Chargifi Limited

Data Protection and Retention Policy

Date of Issue: May 15th, 2019

Contents

1. Introduction

Data protection is about regulating the way Chargifi uses, stores and deletes ('processes') information about identifiable people (personal data). It also gives people various rights regarding their data, which are defined in **section five** below.

This policy is about your obligations under data protection legislation, and Chargifi's defined retention periods for personal data (that is, the length of time after which such information should be securely destroyed).

The General Data Protection Regulation (GDPR) provides that organizations which process personal data must not retain that data for any longer *than is necessary* for the purposes for which the personal data are processed.

As a company, we will collect, store and process personal data about our customers, employees, suppliers and other third parties. We recognize that the correct and lawful treatment of this data will maintain confidence in the company and will ensure that the company operates successfully.

You are obliged to comply with this policy when processing personal data on Chargifi's behalf. Any breach of this policy may result in disciplinary action.

Any questions on the details contained within this policy, or on actions required, should be directed to Chief Financial Officer who is charged with oversight of Chargifi's data protection procedures (and who is referred to as the Data Controller at data@chargifi.com hereafter).

2. Aims and Objectives of this Policy

This policy is aimed at all employees working at Chargifi (whether directly or indirectly), whether paid or unpaid, whatever their position, roles or responsibilities, which includes contractors, agency staff and volunteers.

This Policy details our approach to data protection and the retention and deletion or destruction of personal data. All members of management and staff should familiarize themselves with this policy and refer to it on an ongoing basis to ensure that its terms are implemented and complied with.

3. What Information falls within the Scope of this Policy

Data protection concerns information about individuals. Personal data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available. In order for you to do your job, you will need to use and create personal data.

Chargifi may collect Personal Information in a variety of ways including directly from customers while online when they use any of our online tools or features, applications, or when they enter one of our promotions. This may include:

- Name and contact details of employees and customers
- Sex/gender of customers and employees
- Online identifiers, including IP addresses
- Financial information about employees and customers such as that which could be used to process invoices and payments
- Credit card information;

- Payment details
- Product preference
- Purchasing history
- Some web browsers may transmit "do not track" signals. Web browsers may incorporate or activate these features differently, making it unclear if users have consciously activated them. As a result, at this time we do not take steps to respond to such signals.

Under GDPR, personal data includes special category data, which is considered particularly sensitive. This includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership / activities
- Medical data (both physical and mental health related)
- Sexual orientation and data concerning a person's sex life
- Genetic and biometric data
- Criminal records, administrative judgements or sanctions, and details of alleged offences.

Special category data must have higher levels of protection enforced.

4. Our obligations

The GDPR has six key principles which you must abide by when we are working with personal data:

1. Personal data must be processed fairly, lawfully and transparently

"Processing" covers virtually everything which is done in relation to personal data, including using, disclosing, copying and storing personal data.

People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is often provided in a document known as a privacy notice or a transparency notice. Copies of Chargifi's privacy notices can be obtained from data@chargifi.com . You must familiarize yourself with Chargifi's privacy notices.

You must only process personal data for the following purposes:

- The administration of customer, staff, volunteer, and service provider records
- Conduct business with customers
- Improve customer experiences
- Direct customers to an online platform of a retailer to make a purchase
- Create and maintain accounts for retail partners
- Help customers receive email and direct mail for Chargifi's retail partners
- Help customers register for promotions, lotteries, loyalty programs and competitions

through social media channels

- Help customers send Chargifi reviews, enquiries and complaints
- Permit individuals to apply for a job
- Performing marketing, and analysis of marketing statistics
- Protecting and promoting Chargifi's interests, objectives and services
- To fulfil Chargifi's contractual and other legal obligations.

If you want to do something with personal data that is not on the above list, or is not set out in the relevant privacy notice(s), you must contact the Data Controller at data@chargifi.com. This is to make sure that Chargifi has a lawful reason for using the personal data.

We may sometimes rely on the consent of the individual to use their personal data. This consent must meet certain requirements and therefore you should contact the Data Controller at data@chargifi.com if you think that you may need to obtain consent.

2. Personal data must be processed for limited purposes only and in an appropriate way

When data is collected for one purpose (usually identified in the privacy policy) it cannot be used for a different purpose at a later date.

3. Personal data held must be adequate and relevant for the purpose. Personal data held must not be excessive or unnecessary

The data collected must be adequate for the identified processing, and therefore decisions should not be made based on incomplete data.

Personal data must not be collected if it is not required for the purpose identified.

