

Perfect Pitch Consultancy Ltd – GDPR Data Protection Policy

1 Introduction

For the purpose of this document Perfect Pitch Consultancy Ltd (the company) will be described as Perfect Pitch.

In its everyday business operations Perfect Pitch needs to collect, store and process data belonging to a diverse variety of identifiable individuals.

These can include: Current, past and prospective employees; customers, prospects and business contacts; contractors and suppliers; users and subscribers to websites; visitors; personal data belonging to Perfect Pitch clients (third party data) and other individuals with whom the organisation has a relationship.

This policy describes how these personal data records are collected, stored and handled to meet the company's data protection standards and comply with relevant legislation relating to data privacy, including the GDPR. Breaches of confidentiality and failure to respect the rights of individuals, can lead to fines, legal actions and reputational damage.

2 Scope

The policy applies to all people, processes and systems in all group organisations that have access to, or use, personal data pertaining to citizens. These include employees, contractors, directors, board members and any third parties who have access to the data for lawful reasons.

3 Data Privacy

3.1 GDPR Principles

The EU GDPR describes how organisations must collect, store and handle personal data. There are a number of fundamental principles upon which the GDPR is based. These state that personal data should be:

- collected and processed legally, fairly and the individual should be aware what data is collected, for how long and for what purpose;
- collected only for the purpose specified and agreed and not used for any other purpose, with some exceptions, for example public interest;
- “minimised”, i.e. no more data should be collected than is required to fulfil the purpose for which they were obtained;
- accurate and kept up to date, completed and corrected;
- not retained for longer than they are required, with some exceptions in public interest;
- protected, through the appropriate systems and procedures, against unauthorised or unlawful processing or accidental loss, modification, destruction or damage;
- not transferred to a country outside the EU-approved list of nations, unless the appropriate security and contractual clauses are in place.

The organisation is responsible for, and must be able to demonstrate compliance with, the above requirements. This can be in relation to current and future, planned, processing activities or systems.

3.2 GDPR Rights

The individual has a number of rights under the GDPR. These consist of:

- The right to be informed that data is held, why, where and for how long; and of their rights
- The right of access to their data

- The right to rectification (correction, completion)
- The right to erasure
- The right to restrict processing of data
- The right to data portability
- The right to object to processing of their data
- Rights in relation to automated decision making and profiling

These rights must be respected and responded to, through implementation of the appropriate systems and procedures.

3.3 Lawful Basis / Consent

Unless there is a valid contractual or legal reason (lawful basis) for collecting and processing a person's data, it is often necessary to obtain their explicit consent. In the case of children (under 13 years old in the UK and between 13 and 16 in other EU countries), the consent of a parent or legal guardian must be obtained for their data to be collected and processed. Special category or sensitive data needs particularly careful consideration and the processing of this data is prohibited, unless there is a lawful basis for collecting and processing them.

People must be clearly told how their data will be used, on what basis and for how long, at the time it is collected. A clear explanation must also be given of their rights in relation to the data, including the right to withdraw consent. In cases where the data is obtained from a third party, this information should be provided within a month of the data being acquired by the organisation.

3.4 Complying with the GDPR

Perfect Pitch is committed to complying with the GDPR and other relevant legislation in relation to the privacy of individuals whose data the organisation collects, holds and processes. The following measures are taken to support the principles and rights specified by the legislation:

- All staff and third parties involved in handling personal data understand their responsibilities in terms of data protection and privacy
- Training in data security and privacy has been provided to all staff
- Policies and codes of conduct are in place to ensure data protection and privacy
- There are regular reviews of policies and procedures around personal data
- Privacy by design and by default, including Data Protection Impact Assessments, is adopted for all new or changed systems and processes impacting personal data
- Data is disposed of as required by the data retention policies and the GDPR
- Controls are in place around transfers of personal data to non-EU approved countries
- Contractual agreements are in place with third party Processors, Joint Controllers and cloud service providers; they adequately handle personal data privacy and security; and the appropriate data transfer security measures are in place
- All processing activities and transfers involving personal data records have been identified by the organisation and are covered by the measures above and respect the requirements of the GDPR
- The risks for each type of personal data have been assessed and controls are in place to mitigate risks
- The lawful basis for processing personal data has been defined and all processing is lawful and justified
- Valid Privacy Notices are in place for all individuals whose personal data is collected, held and processed
- Special category data is identified and handled in the appropriate manner, given its sensitivity
- Rules regarding consent are followed
- Processes are in place to enable individual citizens to exercise their rights in relation to their personal data and these requests are handled within the required timeframes
- The organisation has documented all personal data processing activities and can demonstrate the appropriate data protection and privacy measures are in place, as well as compliance with the GDPR

These measures and controls are regularly reviewed, as part of the management review of data privacy and protection.

4 Data Protection

Personal data and its privacy are protected by means of a number of organisational, technical and physical measures designed to secure the data. The GDPR requires organisations to have the appropriate security to prevent the data being accidentally or deliberately compromised.

This section provides an overview of how personal information is kept safe and secure.

4.1 Risk Assessment

The organisation reviews all processes that involve the collection, storage, use and disposal of personal data. This review process considers how valuable, sensitive and confidential the data are and what damage or distress could be caused to individuals should their data be breached. The outcome of this process enables Perfect Pitch to identify the most suitable security measures for its purpose.

4.2 IT Controls

The organisation employs a number of controls to ensure the right level of security. These controls are in line with the UK Government's Cyber Essentials Scheme.

