Data Protection Policy

1. Introduction

1.1 Atlantic Comms takes its responsibilities regarding the management of the requirements of the UK General Data Protection Regulation (UK GDPR) very seriously. This policy sets out how Atlantic Comms manages those responsibilities.

1.2 Atlantic Comms obtains, uses, stores, and otherwise processes personal data relating to potential employees, current employees, former employees, contractors, website users and contacts, and customers of Atlantic Comms, collectively referred to in this policy as data subjects. Customer personal data is:

- Identity Data - includes first name, last name, title.
- Contact Data - includes billing address, delivery address, email address and telephone numbers.
- Financial Data - includes bank account and payment card details. Atlantic Comms will also keep a record of any financial transaction's customers make with Atlantic Comms, but do not directly collect, process, or store customer credit or debit card information.
- Transaction Data - includes details about payments to and from the customer and other details of products and services customers have purchased from Atlantic Comms.
- Contractual Data - includes details of the customers Atlantic Comms account in relation to their purchase and / or use of Atlantic Comms services or those of any business partners or networks.
- Technical Data - includes (IP) address, customer login data, browser type / plug-in types and versions, operating system and platform and other technology on the device's customers use to access the Atlantic Comms website or any subsidiary company website.
- Marketing and Communications Data - includes customer preferences in receiving marketing from Atlantic Comms.

1.3 When processing personal data, Atlantic Comms is obliged to fulfil individuals' reasonable expectations of privacy by complying with the UK GDPR and other relevant data protection legislation (data protection law).

1.4 This policy therefore seeks to ensure that we:

a) are clear about how personal data must be processed and Atlantic Comms expectations for all those who process personal data on its behalf.
b) comply with data protection law and with good practice.
c) protect Atlantic Comms reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights.
d) protect Atlantic Comms from risks of personal data breaches and other breaches of data protection law.

2. Scope

2.1 This policy applies to all personal data we process regardless of the location where that personal data is stored and regardless of the data subject. All employees and others processing personal data on Atlantic Comms behalf must read it. A failure to comply with this policy may result in disciplinary action.
2.2 All Directors, Heads of Service and Managers are responsible for ensuring that all Atlantic Comms employees within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls, and training to ensure that compliance.

3. Personal Data Protection Principles

3.1 When you process personal data, you should be guided by the following principles, which are set out in the UK GDPR. Atlantic Comms is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below. Details of each

of the principles and accompanying checklists can be found in Appendix 1.

3.2 Those principles require personal data to be:

a) processed lawfully, fairly and in a transparent manner (Lawfulness, fairness, and transparency).

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).

c) adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).

d) accurate and where necessary kept up to date (Accuracy).

e) not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).

f) processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, integrity, and confidentiality).

3.3 In addition, the Data Controller shall be responsible for, and be able to demonstrate compliance with, the above 6 principles (Accountability).

4. Data Subjects' Rights

4.1 Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

a) where the legal basis of our processing is Consent, to withdraw that Consent at any time.

b) to ask for access to the personal data that we hold (see below).

c) to prevent our use of the personal data for direct marketing purposes.

d) to object to our processing of personal data in limited circumstances

e) to ask us to erase personal data without delay:

- if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data.
- if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest, or the public interest and we can show no overriding legitimate grounds or interest.
- if the data subject has objected to our processing for direct marketing purposes.
- if the processing is unlawful.

f) to ask us to rectify inaccurate data or to complete incomplete data.

g) to restrict processing in specific circumstances e.g., where there is a complaint about accuracy.

h) to ask us for a copy of the safeguards under which personal data is transferred outside of the EU.

i) the right not to be subject to decisions based solely on automated processing, including customer profiling, except where necessary for entering, or performing, a contract, with Atlantic Comms; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards.

j) to prevent processing that is likely to cause damage or distress to the data subject or anyone else.

k) to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.

l) to make a complaint to the ICO; and

m) in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g., another provider to which the customer is transferring, or another employer to which the employee is moving) in a structured, commonly used, and machine-readable format.

4.2 You must verify the identity of an individual requesting data under any of the rights listed.

4.3 Requests (including for data subject access - see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to the Managing Director. A charge can be made for dealing with requests relating to these rights, but only if the request is excessive or

burdensome.

5. Accountability

5.1 Atlantic Comms must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. Atlantic Comms is responsible for, and must be able to demonstrate compliance with, the data protection principles.

5.2 We must therefore apply adequate resources and controls to ensure and to document UK GDPR compliance including:

a) appointing a suitably qualified DPO.
b) implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects.
c) integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches.
d) training staff on compliance with Data Protection Law and keeping a record; accordingly, and
e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

6. Responsibilities

6.1 Atlantic Comms responsibilities
As the Data Controller*, Atlantic Comms is responsible for establishing policies and procedures to comply with data protection law.
6.2 Data Protection Officer responsibilities The DPO is responsible for:
a) advising Atlantic Comms and its employees of its obligations under UK GDPR.
b) monitoring compliance with this Regulation and other relevant data protection law, Atlantic Comms policies with respect to this and monitoring training and audit activities relate to UK GDPR compliance.
c) to provide advice where requested on data protection impact assessments.
d) to cooperate with and act as the contact point for the Information Commissioner's Office
e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context, and purposes of processing.

