CMNet CIC Ltd
Data Protection Policy
25th May 2018

1. Introduction

This Policy sets out the obligations of CMNet CIC a company registered in the United Kingdom under number 456738, whose registered office is at **Fernaig House, Stromeferry, Wester-Ross IV53 8UW** ("the Company") regarding data protection and the rights of CMNet customers ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

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

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

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

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

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to

implementation

2.6 of the appropriate technical and organisational measures required by the GDPR

2.7 in order to safeguard the rights and freedoms of the data subject.

2.8 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.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data;

3.1 The right to be informed.

3.2 The right of access.

3.3 The right to rectification.

3.4 The right to erasure.

3.5 The right to restrict processing.

3.6 The right to data portability.

3.7 The right to object.

3.8 Rights with respect to automated decision-making and profiling.

4. Lawful, Fair, and Transparent Data Processing

4.1 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:

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

4.1.2 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;

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

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

4.1.5 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

4.1.6 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.

5. **Specified, Explicit, and Legitimate Purposes**

5.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects**.**

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. **Adequate, Relevant, and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. **Accuracy of Data and Keeping Data Up-to-Date**

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. **Data Retention**

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

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

9. **Secure Processing**

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. **Accountability and Record-Keeping**

10.1 The Company's Data Protection Officer is Joe Grimson. He can be contacted at 1, Riverside Cottages Braeintra, or by email at j.grimson@btinternet.com. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy,

the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

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

10.2.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

10.2.2 The purposes for which the Company collects, holds, and processes personal data;

10.2.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates

10.2.4 Details of how long personal data will be retained by the Company.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data **[**which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR**]**.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed; The purpose(s) for which personal data is to be used;

11.2.2 The Company's objectives;

11.2.3 How personal data is to be used.

11.2.4 Risks posed to data subjects;

Risks posed both within and to the Company; and the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.5 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

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

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

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

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

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

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

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

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Details of data retention;

12.2.5 Details of the data subject's rights under the GDPR;

12.2.6 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.7 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.8 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

12.2.9 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.

13. Data Subject Access

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

13.2 Data subjects wishing to make a SAR may do so in writing, using the Company's Subject Access Request Form, or other written communication. SARs should be addressed to the Company's Data Protection Officer at 1, Riverside Cottages Braeintra, or by email at j.grimson@btinternet.com. 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.

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

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

14. Rectification of Personal Data

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

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

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

15. Erasure of Personal Data

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

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

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

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

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

15.3 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).

16. Restriction of Personal Data Processing

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

16.2 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).

17. **Data Portability**

17.1 The Company processes personal data using automated means. This processing is necessary to inform the data subject of the status of their quota and to inform them if they have exceeded their contracted quota.

17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data.

17.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format**.**

17.3.1 email or written letter.

17.4 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.

18. **Objections to Personal Data Processing**

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

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

19. **Automated Decision-Making**

19.1 The Company uses personal data in automated decision-making processes. This process is to inform subjects of the status of their monthly quotas and to inform them if they have exceeded their quotas. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions under the GDPR.

19.2 The right described in Part 19.1 does not apply in the following circumstances:

19.2.1 The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;

19.2.2 The decision is authorised by law; or

19.2.3 The data subject has given their explicit consent.

20. **Profiling**

20.1 The Company uses personal data for profiling purposes. This takes the form of calculating usage to allow the company to plan ahead to ensure that they have enough capacity for current and future customers.

20.2 When personal data is used for profiling purposes, the following shall apply:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling when requested.

20.2.2 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected.

21. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
1.	Email address	To communicate with customers and to inform them of any faults or changes to the system or their equipment. To inform them of the status of their account.
2.	Address	Required to allow fitting of equipment.
3.	Telephone number	To allow communication
4.	IP Address	To Allow access to company equipment to carry out remote repairs, software and firmware changes.
5	IP Addresses accessed	Required by law under the Investigatory Powers Act 2016
6.	Bank account description	Accounting
7.	Volume of data uploaded and downloaded	Accounting
8.	Quota allowance	Accounting
9.	Subscription Charge	Accounting.

22. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data

22.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

22.2 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

23. **Data Security - Storage**

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

23.1 All electronic copies of personal data should be stored securely using passwords;

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

24. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

25. **Data Security - Use of Personal Data**

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

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

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

26. **Organisational Measures**

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

26.1 All employees shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

26.2 Only that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

26.3 All employees handling personal data will be appropriately trained to do so;

26.4 All employees handling personal data will be appropriately supervised;

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

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

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

26.8 All employees handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy.

27. **Data Breach Notification**

27.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

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

27.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

27.4 Data breach notifications shall include the following information:

27.4.1 The categories and approximate number of data subjects concerned;

27.4.2 The categories and approximate number of personal data records concerned;

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

27.4.4 The likely consequences of the breach;

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

27.4.6 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.

This Policy has been approved and authorised by:

Name: J.E. Grimson

Position: Data Protection Officer CMNet CIC

Date: 25th May 2018

Due for Review by: May 2019

Signature: