BENDER DATING LIMITED

DATA PROTECTION POLICY

Effective Date of Policy: 17th July 2021

Contents

1 Introduction & Key Definitions

Bender Dating Limited ("Bender Dating") is committed to conducting its business in accordance with all Data Protection laws and regulations and in line with the highest standards of ethical conduct.

The main Data Protection law relevant for the purposes of this Policy is the General Data Protection Regulation (EU) 2016/679, as applicable to the United Kingdom (the "GDPR"). Also applicable is the Data Protection Act 2018.

Under the GDPR, the following defined terms are used. These terms are also used in this Policy.

> 'Personal Data' is any information (including opinions and intentions) which relates to a Data Subject.
>
> 'Process' is given a very wide meaning under the GDPR and includes any operation or set of operations which is performed on Personal Data (whether or not by automated means) and includes collecting, recording, organising, adapting, retrieving, erasing and even just storing Personal Data (and in this Policy the terms 'Processing', 'Processes' and Processed' apply accordingly).
>
> 'Data Subject' is a living person who is identified or who could be identified, directly or indirectly (including by reference to a name, an identification number, location data, or various other factors).
>
> 'Controller' is a person or organisation who or which (whether alone or jointly with others) determines the purposes and means of the Processing of Personal Data.
>
> 'Processor' is any person or organisation who or which Processes Personal Data on behalf of the Controller.
>
> 'Personal Data Breach' is a breach of security leading to the accidental or unlawful destruction, loss or alteration of Personal Data, or unauthorised disclosure of or access to Personal Data.

Personal Data are subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may Process Personal Data.

Bender Dating, as a Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this Policy. Some of the requirements outlined in this Policy will also apply when Bender Dating is a Processor and (subject to acting in accordance with the Controller's instructions and the terms of the contract between Bender Dating and the Controller) the relevant safeguards and requirements in this Policy should also be observed when Bender Dating operates in that capacity.

2 Policy Objectives

This is the Data Protection Policy for Bender Dating.

The objective of this Policy is to ensure that all colleagues have a clear understanding of their responsibilities in achieving and maintaining GDPR compliance and managing and controlling the associated risks. It is also intended to promote awareness throughout Bender Dating of the importance of compliance with the regulations and of the standards and values underpinning the GDPR.

The effectiveness of this Policy will be reviewed regularly, to ensure it keeps up to date with developments in the law and Bender Dating's strategy for managing and protecting Personal Data.

Failure to comply with the regulations and ineffective management or control of Data Protection poses several risks including:

- legal and/or regulatory sanctions;
- financial loss;
- loss of contracts with subscribers and suppliers; and
- reputational damage.

Ultimately, failure to comply with Data Protection laws could result in Bender Dating being prohibited from Processing any Personal Data, which would effectively mean it could no longer operate.

3 Scope

This Policy applies to Bender Dating and all colleagues within any part of the organisation (including its affiliated companies) and applies in respect to all activities, including those relating to outsourced providers and other external contractors.

For the purposes of this Policy, the term "colleague" includes (but is not limited to) an individual who has entered into a contract of employment, as well as independent contractors, agency staff, outsourced service suppliers, consultants and third parties contracting on behalf of Bender Dating and all associated companies.

This Policy applies to all Processing of Personal Data in electronic form, including electronic mail and documents created with word processing software, or where data are held in manual files that are structured in a way that allows ready access to information about Data Subjects.

This Policy has been designed to establish a standard for the Processing and protection of Personal Data by Bender Dating. Where any applicable law imposes a requirement which is stricter than imposed by this Policy, the requirements in law must be followed. Furthermore, where applicable law imposes a requirement that is not addressed in this Policy, the relevant law must be adhered to. If there are conflicting requirements in this Policy and applicable law, please consult with the Data Protection Manger for guidance.

If a colleague is in any doubt as to whether any information or data is Personal Data and/or about the scope and application of this Policy, they should contact the Data Protection Officer for guidance.

4 Responsibilities

4.1 Directors

The Directors are ultimately responsible for ensuring that this Policy remains up to date and is implemented effectively, ensuring that all colleagues responsible for the Processing of Personal Data are aware of and comply with the contents of this Policy.

