There are restrictions on international transfers of personal data. Neither we, nor Partner organisations, will transfer personal data abroad, or anywhere else outside of normal rules and procedures, without express permission from the Optix DPO.

4. Reporting Breaches (Optix, Client and Partner Responsibilities)

Any breach of this policy or of data protection laws must be reported as soon as is practically possible. This means that as soon as you become aware of a breach you should report it to us. Optix Solutions has a legal obligation to report data breaches to the Information Commissioner's Office within 96 hours. All members of Client, Partner and Optix staff have an obligation to report actual or potential data protection compliance failures.

This allows us to:

● investigate the failure and take remedial steps if necessary,

● maintain a register of compliance failures, and

● notify the Information Commissioner's Office of any compliance failures that are material either individually or as part of a pattern of failures

Any member of Optix staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

5. Policy

5a. Passwords

All Client passwords, digital keys and unique identifiers will be stored by Optix, and/or our Partners when acting on our behalf, in Sharepoint in a password protected, shared folder that has only the need to know team included and is removed from all other storage locations.

5b. Intellectual Property

Optix Solutions handles large amounts of sensitive Client property, ranging from ideas to design materials.

This property is protected by these rules:

● physical properties should not leave our offices,

● laptops and computers should be locked when unattended,

● laptops, computers and documents should be stored securely when at employee homes and should not be left unattended when travelling, and

● data no longer required should be backed up to Optix Solutions cloud storage and then destroyed locally.

5c. Access

Access to data will be on a “need to know” only basis, which means that it will only be shared with staff or contractors that require it to fulfil their duties. All contractors and staff will have completed a Non-Disclosure Agreement (NDA) as part of their employment contract before receiving access.

Access to sensitive performance information and infrastructure will be secured by a physical security device. All accounts with access to these services will require a Director’s authorisation.

Devices and passwords are issued by the Directors on a need to access basis only.

6. Suppliers

6a. Storage

Optix Solutions backs up its data to the cloud regularly, this includes all emails, files and logs. Our cloud provider is Google Cloud Platform.

Code repositories are hosted by Eloquent's Gtlab instance, and the legacy sites (those older than 2019 build date) on Bitbucket.

6b. Hosting

All server and application infrastructure managed by Optix Solutions is supplied by Google Cloud Platform, Eloquent, Krystal Hosting and Solve IT which includes:

- Virtual Machines
- Container Storage
- Data Storage
- Networking
- Database Storage
- Authentication
- Backups
- Analytics

Some customers may also have secure services managed by Optix Solutions that are supplied from Eloquent, Krystal Hosting and Solve IT which includes:

- DNS management
- SSL management and authoring
- WAF
- Origin certificate authoring
- Intelligent routing

Optix Solutions 1st Floor Alphin Brook House Alphin Brook Road Marsh Barton Exeter EX2 8RG