4. Personal data held must be accurate

You must ensure that personal data is complete and kept up to date. For example, if a customer notifies you that their contact details have changed, you should update Chargifi's systems to reflect this change.

5. Personal data must not be kept longer than necessary

This policy includes details of how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data. This information is included in **Appendix 1.**

6. Personal data must be kept secure, and must not be transferred outside the EEA without adequate protection

Appropriate security measures must be in place to protect personal data. You must comply with the following company policies and guidance relating to the handling of Personal Data:

- Chargifi's Information security policy;

- IT acceptable use policy for staff, and
- Data Breach Policy and Procedure.

If you need to transfer personal data outside the EEA please contact the Data Controller at data@chargifi.com. Subject to the exception below

Personal Data that originates outside the EEA will be stored in accordance with this policy, with the exception of employee and payroll data which will be stored locally in accordance with appropriate equivalent regulation.

5. Individuals' Rights Regarding Personal Information

Individuals have a number of rights regarding their information under GDPR. You are obligated to uphold these rights when performing your work with Chargifi. You, as an individual that the company holds data about, also have these rights.

1. The right to be informed

People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as what rights they have over their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

2. The right of access

All individuals have the right to request access to see all the information that Chargifi holds on them. This is called a Subject Access Request. Chargifi has a policy document detailing the process to respond to such a request (Data Subject Rights Policy). In the event any such requests are received, you must inform the Data Controller at data@chargifi.com immediately.

3. The right to rectification

Individuals have the right to request any inaccurate or incorrect information held on them to be amended as necessary.

4. The right to erasure

Individuals have the right to request all personal data held on them by Chargifi be destroyed securely. Where such a request has been received, you must inform the Data Controller immediately.

A data subject may insist on erasure of their personal data where:-

a. it is no longer necessary for the purposes for which it was processed;
b. where consent has been withdrawn by the data subject;
c. where there is no legal basis for the processing of the data; or
d. where there is a legal obligation to delete the data.

The data subject's rights to erasure are not absolute and do not apply to personal data where processing is necessary for:

a. exercising the rights of freedom of expression;
b. to comply with a legal obligation in the public interest or in the exercise of an official authority;
c. for public health reasons;
d. for archiving purposes; and
e. for the establishment, exercise or defense of legal claims.

Where personal data is erased following receipt of a request by a data subject, Chargifi will confirm in writing to the data subject that their personal data has been destroyed. Such a response shall be issued to the data subject unless it is impossible or requires disproportionate effort to do so.

Where any request for erasure is refused, Chargifi will advise the data subject in writing that their request has been refused and detail the reasons for refusal.

5. The right to restrict processing

In specific situations, the individual has the right to restrict Chargifi from processing their data. If such a request is received, you must inform the Data Controller at data@chargifi.com immediately.

6. The right to data portability

Personal data is owned by the individual and they can request their data to be transferred to them, or another organization in a format that is standardized, and therefore is likely to be able to be used directly by them/ the other organization. Where such a request has been received, you must inform the Data Controller at data@chargifi.com immediately.

7. The right to object

Individuals have the right to object to their data being processed for direct marketing purposes.

8. Rights in relation to automated decision making and profiling

Where processing is performed automatically (that is, without human involvement) and includes completing a decision on the individual, the individual has the right to ask for this to be stopped and for the decision to be made by manual means (that is, by a person reviewing the data).

6. Storage Mediums

Chargifi stores personal data in a variety of ways. This includes hard copy documents, emails, data stored on our servers and in cloud based storage and data stored by third parties on our behalf. When updating, rectifying, erasing and deleting data, care must be taken to ensure that personal data held in all locations (including back-up storage) and in all forms is dealt with appropriately and a consistent and accurate record of personal data is maintained.

7. Retention of Personal Data

Different types of personal data may need to be retained for different periods of time depending on the purposes for which the data is processed and the legal and regulatory retention requirements in relation to certain categories of data. In determining the appropriate retention period consideration should be given to the following factors:-

- the purposes for which the personal data is processed;
- the legal basis for processing that personal data;
- legal requirements for retention (particularly employment and health and safety law); and
- regulatory requirements.

An appropriate retention period should be identified for each category of personal data. Individuals must be informed of the retention period which applies to their personal data or, if there is no fixed retention period, the criteria used to determine that period; and where the purposes for which the data is processed have changed, any new retention period.

All personal data processed by Chargifi shall be retained in accordance with the periods set out in the Appendix to this policy.

