Studio idir Data Protection Policy
in accordance with the EU General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018

General team members guidelines

Access to data

- Only those who need access to data for their work should have access to it.
- Personal data should never be disclosed to unauthorised people, either within Studio idir or externally.
- If access to confidential information is required, it can be requested through Aisling Rusk
- Team members should keep all data secure, both in terms of accessibility and encryption, and strong passwords must be used and should never be shared.
- Login restricted access to computers protects access to data; team members should ensure their computer is locked when not in use.

Saving data

- All data should be saved securely on the company server and backed up in-line with Studio idir's backup procedures, which are in-line with GDPR and the Data Protection Act 2018.
- Data should never be saved directly to mobile or personal devices such as tablets or smartphones.
- Personal data stored on memory sticks must be locked away securely when they are not being used and the data should be deleted when finished with.

Sending/receiving data

- All team members must attend an internal training session on data protection methods. Topics covered are how we handle research-specific data, provides details on how to limit the data we receive, and advice for sending and receiving data securely.
- If data in an email must be encrypted, the password should be provided to the recipient separately by telephone.
- Only send work-related information and data, including passwords, names or contact details, through Studio idir's internal communication channels. Never send information via your personal device e.g. Whatsapp, text message, etc.

Paper data

- Where personal data is stored on paper, it should be kept in a secure place where only authorised team members can access it e.g. locked filing.
- Printed personal data should be shredded when it is no longer needed.

Reviewing data

- Data should be regularly reviewed/updated and deleted/disposed of as per the retention schedule and/or privacy statements.

Email addresses

- Always 'BCC' email addresses when sending a bulk email using Gmail. A work email address that identifies an individual e.g. initials.lastname@company.com is personal data and GDPR and the Data Protection Act 2018 applies.
- Never provide an individual's personal or work email address to someone outside Studio idir without their consent; this is classed as personal data under GDPR and the Data Protection Act 2018. Consent can be verbal but needs to be documented.

Working remotely

- Never use free public or open WiFi networks when working remotely and accessing personal data.
- If you are working from home, you must ensure your internet/WiFi connection is secure. Here are examples and further information is available on the ICO website:
    - password-protected network with a strong password i.e. not using the default administrator username/password for your router
    - wireless network protection is turned on e.g. WPA or WPA2
    - security software up-to-date on your computer
    - router firewall turned on; etc.

Introduction

Studio idir needs to gather and use certain information about individuals. These can include clients, customers, suppliers, employees, and other project stakeholders the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet data protection standards and to comply with the law i.e. the General Data Protection Regulation and the UK Data Protection Act 2018.

Why have this policy?

It ensures Studio idir:

- Complies with data protection law and follows good practice
- Protects the rights of clients, team members, stakeholders and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Principles of data protection

Anyone processing personal data must comply with the GDPR and Data Protection Act 2018 principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Appendix 2 provides the full definition for each principle from Article 5 of the GDPR listed above and you can also refers to Article 5 of GDPR here: https://gdpr-info.eu/art-5-gdpr/.

Who is responsible?
All team members are responsible and must be familiar with this data protection policy and ensure their actions comply with its terms.

Aisling Rusk is ultimately responsible for ensuring that Studio idir meets its legal obligations.

Due to size and type of organisation, Studio idir is not required to appoint a Data Protection Officer (DPO) under GDPR and the Data Protection Act 2018. However significant steps have been taken to ensure the organisation is well-informed and keeping up-to-date with legislation.

Scope of personal information
All personal information is held on a confidential basis and must not be disclosed to third parties. It is a disciplinary offence for team members to disclose personal data to a third party without authorisation.

Data is collected and stored as below:

- Events

Name, email address and organisation is collected for event attendees and stored securely on Googledrive. After 1 year, personal data will be removed to leave the organisation name only.

- Customers/Clients

We hold name, email address, address and phone number for anyone who pays us for a product or service. Details are contained in the relevant invoices or project agreements saved securely.

- Suppliers

We hold contact details (e.g. name, email, telephone, postal address) in supplier contracts and bank details on invoices.

Studio idir only uses GDPR-complaint suppliers. Their data protection responsibility is outlined clearly in the contract we provide and which they agree to when they sign.

