GDPR DATA PROTECTION [JG]

Introduction

TRP Research is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of the Company's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Company Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. An organisation that handles data on behalf of a Data Controller is called a Data Processor. The Company, as both a Data Controller and a Data Processor, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose the Company to complaints, regulatory action, fines and/or reputational damage.

The Company's Board of Directors is fully committed to ensuring continued and effective implementation of this policy, and expects all Company Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

Scope

This policy applies where a Data Subject's Personal Data is processed:

- In the context of business activities
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge)
- To actively monitor the behaviour of individuals
    - Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
        - Taking a decision about them
        - Analysing or predicting their personal preferences, behaviours and attitudes

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a baseline standard for the Processing and protection of Personal Data. Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

Definitions

Data Protection:	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority (DPA):	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law, currently the ICO in the UK.
Data Controller:	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processor:	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Identifiable Natural Person:	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Subject:	The identified or Identifiable Natural Person to which the data refers.
Personal Data:	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Consent:	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Employee:	An individual who works part-time or full-time for the Company under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Contact:	Any past, current or prospective Company client, research participant or employee.
Third Party:	An external organisation with which the Company conducts business and is also authorised to, under the direct authority of the Company, Process the Personal Data of Company Contacts.
Process, Processed, Processing:	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special Categories of Data:	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Profiling:	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Third Country:	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data. See Appendix B for a list of countries recognised as having an adequate level of legal protection.
Personal Data Breach:	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Binding Corporate Rules:	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Encryption:	The process of converting information or data into a code, to prevent unauthorised access.
Pseudonymisation:	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Anonymisation:	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
Data Protection Impact Assessment (DPIA):	A process designed to help identify and minimise the data protection risks of a project or aspect of a project.

Governance

Policy Dissemination & Enforcement

Information Asset Owners of Information Assets that contain Personal Data must ensure that all Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, each Information Asset Owner will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by the Company.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes that will process Personal Data, each of them must go through an approval process before continuing.

Each Information Asset Owner, of an asset identified as containing Personal Data must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which they have responsibility. The subsequent findings of the DPIA must then be submitted to the Technical Director for review and written approval. Where applicable, the Technology department, as part of its IT systems and application design review process, will cooperate with the Technical Director to assess the impact of any new technology uses on the security of Personal Data.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by the Company in relation to this policy, relevant compliance metrics have been built into the Company's intelligence gathering and performance monitoring systems. These compliance metrics must be completed by Information Asset Owners each month in line with the 'Management Reporting Process' as defined in the 'Levels and Development' policy. From this system the Technical Director will receive a monthly report which details the health of all of the Company's Information Assets, including the health status of any Personal Data held as part of the Information Asset. Health Status indicators include:

- Legitimate Business Activities
- Level of sensitivity of data
- Requirement for automated decision making, including profiling
- Status of procedural documentation, including DPIA's
- Review cycles

Data Protection compliance audits will be carried out in conjunction with Information Asset Owners against each Business activity as required. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities
  - Raising awareness
  - Training of Employees
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights
  - Personal Data transfers
  - Personal Data incident management
  - Personal Data complaints handling
- The level of understanding of Data Protection policies and Privacy Notices
- The currency of Data Protection policies and Privacy Notices
- The accuracy of Personal Data being stored
- The conformity of Data Processor activities
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches

Data Protection Principles

The Company has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of all Personal Data:

- **Principle 1: Lawfulness, Fairness and Transparency**
  Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the Company must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

- **Principle 2: Purpose Limitation**
  Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means the Company must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

- **Principle 3: Data Minimisation**
  Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means the Company must not store any Personal Data beyond what is strictly required.

- **Principle 4: Accuracy**
  Personal Data shall be accurate and, kept up to date. This means the Company must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

- **Principle 5: Storage Limitation**
  Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means the Company must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

- **Principle 6: Integrity & Confidentiality**
  Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. The Company must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

- **Principle 7: Accountability**
  The Data Controller shall be responsible for, and be able to demonstrate compliance. This means the Company must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- National law expressly provides for the collection, Processing or transfer of the Personal Data

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient

Data Subject Consent

The Company will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, the Company is committed to seeking such Consent.

Each Information Asset Owner, in cooperation with the Technical Director, shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract)
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given
- Providing a simple method for a Data Subject to withdraw their Consent at any time

The Company will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures (see Appendix A) will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent

The disclosures must be given electronically or in writing. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each external website provided by the Company will include an online 'Privacy Notice' and an online 'Cookie Notice' (where cookies are used) fulfilling the requirements of applicable law. All Privacy and Cookie Notices must be drafted by the Information Asset Owner/s for that website and relate to the activities of the website and then brought to both the Technical Director and the Legal Agreement Business Service for approval prior to publication on that website.

Data Use

Data Processing

The Company uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of the Company
- To provide services to the Company's clients
- To carry out primary research
- The ongoing administration and management of client services

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by the Company to respond to a Contact request for information about the services on offer. However, it will not be within their reasonable expectations that the Company would then provide their details to Third Parties for marketing purposes.

The Company will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, the Company will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child)

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and written approval must be obtained from the Technical Director before any such Processing may commence.

In any circumstance where Consent has not been gained for the specific Processing in question, the Company will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed
- The possible consequences of the intended further Processing for the Data Subject
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation

Special Categories of Data

The Company will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject
- The Processing is necessary for the establishment, exercise or defence of legal claims
- The Processing is specifically authorised or required by law
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health

In any situation where Special Categories of Personal Data are to be Processed, prior approval must be obtained from the Technical Director under Information Asset rules and the basis for the Processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being Processed, the Company will adopt additional protection measures. Each Information Asset Owner will adopt these additional measures to address specific activity over the Processing of Special Categories of Data after approval is obtained in writing from the Technical Director for the activity in question.

