Data Protection Policy

Scope

Applies to personal data processed in a structured file system whether automated or paper based.

Territorial Scope

Applies to all EU citizen personal data pertaining to a natural person that the Company holds and processes.

Would apply to office(s) outside of EU that offer goods, services or monitors behaviour of EU citizens if the Company had any.

Definitions

Natural person
An individual who is alive, does not apply to other legal entities

Data Subject
Any living individual whose personal data is processed by the Company.

Personal Data
Any information referring to an identified or identifiable natural person, an identifiable natural person is someone who can be identified directly or indirectly by reference including:

- Name
- ID Number
- Location data – Address, GPS location, Online location
- Online Identifier – persistent cookies, RDIF tags, IP address etc.
- Factors relating to physical, economic, cultural, social identity

(This list is non-exhaustive)

Special Category Personal Data
Personal Data that relates to:

- Beliefs
    - Religious, Philosophical, Trade Union, Political
- Racial or Ethnic origin
- Health
- Genetic Information
- Biometric Data
- Sexual activity and orientation

Data Controller
The natural person or legal entity which alone or jointly with others, determines the purpose and means of the processing of personal data.

Data Processor
A natural person or legal entity who processes data with the specific authority of the data controller.

Processing
Any operation or set of operations including:

- Collection, Recording, Organisation, Structuring, Storage, Adaptation, Alteration, Retrieval,
- Consolidation, Disclosure by Transmission, Making available, Alignment or Combination, Restriction, Erasure or Destruction

Profiling
Automated processing intended to evaluate certain personal aspect relating to a natural person to analyse or predict:

- Performance at work, Economic Situation, Location, Health, Personal Preference, Reliability, Behaviour

Personal Data Breach
Breach of security leading to accidental or unlawful:

- Destruction
- Loss
- Alteration
- Unauthorised Disclosure
- Unauthorised Access to

Data Subject Consent
Consent can only be regarded as obtained if:

It is freely given, Specific, Unambiguous

It should reflect the wishes of the data subject given by clear, affirmative action.

Children
If the data subject is under the age of 13 then they are classified as a child and parent/guardian consent must be gained before processing, their data.

Policy Statement

The board of directors and management are committed to compliance will all UK and EU regulations in respect to personal data and the protection of the "rights and freedoms" of the data subject's information held by the Company.

Compliance with the General Data Protection Regulations (GDPR) (as enacted by the Data Protection Act (2018)) is described in this policy and other relevant policies along with the policies and procedures connected with this policy.

This policy applies to all personal data held by the Company and all processing activities of such data.

GDPR Owner is responsible for reviewing the register of processing annually considering changes of processing performed by the Company.

This policy applies to all Employees of the Company included outsource suppliers. Any breaches of this policy or related policies and procedure will be dealt with using the Company disciplinary procedures.

Partners and any third parties working with or for the Company, and who have access to personal data must have read, understood and comply with this policy. Partners and third parties may only access the personal data held by the Company after signing a confidentiality agreement.

Responsibilities and roles

The Company is a data controller and processor under the Data Protection Act 2018

If a Data Protection Officer has been appointed, then they are the GDPR Owner.

GDPR Owner is responsible for the development and implementation of the GDPR as required by this policy and security and risk management in relation for compliance with this policy.

GDPR Owner has specific responsibilities in respect to Subject Access Requests and complaints, they are also the first point of contact for employees seeking clarification on any aspect of data protection compliance.

Compliance with this policy and the data protection regulations is the responsibility of all employees who process personal data.

Employees of the Company are responsible for any personal information supplied by them and processed by the Company is accurate.

Data Protection Principles

All personal data processing activities must adhere to the data protection principle, as laid out in Article 5 of the GDPR. These principles are:

All processing must be "fair, lawful and transparent"

Fair- for the processing to be fair, the data controller has to ensure that certain information is available to the data subjects at point of collection or if the personal data was collected indirectly.

Lawful – The processing of each piece of personal data must have a lawful basis before processing can begin.

Transparent – Privacy notices describing the purpose of use of the personal data being collected must be given to the data subject when collecting data, this includes

- Identity and contact details of the controller
- Purposes of processing
- Lawful basis for processing
- The retention period of the data
- The rights of the data subject in respect of access, rectification, erasure, restriction and objection
- The categories of personal data being collected

- The recipients of the personal data, if applicable
- Whether the data will be transferred to a third country

See the Privacy Notice procedure for more details.

Data can only be collected for specific, explicit and legitimate purposes
Data obtained for specific purposes must not be used for purposes that are different from the purpose for which it was originally obtained.

Personal data must be adequate, relevant and limited for what is necessary for purposes
The Company will ensure that it will not collect more data than is necessary to perform the processing.

Personal Data must be accurate and kept up to date with every effort to erase or rectify without undue delay
Data that is stored must be reviewed and updated as necessary. Data must not be kept unless it is reasonable to assume that it is up to date.

GDPR Owner is responsible for responding to requests for rectification within one month of receipt of the request.

GDPR Owner is responsible for ensuring that if data is rectified then all organisations that the data has been past to have been notified of the change.

Personal Data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
Personal data will only be kept for the retention period identified and recorded in the Retention policy. Once expired personal data will be securely destroyed as detailed in procedure.

Where personal data is kept beyond the processing date, it shall be encrypted/Pseudonymised and minimised, in order to protect the identity of the data subject.

GDPR Owner must specifically authorised any data retention beyond the retention periods defined in the Retention of Records procedure and must ensure that any justification is recorded and is in line with the GDPR.

Personal data must be processed in a manner that ensures the appropriate security of the data
GDPR Owner is will carry out a risk assessment taking into account all of the Company controls and processing.

