

GDPR Data Protection Policy

Table of Contents

1. Introduction.....	2
2. Scope	2
3. Definitions	2
4. Policy	4
4.1 Governance	4
4.1.1 Data Protection Administrator	4
4.1.2 Policy Dissemination & Enforcement	5
4.1.3 Data Protection by Design	5
4.1.4 Compliance Monitoring	5
4.2 Data Protection Principles	6
4.3 Data Collection	7
4.3.1 Data Sources.....	7
4.3.2 Data Subject Consent	7
4.3.3 Data Subject Notification.....	7
4.3.4 External Privacy Notices	8
4.4 Data Use	8
4.5 Data Retention.....	11
4.6 Data Protection.....	11
4.7 Data Subject Requests	12
4.8 Law Enforcement Requests & Disclosures.....	13
4.9 Data Protection Training	13
4.10 Data Transfers	14
4.11 Complaints Handling	15
4.12 Breach Reporting	15
5. Policy Maintenance	15
5.1 Publication	15
5.2 Revisions.....	15

1. Introduction

Harrogate Food and Drink Company (“the company”) 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 Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a The 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.

The Company, as a Data Controller, 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 leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all The 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. This policy has been approved by The Company’s Managing Director.

2. Scope

This policy applies to all The Company activities where a Data Subject’s Personal Data is processed:

- ✓ In the context of the business activities of The Company.
- ✓ For the provision or offer of services to individuals (including those provided or offered free-of-charge) by The Company.

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 baseline standard for the Processing and protection of Personal Data by all The Company activities. If there are conflicting requirements in this policy and national law, please consult with the Director for clarity.

3. Definitions

- “Employee” An individual who works part-time or full-time for The Company under a contract of employment or a contract for services, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
- “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 The Company Contacts.
- “Personal Data” Any information which relates to an identified or Identifiable Natural Person.
- “Contact” Any past, current or prospective Individual that The Company has or will be in contact with in the course of its business including but not limited to Employees, Temporary Workers and Client Contacts..
- “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 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.
- “The Company”
A The Company establishment, including subsidiaries and joint ventures over which The Company exercise management control.
- “Data Subject” The identified or Identifiable Natural Person to which the data refers.
- “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.
- “Data Protection”
The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
- “Data Protection Authority”
Means the Information Commissioner’s Office (ICO)
- “Data Processors”
A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
- “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.

“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.

“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.

“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.

“Encryption” The process of converting information or data into code, to prevent unauthorised access.

4. Policy

4.1 Governance

4.1.1 Data Protection Administrator

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, The Company has appointed a Data Protection Administrator (DPA). The DPA operates with independence with a suitability skilled individual granted all necessary authority.

The DPAs duties include:

- ✓ Informing and advising The Company and its Employees who carry out Processing pursuant to Data Protection regulations.
 - ✓ Ensuring the alignment of this policy with Data Protection regulations.
 - ✓ Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
 - ✓ Acting as a point of contact for and cooperating with the ICO
 - ✓ Determining the need for notifications to the ICO as a result of The Company’s current or intended Personal Data processing activities;
 - ✓ Making and keeping current notifications to the ICO as a result of The Company’s current or intended Personal Data processing activities;
 - ✓ The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
-
- ✓ Informing senior managers and directors of The Company of any potential corporate, civil and criminal penalties which may be levied against The Company and/or its Employees for violation of applicable Data Protection laws.
 - ✓ Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:

- ✓ provides Personal Data to The Company.
- ✓ receives Personal Data from The Company
- ✓ has access to Personal Data collected or processed by a The Company Entity.

4.1.2 Policy Dissemination & Enforcement

The management team of each The Company location must ensure that all The Company Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, The Company 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.

4.1.3 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, each of them must go through an approval process before continuing.

Senior Management must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the DPA, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings must then be submitted to the Managing Director for review and approval.

Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the DPA to assess the impact of any new technology uses on the security of Personal Data.