4.2 Line Management

Relevant management personnel are responsible for managing Data Protection Risk arising in their areas of responsibility. This includes:

- ensuring that colleagues fully understand this Policy and are able to apply this Policy's standards within their business function;
- ensuring that colleagues complete any applicable Data Protection training;
- taking responsibility for the ongoing assessment and management of identified Data Protection risks within their business area; and
- working in conjunction with Bender Dating's legal advisors and the Data Protection Officer, as applicable, to ensure that all third parties who process Personal Data on behalf of Bender Dating are compliant with this Policy.

Line Managers are responsible for designing, implementing and operating controls that ensure the Information Security Policy is adhered to in their area, in addition to the requirements of this Policy.

5 Data Protection Officer

To demonstrate the commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, Bender Dating has appointed a Data Protection Officer. The contact details of the Data Protection Officer are set out at the end of this Policy, in section 19.

The Data Protection Officer reports to the Directors and their duties include:

- determining the need for registration with one or more supervisory authorities as a result of Bender Dating's current or intended Processing activities (and maintaining any requisite registrations);
- acting as the first point of contact for supervisory authorities and Data Subjects;
- cooperating with supervisory authorities;
- informing and advising Bender Dating and colleagues who carry out Processing about their obligations to comply with the GDPR and other applicable Data Protection laws;
- ensuring the alignment of this Policy with applicable laws;
- providing advice and guidance with regards to carrying out a Data Protection Impact Assessment ("DPIA");
- assisting and consulting when projects are initiated after a DPIA to ensure that all relevant Data Protection requirements are observed;
- establishing and operating policies and procedures to provide prompt and appropriate responses to Data Subject requests;
- informing the Directors of any potential civil and criminal penalties which may be levied against Bender Dating and/or its employees for violation of applicable Data Protection laws;
- ensuring establishment of procedures and implementation of standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides Personal Data to Bender Dating;
- receives Personal Data from Bender Dating; and/or
- has access to Personal Data collected or Processed by Bender Dating;

- promoting and maintaining awareness of this Policy and the Data Protection laws;
- training employees and/or ensuring that appropriate training programmes are in place for employees regarding the Data Protection laws; and
- auditing and monitoring compliance with this Policy and Data Protection laws, including managing internal Data Protection activities and conducting internal audits;

6 Data Protection Principles

The GDPR sets out the following six principles to govern the collection, use, retention, transfer, disclosure and destruction of Personal Data. Bender Dating must comply with these principles and must also be able to demonstrate that it complies.

6.1 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 - Bender Dating must tell the Data Subject what Processing will occur and give appropriate 'fair processing' notices/Privacy Notices (as set out further below, including by way of Bender Dating's Privacy Policy);
- Fairness - the Processing must accord with the description given to the Data Subject; and
- Lawfulness - there must be legitimate grounds for collecting and using the personal data, in accordance with one of the purposes specified in the GDPR.

6.2 Principle 2: Purpose

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 Bender Dating must specify why Personal Data are being collected and what will be done with that Personal Data (including giving appropriate 'fair processing' notices/Privacy Notices) and must limit the Processing of that Personal Data to only what is necessary to meet the specified purpose (unless it has other lawful grounds for the Processing).

6.3 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 Bender Dating must:

- obtain and use Personal Data that are sufficient for the purposes the Personal Data is needed for; and

- not hold more information than is required for that purpose.

6.4 Principle 4: Accuracy

Personal Data shall be accurate and kept up to date and every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

This means Bender Dating must take steps to ensure the accuracy of any Personal Data it obtains (checking the source of the information if appropriate) and have in place processes for identifying and addressing out-of-date and incorrect Personal Data (including to deal with any challenges to the accuracy of information).

6.5 Principle 5: Retention

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 are Processed.

This means Bender Dating must have in place processes to review the length of time Personal Data are kept (having regard to the purpose or purposes they are held), to update, archive or securely delete information if it goes out of date and to securely delete information that is no longer needed.

6.6 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, using appropriate technical or organisational measures.

