



Data Protection Policy

For this policy, Squaricle Group will comply with UK Data Protection Legislation by following several important principles regarding the privacy and disclosure of information in respect of individuals.

The purpose of this policy is to ensure that Squaricle Group staff and all associated third parties are aware of their obligations when handling personal information which identifies a natural living person, and that individuals internally and externally are aware of their rights. This is a public facing document and an additional Privacy notice is available to employees, associates, contractors or other 3rd parties.

Data Protection law

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 2018 and General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) are underpinned by important principles. These say that personal data must:

- Be processed fairly, lawfully, and transparently
- Be obtained only for specific, lawful purposes
- Be adequate, relevant, and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

When does this policy apply?

The Data Protection Legislation and therefore this policy applies to any situation where personal data for a natural living person can be identified. The protection of personal privacy



is very important to Squaricle Group, and any personal data collected and used MUST be treated in accordance with current Data Protection Legislation.

This policy applies to all employees, Partners, contractors, suppliers, and any other individuals working for or on behalf of Squaricle Group.

What is covered by this policy?

The processing, controlling, capture, storage, processing, management, distribution, and secure destruction of any personal data for natural living persons connected with Squaricle Group.

What personal data do we control/process?

We control/process a range of personal data which will be supplied to us or obtained during our work. This might include (this is not an exhaustive list, see Privacy Notices for completion):

- Name, personal address, telephone numbers and email address details
- Date of birth, nationality, passport numbers and passport images
- Bank account details
- National Insurance numbers, HMRC reference numbers
- Client data
- Client's client data
- Details relating to pensions and payroll

Data Protection Risks

This policy helps protect Squaricle Group from some real and every day security risks, including:

- Breaches of confidentiality (i.e. blagging offences or information being give out inappropriately)
- Failure to offer choice. (i.e. all individuals are free to choose how Squaricle Group uses their information (subject to other contractual obligations))
- Reputational damage (i.e. damage as a result of a hacking attack)

Responsibilities

The Board is committed to ensuring that Squaricle Group takes its responsibilities to comply with the Data Protection Legislation throughout the firm seriously. In order that we can operate our business and carry out our contractual obligations and duties Squaricle Group is



required to collect and use personal information relating to current, past and prospective clients, staff, business contacts, suppliers, third parties, third party service providers and others with whom we are required to communicate.

We may also be required by law or as part of our responsibilities as professional service providers to collect, use and share personal information with government departments, agencies, and regulators, or in some cases as part of the public interest. We will process this personal information lawfully, fairly and in a transparent way.

We believe that the lawful and correct way in which we deal with personal data is critical to our success, maintaining our reputation, integrity, and our clients' confidence in us as an open and professional organisation.

To enable Squaricle Group to meet our data protection commitments, whilst protecting our reputation, we will adopt appropriate and relevant data protection and privacy standards, guidelines, and requirements for legal, regulatory, or legitimate organisational purposes. When dealing with personal data Squaricle Group will:

- voluntarily appoint external resource to assist.
- process personal information only where this is strictly necessary in a fair and lawful way, ensuring it is relevant and adequate
- keep the information we hold to a minimum and only while we have a purpose to retain it in line with what is required of us by law and as set out in Squaricle Group Data Retention Policy
- where appropriate, we will carry out a Data Protection Impact Assessments where personal data is being processed
- have in place written contracts with organisations who process personal data on our behalf in support of delivering our business
- provide clear details about how personal information is used and by whom, taking particular care when dealing with high-risk personal information i.e. financial or payment information, sensitive or special category data & protected characteristics information.
- maintain full records of personal information processed by ourselves including the categories and purposes for each category



- keep accurate personal information, update as appropriate, store securely and do not hold for any longer than necessary, ensuring that we dispose of it appropriately
- take a 'data protection by design and default' approach, adopting and implementing the appropriate technical and organisational security measures
- throughout the entire lifecycle of our processing/controlling of data operations, including maintaining effective data protection policies to safeguard personal information
- adhere to relevant codes of conduct and sign up to certification schemes where appropriate and necessary
- only transfer personal information outside the UK in circumstances where it can be adequately protected
- provide a strategy for dealing with regulators across the EU (EEA) where services are offered to those who are resident in other EU (EEA) countries
- ensure that people know about their rights to see the personal information we hold about them and that we respond appropriately, taking into account the exemptions allowed by Data Protection Legislation, should a request for access, rectification or erasure (the right to be forgotten) be received.

