

Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period..

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points affecting ChaletFinder.co.uk.

All ChaletFinder.co.uk staff are required to follow this Data Protection Policy at all times.

The Managing Director has overall responsibility for data protection within ChaletFinder.co.uk but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of information – how information is held and managed.

Information Commissioner - formerly known as the Data Protection Commissioner.

Notification – formerly known as Registration.

Data Subject – used to denote an individual about whom data is held.

Data Controller – used to denote the entity with overall responsibility for data collection and management. ChaletFinder.co.uk is the Data Controller for the purposes of the Act.

Data Processor – an individual handling or processing data

Personal data – any information which enables a person to be identified

Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by ChaletFinder.co.uk.

Data Protection Principles

As data controller, ChaletFinder.co.uk is required to comply with the principles of good information handling.

These principles require the Data Controller to:

- Process personal data fairly, lawfully and in a transparent manner.
- Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
- Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
- Ensure that personal data is accurate and, where necessary, kept up-to-date.
- Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
- Ensure that personal data is kept secure.
- Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects being:

- 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 (we do not use automated decision-making or profiling).

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that 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 with them;
- 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 data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- a. 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);
- b. 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);
- c. 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;
- d. 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;

- e. The processing relates to personal data which is clearly made public by the data subject;
- f. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- g. 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;
- h. 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;
- i. 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
- j. 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.

Specified, Explicit, and Legitimate Purposes

We only collect, process, and hold personal data of our customer's data subjects for the specific purposes set out above in this Policy (or for other purposes expressly permitted by the GDPR).

Adequate, Relevant, and Limited Data Processing

We 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) set out above.

Data Retention

- a. As required by law, we shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
- b. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- c. When establishing and/or reviewing retention periods, the following shall be taken into account:

- i. Our objectives and requirements;
- ii. The type of personal data in question;
- iii. The purpose(s) for which the data in question is collected, held, and processed;
- iv. Our legal basis for collecting, holding, and processing that data;
- v. The category or categories of data subject to whom the data relates;

d. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

e. Notwithstanding defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made by us to do so (whether in response to a request by a data subject or otherwise).

f. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Secure Processing

We have taken measures to ensure that all personal data collected, held, and processed by us is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Accountability and Record-Keeping

The Managing Director shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, our other data protection related policies, and with the GDPR, Data Protection Act 2018 and other applicable data protection legislation.

The Managing Director can be contacted by email: office@chaletfinder.co.uk

Disclosures and exchange of information

We may disclose and exchange information with our group companies, customers, credit reference agencies, service providers, representatives, sub-contractors, contractors and agents, as well as with law enforcement agencies and regulatory bodies for the above reasons.

Direct marketing

Information relating to data subjects may be used to notify them by post, email or other electronic means of our services and those of our group companies and third-party business partners, in which we believe you may be interested.

can withdraw your consent to use of personal data for marketing at any time by contacting our Managing Director.

Keeping Data Subjects Informed

The following information has been made available via our customers to every data subject:

- a. Our contact details;
- b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 2 of this Policy) and the legal basis justifying that collection and processing;
- c. Where applicable, the legitimate interests upon which we are justified in collecting 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 European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;
- g. Details of data retention;
- h. Details of the data subject's rights under the GDPR;
- i. Details of the data subject's right to withdraw their consent to our 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 GDPR);
- k. 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

I. Where applicable, 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.

Data Subject Access

Data subjects may make Subject Access Requests (“SARs”) at any time to find out more about the personal data which we hold about them, what we are doing with that personal data, and why.

Data subjects wishing to make a SAR may do so in writing, using our Subject Access Request Form, or other written communication. SARs should be addressed to the Managing Director at 3 Slaters Court, Knutsford, Cheshire, WA16 6BW, UNITED KINGDOM.

Responses to SARs shall 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 our Managing Director or our Management Team.

We do not charge a fee for the handling of normal SARs. We reserve 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.

Rectification of Personal Data

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

Where applicable, we shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing us 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. We will not be able to remove any data provided by a data subject of one of our customers.

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

Erasure of Personal Data

Data subjects have the right to request that we erase the personal data we hold about them in the following circumstances:

- a. It is no longer necessary for us 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 us holding and processing their personal data. You are not able to do this if we are holding data to perform a contract or to demonstrate compliance with our customer contracts;

- c. The data subject objects to us holding and processing their personal data (and there is no overriding legitimate interest to allow us to continue doing so). We have an overriding legitimate interest where we are performing a contract with one of our customers and personal data has been provided to us;
- d. The personal data has been processed unlawfully;
- e. The personal data needs to be erased in order for us to comply with a particular legal obligation;
- f. The personal data is being held and processed for the purpose of providing information society services to a child.

Unless we have 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).

Restriction of Personal Data Processing

Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we 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. We may have to process personal data on behalf of a data subject even once they have sought to restrict processing where we are performing a contract on behalf of our customer.

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).

Data Portability

Where data subjects have given their consent to us to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between us and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, we shall make available all applicable personal data to data subjects in electronic documents.

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections to Personal Data Processing

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

Where a data subject objects to us processing their personal data based on its legitimate interests, we shall cease such processing immediately, unless it can be demonstrated that our legitimate grounds for such processing overrides 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 us processing their personal data for direct marketing purposes, we shall cease such processing immediately.

Data Security – Storage

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

- a. All electronic copies of personal data shall be stored securely using passwords and data encryption;
- b. We have no hardcopies of personal data of our customers data subjects.

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 shall be securely deleted and disposed of.

Organisational Measures

We take the following measures with respect to the collection, holding, and processing of personal data:

- a. All employees, agents, contractors, or other parties working on our behalf have been made fully aware of both their individual responsibilities and our responsibilities under the GDPR;
- b. All our employees, agents, contractors, or other parties working on our behalf handling personal data have been appropriately trained to do so;
- c. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- d. The performance of those employees, agents, contractors, or other parties working on our behalf handling personal data shall be regularly evaluated and reviewed.

Transferring Personal Data to a Country Outside the EEA

We 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 consent of the relevant data subject(s);
- d. The transfer is necessary for the performance of a contract between us and the data subject (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.

Personnel Records

The Regulations apply equally to volunteer and staff records. ChaletFinder.co.uk records personal data as part of a staff member's contract of employment.

How to complain

We hope that our Management Team can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at <https://ico.org.uk/concerns/> for further information about your rights and how to make a formal complaint.

Implementation of Policy

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