This means Bender Dating must have appropriate security to prevent Personal Data from being compromised, ensuring that appropriate technical and organisational measures are in place to ensure that the integrity and confidentiality of Personal Data is maintained at all times.

Bender Dating needs to design and organise its security to fit the nature of the Personal Data held and the harm that may result from a Personal Data Breach (which will include having regard to any 'special categories' of Personal Data as referred to in section 7.2). Apart from having the right physical and technical security, Bender Dating must ensure this is supported by robust policies and procedures (and reliable, well-trained staff).

7 Sources and Types of Personal Data

7.1 Data Sources

Bender Dating should collect Personal Data only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.

- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

- Bender Dating is acting as a Processor on behalf of a Controller.

7.2 Special Categories of Personal Data

The GDPR refers to ‘special categories’ of Personal Data (also sometimes referred to as ‘sensitive’ Personal Data), which means the following categories of data:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life or sexual orientation;
- genetic data; and
- biometric data where processed to uniquely identify a person.

The Processing of special categories of Personal Data is prohibited by law, with certain exemptions. Accordingly, Bender Dating will not Process special categories of Personal Data unless any of the following conditions are met:

- the Data Subject has given explicit consent to the Processing of those special categories of Personal Data, for one or more specified purposes (unless any applicable law provides that the Data Subject cannot give consent as an exception to that general prohibition);
- the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law or a collective agreement;
- 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;
- the Processing relates to Personal Data which are manifestly made public by the Data Subject; or
- the Processing is necessary for the establishment, exercise or defence of legal claims.

There are also additional rules applicable to the Processing of Personal Data relating to criminal convictions or offences. Data Bending will treat this Personal Data in the same way as the special categories of Personal Data outlined above.

If a colleague is in any doubt about the Processing of special categories of Personal Data, the Data Protection Officer must be consulted for guidance.

8 Data Collection - Information to be given to Data Subjects

When Bender Dating is acting as Controller, the Data Subject must be given certain information about the collection and use of their Personal Data, regardless of whether Personal Data are collected from the Data Subject or from someone other than the Data Subject. A list of the disclosures that need to be made available to the Data Subject is provided in Appendix 1.

When the Personal Data are obtained directly from the Data Subject, that information has to be provided at the time the Personal Data are obtained.

When the Personal Data are not obtained directly from the Data Subject, that information has to be provided:

- within a reasonable period of having obtained the Personal Data (but no later than one month from when the Personal Data was obtained); or
- if the Personal Data are used to communicate with the Data Subject, no later than when the first communication takes place; or
- if the Personal Data are to be disclosed to another recipient, before the data are disclosed.

9 Lawful Processing & Disclosures

9.1 Data Subject Consent

Bender Dating will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and consent of the Data Subject. Where a need exists to request and receive the consent of a Data Subject prior to the collection, use or disclosure of their Personal Data, Bender Dating will ensure that such consent is obtained.

The Data Protection Officer, in consultation with other relevant business representatives, shall establish policies and procedures for obtaining and documenting Data Subjects' consent for the collection, Processing and/or transfer of their Personal Data. The policies and procedures must include provisions for:

- determining what disclosures should be made in order to obtain valid consent;
- ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language;
- ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract);
- documenting the date, method and content of the disclosures made and the consents given; and
- providing a simple method for a Data Subject to withdraw their consent at any time.

9.2 Other Grounds

The consent of a Data Subject to Process their Personal Data is only one ground on which Bender Dating may lawfully Process any Personal Data. Other grounds on which Personal Data may be Processed (without the consent of a Data Subject) include:

- the Processing is necessary for the performance of a contract to which the Data Subject is party or is necessary in order to take steps (at the request of the Data Subject) prior to entering into a contract;
- the Processing is necessary for compliance with a legal obligation to which Bender

Dating (as a Controller) is subject;

- the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; and

- the Processing is necessary for the purposes of the legitimate interests pursued by Bender Dating (as a Controller) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of the Personal Data.

Accordingly, Bender Dating may be permitted (or required) to Process Personal Data in various circumstances. If a colleague is in any doubt as to whether any Personal Data can be lawfully Processed, they should contact the Data Protection Officer for guidance before undertaking any such Processing.