To effectively manage our responsibilities Squaricle Group will ensure:

- the DPO has specific responsibility for data protection within Squaricle Group. You can contact our GDPR DPO by emailing roxy@squariclegroup.com It should be noted that appointing a DPO is not a legal requirement for Squaricle Group but an act of best practice.
- we document our approach to managing breach activity, managing Subject Access Requests (SAR's) and keep evidence of the steps we take to comply
- we regularly review and audit how we handle personal information
- we clearly describe the ways in which personal information is treated with a commitment to continuous improvement and will communicate to train and support internal departments as appropriate
- staff handling personal information understand that they are responsible for following good practice, they will receive appropriate training and are properly supervised. We regularly assess the performance of all our people who handle personal information.



- in the event of a data or privacy breach, we take swift and appropriate steps to minimise any reputational damage to Squaricle Group and any affected third parties and endeavour to minimise any associated business disruption
- we have appropriate systems and procedures in place to deal with breaches occurring outside of core office hours and that these will be managed in line with the defined company approach.

Special Category

We will only process special category data with the explicit consent from a data subject for one or more specified purposes, except:

- where processing is necessary for the purposes of carrying out our legal obligations, i.e. contractual, employment, social security, legal claims, judicial or criminal activity
- to protect the vital interests of the data subject or of another natural person
- processing is necessary for reasons of substantial public interest or archiving purposes in the public interest

When this approach is undertaken, this will be documented, shall be proportionate to the aim pursued, providing suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Special Category is defined as:

Personal data revealing racial or ethnic origin; personal data revealing political opinions; personal data revealing religious or philosophical beliefs; personal data revealing trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation.

Individual's rights

Squaricle Group ensures we are legal, fair, compliant, and transparent when we process personal information and subject to Data Protection guidelines, individuals have the right to the following:

- To be informed as to the purpose of the processing and the lawful basis for this processing.



- To access their personal data and to request rectification or erasure if it is inaccurate or incomplete.
- To restrict and/or object to the processing of their data.
- To data portability, allowing them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.
- We do not use automated individual decision-making or profiling. Should the need for us to do so ever arise we will ensure this is necessary as part of a contract, is lawful and/or based on the individual's consent.

Subject Access Requests

Everyone has the right to request a copy of the personal information we hold about them. We are required to complete any request we receive within one month of receipt and therefore it is very important that these requests are recognised, dealt with effectively, promptly and in line with our documented approach. The requestor should write to us to request this. If a request is received, you are to contact the Director of Operations: Brands, People & Quality immediately.

Privacy breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. For example, a data breach could include leaving a screen unlocked with personal data on the screen that is seen by someone without authority. An email sent to the wrong person with personal data included. A more serious breach could include a cyber-attack that sees you opening an attachment that contains a virus.

If a data breach occurs, the GDPR team must be informed by telephone or email **roxy@squariclegroup.com** immediately. We will investigate, record, and take any steps required to minimise the risk of further unlawful disclosure. If necessary, we will inform the data subject as soon as practical and inform the relevant authority within 72 hours of the data breach. If we appreciate that if fail to notify a breach when required to, this can result in a significant fine.

What is excluded from this Policy

This policy is not required to cover information held for deceased individuals. However, Squaricle Group will always apply best practice and therefore we will apply the same principles to deceased individuals.



Failure to comply with this policy

Data processing arrangements that are not in line with Data Protection Legislation create unnecessary risk. Staff who do not comply with this policy may be subject to disciplinary action.

Complaints

If you believe that Squaricle Group has processed your personal data in way that is unlawful and in breach of the guidelines set out by the GDPR you have the right to complain.

The Information Commissioners Office (ICO) is the independent supervisory authority set up to promote and oversee compliance with Data Protection Legislation in the UK. You can contact them at the Information Commissioner's Office, Wycliffe House, Water Lane, Cheshire, SK9 5AF, telephone number +44 (0)162 554 5745 or via their website at www.ico.org.uk.

Governance

The Squaricle Group Board have overall responsibility for the implementation of this policy.

Impact and effectiveness

The Director of Operations: Brands, People & Quality is responsible for the management and monitoring of effectiveness of this policy.

They can be contacted at roxy@squariclegroup.com