**Data Protection Policy**

Frame Perfect, The Collective Production compny collects personal data and makes use of certain information about individuals who interact with Frame Perfect and the information they share. This can include customers, suppliers, business contacts, employees and other people Frame Perfect has a relationship with or may need to contact.

This policy details how personal data is collected, handled and correctly stored in a safe location, the standards provided are to comply with the law.

The Data protection policy ensures Frame Perfect

1. Complies with general data protection legislation and follows in good practice
2. Protect the rights of staff, customers and individuals who interact with Frame Perfect
3. Is clear on how data is stored and how we process individual’s data
4. Protects the organization from the risk of a data breach

The General Data Protection Regulation 2016 is a significant regulation in EU law on data protection and privacy for all individuals within the European Union. It is how Frame Perfect manages data protection as a corporate issue by documenting the personal data held; state where it came from and whom the data shared with. Frame Perfect complies with all of the GDPR principles and personal data follows:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes.

Adequate, relevant and limited to what is necessary.

Kept for no longer than is necessary.

Processed in a manner that ensures appropriate security of the personal data collected.

This policy applies to the head office of Frame Perfect, The Collective Production Agency,

All staff of Frame Perfect

All Contractors, suppliers and other people working on behalf of Frame Perfect.

The systems and processes that the above people have access to, applies to all data that the company holds relating to identifiable individuals and the purposes for which we use the detailed information. Refer to the Frame Perfect Privacy Policy.

This policy helps to protect Frame Perfect from data security risks including:

1. Breaches of confidentiality.
2. Information given out inappropriately.
3. Failing to offer choice. All individuals should be free to choose how the company uses data relating to them.
4. Reputational damage. The company could suffer if hackers successfully gained access to sensitive data.

Everyone who works for or with Frame Perfect has responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data must ensure data is processed in line with this policy and GDPR principles.

The key people responsible and their definitions

Accountable Managing Director, the person who has ultimate accountability and authority for the policy.

Responsible, Data protection officer, the person responsible for developing and implementing policy.

Consulted, Director, the people consulted prior to final policy implementation or amendment.

Informed staff including temporary staff, the people informed after policy implementation or amendment.

These rules describe how and where data should be safely stored. Question about storing data safely directed to the Data Protection officer or Director. When data is stored on paper it is to be in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but printed out for some reason;

When not required, the paper or files held in a locked drawer or filing cabinet.

Employees should make sure paper and printouts, are not left where unauthorised people could see them.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

Data should be protected with strong passwords that are changed regularly and never shared between employees.

If data is stored on a removable media, then these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.

Servers containing personal data, should be placed in a secure location away from general office space.

Data should be backed up frequently. Those backups should be tested regularly in line with the company’s standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by approved security software and a firewall.

Personal data is of no value to Frame Perfect unless the business can make use of it. However, it is when personal data used; it can be at the greatest risk of loss, corruption or theft.

When working with personal data, employees should ensure the screens of their computers locked when left unattended.

Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

The regulation requires Frame Perfect to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

1. Data will be held in places as necessary. Staff should not create any unnecessary additional data sets.
2. Staff should take every opportunity to ensure data is updated. EG. By confirming a client’s details when they call.
3. Frame Perfect will make it easy for data subjects to update the information Frame Perfect holds about them.
4. Data should be updated as inaccuracies are discovered. If a client no longer can be reached on their stored telephone number, it should be removed from the database.
5. It is Directors responsibility to ensure marketing databases are checked against industry suppression files every six months.

All individuals who are the subject of personal data held by Frame Perfect are entitled to

1. Ask what information the company holds about them and why.
2. Ask how to gain access to it.
3. Be informed how to keep it up to date.
4. Be informed how the company is meetings its data protection obligations. If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, address to the data protection officer. The data protection officer can supply a standard request form, although individuals do not have to use this. The data protection officer will aim to provide the relevant data within 14 days. The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Frame Perfect will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisers where necessary.

Frame Perfect aims to ensure that individuals are aware that their data is being processed and that they understand

How the data is being used

How to exercise their rights

To these ends, the company has a privacy policy, setting out how data relating to individuals is used by the company.