In some circumstances, Bender Dating may receive a request from a court or any regulatory or law enforcement authority (including the Police) for information relating to a Data Subject. In these circumstances, the Data Protection Officer must be immediately notified and they will provide guidance and assistance.

10 Privacy Notices

Bender Dating's Privacy Policy (also known as a 'fair processing' notice) sets out details of how Bender Dating collects and otherwise Processes any Personal Data.

The Privacy Policy will be brought to the attention of Data subjects at the appropriate point, in accordance with the requirements outlined above.

Bender Dating's app and website will also include its Privacy Policy and an online 'Cookie Notice' fulfilling the requirements of applicable law.

11 Data Subject Rights

The Data Protection Officer will establish policies and procedures to enable and facilitate the exercise of Data Subject rights set out below.

Section 11.9 sets out the timescales and other information requirements which Bender Dating must comply with regarding the exercise of each of those rights, together with details about the circumstances when charges can be levied.

If a request is received relating to any of the rights listed above, Bender Dating will consider each such request in accordance with all applicable Data Protection laws and regulations (and having regard to the relevant provisions of this Policy).

Bender Dating must verify the identity of the person making the request, using "reasonable means". Appropriate verification must confirm that the requestor is the Data Subject or is authorised to make the request on their behalf. Bender Dating should not provide any information or take any action in response to a request pending verification of such identity or authority, because of the risk of disclosing information to someone who is not entitled to it. Where Bender Dating has reasonable doubts concerning the identity and/or authority of the person making the request, Bender Dating may request the provision of additional information necessary to confirm this.

All requests received must be directed to the Data Protection Officer, who will log each request as it is received and deal with it accordingly.

11.1 Right of Access

Data Subjects have the right to obtain:

- confirmation that their Personal Data are being Processed;
- access to their Personal Data; and
- other supplementary information (which largely corresponds to the information that should be provided in the Privacy Notices referred to in section 10 and in Appendix 1).

If the request is made electronically, Bender Dating should provide the information in a 'commonly used electronic format' where possible.

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

11.2 Data Rectification

A Data Subject has the right to have their Personal Data rectified if they are inaccurate or incomplete.

If Bender Dating has disclosed the relevant Personal Data to any third parties, it must inform those third parties about the rectification, unless it is impossible or involves disproportionate effort to do so. If the Data Subject so requests, Bender Dating must also inform the Data Subject about those third parties.

11.3 Data Erasure

A Data Subject has a right to have their Personal Data erased and to prevent Processing in certain circumstances. The right to erasure is also known as 'the right to be forgotten', but the right to erasure does not provide an *absolute* 'right to be forgotten'.

A Data Subject has a right to have their Personal Data erased and to prevent further Processing of it any of the following circumstances:

- Where the Personal Data are no longer necessary in relation to the purpose for which it was originally collected/Processed.
- When the Data Subject withdraws consent.
- When the Data Subject objects to the Processing and there is no overriding legitimate interest for continuing the Processing.
- When the Personal Data was unlawfully Processed (i.e. in breach of applicable Data Protection laws).
- The Personal Data has to be erased in order to comply with a legal obligation.

A Data Subject does not have to show that the Processing causes damage or distress when requesting erasure of the Personal Data, but if the Processing does cause damage or distress then this is likely to make the case for erasure stronger and Bender Dating would need to consider the request accordingly.

There are some specific circumstances where the right to erasure does not apply. Bender Dating can refuse to comply with a request for erasure where the Personal Data are Processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes for certain research or statistical purposes; or
- the exercise or defence of legal claims.

There are also specific rules relating to the right of erasure for children's Personal Data (which may be processed via Bender Dating's HR department for life assurance/pensions purposes) and where relevant guidance should be sought from the Data Protection Officer.

If Bender Dating has disclosed the relevant Personal Data to any third parties, it must inform those third parties about the erasure, unless it is impossible or involves disproportionate effort to do so. If the Data Subject so requests, Bender Dating must also inform the Data Subject about those third parties.

11.4 Restriction of Processing

Data Subjects have a right to restrict Processing of their Personal Data. Bender Dating must restrict the Processing of Personal Data in any of the following circumstances:

- Where a Data Subject contests the accuracy of the Personal Data, the Processing of that Personal Data should be restricted until Bender Dating has verified its accuracy.
- Where a Data Subject has objected (as referred to in section 11.5) to the Processing of their Personal Data for the purposes of legitimate interests and Bender Dating is considering whether its legitimate grounds override those of the Data Subject.
- When the Processing of Personal Data is unlawful and the Data Subject requests restriction of the Processing (instead of erasure of the Personal Data).
- If Bender Dating no longer needs the Personal Data, but the Data Subject requires the Personal Data to establish, exercise or defend a legal claim.

When Processing is restricted, Bender Dating may store the Personal Data, but not further Process it. Bender Dating is also permitted to retain just enough information about the Data Subject to ensure that the restriction is respected in future (but no more than this).

If Bender Dating has disclosed the relevant Personal Data to any third parties, it must inform those third parties about the restriction on the Processing of that Personal Data, unless it is impossible or involves disproportionate effort to do so. If the Data Subject so requests, Bender Dating must also inform the Data Subject about those third parties.

If Bender Dating decides to lift a restriction on Processing then it must inform the Data Subject of this decision.

11.5 Objection to Processing

Data Subjects have the right to object to:

- any Processing based on 'legitimate interests';
- direct marketing (including profiling); and
- any Processing for the purposes of certain research and statistics.

For objections relating to Processing of data for the performance of a legal task or Bender Dating's legitimate interests, Data Subjects must have an objection on "grounds relating to his or her particular situation". Bender Dating must stop Processing the Personal Data on request unless:

- it can demonstrate compelling legitimate grounds for the Processing, which override the interests, rights and freedoms of the Data Subject; or
- the Processing is for the establishment, exercise or defence of legal claims.

For objections relating to Processing of Personal Data for direct marketing purposes, Bender Dating must stop Processing Personal Data for those purposes as soon as the objection is received.

For objections relating to Processing of Personal Data for the purposes of certain research and statistics, Data Subjects must have an objection on "grounds relating to his or her particular situation".

Bender Dating cannot charge for dealing with these objections.

Where the relevant Processing activities fall into any of the above categories and are carried out online, Bender Dating must offer a way for Data Subjects to object online.

11.6 Rights related to automated decision making and profiling

Data Subjects have rights in certain circumstances to object to decisions being taken about them without human intervention, including profiling (which means any form of automated processing intended to evaluate certain personal aspects of a Data Subject).

Bender Dating should not undertake any processing operations which constitute automated decision making without the approval of the Data Protection Officer (who will consider whether new policies and procedures are required to deal with the rights of the Data Subjects in this regard).

11.7 Data Portability

The right to data portability allows a Data Subject to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to Personal Data the Data Subject has provided to Bender Dating (as a Controller);
- where the Processing is based on: (a) the Data Subject's consent, or (b) for the performance of a contract; and

- when Processing is carried out by automated means.

Where the right of data portability applies, Bender Dating must provide the Personal Data in a structured, commonly used and machine-readable form (such as CSV files). 'Machine-readable' means that the information is structured so that software can extract specific elements of the data, which enables other organisations to use the information.

Bender Dating must provide the information free of charge.

If the Data Subject requests it, Bender Dating may be required to transmit the Personal Data directly to another organisation if this is technically feasible.

11.8 Right to make complaints

Data Subjects have a right to make complaints. For more details, see section 14.

11.9 Timescales, Charges and Information Requirements

The provisions below apply to any exercise by a Data Subject of any of the above rights, except as otherwise stated above with regard to any specific right.

Bender Dating must provide the information and/or complete the request (as applicable) without delay - and at the latest within one month of receipt of the request. However, this period can be extended by a further two months where requests are complex or numerous. If this is the case, Bender Dating must inform the Data Subject within one month of the receipt of the request and explain why the extension is necessary.

Where the Data Subject makes the request by electronic means, the relevant information must be provided by electronic means where possible (unless otherwise requested by the Data Subject).