Personal data should then be retained in accordance with the appropriate retention period and permanently deleted and/or securely destroyed in accordance with this policy. No personal data shall be destroyed or deleted other than in accordance with this policy.

8. Review and Deletion of Personal Data

A review of the personal data processed by Chargifi will be carried out on an annual basis. During the course of this review Chargifi will:-

- Review the retention periods for each category of personal data processed and whether any alteration to these periods is required
- Identify personal data which is due for destruction and deletion
- Arrange for the secure deletion and destruction of personal data which will no longer be retained.

9. Lawful Basis for Processing Data

The GDPR requires there to be a lawful basis for the processing of any personal data. This means that for personal data to be collected, used, stored or transferred, there must be a legal

basis to do so. The lawful bases identified by the GDPR are:

- Consent has been given (which is specific to the purpose, informed via a clear and transparent consent form, easily withdrawable at any stage, freely given whereby the individual has not been forced to consent to inappropriate data processing in order to receive a service, verifiable, and based on affirmative action);
- Contractual, that is the processing is required to perform the contract in place;
- For legal compliance;
- To protect the vital interest of the individual;
- To carry out a task in the public interest or required by an official authority; and
- Under legitimate interest (see below).

Where special category personal data is being processed (that is, particularly sensitive data, as defined in section 3 above), additional checks must be made. In these cases, at least one of the following must be met before the personal data can be processed:

- The individual has given explicit consent;
- The processing is required under employment, social security or social protection laws;
- To protect the vital interest of the individual where they are incapable of consent;
- For a legitimate reason by a non-profit body with a political/ philosophical/ religious/ trade union aim
- Where the personal data was made public by the individual;
- Where it is necessary for the establishment, exercise or defense of legal claims;
- Where there is substantial public interest;
- Where it is necessary for medicinal, health or social care;
- Where it is necessary for public health and processing is bound by professional secrecy; and/ or
- It is for scientific/ historical/ statistical research purposes, or archiving purposes, which are in the public interest.

Under GDPR, the lawful basis for processing each type of data must be recorded and also notified to the individual whose data is being processed, via a privacy notice. You are obligated to ensure that the data you process is being processed under one of these lawful bases. See **Section 4.1** above for further details of your obligations in this area.

Legitimate Interest

GDPR allows Chargifi to use its own legitimate interest as a basis for processing data, where this interest does not outweigh the rights of the individual. This can include processing around network security, fraud prevention, maintenance of existing member relationship and direct marketing, among others.

To ensure that Chargifi's interest is not overriding the individual's rights, a Legitimate Interest Assessment (LIA) must be performed for each type of processing where this is being used as

the lawful basis for processing. This is the responsibility of the Data Controller. All LIAs must be formally documented and retained. The LIA must cover what the legitimate interest is, why processing is necessary to achieve this interest, and balance this against the individual's interests, rights and freedoms.

Where data is being used in ways that may be reasonably expected and which have a minimal privacy impact, or if there is a compelling justification for the processing, legitimate interest may be the most appropriate lawful basis to use.

If the individual would not reasonably expect the processing, or if it would cause unjustified harm, it is likely that the individual's interests will override Chargifi's interests. Where the processing is not necessary to achieve the described aim, legitimate interest cannot be used.

If circumstances change, a new LIA will need to be performed.

The GDPR highlights some processing activities where the legitimate interest basis is likely to apply to Chargifi. These include:

- Processing employee or client data;
- Direct marketing

10. Personal data of customers

Per the guidance of the ICO, Chargifi must obtain consent from customers to obtain, process and keep their personal data, unless the company is using one of the other above lawful bases for processing such data, the data will be used in accordance with the Chargifi Privacy Policy.

Where consent is used, a 'Consent form' must be sent to customers by Chargifi, in order to obtain personal data. Customers have the right to withdraw consent at any time; at which point all personal data collected under the consent will be disposed of in a secure manner.

Chargifi may disclose or transfer Personal Information in connection with, or during negotiations of, any merger, sale of company assets, product lines or divisions, or any financing or acquisition. We may also disclose Personal Information to prevent damage or harm to us, our Services, or any person or property, or if we believe that disclosure is required by law (including to meet national security or law enforcement requirements), or in response to a lawful request by public authorities. Except as described in the Chargifi Privacy Policy, we will not otherwise disclose Personal Information to third parties unless the customer has been provided with an opportunity to opt in to such disclosure.

Chargifi does not release the Personal Information it collects from customers to any unrelated third parties so that they may send you commercial promotions or offers for products or services.

