GDPR Policy

Document Description

This document outlines our legal requirement under the General Data Protection Regulations (GDPR) and the processes The Prairie Cottage implement in order to meet them.

Implementation

Implementation is immediate, and this policy shall stay in force until any alterations are formally agreed. The policy will be reviewed every two years by the owners, sooner if legislation, best practice or other circumstances indicate this is necessary.

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 following guidance is not a definitive statement on the Regulations but seeks to interpret relevant points where they affect The Prairie Cottage.

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

We have overall responsibility for data protection for The Prairie Cottage.

Definitions

Processing of information	How information is held and managed
Information Commissioner	The Data Protection Commissioner
Notification	Formerly known as Registration
Data Subject	Used to denote an individual about whom data is held
Data Controller	Individual or entities who determine the purpose and manner in which data is processed.
Data Processor	Individual or entities handling or processing data
Personal data	Any information which enables a person to be identified

Data Protection Principles

As a data controller, The Prairie Cottage 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.

Lawful basis for Processing

We must have a valid lawful basis for processing information:

Consent	The individual has given clear consent for you to process their personal data for a specific purpose
Contractual	The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal Obligation	The processing is necessary for you to comply with the law (not including contractual obligations).
Vital Interests	The processing is necessary to protect someone's life.
Public Task	The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate Interests	The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Consent

We record users explicit consent to storing personal data on file.

For the purposes of the Regulations, we will record:

- Online identifiers such as an IP address
- Name
- Email Addresses
- Telephone Numbers

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case will need to be reviewed by the owners for further consideration.

Obtaining Consent

Consent may be obtained in a number of ways:

- Contractual
- Face to Face

- Written
- Telephone Conversation
- Electronically, for example Email, Web Form, Social Media, Text Message, etc.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing was to be undertaken.

Subjects under 18 years of age require parental / guardian consent.

Individuals have a right to withdraw consent at any time. If this will affect the provision of services, then we will review this at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

Consent to share information should always be checked before disclosing personal information to another agency.

Where such consent does not exist, information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned.

Personal information should only be communicated on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data.

Where possible, all records and communications should be processed and stored in an electronic format, for example Word Documents, Emails and Cloud CRM records.

In instances where a paper record has been received and needs to be retained, it will be scanned into an electronic format and stored appropriately, at which point the paper copy will be disposed of.

Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computers being used in public areas, should be positioned in such a way so that passers-by cannot see what is being displayed

Computers should be locked / logged out when unattended.

Firewalls and virus protection are to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Cloud Computing

When commissioning cloud-based systems, we will take steps to check their robustness and compliance of data protection principles.

We currently use one cloud-based systems to hold and manage information.

Microsoft OneDrive

We use this in order to store a backup of data held on personal computers.

External Agents

In order to provide our service, we outsource to an external agent.

Keys Holidays

Keys Holidays are our sole letting agency and will process all customer data on our behalf.

This data may be:

1. Transferred to them from The Prairie Cottage. For example, a potential customer contacts us directly and we pass on their contact details to Keys Holidays in order for them to handle the booking. We will keep the initial contact communications in accordance to our retention of records policy.
2. Controlled by Keys Holidays. For example, clients making a booking for The Prairie Cottage direct from the Keys Holidays website, or the booking widget on the Prairie Cottage website.

In both respects Keys Holidays act as an independent Data Controller.

We are given access to the following data in order to provide the service:

1. Full Name of customer
2. Date of booking
3. Size of party
4. Cost of booking
5. Any additional requests, such as pets, room preferences, etc.
6. Guest Feedback

Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable response, such as a visit to a website. The communications may be any of a variety of forms including mail, social media or email.

We do not undertake any direct marketing.

We do not share or sell any data with outside organisation for marketing purposes.

Retention of Records

Emails and other documentation should be destroyed as soon as it is no longer needed for the task in hand.

What to Do If There Is a Breach

If we discover, or suspect, a data protection breach, we will take immediate actions to determine whether it needs to be reported to the Information Commissioner. There is a time limit for reporting breaches to ICO.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing their data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).
- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
- Where data is no longer necessary in relation to the purpose for which it was originally collected
- When an individual withdraws consent
- When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, The Company is permitted to store the personal data but not further process it. The Company can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

Data Subjects can ask, in writing to the owners, to see all personal data held on them, including e-mails and computer or paper files. We will aim to comply with such requests within 30 days of receipt of the written request.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

The Information Commissioner

Further information is available at www.informationcommissioner.gov.uk

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard: 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740