In most cases, Bender Dating must provide the information or take the action requested free of charge. However, a 'reasonable fee' can be charged when (a) a request is manifestly unfounded or excessive (particularly if it is repetitive); or (b) requests are made for further copies of the same information previously provided by Bender Dating. Note that this does not mean that Bender Dating can charge for all subsequent requests. The fee must be based on the administrative costs of providing the information or communication or taking the action requested).

Where requests are manifestly unfounded or excessive (particularly where they are repetitive), Bender Dating may, instead of charging a reasonable fee as set out above, refuse to respond. In this case, Bender Dating must explain to the Data Subject (without undue delay and in any event within one month from the date of the request) why it has refused, informing the Data Subject of their right to complain to the supervisory authority and to a judicial remedy.

12 Data Transfers

Bender Dating must comply with strict rules regarding transfers of Personal Data outside of the UK (including to an international organisation), whether the transfer is to an affiliated company or to a third party. These rules are in place to ensure that the level of protection of Data Subjects afforded by the GDPR is not undermined. Bender Dating must only transfer Personal Data outside of the UK or to an international organisation where permitted as set out below.

12.1 Data Transfers to Another Country or International Organisation

Transfers on the basis of an adequacy decision

Bender Dating may transfer Personal Data to another country or an international organisation where that country is recognised by law as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects or the international organisation in question ensures an adequate level of protection.

For a list of countries currently recognised as having an adequate level of legal protection, see Appendix 2. This list may change from time to time (where authorisations or approvals are amended, replaced or repealed) and accordingly the Data Protection Officer shall ensure that Appendix 2 is updated when applicable.

Transfers subject to appropriate safeguards

Bender Dating may only transfer Personal Data to another country (including third parties located in another country) which is not approved as above, where one of the transfer scenarios listed below applies:

- standard Data Protection clauses in the form of template transfer clauses adopted or approved by law or a supervisory authority;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR; and
- contractual clauses agreed or authorised by a supervisory authority.

Transfers in other situations

In the absence of an adequacy decision or of appropriate safeguards as outlined above, Bender Dating may only transfer Personal Data to another country or an international organisation where one of the following conditions is met:

- The Data Subject has given informed 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 at the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract with a third party, where the contract was made in the interest of the Data Subject.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject or other persons, where the Data Subject is physically or legally incapable of giving consent.

Where none of the conditions above apply, the only other situation in which a transfer to another country or an international organisation may take place is where the transfer:

- is not repetitive (similar transfers are not made on a regular basis);

- involves data related to only a limited number of Data Subjects;

- is necessary for the purposes of the compelling legitimate interests of Bender Dating (provided such interests are not overridden by the interests of the Data Subject); and

- is made subject to suitable safeguards put in place by Bender Dating (in the light of an assessment of all the circumstances surrounding the transfer) to protect the Personal Data.

In the above situation, Bender Dating is obliged to: (a) inform the supervisory authority of the transfer and (b) inform the Data Subject of the transfer and of the compelling legitimate interests pursued for the transfer, in addition to providing the other information which is required to be provided to Data Subjects as outlined in section 8.

12.2 Transfers to Third Parties

Bender Dating will only transfer Personal Data to, or allow access by, any 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, Bender Dating will first identify the role of Bender Dating and the third party and ensure that an appropriate written agreement is in place, as referred to in section 12.3.

When Bender Dating is outsourcing services to a third party (including for data centres and similar services), it will identify whether the third party will Process Personal Data on its behalf and whether the outsourcing will entail any transfers of Personal Data to another country or international organisation.

Where third parties, whether companies or individuals, are engaged to Process Personal Data on Bender Dating's behalf (i.e. Processors), assurance of such compliance must be obtained from such third parties prior to granting them access to Personal Data controlled by Bender Dating. Written contracts should also be place, which include the minimum required terms pursuant to the GDPR, prior to any Processing.

The Data Protection Officer shall conduct regular audits of Processing of Personal Data performed by third parties on behalf of Bender Dating, especially in respect of technical and organisational measures they have in place. Any deficiencies identified will be reported to the Directors and may be monitored further accordingly.

