PRIVACY POLICY

I. Legal Basis and Purpose of this Privacy Policy; Data Controllers

For the drafting of this policy, special consideration was given to the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the provisions of Act VI of 1998 regarding the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" of 28 January, 1981, enacted in Strasbourg, and the recommendations of the 'ONLINE PRIVACY ALLIANCE'.

This Privacy Policy and all data protection issues therein shall be governed by Hungarian law, and any legal disputes arising in any data protection context shall fall under the jurisdiction of Hungarian courts of law, stipulating the exclusive jurisdiction of Hungarian courts of law that have competence for the relevant area according to the postal code of the Data Controller's or Controllers' registered seat.

The purpose of this Privacy Policy is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him („data protection") for the full range of our services.

Data Controllers:

Dating Central Europe Zártkörűen Működő Részvénytársaság

registered seat: H-7623 Pécs, Móré Fülöp utca 33.

company registration number: Cg. 06-10-000496

(hereinafter: Data Controller)

II. Definition of personal data related terms

"personal data" means data which can be traced back to a given natural person (hereinafter "data subject") and inferences drawn from such data in regard to data subject. Personal data shall have above definition throughout data processing as long as it can be linked to the data subject;

"sensitive data" means personal data relating to data subject's racial or ethnic origin, nationality, political opinion or party affiliation, religious or other beliefs, physical or mental health or condition, addictions, sexual life and criminal convictions;

"data management" means the collecting, recording and storing, processing, using (including forwarding and public disclosure) and deleting of personal data, regardless of the process being used. Data management also includes modifying personal data or preventing any further use thereof;

“data processing” means executing data management operations and technical tasks, regardless of the method and devices used to execute such operations, and regardless of the location in which they are used;

“data transfer” means making data accessible to a third party;

“publication” means making data accessible to anyone;

“data controller” means the natural or legal person or unincorporated organisation who or which decides the purpose of personal data management, makes and implements decisions regarding data management, and is entitled to delegate execution to data processor. In the case of mandatory data management, the purpose and terms of data management as well as data controller are governed by an act or municipal decree requiring data management;

“data processor” means the natural or legal person or unincorporated organisation who or which processes personal data on behalf of the data controller;

“erasure of data” means rendering data unrecognisable by making it unrecoverable

“automated data file” means any set of data undergoing automatic processing;

“automatic processing” includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

III. Basic Principles of Data Management

1. personal data shall be obtained and processed fairly and lawfully;
2. personal data shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
3. personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are stored;
4. personal data shall be accurate and, where necessary, kept up to date;
5. personal data shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored,
6. personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions,
7. appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

IV. Additional Safeguards for Data Subject

Any person shall be enabled:

1. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
2. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

3. to have such data corrected or erased for reasonable cause in the simplest possible manner and as soon as possible;
4. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to laws is not complied with. At data subject's request, data controller shall provide information on the data managed by data controller or processed by data controller's authorised data processor, on the purpose, legal grounds, time period of the data management, on data processor's name, address (registered seat) and data management activities, and on the identity of the person(s) receiving the data and on the purpose such data were received. Data controller shall provide the requested information in writing in intelligible form at the earliest possible time upon receipt of data subject's request, but within no later than 30 days. In case of any violation of its rights, data subject may lodge a formal complaint against the data controller in a court of law. Data controller is liable to pay compensation for any damage caused to another party by its unlawful handling of data relating to data subject or by breaching technical data protection requirements. Data controller is also liable to pay compensation to data subject for any damage caused by its data processor. Data controller is exempt from liability if it can prove that the damage resulted from unavoidable causes outside the scope of data management. No compensation is payable if damage is caused by the injured party's deliberate or grossly negligent conduct.

Personal data may be processed on condition that

1. data subject has given its consent thereto, or
2. data processing is required by law or by a decree of a local municipality acting by its mandate granted by law and strictly within the scope defined by the law in question. Personal data may be required by law to be disclosed for the public interest, specifically by outlining the scope of data to be disclosed. In all other cases personal data may be made public strictly only with data subject's consent, and sensitive data may be disclosed only with data subject's written consent. In case of any doubt, the assumption must be that data subject did not consent to the disclosure. Data subject's consent shall be deemed given in relation to any information disclosed by data subject during a public appearance or disclosed by it with the intention of being published.

Sensitive data may be processed on condition that

1. data subject has given its consent in writing thereto, or
2. in respect of data relating to racial origin, nationality, ethnic minority identity, political opinion or party affiliation, religious or other philosophical creed and trade union membership, the processing of such data is required based on an international convention, is necessitated by the enforcement of a fundamental constitutional right or is required by law in the interests of national security, prevention of crime or fight against crime;
3. is otherwise required by law.

Policies regarding data management and protection of personal data of visitors apply only to natural persons having regard to the fact that personal data can be interpreted in relation only to natural persons (in accordance with Act CXII of 2011 on Informational Self-Determination and Freedom of Information), therefore, this Data Protection Policy has a binding force strictly to the management of personal data of natural persons registering on the website.

