CLIENT DATA POLICY

Handling Sensitive Client Data

Data Protection Officer: Richard Burrow

Version	Date	Author	Notes
1	20/09/2019	Laurent Brickell	

Principles

Organic shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. 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 cannot store data longer than necessary.
6. **Integrity and confidentiality** - The data we hold must be kept safe and secure.

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 show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for complying with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- 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

Responsibilities

Organics Responsibilities:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess 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 which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Ensure 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 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 with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Your Responsibilities:

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

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 DPO.

Data Security

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

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- All staff **must** use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The Technical Director must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should 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 must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO.

Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Organic has a legal obligation to report any data breaches to the Information Commissioner's Office within 96 hours. All members of 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
- Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of 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.

Policy

Passwords

All client passwords, digital keys and unique identifiers **must** be stored in Lastpass under a shared folder that has only the need to know team included and removed from all other storage locations. If you have any queries please contact your administrator.

Intellectual Property

Organic handles large amounts of sensitive client property, this ranges from ideas to design materials. Every effort should be made to ensure this property is protected by following these rules:

- Physical properties should not leave the office
- Laptops and computer should be locked when away from your desk
- Laptops, computers and documents should be stored securely when at home and should not leave your persons when traveling
- Data no longer required should be backed up to Organic's cloud storage and then destroyed locally

Lost Data

In the event that a device or sensitive document is lost, you **must** report the loss to your DPO within 24 hours with a full explanation of events, type of data and details of the potential data loss.

Access

Access to data should be on a needs basis, this means that should only be shared with staff or contractors that require it to fulfill their duties. All contractors and staff must complete an NDA as part of their employment contract before receiving access. If you notice staff who have incorrect access to data please report this to the DPO immediately.

Access to sensitive performance information and infrastructure **must** be secured by a physical security device. All accounts with access to these services will require a Yubikey 2FA device to unlock, 2FA devices are issued by the Technical Director on a need to access basis. It is your responsibility as a key holder to ensure the safekeeping of your security device and report loss immediately.

If you discover sensitive performance data or infrastructure that is not secured behind a physical key, or you think you require a key to perform your duties please contact the Technical Director immediately.

Suppliers

Storage

Organic backs up it's data to the cloud regularly, this includes all emails, files and logs. Our cloud provider is Google Cloud Platform.

Code repositories are hosted by Atlassian Bitbucket.

Hosting

All server and application infrastructure managed by Organic is supplied by Google Cloud Platform which includes:

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

Some customers may also have secure services managed by Organic that are supplied from Cloudflare which includes:

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