



Data Protection Marketing Compliance Policy

Document SQ01539

Version 1.0

©Squire Technologies

This document is the property of Squire Technologies. Information contained herein is confidential. This document, either in whole or in part, must not be reproduced or disclosed to others or used for purposes other than that for which it has been supplied, without Squire Technologies prior written permission, or, if any part hereof is furnished by virtue of a contract with a third party, as expressly authorised under that contract.

Contents

1.0	Introduction.....	3
1.1	Background.....	3
1.2	Data protection.....	3
1.2.1	Key definitions.....	3
1.3	Privacy regulations.....	3
1.4	Marketing compliance.....	4
2.0	Roles and responsibilities.....	4
3.0	The right to be informed.....	4
4.0	Collecting data directly from the Data Subject, for the purposes of marketing, where consent is the lawful basis for processing (e.g. 'cold collection' of data).....	4
5.0	Using data for marketing purposes when the Data subject is about to be, or could be, a customer.....	5
6.0	Withdrawing consent.....	5
7.0	Use of data supplied by a third party.....	5
8.0	Policy Review.....	5

1.0 Introduction

1.1 Background

This policy complements the General Data Protection Policy by providing guidance on how Squire Technologies Ltd process data for marketing purposes, in line with the current requirements in law:

- The General Data Protection Regulation (“GDPR”)
- Any UK specific implementation of aspects of the GDPR into UK law
- Guidance from the Information Commissioner’s Office
- The Privacy and Electronic Communications Regulations (“PECR”)

Squire Technologies take compliance seriously and place high importance on the correct and lawful processing of all personal data as well as respecting the rights and privacy of our clients and employees. As such, this policy sets out the company procedures that are to be followed when processing data for marketing purposes.

1.2 Data protection

The GDPR is a European regulation which was ratified on 27th April 2016 and is enforced across the whole of the European Union, including the UK, from 25th May 2018. The Regulation replaces existing member state laws that implemented the previous EU data protection Directive and replaces the UK’s Data Protection Act 1998.

1.2.1 Key definitions

- “Personal data” relates to information that enables the identification directly or indirectly of a living individual, this includes the identification of an employee within a business but does not include generic business data.
- “Special categories of personal data” relates to more sensitive personal data including racial or ethnic origin, religious beliefs and health
- “Processing” means any activity carried out on the personal data including storage, collection, organisation and general use.
- A “Data Subject” is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor.
- A “Data Controller” is an organisation who determines the purposes of processing of data - typically this is the organisation that has collected the data in the first place and wishes to process it, i.e. Squire Technologies

A “Data Processor” is a person or organisation who processes data on behalf of the Data Controller (usually a third party).

1.3 Privacy regulations

The Privacy and Electronic Communications Regulations work alongside data protection. They give Data Subjects specific privacy rights in relation to how their data is used in electronic communications. Whilst the Regulations cover a much wider range of electronic communication areas (e.g. they govern the use of cookies on websites), in terms of marketing they govern the use of personal data for marketing calls, emails, texts and faxes.

This policy addresses marketing compliance relating to the use of data for electronic marketing purposes only.

1.4 Marketing compliance

- Where the data relates to a private individual who is a customer (or is about to be), provided the individual has been given a chance to opt-out at the point the data was collected initially, the marketing relates to the services we provide and we provide an opt-out in every subsequent marketing communication, we can market without seeking consent
- Data relating to an individual within a business can be used for marketing purposes provided they can opt-out of future communications
- Generic business data (that doesn't identify an individual employee within the business) can be used for marketing as it's not classed as personal data

2.0 Roles and responsibilities

2.1 All employees or teams responsible for marketing within our business are responsible for ensuring their marketing is compliant with this policy and any data protection or privacy rules.

3.0 The right to be informed

3.1 Under data protection rules the data subject has the right to be informed about what data is being collected, how it will be used along with other pieces of information:

- Details of who we are, why we're collecting the data, what it will be used for and how long we will use and keep the data, and the legal basis for processing
- Details of the Data Subject's rights:
 - Data Subject access requests
 - Have their data corrected if details change
 - Have their data deleted when it is no longer needed
 - Object to processing
 - Right to complain to the Information Commissioner's Office
- Details of how to withdraw consent

This information is provided at the point the data is collected.

3.2 Squire Technologies will ensure that website privacy policies, terms and conditions or other legal terms contain the required information to be supplied to Data Subjects at all relevant data capture points

3.3 The marketing employee or team will ensure that the correct information is supplied in all other scenarios where data is collected for marketing purposes (e.g. over the phone, via the post, at trade shows, etc)

4.0 Collecting data directly from the Data Subject, for the purposes of marketing, where consent is the lawful basis for processing (e.g. 'cold collection' of data)

4.1 To be compliant Squire Technologies will:

- Be open and transparent about why we are collecting the data and what is being consented to
- Provide an opt-in for the Data Subject to provide their consent
- Record the place and time that consent was given

4.2 Squire Technologies will collect consent in an open and transparent manner. This will include ensuring that the Data Subject takes a positive action to confirm consent for marketing purposes.

4.3 A record of time and place consent is given by the Data Subject is to be kept by the Squire Technologies marketing team. This may be automated via a system being used for collecting consent.

4.4. The purposes of the consent will be reviewed annually to ensure that consent continues to be the relevant lawful basis for processing and that the purposes for collecting the data in the first place have not changed

5.0 Using data for marketing purposes when the Data subject is about to be, or could be, a customer

5.1 As a matter of best practice at the point Squire Technologies collect the information necessary for offering the service, we will provide appropriate opt-ins to allow the Data Subject to opt-in to marketing materials.

6.0 Withdrawing consent

6.1 In all circumstances and on every occasion a marketing communication is sent, an option to opt-out of future marketing is provided. When marketing emails are sent an unsubscribe option is included.

6.2 We will accept a request to opt-out via any means including verbally or in writing, not just from clicking an unsubscribe link at the bottom of an email.

7.0 Use of data supplied by a third party

7.1 Where marketing data is provided by a third party Squire Technologies will ensure that the data was collected lawfully, particularly regarding the rules on consent. We shall therefore only use data from sources who are GDPR compliant.

7.2 Where marketing data is collected on our behalf it is our responsibility to provide the third party with the relevant wording and information needed to meet the consent requirements.

8.0 Policy Review

This policy will be reviewed periodically by the Data Protection Manager to ensure it is still relevant and up to date with any changes in the law, guidance or precedents set.