6.3 Staff responsibilities

Employees who process personal data about employees, customers, website users or any other contact or individual must comply with the requirements of this policy. Employees must ensure that:

a) all personal data is kept securely.
b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
c) personal data is kept in accordance with Atlantic Comms data retention schedule.
d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to Managing Director.
e) any data protection breaches are swiftly brought to the attention of the Managing Director, and that they provide support in resolving breaches.
f) where there is uncertainty around a data protection matter advice is sought from the Managing Director.

Employees who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Managing Director.

7. Third-Party Data Processors

7.1 Where external companies are used to process personal data on behalf of Atlantic Comms, responsibility for the security and appropriate use of that data remains with Atlantic Comms.

7.2 Where a third-party data processor is used:

a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data.

b) reasonable steps must be taken that such security measures are in place.

c) a written contract establishing what personal data will be processed and for what purpose must be set out.

d) a data processing agreement, available from the Managing Director, must be signed by both parties.

8. **Contractors/Consultants, Suppliers and Short-Term Staff**

8.1 Atlantic Comms is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, consultants, suppliers, or short-term staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

a) any personal data collected or processed in the course of work undertaken for Atlantic Comms is kept securely and confidentially.

b) all personal data is returned to Atlantic Comms on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and Atlantic Comms receives notification in this regard from the contractor, consultant, supplier, or short-term member of staff.

c) Atlantic Comms receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor.

d) any personal data made available by Atlantic Comms, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from Atlantic Comms.

e) all practical and reasonable steps are taken to ensure that contractors, consultants, suppliers, or short-term staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

9. **Data Subject Access Requests**

9.1 Data subjects have the right to receive copy of their personal data which is held by Atlantic Comms. In addition, an individual is entitled to receive further information about Atlantic Comms processing of their personal data as follows:

a) the purpose(s)

b) the categories of personal data being processed

c) recipients/categories of recipient

d) retention periods

e) information about their rights

f) the right to complain to the ICO,

g) details of the relevant safeguards where personal data is transferred outside the EEA

h) any third-party source of the personal data

9.2 You should not allow third parties to persuade you into disclosing personal data without proper authorisation. For example, a wife/husband does not have an automatic right to information regarding their mobile phone/data plan if the account/contract is not in their name.

9.3 The entitlement is not to documents per se, but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

9.4 You should not alter, conceal, block, or destroy personal data once a request for access has been made. You should contact the Group Compliance & Internal Projects Manager before any changes are made to personal data which is the subject of an access request.

10. **Reporting a personal data breach**

10.1 The UK GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the personal data breach results in a high risk to the data subject, he/she also must be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g., encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter

circumstances, a public communication must be made, or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

10.2 If you know or suspect that a Personal data breach has occurred, you should immediately contact Insert Name/Job Title. You must retain all evidence relating to personal data breaches to enable Atlantic Comms to maintain a record of such breaches, as required by the UK GDPR.

11. Limitations on the transfer of personal data

11.1 The UK GDPR restricts data transfers to countries outside the UK* to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

**there are provisions which permit the transfer of personal data from UK to the EEA and to any countries which, as of 31 December 2020, were covered by a European Commission 'adequacy decision'. This is to be kept under review by the UK Government.*

11.2 You may only transfer personal data outside the UK if one of the following conditions applies:

a) the UK has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms.

b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by UK Government, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO.

c) the data subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the UK GDPR including: reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving Consent.

12. Record Keeping

12.1 The UK GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

12.2 These records should include, at a minimum, the name and contact details of Atlantic Comms as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

12.3 Records of personal data breaches must also be kept, setting out:

a) the facts surrounding the breach
b) its effects; and
c) the remedial action taken

13. Training and Audit

13.1 We are required to ensure that all Atlantic Comms staff undergo adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess compliance.

13.2 You must regularly review all the systems and processes under your control to ensure they comply with this policy.

14. Data privacy by design and default and Data Protection Impact Assessments (DPIAs)

14.1 We are required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data-protection principles. Atlantic Comms must ensure therefore that by default only personal data

which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. By default, personal data should not be available to an indefinite number of persons. You should ensure that you adhere to those measures.

14.2 As well as complying with Atlantic Comms practices designed to fulfil reasonable expectations of privacy, you should also ensure that your own data-handling practices default to privacy to minimise unwarranted intrusions in privacy e.g., by disseminating personal data to those who need to receive it to discharge their duties.

14.3 Atlantic Comms must also conduct DPIAs in respect of high-risk processing before that processing is undertaken.

14.4 You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:

a) the use of new technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes).

b) automated processing.

c) any large-scale processing of sensitive (special category) data; and

d) large scale, systematic monitoring of a publicly accessible area.

14.5 A DPIA must include:

a) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate.

b) an assessment of the necessity and proportionality of the processing in relation to its purpose.

c) an assessment of the risk to individuals; and

d) the risk-mitigation measures in place and demonstration of compliance.