4.1.4 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all The Company activities in relation to this policy, the DPA will carry out an annual Data Protection compliance audit for all such activities.

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.

The DPA, in cooperation with key business stakeholders of The Company, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the The Company Executive Management team.

4.2 Data Protection Principles

The Company has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of 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.

4.3 Data Collection

4.3.1 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.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than 72 hours after the breach was discovered.

4.3.2 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. The DPA, in cooperation with Operations and IT (and other relevant business representatives) 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.

4.3.3 Data Subject Notification

Each The Company Entity 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 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 may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the DPA. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

4.3.4 External Privacy Notices

Each external website provided by The Company will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

4.4 Data Use

4.4.1 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 customers.
- ✓ To provide work finding services for The Company Candidates and Workers.
- ✓ The ongoing administration and management of customer 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 any potential roles or work opportunities 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 deciding as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the DPA 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.

4.4.2 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 Data are to be Processed, prior approval must be obtained from the DPA 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.

4.4.3 Children's Data

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 any The Company Entity foresee a business need for obtaining parental consent for services offered directly to a child, guidance and approval must be obtained from the DPA before any Processing of a child's Personal Data may commence.

4.4.4 Data Quality

The Company 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.
- ✓ 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.

4.4.5 Digital Marketing

As a general rule The Company will not send promotional or direct marketing material to a The Company Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any The Company Entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the DPA. 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.

4.5 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 The Company needs to retain Personal Data is set out below:

Client Files:

- ✓ These should be kept for one year from the date that our relationship with the client ended.

Candidate Files:

- ✓ For candidates we have placed in a temporary assignment, we should keep the files for three years from the last assignment date.
- ✓ For candidates we have not used or placed in a permanent role, we should keep their details for one year from the date of registration or placement.

All documents should be securely destroyed (for example by shredding).

Financial Records:

- ✓ These should be kept for six years.

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.

4.6 Data Protection

The Company will adopt physical, technical, and organisational measures 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. The minimum set of security measures to be adopted by The Company are provided in the The Company 'Information Security Policy'.

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 Data Controller.
- ✓ Ensure that Personal Data is protected against undesired destruction or loss.
- ✓ Ensure that Personal Data collected for different purposes can and is Processed separately.
- ✓ Ensure that Personal Data is not kept longer than necessary.

4.7 Data Subject Requests

The DPA will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- ✓ Information access.
- ✓ Objection to Processing.
- ✓ 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 DPA 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.

All requests received for access to or rectification of Personal Data must be directed to the DPA, 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, the DPA 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 The Company individual 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.

4.8 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 any The Company Employee receives a request from a court or any regulatory or law enforcement authority for information relating to a The Company Contact, you must immediately notify DPA who will provide comprehensive guidance and assistance.

4.9 Data Protection Training

All The 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. In addition, each The Company Entity will provide regular Data Protection training and procedural guidance for their staff.

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

- ✓ The Data Protection Principles set forth in Section 4.2 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 tokens 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 secure shredding facilities.
- ✓ Any special risks associated with particular departmental activities or duties.

4.10 Data Transfers

The Company may transfer Personal Data to Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection 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. The Company may only transfer Personal Data where one of the transfer scenarios list 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.

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 The Company Entity 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 The Company Entity will enter into, in cooperation with the DPA, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred. Where the Third Party is deemed to be a Data Processor, the The Company Entity will enter into, in cooperation with the DPA, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with The 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.

When The Company is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the

outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the DPA, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

4.11 Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the DPA. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.

The DPA 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 DPA, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the ICO.

4.12 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the DPA providing a description of what occurred. Notification of the incident can be made via e-mail, by calling or letter.

The DPA will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the DPA will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved.

For severe Personal Data Breaches, the The Company DPA will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

5. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the DPA via e-mail.

5.1 Publication

This policy shall be available to all The Company Employees through the The Company intranet or via alternative means as deemed appropriate by the DPA.

5.2 Revisions

The DPA is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to The Company Employees through the Human Resources department.