TINDER CORP
TECHNOLOGY TO IGNITE YOUR BUSINESS

DATA PROTECTION POLICY

GDPR Version

Date of Publication	24 April 2018
Date of Review	24 April 2020
Approved by	Corporation
Revision Number	001

Throughout this document the Company and Employer shall mean Tinder Corporation Ltd.

1. POLICY STATEMENT

Tinder Corporation Ltd 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 Tinder Corporation Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Tinder Corporation 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. Tinder Corporation, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Tinder Corporation to complaints, regulatory action, fines and/or reputational damage.

Tinder Corporation's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Tinder Corporation 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.

2. SCOPE

This policy applies to all Company entities where a data subject's personal data is processed:

- In the context of the business activities of the Company.
- To fulfil an agreement/contract
- 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 standard for the processing and protection of personal data by the Company. 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. If there are conflicting requirements in this policy and national law, please consult with a Director for guidance.

3. KEY DEFINITIONS

Employee – An individual who works part-time or full-time for the Company under a contract of employment. This includes temporary employees.

Third Party – An external organisation with which the Company conducts business and is also authorised to, under the direct authority of the Company to process the personal data of Tinder Corporation Ltd contacts.

Consultant/Contractor – Freelance consultants/contractors are self-employed. They may work on a freelance basis for a variety of companies.

Personal Data – Any information (including opinions and intentions) which relates to an identified or identifiable natural person.

Contact – Any past, current or prospective Company customer or supplier and any data that we process on their behalf.

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.

Company – A Company establishment, including subsidiaries and joint ventures over which the Company exercises 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 – An independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in national law.

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 Personal Data – 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.

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.

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.

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.

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.

4. GOVERNANCE

4.1 DIRECTOR RESPONSIBILITY

Directors duties include:

- Informing and advising the Company on Data Protection regulations, national law or European Union based Data Protection provisions;
- Ensuring the alignment of this policy with Data Protection regulations, national law or European Union based Data Protection provisions;
- Providing guidance on carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs because of the Company's current or intended Personal Data processing activities;
- Making and keeping current notifications to one or more DPAs because 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 managers, officers, 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 the 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 the Company

4.2 DISSEMINATION & ENFORCEMENT

Directors and Line Managers should ensure that all Company Employees 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.

4.3 DATA PROTECTION BY DESIGN

To ensure that all Data Protection requirements are identified and addressed, the Company will ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with a Director, for all new and/or revised systems or processes. The subsequent findings of the DPIA will be reviewed and approved by a Director.

Where applicable, the IT department, as part of the software system and application design review process, will cooperate with a Director to assess the impact of any new technology uses on the security of Personal Data.

4.4 COMPLIANCE MONITORING

A Director will continually audit compliance to ensure that the Company is sufficiently compliant with this policy. This audit will assess:

- Compliance with the Policy in relation to the protection of Personal Data, including:
- The assignment of responsibilities.
- Training and awareness including the level of understanding around Data Protection policies and privacy notices
- The effectiveness of Data Protection related operations, including:
- data Subject rights.
- data transfers.
- incident management.
- complaints handling.
- The accuracy 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.

A Director will devise a plan for correcting any identified deficiencies within a defined and reasonable time frame

5. DATA PROTECTION PRINCIPLES

The following principles from the General Data Protection Regulation (GDPR) govern the Company's collection, use, retention, transfer, disclosure and destruction of Personal Data:

5.1 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:

- Transparency-the Company must tell the Data Subject what Processing will occur.
- Fairness-the Processing must match the description given to the Data Subject.
- Lawfulness-It must be for one of the purposes specified in the applicable Data Protection regulation.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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 always.

5.7 PRINCIPLE 7: ACCOUNTABILITY

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

6. DATA COLLECTION

6.1 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 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.
- A 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.

6.2 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.

A Director shall ensure that where possible Provenance is activated on all data capture points for the purposes of documenting consent from a Data Subject.

6.3 DATA SUBJECT NOTIFICATION

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

6.4 EXTERNAL PRIVACY NOTICES

Each Company website will include an online privacy Policy which contains a cookie policy fulfilling the requirements of applicable law. All privacy and cookie policies/notices must be approved by a Director prior to publication on any Company website.

7. DATA USE

7.1 DATA PROCESSING

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

- The administration of the Company
- To provide services to clients
- The ongoing administration and management of client relationships
- To fulfil the contract/agreement between the Company and a client

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 Company to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that 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 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 approval must be obtained from a 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.

Note: Staff should refer to the Employee Privacy Notice for more information about the processing of staff personal data.

7.2 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 a Director 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.