- Research data

The personal data collected for research is typically name and address, but where organisations are collecting responses with a view to facilitating an online draw to incentivise their research and/or add to their mailing list, this may also require email address and phone number.

We brief clients who share data with Studio idir to ensure we only receive the data that we require.

Access is restricted to the relevant team members only for customer data files. Only research results are shared, not the source information i.e. personal data.

We monitor what we are doing and avoid keeping duplicates of data; and we do not hold long-term records for our research activity.

Data uses and conditions for processing

The conditions for processing are made publicly available to data subjects in the form of a privacy notice which links to a detailed research privacy notice

The data Studio idir collects is subject to active consent by the data subject, and is freely given, specific, informed and unambiguous. This consent can be revoked at any time.

Studio idir may have good reason to process personal data without consent – but will ensure there is no unwarranted impact on the individual, and it is still fair, transparent and accountable.

Consent is not appropriate when processing is necessary for:

- the performance of a contract or to take steps to enter into a contract
- compliance with a legal obligation
- protection of the vital interests of an individual
- a public task
- legitimate interests

Conditions for processing personal data are detailed in the data audit registers saved on SharePoint. Further information is available about the legal basis for processing research-specific data in the internal research protocols document.

Data retention and audit

Studio idir will retain personal data for no longer than is necessary.

Data audit and registers contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Both documents will be reviewed on an annual basis by Aisling Rusk, to manage and mitigate risks.

Data Protection Impact Assessments (DPIAs) and data sharing
If data is deemed high risk, a DPIA will be completed on an individual basis.

Security measures
Personal data is stored securely on Googledrive or in locked filing. It is kept for no longer than is necessary, as per the retention schedule.

Data should be deleted securely:

- Paper copies shredded
- Electronic copies deleted from the server and, if relevant, from your computer and its Recycle Bin
- From Google Workspace, ensuring you delete it from your inbox and 'Trash' folder

Log-in restricted access is set up for all Studio idir equipment. And access to data on Googledrive is restricted to only those who need access to do their job. Access is updated when someone changes job within Studio idir or removed when someone leaves the company.

Compliancy is sought from all third-party services Studio idir uses to store or process data. GDPR compliancy has been sought and recorded for any suppliers based outside the EEA.

Where data sharing is required for research purposes, client agreements are in place to ensure that Studio idir only receives what information is necessary to complete a task. Data should be shared using password-protected documents with passwords provided separately by telephone.

Data breaches
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Steps for dealing with a data breach:

- Report any actual or potential data compliance failures to Aisling Rusk as soon as possible.
- Aisling Rusk will assess if it can be dealt with in-house in compliance with GDPR and Data Protection Act 2018
- If necessary, it will be reported to the Information Commissioner's Office within 72 hours of breach
- If it affects someone specifically, they must be informed

All suspected or actual data breaches must be recorded in the breach of data register.

Subject Access Requests (SARs) i.e. access to personal data

A data subject has the right to request a copy of their data and receive it in a structured, commonly used format.

All individuals who are the subject of data held by Studio idir are entitled to:

- Ask what information Studio idir holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up-to-date
- Be informed of how the company is meeting its data protection obligations

SARs should be processed within one month. All requests and responses to SARs should be dealt with in writing for audit purposes and to record compliance.

Right to be forgotten (right to erasure)
A data subject may request that any information held on them is deleted or removed where there is no compelling reason for its continued processing.

Aisling Rusk is responsible for recording all requests and emailing the recipient to confirm deletion of their personal data.

Privacy notices
Studio idir is transparent and provides accessible information to individuals about how their personal data is used.

The privacy notice details:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights

Data protection compliance and protocols
Studio idir is registered with the Information Commissioner's Office (ICO).

Studio idir has taken the following steps to ensure compliance:

- created a data audit and risk register
- created a retention schedule
- completed a mapping personal data grid
- reviewed data sharing agreements in the last 12 months
- obtained compliance statements from suppliers based outside EEA
- ensured all team members are familiar with this policy and compliant with its terms; and the policy will be included in team members inductions.

The items listed above include details of business compliance processes and procedures.