12.3 Assessing the Role of Controller and Processor

Before any Personal Data are transferred to or from Bender Dating, it is imperative to ascertain which party is the Controller and which is the Processor of the relevant Personal Data.

In either case, Bender Dating must enter into, in consultation with the Data Protection Officer, an appropriate written agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred, prior to any Processing taking place.

Where the third party is a Processor, that agreement must also include certain minimum required terms pursuant to the GDPR (which the Data Protection Officer, or Bender Dating's legal advisors, can advise on). Bender Dating must also ensure, prior to any Processing taking place, that appropriate assurance of compliance with the requirements of all applicable Data Protection laws is obtained from the Processor.

In some instances, it is possible that both Bender Dating and a third party could be a Controller

of the relevant Personal Data, in which case the Data Protection Officer will provide guidance and advice on the relevant procedures to be followed.

13 Data Protection by Design

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

Bender Dating must ensure that a Data Protection Impact Assessment ("DPIA") is conducted, in consultation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Directors for review and approval.

Where applicable, Bender Dating's Information Technology (IT) department or outsourced IT providers will consult with the Data Protection Officer to assess the impact of any new technology uses on the security of Personal Data.

14 Complaints Handling

Data Subjects who wish to complain about the Processing of their Personal Data will be notified that they should put the complaint in writing to the Data Protection Officer.

If any colleague receives a complaint directly from a Data Subject (whether or not made in writing), they should inform the Data Protection Officer.

An investigation of the complaint will be carried out by the Data Protection Officer to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period (and, where appropriate, will ensure that colleagues are appraised of the progress and/or outcome of the complaint).

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their discretion, seek legal redress and/or complain to the relevant supervisory authority.

15 Breach Reporting

Any colleague who suspects that a Personal Data Breach has occurred must immediately notify the Data Protection Officer, providing a full description of what occurred and (as far as possible) the Personal Data involved.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will follow the relevant procedure in Bender Dating's Data Breach Policy based on the criticality and quantity of the Personal Data involved.

16 Accountability & Records

Bender Dating must be able to demonstrate compliance with the GDPR. All colleagues should undertake their activities accordingly, so that compliance can be readily demonstrated as applicable. This includes making and maintaining written records of all relevant activities relating to the Processing of Personal Data (including with regard to decisions made, actions taken and analysis of Data Protection Impact Assessments).

Bender Dating also has specific legal responsibilities to maintain certain internal records regarding Processing activities which are under its responsibility, as follows.

16.1 Where Bender Dating has less than 250 employees

For so long as Bender Dating has less than 250 employees, it only needs to document Processing activities (in its capacity as a Controller or Processor) that:

- are not 'occasional'; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of Personal Data (which, as stated in section 7.2, will be treated by Bender Dating as including Personal Data relating to criminal convictions or offences).

To the extent applicable, the documentation of the above shall include all relevant records referred to in section 16.2.

16.2 Where Bender Dating has 250 employees or more

Once Bender Dating has 250 employees or more, Bender Dating must (in its capacity as a Controller) maintain written/electronic records of the following information:

- the name and details of the relevant Bender Dating entity (and where applicable, of other Controllers and Bender Dating's representative) and the Data Protection Officer;
- purposes of the Processing;
- description of the categories of Data Subjects and categories of Personal Data;
- categories of recipients of Personal Data (including recipients in other countries or international organisations);
- where applicable, details of transfers of Personal Data to another country or an international organisation (including the identification of that country or international organisation) and documentation of the transfer mechanism safeguards in place;
- where possible, the envisaged time limits for erasure/retention of Personal Data; and
- a description of the technical and organisational security measures in place to protect Personal Data.

Once Bender Dating has 250 employees or more, Bender Dating must (In its capacity as a Processor) maintain written/electronic records of all categories of Processing activities carried out on behalf of the Controller, containing:

- the name and details of the relevant Bender Dating entity and of each Controller on behalf of which it is acting (and, where applicable, of the Controller's or Bender Dating's representative) and the Data Protection Officer;
- the categories of Processing carried out on behalf of each Controller;
- where applicable, details of transfers of Personal Data to another country or an international organisation (including the identification of that country or international organisation) and documentation of the transfer mechanism safeguards in place; and

- a description of the technical and organisational security measures in place to protect Personal Data.