Except as described in the Chargifi Privacy Policy, Chargifi will not otherwise disclose personal data to any third parties unless the customer has provided consent to such disclosure and, in the case of personal data collected from children, the appropriate verifiable consent is obtained.

If an individual wishes to opt out or limit the use and disclosure of their personal data to a third party or a use that is incompatible with the purpose for personal data was originally collected or authorized, the individual may send such request to data@chargifi.com.

When Chargifi transfers Personal Information to countries other than the country where it was provided, it does so in compliance with applicable data protection laws. Copies of the Personal Information at the point of origin are deleted on a regular basis.

Any transfers of Personal Information from customers outside the European Economic Area (the "EEA"), will comply with GDPR requirements, as appropriate, in all respects

11. Children's Privacy

Chargifi is committed to protecting children's privacy on the Internet. No one under age 16 may provide any Personal Information to or on the websites. Chargifi does not knowingly collect Personal Information from children under 16.

If Chargifi learns that it has collected or received Personal Information from a child under 16 without verification of parental consent, Chargifi will delete that information. If you believe we might have any information from a child under 16, please report this to the Data Controller at data@chargifi.com.

12. Monitoring and Review

This policy shall be regularly monitored and reviewed annually.

Appendix 1. Summary of Retention Schedules – Customer & Marketing Data

Document	Information description (includes but not limited to)	Retention Period	Owner
Platform data – inclusive of Video data, comments, attachments, profile picture, email address, first and second name	Name Date of Birth Gender Addresses Phone numbers Email & Social Media Address	Retained whilst organisation or indvidual remains a customer or deleted by user. Once an organisation or individual requests all records to be deleted, data will be removed from the back-ups within 12 months	Product Team
Live chat history	As left	Records deleted after 1 year	Support Team
Screen recordings from support session	As left	Automatically deleted after one year after the need to retain for Service Level Compliance has expired	Support Team
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries and call recordings.	As left	Retained whilst organisation or individual remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be removed from the back-ups within 12 months	Sales and Marketing Team
Metrics Data	As left	Retained whilst organisation remains a customer or deleted by user. Once an organisation requests all records to be deleted, data will be anonymised	Development Team

Appendix 2. Summary of Retention Schedules – Commercial Data

Document	Information description (includes but not limited to)	Retention Period	Owner
Non-Disclosure Agreements	As left	7 Years	Finance
Signed Contracts	As left	7 Years	Finance
Contract amendments	As left	7 Years	Finance
Successful tender documents	As left	7 Years	Finance
Unsuccessful tenders' documents	As left	7 Years	Finance
Tender Documents, including Proposal (RFP) and Request for Information (RFI) documents user requirements, technical specifications, floor plans and evaluation criteria,	As left	7 Years	Finance
Subcontractors Reports (including retained Sales, Channel and Distribution Management Partners).	As left	7 Years	Finance
Sales and Sales Channel Partner Reports	As left	7 Years	Finance
Reports from Distributors	As left	7 Years	Finance

Appendix 3a. Summary of Retention Schedules – Employment Data

Document	Information description (includes but not limited to)	Retention Period	Owner
Employee details	DOB's; Addresses; Phone numbers; NI numbers; Passport information; CVs;	6 + 1 years after the date they cease being employees	Finance and HR
Medical information	Employee medical records; Related Doctor's notes; Related medical data; Hospital appointments. Sick leave notices	3 years from the data the record was made	Finance and HR.
Employee HR Documents	Appraisals and KPI's; Return to work documents; Disciplinary and performance information; Grievance notices; Holiday records;	6 years +1 after the records made	Finance and HR
Payroll and Salary	Salary, benefits, bank details, pension details	6 + 1 years after the record was made	Finance and HR

Contracts	Contracts of Employment; Director contracts; Contracts for services; Related sub-contracts;	6 + 1 years after they leave employment	Finance and HR
Non-Employee information	Prospective applicants' information e.g. sent in a CV;	3 months;	Finance and HR
Unsuccessful applicants (no prospect of employment)	DOB's; Addresses; Phone numbers; NI numbers; Passport information; CVs;	3 months after selection process	Finance and HR
Training information	Training information; Qualifications; Certificates held;	6 + 1 years after employment ceases	Finance and HR
Insurance Data	Personal information involving insurance claims; Insurance policies; Insurance related correspondence, outcomes and notices;	6 + 1 years	Finance and HR

