Data Policy			
Author:	Emma Lister		
Approving member of staff:	Paul Hayes	**Latest approval date:**	13/09/2023
Revision frequency:	Annual	**Next review date:**	September 2024
Live version number:	1.1		
SharePoint Location:	Documents > Governance > Policies and Procedures > Live Documentation		
Confidentiality:	Public		

Document History/Version Control		
Version	**Date**	**Notes on Revision**
1.0	August 2020	Originally written by Emma Lister.
1.1	17/09/2020	Document reviewed by Paul Hayes and Ellie South
1.1	07/09/2021	Document reviewed by Paul Hayes and Sonal Mittoo

Contents

Data Policy

Introduction

This Policy sets out the obligations of Tinder Corporation Limited regarding data protection and the rights of employees, agents, contractors or other parties working on behalf of the business as well as clients, prospective clients ("data subjects") in respect of their personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, and any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to employees, agents, contractors or other parties working on behalf of the business, as well as clients, prospective clients used in our business for our commercial purposes;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom the Company holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;

"personal data breach"	means 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;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as 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;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

Scope

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Company's Data Protection Officer is Paul Hayes. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

All managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for assisting us in ensuring that the data protection principles are applied to all that we do. All parties working on behalf of the Company are required to help us to meet our data protection obligations.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and/or process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The law sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance.

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for ensuring that all personal data is:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to

ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

e) 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. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the law in order to safeguard the rights and freedoms of the data subject;

f) 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, using appropriate technical or organisational measures.

The Rights of Data Subjects

Data Protection Law sets out the following key rights applicable to data subjects:

a) The right to be informed;

b) the right of access;

c) the right to rectification;

d) the right to erasure (also known as the 'right to be forgotten');

e) the right to restrict processing;

f) the right to data portability;

g) the right to object; and

h) rights with respect to automated decision-making and profiling.

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for ensuring that the rights of data subjects are maintained.

To ask the business to take any of these steps, a request should be sent to the Data Protection Officer. Any employees, agents, contractors, or other parties working on behalf of the Company who receives such a request from a third party must ensure that this request is sent to the Data Protection Officer immediately following receipt.

Lawful, Fair, and Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, that the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the 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; or

f) the 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 fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

n) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

o) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

p) 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;

q) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

r) the processing relates to personal data which is manifestly made public by the data subject;

s) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

t) the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

u) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

v) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high

standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

w) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for ensuring that personal data is only used for the lawful purposes for which it has been collected.

Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

a) Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

b) Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

c) Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

d) If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

e) If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

f) In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for ensuring that the above principles are applied across all data processing activities.

Any questions or concerns regarding the issue of consent and the collection, holding and/or processing of personal data should be addressed to the Data Protection Officer.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data as set out in the section *Personal Data Collected, Held and Processed* of this Policy. This includes personal data collected directly from data subjects**.**

The Company only collects, processes, and holds personal data for the specific purposes set out in the section *Personal Data Collected, Held and Processed* of this Policy (or for other purposes expressly permitted by law).

All employees, agents, contractors, or other parties working on behalf of the Company are responsible for ensuring that personal data is only used for the lawful purposes for which it has been collected.

Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to the section *Keeping Data Subjects Informed* for more information on how this should be achieved.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed). (See sections relating to *Specified, Explicit and Legitimate Purposes* and *Personal Data Collected, Held and Processed* for more information).

Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

Accuracy of Data and Keeping Data Up-to-Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in the section *Rectification of Personal Data* below.

Employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure the accuracy of personal data is checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps must be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Retention Periods

Formal or official records. Any data that is part of any of the categories listed in the Record Retention Schedule below, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Records Management Officer.

Disposable information

The Record Retention Schedule below will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

Personal data

Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule below, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, we will take into account the principle of storage limitation when deciding whether to retain this data.

What to do if data is not listed in the Record Retention Schedule?

If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Data Controller.

TYPE OF DATA	RETENTION PERIOD
Personal Employee Data	
Recruitment records These may include: • Completed online application forms or CVs. • Equal opportunities monitoring forms. • Assessment exercises or tests. • Notes from interviews and short-listing exercises. • Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.)	Six months after notifying candidates of the outcome of the recruitment exercise.

TYPE OF DATA	RETENTION PERIOD
• Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	
Immigration Checks	Three years after the termination of employment.
Contracts These may include: • Written particulars of employment. • Contracts of employment or other contracts. • Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Collective Agreements Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and Wage Records • Payroll and wage records • Details on overtime. • Bonuses. • Expenses. • Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
• Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
• PAYE Records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
• Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
• Travel and subsistence.	While employment continues and for seven years after employment ends.
• Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel Records	While employment continues and for seven years after employment ends.