- **Boundary Firewalls and Internet Gateways** – this is the first line of defence against unauthorised intrusions via the internet. A well-configured firewall prevents breaches from happening within the network. An internet gateway stops users within the organisation accessing websites or other online services that represent a potential or real threat
- **Secure Configuration** – of hardware and software.

Unused software and services, especially old versions of widely used software, are removed from devices to reduce the number of potential threats.

Regular checks are made on what software or services are running on the network and any unnecessary or unknown software is reviewed for removal.

Regular vulnerability scans and penetration tests are run to test the network and systems for weaknesses. Vulnerabilities are addressed promptly.

Default passwords for hardware and software are changed.

- **Access Control** – access is only given to users who are authorised to use systems; and the user only has permission to use functionality appropriate to their current role.

Every user must use their own unique user ID and a strong password and must not share log-in credentials. Passwords are changed every 3 months.

When personnel leave the organisation, access and passwords are cancelled immediately. The same process is followed in the case of long-term absence.

- **Malware Protection** – the organisation has installed anti-virus and anti-malware software that constantly scans the network to detect and prevent threats. Alerts are dealt with promptly following detection. This software is reviewed for the latest updates and patches, which are deployed in a controlled way as quickly as possible after release, to ensure any vulnerabilities are removed.

Staff are trained to, as far as possible, recognise phishing emails and websites and to exercise extreme caution when opening emails and using the internet.

- No personal data is stored on individual PCs and Laptop computers. Data may be uploaded to approved cloud service providers and transferred to clients using secure FTP sites or unique password encryption.
- Personal data should be protected using techniques such as encryption, anonymization and pseudonymisation:
 - Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity with access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.
 - Anonymisation is a tool that allows data to be shared, whilst preserving privacy. The process of anonymising data requires that identifiers are changed in some way such as being removed, substituted, distorted, generalised or aggregated.
 - Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example, a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention.

4.3 Data Management

In order to protect personal data when they are being used or processed, the organisation has the following policy:

- When working with personal data, employees must ensure that screens are locked when not in use or left unattended. Employees should avoid having their screens overlooked when working with personal data
- Induction training, and regular follow-up training, for all employees on data security, data management and physical security.
- A clean desk policy is in place
- Personal data should not be shared informally. In particular, it should not be sent by email without secure encryption.
- Data must be encrypted before being transferred electronically
- Personal data must never be sent to a country outside the EU-approved list of countries
- Employees should not save copies of personal data to their own computers. Data should be accessed and updated on a centrally and securely held version
- Data must be held in as few places as necessary and the creation of unnecessary data sets avoided
- Data should be updated as inaccuracies are discovered
- Marketing databases should be checked against industry suppression files on a regular basis

4.4 Mobile Devices

The organisation also protects personal data on mobile devices, such as laptops, mobile phones and USB drives. It is the policy of Perfect Pitch that the data on mobile devices is secured, for example by file or full disk encryption.

Employees and contractors must ensure that all mobile devices are locked away securely, both in and out of the office, when not being used.

Personal data should never be saved directly to laptops and other mobile devices.

Employees and contractors should avoid, where possible, having personal data on their device; are prohibited from downloading software without IT approval and from connecting their device to unknown or untrusted devices, networks or software.

4.5 Cloud Security

Where data are stored in, or transferred to, a cloud environment, the organisation collaborates with the cloud service provider to satisfy itself that the security measures employed by the cloud provider are adequate and appropriate.

The organisation carries out regular data audits to ascertain which personal data are stored in the cloud.

4.6 Data Minimisation and Disposal

Perfect Pitch regularly reviews personal data to identify information that is out-of-date, inaccurate, excessive, no longer required or exceeding retention limits. This restricts the amount of data at risk and enables the organisation to control and secure the data more effectively.

Following these reviews, a number of actions are taken:

- Inaccurate or incomplete data are updated
- Excessive data, i.e. data that exceeds the requirement of the processing, are deleted
- If the data are still required, the storage facility is reviewed to ensure they are stored in the appropriate place
- Data that are not required regularly, or archived, are moved to a more secure location to prevent unauthorised access
- Data that are no longer required are disposed of according to the [Personal Data Retention Policy](#).

4.7 Outsourced IT Contractors

Where Perfect Pitch considers outsourcing certain services to a third-party IT provider, it satisfies itself that the third party employs the required security measures and controls. This includes:

- Requesting a security audit of the third-party systems containing the organisation's data
- Reviewing the findings of the review and ensuring improvements are made
- If appropriate, carrying out an on-site visit to ensure physical and IT security are in place and that the provider can be trusted to work securely
- Having strong access controls in place
- Ensuring written contracts are in place and that they contain specific clauses to act only on the instructions of Perfect Pitch and to comply with the requirements of the GDPR
- If the third-party erases data or disposes of IT equipment held by the organisation, Perfect Pitch must ensure that the safeguards around disposal are adequate

4.8 Physical Security

Perfect Pitch takes physical security very seriously, ensuring that external doors and windows, and internal secure areas, are adequately protected and robust access controls are in place for all

employees, contractors and visitors. Employees and visitors must be registered and accompanied, at all times.

The practice of storing personal data in any paper form should be avoided where possible. When it is necessary to keep and store physical paper files that contain personal data, temporarily or otherwise, they should be kept in a secure place (a lockable filing cabinet or lockable storage room), where unauthorised people do not have access to its contents. Examples of such physical files may include but are not limited to, client or internal meeting notes, invoices, personnel records, client agreements or contracts and supplier details or agreements. Such records should only be kept as long as we are legally required to do so and when they are no longer required, they must be disposed of securely by shredding or incineration. A clean desk policy is in place meaning that no confidential files or paper documents containing any confidential information or personal data is allowed to be kept on desks overnight.