Purpose-Bound Data Management:

Personal data can be managed strictly only for a specific purpose, to exercise a right and to meet an obligation. Data management must meet this objective in every step of the way. Personal data can be managed only insofar as it is essential for satisfying the purpose of data management, it is adequately suited to satisfying that purpose, and its scope and duration is limited to achieving the objective.
Purpose of data management: to provide a dating service and, in regard to that service, to meet contractual rights and obligations, to generate website traffic statistics, to make data accessible to other users, i.e. to ensure that the service is efficient and meets the highest standards, further, by user consent, to use such data for marketing purposes, to send newsletters (commercial offers), to generate direct business leads, and, also by user consent, to show user's location to other users.

By registering, User will also become registered in the databases of all dating websites operated by Dating Central Europe Zrt (for an up-to-date list of dating websites operated by Dating Central Europe Zrt. go to http://dace.hu/cegcsoport).

"Scope of Data Managed" means any personal data provided by User on the website during registration or thereafter, and User's IP address

Data Controller may send users system messages in connection with operating the website and in conjunction with its services. By registering, User agrees that Data Controller may process its voluntarily provided data and that Data Controller may use such data for its advertising purposes in a data format specified by applicable laws.

Data Transfer, Linking Data Management Operations:

Data Controller may also use personal data provided during user registration for promoting its own sales and direct business lead generation, as well as those of other member companies within Data Controller's group and their partners in connection with promoting its products, provided that User has specifically agreed to receiving newsletters. By completing his registration on the website, by providing personal data and by expressly agreeing thereto by clicking on the registration hypertext link, User agrees to being contacted by Data Controller on the contact details provided by it. User may be contacted electronically, by phone or by post.

Upon User's express consent, whether granted during registration or at any time thereafter, all personal data of User managed by Data Controller may be transferred to other members of the Dating Central Europe Zrt Group (for an up-to-date list of Group members go to http://dace.hu/cegcsoport). The purpose of data transfer defined in this section is to facilitate the provision of Group members' services, to enable Group members to directly promote their own services and the services of other Group members, to send out newsletters, and to generate direct business leads for their own purposes and for the purposes of their partners.

Data Controller may send users system messages in connection with operating the website and in conjunction with its services. By registering, User agrees that Data Controller may process its voluntarily provided data and that Data Controller may use such data for its advertising purposes in a data format specified by applicable laws.

Data Security:

Data Controller and, within its own scope of operations, Data Processor shall keep data under their management secure, and adopt technical and organisational measures and formulate procedural policies as may be necessary to enforce the provisions of the Data

Protection Act as well as other data and confidentiality regulations. Data shall be protected especially against unlawful access, alteration, publication or erasure, as well as against damage or destruction.

V. Data Protection Principles

Data Controller shall give its users clear, noticeable and unambiguous warning before capturing, recording or handling any of their data (privacy statement) to provide them with information on their data is captured, for what purposes and in accordance with what principles. Further, Data Controller shall call User's attention to the voluntary nature of data disclosure. Data Subject shall be informed about the purpose of data management, as well as the identity of the person(s) who manage and process the data. Data Controller's entire staff and senior officers are entitled to the access data managed by Controller. The requirement to provide information on data management is also deemed fulfilled when applicable laws govern data to be captured by transfer from an already existing data management pool or by linking existing databases.

Whenever Data Controller intends to use provided data for purposes other than determined when the data was originally captured, it shall inform User of those purposes accordingly and obtain User's prior express consent; Data Controller shall also ensure that User may opt to prohibit use of its data for such other purposes.

Data Controller shall, without fail, adhere to the restrictions stipulated under Basic Principles when capturing, recording and managing data, and it shall keep Data Subject informed of its activities via electronic correspondence, at Data Subject's request. Data Controller shall refrain from imposing any sanctions against users who decline to provide requested non-mandatory information.

Data Controller shall keep data under its management secure and adopt technical and organisational measures and formulate procedural rules as may be necessary for ensuring that the data captured, stored and managed is protected; Data Controller shall prevent destruction, unlawful use and unlawful alteration of data under its management. Data Controller shall notify any third party to whom it may transfer or disclose data, as the case may be, of their obligations to the above.

Whereas Dating Central Europe Zrt is currently not offering any services designed specifically for individuals aged under 16, it represents and warrants that it does not collect or handle personal data on individuals aged under 16. Should it be approached by a user with a request to manage the personal data of an individual aged under 16, Dating Central Europe Zrt may record such data only if it is provided with a properly completed consent form or written authorisation issued in a verifiable format by a parent or legal guardian. In the absence of such authorisation we shall not record personal data of children (even if the use of service is rejected thereby).

As a general rule, users visiting our website are not obligated to disclose their identity and provide personal data of any kind. When providing their name and email address, users may, as a matter of course, opt not to enter their real name but provide an alias instead.

Data and information suitable for personal identification shall be construed as personal data of natural persons that can be used to identify an individual, to communicate with them or to identify their physical location, including but not limited to name, residential address, postal address, phone number, fax number and e-mail address.

Anonymous information collected by eliminating personal traceability does not constitute personal data as it cannot be linked to a natural person, neither does demographic data constitute personal data when it is collected without linking it to personal data of identifiable individuals, and therefore no connection can be made to natural persons.