GDPR Owner will assess the risks against the requirements of the company and risks to the data subjects and ensure that the risks are mitigated or signed off by the board of directors.

When assessing the appropriate level of technical controls in place to protect personal data the following will be taken into consideration:

- Password Protection
- Automatic locking of terminals
- Anti-malware protection and firewall configuration and protection
- Encryption of devices
- Security of local network

- Use of privacy technologies such as pseudonymisation and anonymisation
- Role-based access control to resources
- Control of USB devices and media

GDPR Owner will also consider the following organisational controls:

- Appropriate level of training
- Employee reliability, such as references and employee contracts
- Disciplinary action against breaches
- Monitoring of staff against the relevant standards
- Physical access to personal data in electronic and paper-based records
- Use of mobile devices to access personal data
- Paper based storage of personal data
- Clear desktop policy of personal data
- Password guidance and policies
- Organisations backup and testing processes
- Contractual obligations with third parties either importing information or exporting information
- Control of employee use of mobile devices to access personal data outside of the organisation

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)
The GDPR requires all data controllers and processor to show accountability and governance, these complement the data protection principles and allows the controller or processor to demonstrate compliance with the data protection principles

The Company will demonstrate compliance by implementing the following:

- Data Protection Policies and procedures
- Adhering to codes of conduct
- Implementing appropriate technical and organisation controls to protect the data
- Documenting the use and location of personal data in the organisation
- Adopting techniques such as privacy by design/default, Data Protection Impact Assessments, breach notification and incidence response plans
- Mapping the flows of personal data into and out of the organisation

Data Subject Rights
The organisation will have procedures in place to ensure that the data subjects rights are upheld.

- The right to access the personal information held about them, along with the purpose and legal basis for holding the data
- The right to rectify inaccurate data held about them
- The right to restrict processing of data if they suspect it is being used unlawfully
- The right to has data that is held about them erased if there is no other lawful reason to keep it
- The right to object to data being processed under legitimate interest
- The right to object to automated profiling using their personal data
- The right to raise a complaint to the ICO if they feel the Company has contravened a provision of the GDPR

If data is corrected, erased or restricted from processing, then all recipients of the data must be informed.

Data subjects have the right to complain to the Company about how their data is being handled, contact for complaints must be made clear at the point of collection of the data.

Consent

Consent must be explicit and freely given, specific, informed and unambiguous indication of the data subjects wishes.

Consent must be given with a clear affirmative action on the part of the data subject, as such pre-ticked boxes will not be used.

Consent will only be taken as given if it is understood that the data subject is fully informed on the intended purpose for the processing. Consent will not have been obtained if it been obtained under duress or by misleading information about the purpose of the processing.

There must be some form of active communication between the controller and data subject to demonstrate active consent, a non-response is not taken as consent. The Company must be able to demonstrate that consent has been given, by recording the time and date of the consent.

Retention of Data

For each piece of personal data held a record of how long the data will be retained considering all regulatory requirements around the retention of records. The retention period for the personal data in the retention policy. This retention period will be communicated to the data subject when collecting the data. The retention period will be either a fixed period of time, or a criterion for calculating the fixed period of time.

Disposal of Data

Once the retention period of the data has been reached then the data should be disposed of in a secure manner, for paper-based records this should be shredded. Electronic data should be deleted so that it is a non-trivial task to recover the data.

Security of Data

All employees are responsible for ensuring that personal data held by the Company that they have access to is kept securely and not disclosed to a third party unless the third party has been authorised by the Company by way of a contract or confidentiality agreement.

Paper based information must not be left anywhere where an unauthorised person can access them and cannot leave the business premises without explicit permission. If the records are no longer required for day-to-day processing but are still within their retention period, then they must be archived to a secure location.

Access to electronic copies of personal data is strictly controlled and only staff authorised by the access control policy will be granted access to the data.

Processing of personal data 'off-site' represents a significant risk to the data, Staff must be specifically authorised to process data off-site.

Disclosure of personal data
The Company will ensure that personal data is not disclosed to unauthorised third parties including family members, friends, government bodies and in certain circumstance the Police. All employees should exercise caution when information is requested by a third party.

All requests must be accompanied by relevant paperwork and authorised by GDPR Owner.

Transfer of data
Generally, transfer of personal data to a non-EEA country is strictly prohibited, unless explicit consent has been sort from the data subject.

Transfer of data will only occur after the controller has assessment and documented the adequacy of the country that the data will be transferred to taking into account:

- Nature of the information being transferred
- The country of the origin or destination of the information
- How the information will be used and for how long
- The laws and practises of the country including codes of practise and obligations
- Security measures that are to be taken about the data in the overseas location

Or the transfer is to a country that is deemed adequate by the European Union.

Data subject must be informed of transfers to a non-EEA country along with the safeguards that have been determined.

Information Register
The Company has established a data inventory and data flow process (NAV and Marketing) as part of its GDPR compliance. The data inventory and data flow allow the Company to determine the following:

- Business process that use personal data
- Sources of personal data
- Volume of data subjects
- Description of each piece of personal data
- Processing activity on personal data
- Maintain an inventory of personal data categories processes
- Document the purpose and justification for each piece of personal data
- The recipients of personal data
- The role of the Company in the lifecycle of the personal data
- Identify key systems and storage locations of personal data
- Identify data transfers
- Establish and record the retention period and disposal requirement for each piece of personal data

The Company will assess the level of risk to data subject associated with the processing of their personal data, and if determined, it would be appropriate will perform a Data Privacy Impact Assessment on any current or new systems. Information in the Asset Register.

Appropriate controls will be applied to mitigate any risks associated with processing of the personal data.