Appendix 3b. Summary of Retention Schedules – Employee Tax & Benefits

Document	Information description (includes but not limited to)	Retention Period	Owner
Record of taxable payments	As left	6 + 1 years	Finance and HR
Record of tax deducted or refunded	As left	6 + 1 years	Finance and HR
Record of earnings on which standard National Insurance Contributions payable	As left	6 + 1 years	Finance and HR
Record of employer's and employee's National Insurance Contributions	As left	6 + 1 years	Finance and HR
NIC contracted-out arrangements	As left	6 + 1 years	Finance and HR
Copies of pay and deductions notices to employees (e.g. P45, P60)	As left	6 + 1 years	Finance and HR
Tax Authority notice of code changes, pay & tax details	As left	6 + 1 years (after Audit)	Finance and HR
Expense claims	As left	6 + 1 years	Finance and HR
Record of sickness payments	As left	6 + 1 years	Finance and HR
Record of maternity payments	As left	6 +1 years	Finance and HR

Income tax PAYE and NI returns (and equivalent Payroll and Tax Information from outside the UK)	As left	6 +1 years	Finance and HR
Redundancy details and record of payments & refunds	As left	12 years	Finance and HR
Detailed returns of pension fund contributions	As left	Permanently	Finance and HR
Annual reconciliations of fund Contributions	As left	Permanently	Finance and HR
Money purchase details	As left	6 + 1 years (After transfer or value taken)	Finance and HR
Pensioner records	As left	12 years after benefits cease	Finance and HR
Records relating to retirement Benefits	As left	6 + 1 years (After the year of Retirement)	Finance and HR

Appendix 3c. Summary of Retention Schedules – Employment Records

Document	Information description (includes but not limited to)	Retention Period	Owner
Terms and conditions of service, both general terms and conditions applicable to all staff, and specific terms and conditions applying to individuals	As left	6 + 1 years (After last date of currency)	Finance and HR
Service contracts for directors (companies)	As left	1 + 1 years (After directorship ceases)	Finance and HR
Remuneration package	As left	6 + 1 years (After last date of currency)	Finance and HR
Former employees' Personnel Files	As left	6 + 1 years	Finance and HR
References to be provided for former employees	As left	20 years or until former employee reaches age 65 (whichever comes first)	Finance and HR
Training programmes and individual training recordd	As left	6 + 1 years (After completion)	Finance and HR
Short lists, interview notes and application forms for successful candidate	As left	6 + 1 years (note application form to be kept for duration of employment)	Finance and HR
Application forms of non-shortlisted candidates	As left	3 + 3 Months	Finance and HR
Time cards (or similar)	As left	2 years (After audit)	Finance and HR
Insurance claims		See Insurances section	Finance and HR

Appendix 3d. Summary of Retention Schedules – Health and Safety

Document	Information description (includes but not limited to)	Retention Period	Owner
Health and Safety assessments	As left	Permanently	Finance and HR
Health and Safety policy statements	As left	Permanently	Finance and HR
Records of consultations with safety representatives	As left	Permanently	Finance and HR
Accident records, reports	As left	6 + 1 years (After date of occurrence)	Finance and HR
Accident books	As left	6 + 1 years (After date of last entry)	Finance and HR
Sickness records	As left	6 +1 years from end of Sickness	Finance and HR
Health and safety statutory notices	As left	6 + 1 years (After compliance)	Finance and HR

Appendix 4. Summary of Retention Schedules – Financial Records

Document	Information description (includes but not limited to)	Retention Period	Owner
Payroll records	As left	See 2a	Finance
Supplier contracts and related records	Includes 1099 Contractor Tax Forms.	See 4	Finance
Chart of Accounts	As left	7 Years	Finance
Fiscal Policies and Procedures	As left	7 Years	Finance
Management Accounts	As left	7 Years	Finance
Audited Financial statements	As left	7 Years	Finance
General Ledger	As left	7 Years	Finance
Investment Records	As left	7 Years	Finance
Invoices - Paid and Issued	As left	7 Years	Finance
Bank Records and Reconciliation Information	As left	7 Years	Finance
Business Expenses Records	As left	7 Years	Finance
Asset Registers	As left	7 Years	Finance

Appendix 5. Summary of Retention Schedules – IT Records

Document	Information description (includes but not limited to)	Retention Period	Owner
Recycle Bins	As left	Cleared Quarterly	Individual Employee
Downloads	As left	Cleared Quarterly	Individual Employee
Inbox	As left	All emails containing PII attachments deleted after 3 years	Individual Employee
Deleted Emails	As left	Cleared Quarterly	Individual Employee
Personal Network Drive	As left	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual Employee
Local Drives & files	As left	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual Employee
Google Drives, Dropbox	As left	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual Employee