Children's Data

Children are unable to Consent to the Processing of Personal Data. The age at which an individual is designated to no longer be a child varies between 13 and 16 in accordance with the national law of EU member states. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Should the Company foresee a business need for obtaining parental consent for an activity that provides a service to or collects data from a child, guidance and approval must be obtained from the Technical Director before any Processing of a child's Personal Data may commence.

Data Quality

Each Information Asset Owner will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the Company to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification (may include data erase and replacement with corrected or supplemented data)
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required
- Restriction, rather than deletion of Personal Data, insofar as:
    - A law prohibits erasure
    - Erasure would impair legitimate interests of the Data Subject
    - The Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

Profiling & Automated Decision-Making

The Company will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with a client or where it is authorised by law.

Where the Company utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a human carry out a review of the automated decision
- Contest the automated decision
- Object to the automated decision-making being carried out

The Company must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

Digital Marketing

As a general rule the Company will not send promotional or direct marketing material to a Company Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Cases for carrying out a digital marketing campaign without first obtaining prior Consent from the Data Subject must be brought to and approved in writing by the Technical Director prior to commencing any such campaign.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Data Retention

To ensure fair Processing, Personal Data will not be retained by the Company for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which Information Asset Owners need to retain Personal Data is to be identified and documented for each individual project. This must take into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the Information Assets data retention schedule which is held within the Information Asset. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Each Company Directorate must adhere to the Company's 'Information Security policy', adopting the physical, technical, and organisational measures described within to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Company (the Data Controller)
- Ensure that Personal Data is protected against undesired destruction or loss
- Ensure that Personal Data collected for different purposes can be and is Processed separately
- Ensure that Personal Data is not kept longer than necessary

Data Subject Requests

Each Information Asset Owner will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing
- Data portability
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, the Company will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Company and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data
- The source(s) of the Personal Data, if it was not obtained from the Data Subject
- The categories of Personal Data stored for the Data Subject
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period
- The use of any automated decision-making, including Profiling
- The right of the Data subject to:
    - Object to Processing of their Personal Data
    - Lodge a complaint with the Data Protection Authority
    - Request rectification or erasure of their Personal Data
    - Request restriction of Processing of their Personal Data

All requests received for access to or rectification of Personal Data must be directed to the Information Asset Owner undertaking that specific activity, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate

verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If the Company cannot respond fully to the request within 30 days, it shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
- The name and contact information of the Company representative who the Data Subject should contact for follow up

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

If the Company Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If the Company receives a request from a court or any regulatory or law enforcement authority for information relating to a Company Contact, you must immediately notify the Technical Director who will provide guidance.

Data Protection Training

All Company Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training or ongoing training as part of their role.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in 'Data Protection Principles' section above
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes
- The need for, and proper use of, the forms and procedures adopted to implement this policy
- The correct use of passwords, security ID's and other access mechanisms
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person
- Securely storing manual files, print outs and electronic storage media
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises

- Proper disposal of Personal Data by using provided shredding facilities
- Any special risks associated with particular Directorate activities or duties

Data Transfers

The Company may transfer Personal Data to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection (see Appendix B) for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism (see Appendix B).

The Company may only transfer Personal Data where one of the transfer scenarios listed below applies:

- The Data Subject has given Consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the Data Subject

Internal Transfers

In order for the Company to carry out its business activities effectively, there may be occasions when it is necessary to transfer Personal Data internally from one Information Asset Owner to another. Should this occur, the transferor (the authorising Information Asset Owner) of the Personal Data remains responsible for ensuring protection for that Personal Data whilst in their care. The transferor must:

- Only transfer the minimum amount of Personal Data necessary for the specified purpose of the transfer (for example, to fulfil a transaction or carry out a particular service)
- Ensure adequate security measures are used to protect the Personal Data during the transfer (including password-protection and Encryption, where necessary).

On receipt of the any Personal Data, the transferee must use the data in accordance with the principles detailed in this policy.

Transfers to Third Parties

The Company will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, each Information Asset Owner will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, the Information Asset Owner will enter into, in cooperation with the Technical Director, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

The agreement may require the Company to protect the Data Controller's Personal Data from further disclosure and to only Process Personal Data in compliance with instructions that are stronger in scope than the Company's

existing instructions. Where stronger measures are required by the Data Controller, they must be agreed by the Technical Director prior to contract acceptance to ensure they are possible. In any case where the Data Controller requires weaker protection than is offered by the Company's existing instructions, the Company's existing instructions must be followed and this must be agreed by both the Data Controller and the Company.

Where the Third Party is deemed to be a Data Processor (including Cloud Computing service providers), the Information Asset Owner will identify whether the outsourcing will entail any Third Country transfers of that Personal Data prior to entering into any agreement with the Data Processor. If no Third Country data transfers are required, the Information Asset Owner can enter into, in cooperation with the Technical Director, an appropriate agreement with the Processor that clarifies each party's responsibilities in respect to the Personal Data transferred. If Third Country data transfers are required as part of the outsourcing, the Information Asset Owner must consult with the Technical Director.

The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Company instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

The Information Asset Owner must conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified must be reported to the Technical Director and will be reported to and subsequently monitored by the Board of Directors.

Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Company. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Company will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Company, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

Any Employee who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Technical Director providing a description of what occurred.

The Company's Board of Directors will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Company's Board of Directors will follow the relevant Data Protection Authority Guidelines based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the Company's Board of Directors will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Technical Director.