As a general principle, whenever we ask our visitors for personal information, they are free to decide whether they want to provide the requested information after having read and interpreted the necessary written information. However, it must be noted that, if an individual decides not to share their personal data, they may not be able to use a service that is conditional on the disclosure of personal data.

This Privacy Policy is in regard to protecting the personal data of visitors provided to Data Controller, i.e. not in regard to their data intended for the public domain. Should an individual voluntarily decide to make all or some of his personal details public, then such information would not be covered by the scope of this Privacy Policy.

Without authorisation, under no circumstances shall we transfer to third parties any personal data provided by our users.

If service provider is requested by any competent authority to provide any personal data in line with applicable laws (e.g.: in connection with a suspected crime, or under an official court resolution ordering the confiscation of data), Data Controller will hand over requested and available information in accordance with its statutory obligation.

Whenever our users make available to us their personal data, we shall take all necessary measures to keep those personal data safe both during the course of network communication (i.e. online data management) and during the course of data storage and safekeeping (i.e. offline data management).

It is Data Controller's responsibility to ensure that visitors can access, correct and supplement their own personal data through the same communication channels and by using the same means through which they shared their personal data with us in the first place. This is meant to ensure that the personal data of our users are always up-to-date, accurate and current. Should any of our users ask us to remove their personal data from our systems, we shall promptly oblige (on the understanding that thenceforth that user will, in some cases, no longer be able to use the service to which the data was relevant, or not in the same way as before). The period of data management starts at the completion of registration and end at the time when the data is erased.

VI. Within this framework, Data Controller shall apply the following rules during the course of data collecting:

Information automatically logged by our servers. Our servers automatically register our users' IP-address, the type of their operating system and browser program as well as some other information. We use such information exclusively in an aggregated and processed form in order to correct certain errors in our services, if any, to improve their quality and for the purpose of generating statistics. We do not link these data to other data provided by our users in any way whatsoever.

Cookies. Data Controller places a unique identifier, also known as 'cookie' on user's PC. Refusal to accept cookies will not prevent user from using our services. The only exception is when Data Controller otherwise informs user in advance. Personal data provided during registration. In order to access certain services, our users have to complete a registration questionnaire. We will treat information generated during the registration process with the

outmost care and in the strictest confidence in order to prevent any unauthorised access to such data. We request information from our users partly to ensure that our services meet the highest possible standards and partly to generate statistical information about our client base. Their help enables us further improve our services to achieve the best possible match with their personal preferences and interests. We may transfer some information to our selected partners at our discretion in an aggregated and processed form in order to ensure that our partners may improve their services to better suit our users' preferences and interests. We may make certain information public in the form of statistical data in order to provide information to interested parties on how ours services work. We shall never ask for sensitive information to be provided in a 'mandatory' fashion in order for a registration to be successful. Providing any such information is entirely dependent on the user's decision and we shall keep such information on record strictly with user's written consent.

Data suitable for contacting individual users. We shall use data suitable for contacting individual users (for example e-mail addresses) strictly for purposes authorised by user in advance and we shall, under no circumstances, disclose them to third parties without user's prior written consent, unless stipulated otherwise by applicable laws.

Data suitable for physically contacting individual users. We shall use data strictly only for purposes authorised by user in advance and we shall, under no circumstances, disclose them to third parties, unless stipulated otherwise by applicable laws.

Open communication options. Open communication channels that are part of our service (e.g. forums) may be used at each individual user's own risk. Individual users are the copyright owners of their own posts but Dating Central Europe Zrt is entitled to quote and circulate multiple copies of such posts without limitation. Third parties may print, download and disseminate postings strictly for their own personal use only, and may use them exclusively with Dating Central Europe Zrt's written consent. Users are reminded that comments posted on open communication channels are governed by separate laws regulating public communications. We are committed to handling data suitable for individually contacting users accessing communication services with outmost care and in the strictest of confidence; no unauthorised access to those data is possible, and such data will not be disclosed to third parties, unless stipulated otherwise by applicable laws.

Links. Our services include links to the websites of other service providers. Data Controller shall not accept liability for the data and information protection practices of such service providers.

VII. At User's request, Data Controller shall provide information on the data managed by data Controller, on the purpose, legal grounds and time period of the data management, on data processor's name, address (registered location) and data management activities, and on the identity of the person(s) receiving the data and on the purpose such data were received. Information may be requested at info@mysecret.love or under 'Customer Service'.

Should our users have any reason to believe that we have breached their personal data protection rights, they may file a formal complaint with a court of law, or may seek assistance at the Hungarian National Authority for Data Protection and the Freedom of Information (H-1125 Budapest, Szilágyi Erzsébet fasor 22/c, www.naih.hu).
Such legal cases are reviewed by courts of law in expeditious procedures. Rulings fall under the jurisdiction of tribunals. Legal cases may also be brought before the tribunal that has jurisdiction over User's (Data Subject's) domicile or residence at User's (Data Subject's) discretion.

Detailed statutory provisions pertaining to legal redress and Data Controller's obligations are stipulated by Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

Data Protection ID: Dating Central Europe Zrt: NAIH-91099/2015.