7.3 CHILDREN'S DATA

Children are unable to Consent to the Processing of Personal Data and Consent must be sought from the person who holds parental responsibility over the child. Consent need not be obtained from either the child or the holder of parental responsibility where Processing is lawful under other grounds, guidance and approval must be obtained from a Director before any Processing of a child's Personal Data may commence.

7.4 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.

7.5 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 the Data Subject 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.

7.6 DIGITAL MARKETING

In general, the Company will not send promotional or direct marketing material to a Company Contact through digital channels such as the Internet, mobile phones and email without first obtaining their Consent. Any digital marketing campaign that is intended to be carried out without obtaining prior Consent from the Data Subject must first be approved by a Director.

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. Furthermore, if they request deletion, a copy of their PII (Personal Identifiable Information) should be kept in a hashed state so that, in the event of a Subject Access Request following deletion, we can locate their record. This is stored alongside their Lead ID, the date their data was deleted, the date they opted in and the source of opt in, so that in the event of a Subject Access Request the complaint/deletion form can be easily located with the details of the complaint/request.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no current 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. If the legislation changes, a Director will update the policy and educate the Company accordingly.

8. 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 in the Company 'Retention Schedule'. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule.

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

9. DATA PROTECTION

The Company has 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 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 being transmitted electronically 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

10. DATA SUBJECT REQUESTS

Data Subjects have rights in relation to:

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

Where a Company entity has been identified by a Director or Line Manager as a Data Controller, they will be advised of and will follow their own specific subject access request handling procedure.

In the unlikely event that a subject access request is received in relation to a client or an external body, these requests should be referred to a Director who will then liaise with the relevant client to resolve the request. The Director will follow the approved Subject Access Request Handling procedure.

For details about subject access requests from past/present members of staff, please refer to the Employee Privacy Notice

11. 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 you receive a request from a court or any regulatory or law enforcement authority for information relating to a Company Contact, you must immediately notify a Director who will provide guidance and assistance.

12. DATA PROTECTION TRAINING

All Company Employees will have their responsibilities under this policy outlined to them as part of their induction. In addition, regular Data Protection training and procedural guidance will be provided to staff.

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

- GDPR training which includes the Data Protection Principles.

- 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 adherence to this policy.
- The correct use of passwords and other access mechanisms.
- The importance of limiting access to Personal Data.
- The importance of securely storing information irrespective of format.
- The requirement to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- The proper disposal of Data (for example using a shredder)
- Any special risks associated with particular business activities

13. 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 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 to protect the vital interests of the Data Subject.

13.1 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, the Company 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 Company will enter into, in cooperation with a Director, 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 Company will enter into, in cooperation with a Director, 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 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 a Director, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

A Director shall 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 will be monitored by a Director.

14. COMPLAINTS HANDLING

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

15. 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 a Director providing a description of what occurred.

The Director will investigate all reported incidents to confirm whether a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Director will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved.

16. POLICY MAINTENANCE

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

17. PUBLICATION

This policy shall be issued to all Company Employees.

17.1 EFFECTIVE DATE

This policy is effective as of 25 May 2018.

17.2 REVISIONS

A Director is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to Company Employees.

APPENDIX A – INFORMATION NOTIFICATION TO DATA SUBJECTS

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.	✓	✓
The Original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.		✓
The contact details of the Data Protection Officer, where applicable.	✓	✓
The purpose(s) and legal basis for Processing the Personal Data.	✓	✓
The categories of Personal Data concerned.	✓	✓
The recipients or categories of recipients of the Personal Data.	✓	✓
Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.	✓	✓
Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.	✓	✓
The existence of Data Subject rights allowing them to request from the Data Controller- information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.	✓	✓
Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.	✓	
The right to lodge a complaint with a Data Protection Authority.	✓	✓
The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.	✓	✓
Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.	✓	✓

APPENDIX B – ADEQUACY FOR PERSONAL DATA TRANSFERS

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

EU Countries		
Austria	Germany	Poland
Belgium	Greece	Portugal
Bulgaria	Hungary	Romania
Croatia	Ireland	Slovakia
Republic of Cyprus	Italy	Slovenia
Czech Republic	Latvia	Spain
Denmark	Lithuania	Sweden
Estonia	Luxembourg	United Kingdom
Finland	Malta	
France	Netherlands	
Other		
Andorra	Iceland	New Zealand
Argentina	Isle of Man	Norway
Canada (commercial organisations)	Israel	Switzerland
Faeroe Islands	Jersey	United States (Privacy Shield certified organisations)
Guernsey	Liechtenstein	Uruguay

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

Appropriate safeguards

- Model clauses
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms

Derogations

- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- DPA approved contracts between Data Controllers and Data Processors.