15. Direct Marketing

15.1 We are subject to certain rules and privacy laws when marketing to our customers, prospective customers, and any other potential user of our services.

15.2 A data subject's prior Consent is required for direct marketing (for example, by telephone*, email, text, or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details during a sale to that person, they are marketing similar services (e.g., an upgrade or alternative to their current tariff), and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

15.3 The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

15.4 A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

**In general, you must not make marketing calls to any number listed on the Telephone Preference Service (TPS) or Corporate TPS (CTPS), unless that person has specifically consented to your calls. You can call a number if it is not listed on the TPS or CTPS and you are not marketing claims management services. So, you need to screen call lists against the TPS and CTPS. You must allow your number to be displayed.*

16. Sharing Personal Data

16.1 In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to Atlantic Comms.

16.2 Some bodies have a statutory power to obtain information (e.g., regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as the Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a

request. If you need guidance, please contact the Managing Director.

16.3 Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies.

16.4 Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards.

Appendix 1

Principle 1 of UK GDPR – Processing personal data lawfully, fairly, and transparently

At a glance:

We must identify valid grounds under the UK GDPR (known as a lawful basis) for collecting and using personal data. We must ensure that we do not do anything with the data in breach of any other laws.
We must use personal data in a way that is fair. This means we must not process the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned.

We must be clear, open, and honest with people from the start about how we will use their personal data. Checklist:

Lawfulness

☐ We have identified an appropriate lawful basis (or bases) for our processing.
☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.
☐ We do not do anything generally unlawful with personal data.

Fairness

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
☐ We do not deceive or mislead people when we collect their personal data.

Transparency

☐ We are open and honest and comply with the transparency obligations of the right to be informed.

Processing Sensitive Personal Data

Sensitive personal data is data containing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

There are 10 specific conditions, of which at least one must be met, to process sensitive personal data. Within Atlantic Comms the only condition would be:

Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement.

Generally, only those employees working within a Human Resource capacity should have access and knowledge of sensitive personal data, unless there is a specific lawful reason, and consent from the Data Subject, for this information to be shared with others.

Principle 2 of UK GDPR - Purpose Limitation

At a glance:

We must be clear about what our purposes for processing are from the start.

We need to record our purposes as part of our documentation obligations and specify them in our privacy information for individuals.

We can only use the personal data for a new purpose if either this is compatible with the original purpose, we get consent, or we have a clear obligation or function set out in law.

Checklist:

☐ We have clearly identified our purpose or purposes for processing.

☐ We have documented those purposes.

☐ We include details of our purposes in our privacy information for individuals.

☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

☐ If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Principle 3 of the GDPR – Data minimisation

At a glance:

We must ensure the personal data we are processing is:

- adequate – sufficient to properly fulfil our stated purpose.
- relevant – has a rational link to that purpose; and
- limited to what is necessary – we do not hold more than we need for that purpose.

Checklist:

☐ We only collect personal data we actually need for our specified purposes.

☐ We have sufficient personal data to properly fulfil those purposes.

☐ We periodically review the data we hold and delete anything we do not need.

Principle 4 of the GDPR - Accuracy

At a glance:

We should take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.

We may need to keep the personal data updated, although this will depend on what we are using it for.

If we discover that personal data is incorrect or misleading, we must take reasonable steps to correct or erase it as soon as possible.

We must carefully consider any challenges to the accuracy of personal data. Checklist:

☐ We ensure the accuracy of any personal data we create.

☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.

☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it, as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

Principle 5 of the GDPR – Storage limitation

At a glance:

We must not keep personal data for longer than we need it.

We need to think about – and be able to justify – how long we keep personal data. This will depend on the purpose for holding the data.

We need a policy setting standard retention periods (see Data Retention Policy) wherever possible, to comply with documentation requirements.

We should also periodically review the data we hold, and erase or anonymise it when we no longer need it.

We must carefully consider any challenges to our retention of data. Individuals have a right to erasure if we no longer need the data.

We can keep personal data for longer if we are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Checklist:

☐ We know what personal data we hold and why we need it.

☐ We carefully consider and can justify how long we keep personal data.

☐ We have a policy with standard retention periods where possible, in line with documentation obligations.

☐ We regularly review our information and erase or anonymise personal data when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Principle 6 of the GDPR – Security, Integrity and Confidentiality

At a glance:

A key principle of the UK GDPR is that we process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Doing this requires us to consider things like risk analysis, organisational policies, and physical and technical measures. We also have to consider additional requirements about the security of our processing – and these also apply to any data processors.

We can consider the costs of implementation when deciding what measures to take – but they must be appropriate both to our circumstances and the risk our processing poses.

Where appropriate, we should look to use measures such as encryption.

Our measures must ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them.

The measures must also enable us to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

We also need to ensure that we have appropriate processes in place to test the effectiveness of our measures and undertake any required improvements.

Checklist:

☐ We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

☐ We have assessed what we need to do by considering the security outcomes we want to achieve.

☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.

☐ We use encryption where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity, and availability for the personal data we process.

☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.