TYPE OF DATA	RETENTION PERIOD
These include: • Qualifications/references. • Consents for the processing of special categories of personal data. • Annual leave records. • Annual assessment reports. • Disciplinary procedures. • Grievance procedures. • Death benefit nomination and revocation forms. • Resignation, termination and retirement.	
<u>Records in connection with working time</u>	
• Working time opt-out	Three years from the date on which they were entered into.
• Records to show compliance, including: • Time sheets for opted-out workers. • Health assessment records for night workers.	Three years after the relevant period.
<u>Maternity Records</u> These include: • Maternity payments. • Dates of maternity leave. • Period without maternity payment. • Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
<u>Accident Records</u> These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.
Personal Customer Data	
• Personal information (i.e. address, contact information) • Sales Records • Confidential Emails	As long as the individual is a customer of the company plus seven years.
• Bank details	As soon as the customer ceases to be a customer.
Planning Data	
• Planning Data	Seven years
Health and Safety	
• Records of major accidents and dangerous occurrences	Seven years
Company and Accounting Records	

TYPE OF DATA	RETENTION PERIOD
Records about the company Details of: • directors, shareholders and company secretaries • the results of any shareholder votes and resolutions • promises for the company to repay loans at a specific date in the future ('debentures') and who they must be paid back to • promises the company makes for payments if something goes wrong and it's the company's fault ('indemnities') • transactions when someone buys shares in the company • loans or mortgages secured against the company's assets	Seven years
Register of 'people with significant control' You must also keep a register of 'people with significant control' (PSC). Your PSC register must include details of anyone who: • has more than 25% shares or voting rights in your company • can appoint or remove a majority of directors • can influence or control your company or trust You still need to keep a record if there are no people with significant control.	Seven years
Accounting records You must keep accounting records that include: • all money received and spent by the company • details of assets owned by the company • debts the company owes or is owed • stock the company owns at the end of the financial year • the stock takings you used to work out the stock figure • all goods bought and sold • who you bought and sold them to and from (unless you run a retail business)	You must keep records for 6 years from the end of the last company financial year they relate to, or longer if: • they show a transaction that covers more than one of the company's accounting periods • the company has bought something that it expects to last more than 6 years, like equipment or machinery • you sent your Company Tax Return late • HMRC has started a compliance check into your Company Tax Return

TYPE OF DATA	RETENTION PERIOD
You must also keep any other financial records, information and calculations you need to prepare and file your annual accounts and Company Tax Return. This includes records of: • all money spent by the company, for example receipts, petty cash books, orders and delivery notes • all money received by the company, for example invoices, contracts, sales books and till rolls • any other relevant documents, for example bank statements and correspondence	
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.]

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided below.

All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

For the avoidance of doubt, no employees, agents, contractors, or other parties working on behalf of the Company must not access personal data that they do not have authority to access or for purposes other than those that have been authorised; treat personal data carelessly, not disclose data except to individuals (whether inside or outside the business) who have appropriate authorisation.

Accountability and Record-Keeping

The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please see below further information).

All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the Company collects, holds, and processes personal data;

c) the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

d) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

e) details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) details of personal data storage, including location(s);

g) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

A failure to observe the requirements of this policy may amount to a disciplinary offence, which will be dealt with under the Company's Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Keeping Data Subjects Informed

The Company shall provide the information set out in the privacy notice to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see section relating to *Transferring Personal Data to a Country Outside the EEA* for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the law;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the law);

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

All employees, agents, contractors, or other parties working on behalf of the Company must familiarise themselves with the relevant Privacy Notices. Any questions relating to the Company's privacy notices should be addressed to the Data Protection Officer.

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form (Employee), sending the form to the Company's Data Protection Officer.

Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Company's Data Protection Officer.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that any subject access request received from a former/current or prospective client, or any other party, is submitted using the standard form, Subject Access Request Form (General), sending the form to the Company's Data Protection Officer.

Please note: if a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administration cost of responding to the request. A subject access request is likely to be unfounded if it is made with the intention of harassing the Company or causing disruption, or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is excessive or unfounded, the Company will notify them that this is the case and whether or not it will respond to it. The decision as to whether or not a request is excessive or unfounded rests with the Data Protection Officer.

Please note: it is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under the Company's Disciplinary Procedure, which could result in dismissal.

Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that any request received relating to the rectification of personal data is

sent to the Company's Data Protection Officer immediately. The Data Protection Officer will advise as to the steps that need to be taken.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that inaccurate data is rectified in accordance with the requirements of the Data Retention Policy.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see below for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation**.**

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that any request received relating to the erasure of personal data is sent to the Company's Data Protection Officer immediately. The Data Protection Officer will advise as to the steps that need to be taken.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that data is erased in accordance with the requirements of the Data Retention Policy.

Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall

be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that any request received relating to restrict the processing of personal data is sent to the Company's Data Protection Officer immediately. The Data Protection Officer will advise as to the steps that need to be taken.

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling).

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

Direct Marketing

The Company is subject to certain rules and regulations when marketing its products and services**.**

The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.

The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that any object to direct marketing that is received is sent to the Company's Data Protection Officer immediately. The Data Protection Officer will advise as to the steps that need to be taken.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company

Type of Data	Purpose of Data
Full Name(s)	Customer account information to enable us to provide sales, consultancy & support services
Address	Customer account information to enable us to provide sales, consultancy & support services
Telephone Number(s) (mobile/landline)	Customer account information to enable us to provide sales, consultancy & support services
Email Address	Customer account information to enable us to provide sales, consultancy & support services
Bank, Account and Sort codes	For the processing of Direct Debit payments, governed under the Direct Debit Guarantee and processed via approved partner "Go Cardless" (Staff) – For payroll purposes.
Credit Card Details	For the processing of credit card payments, processed via approved partner "Stripe" – all details are provided via client/end user directly to Stripe and are not held on file by Tinder Corporation Ltd
Date Of Birth	To enable the sending of birthday greetings/cards
Next Of Kin Contact Information (Staff Only)	For emergency contact
Passport details (Staff Only)	To prove Right To Work in The UK as required by law.
Driving license details (Staff Only)	To confirm identity and for driving at work purposes where applicable.
National Insurance Number (Staff Only)	For payroll purposes
Signature (Staff Only)	For internal use (various) as agreed by staff.

Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

a) All electronic copies of personal data should be stored securely using passwords and data encryption;

b) All hard-copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

c) All personal data stored electronically should be backed up regularly with backups. All backups should be encrypted;

d) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

e) No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy, the Bring Your Own Device Policy and of the law (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that the above principles are applied.

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy. If in doubt, guidance may also be sought from the Data Protection Officer.

Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from their manager – who may be required to seek prior approval for access from the Data Protection Officer;

b) No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of their manager – who may be required to seek prior approval for access from the Data Protection Officer;

c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

e) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the employee, agent, contractor, or other party working on behalf of the Company and who is managing the marketing activity to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that the above principles are applied.

Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

d) No software may be installed on any Company-owned computer or device without the prior approval of the Data Protection Officer.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that the above principles are applied.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c) All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

e) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

f) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

g) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

h) All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

i) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

j) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

k) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the

processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;

Please note: where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Please note: a failure on the part of an employee to observe the requirements of this policy may amount to a disciplinary offence, which will be dealt with under the Company's Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) the transfer is made with the informed and explicit consent of the relevant data subject(s);

d) the transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

e) the transfer is necessary for important public interest reasons;

f) the transfer is necessary for the conduct of legal claims;

g) the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

All employees, agents, contractors, or other parties working on behalf of the Company have a responsibility to ensure that no data is transferred outside of the EEA except in compliance with

the law and authorisation of the Data Protection Officer.

Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Officer using the Data Protection Breach Reporting Form.

A data protection breach occurs when personal data (which includes any information that allows an individual to be identified), is processed without authorisation, and / or in a manner which may result in its security being compromised. For the purposes of this policy, a data protection breach includes both a confirmed and suspected breach.

Most commonly, a data protection breach occurs as a result of human error, theft, unauthorised access, equipment failure, hacking or loss.

Examples of common data protection breaches include:

Type	**Example**
Technical	Data Corruption Malware Corrupt Code Hacking
Physical	Unescorted visitors in secure areas Break-ins to site(s) Thefts from secure site(s) Theft from unsecured vehicles/premises Loss in transit/post Loss / misplacing memory stick/flash drive Confidential papers left on public transport
Other	Data input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures (including verbal)

If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained. Data Protection Breach Reporting form should be completed to the fullest extent possible and submitted to the Data Protection Officer. (The form is designed to help record in full details concerning the breach)

The form should be completed and submitted as soon as possible and in any event within 2 hours of the discovery of the breach. Should help be required to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email. In any event, data breach notifications must include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Once a data protection breach has been reported, an initial assessment will be made by the Data Protection Officer. The assessment will consider the content, quality of data involved, the potential impact and the risks associated with the breach.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described above – e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Not all data protection breaches will result in formal ICO reporting action. Some will be false alarms or "near miss" events that do not cause immediate harm to individuals or the business. However, false alarms and "near miss" events should still be reported, as analysis of these instances will provide valuable process feedback and opportunity for continual improvement.

The Company has a responsibility to ensure that all data protection breaches are recorded. Therefore, all incidents will be logged by the Data Protection Officer in the Company's Data Protection Breach Register.

Implementation of Policy

This Policy shall be deemed effective as of 17th September 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.