17 Data Protection Training

All Bender Dating employees who have access to Personal Data will have their responsibilities under this Policy outlined to them as part of their staff induction training. In addition, Bender Dating will provide regular Data Protection training and procedural guidance for its staff.

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

- the Data Protection Principles set out above;
- the requirement for Personal Data to be accessed and used only by authorised persons and for authorised purposes;
- the need for, and proper use of, the forms and procedures adopted to implement this Policy;
- the correct use of passwords and other access mechanisms for Personal Data;
- the importance of preventing unauthorised access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person;
- securely storing manual files, print outs and electronic storage media which contains Personal Data;
- the need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data (including taking Personal Data out of physical office premises);
- proper disposal of Personal Data by using secure shredding facilities (for paper records) or appropriate methods of deleting electronically held information; and
- any special risks associated with Personal Data in particular departmental activities or duties.

18 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved in relation to this Policy, the Data Protection Officer may carry out a Data Protection compliance audit. An audit, if carried out, will look at some or all of the following areas:

- the level of understanding of this Policy and Data Protection laws;
- compliance with this Policy in relation to the protection of Personal Data, including:
    - the assignment of responsibilities;
    - raising awareness; and
    - training of colleagues;
- the effectiveness of Data Protection related operational practices, including:

    - Data Subject rights;
    - Personal Data transfers;
    - Personal Data incident management; and
    - Personal Data complaints handling;
- the level of understanding of Privacy Notices and the effective use of Privacy Notices;
- the accuracy of Personal Data being stored;
- the manner in which Personal Data are being Processed;
- the conformity of Processor activities and Processor contracts; and
- the adequacy of procedures for Personal Data Breaches.

The Data Protection Officer, in consultation with key business stakeholders, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. The creation of any such rectification plan does not absolve responsibility for the identified deficiencies or any failure to comply with this Policy.

The Data Protection Officer may (at their discretion) report any identified deficiencies to the Directors. The Data Protection Officer (and/or the Directors) may monitor the rectification of the identified deficiencies and conduct further audits.

19 Contact Details

Data Protection Officer:

Scott Barron
Bender Dating Limited
Westgate House
Seedhill
Paisley
Renfrewshire
PA1 1JE

Email: scott@benderdating.com

Appendices

Appendix 1 – Information Notification to Data Subjects

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

Information to be supplied	**Data obtained directly from Data Subject**	**Data not obtained directly from Data Subject**
The identity and the contact details of the Controller and, where applicable, of the Controller's representative.	✓	✓
The source the Personal Data originates from, and if applicable, whether it came from publicly accessible sources.		✓
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 Controller intends to transfer Personal Data to a recipient in another country, details of that transfer and the applicable safeguards.	✓	✓
The period for which the Personal Data will be stored, or the criteria used to determine that period.	✓	✓
Where applicable, the legitimate interests pursued by the Controller or by a third party.	✓	✓
The existence of each of the Data Subject rights - 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.	✓	✓
The right to lodge a complaint with a supervisory authority.	✓	✓

The existence of automated decision-making (including Profiling) along with meaningful information about how decisions are made, the significance and the consequences.	✓	✓
Whether the provision of Personal Data is part of a statutory or contractual requirement and if so the possible consequences of failure to provide such data.	✓	

Appendix 2 – Adequacy for Personal Data Transfers

The following are a list of countries currently 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.

- European Economic Area (EEA) Countries – comprising:
    - EU Countries (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden); and
    - EFTA States (Iceland, Norway and Liechtenstein)
- EU or EEA institutions, bodies, offices or agencies
- Gibraltar
- Andorra
- Argentina
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay

There are also partial findings of adequacy about:

- Japan - private sector organisations only
- Canada - only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details, please see the EU Commission's FAQs on the adequacy finding on the Canadian PIPEDA (https://ec.europa.eu/info/law/law-topic/data-protection_en).