RLC VENTURES GDPR POLICY

Contents

Overview

The purpose of this policy, together with the ancillary documents in the appendix, is to ensure that the Organisation meets the requirements detailed in the General Data Protection Regulation ("GDPR").

Introduction

What is GDPR?

The GDPR took effect in UK from 25th May 2018 and updated the Data Protection Act to reflect changes in technology and data use. It places greater emphasis on documenting data protection procedures, accountability and governance arrangements, and how organisations manage data protection as a corporate issue. As an EU regulation, it is directly binding on member states. The GDPR is regulated and enforced in the UK by the Information Commissioner's Office ("ICO") but the FCA will consider compliance with GDPR when determining whether a regulated Organisation is operating in accordance with the FCA's Senior Management Arrangements, Systems and Controls ("SYSC") rules. The FCA has stated that, in the context of GDPR and as part of their obligations under SYSC, Organisations should establish, maintain and improve appropriate technology and cyber resilience systems and controls.

To whom does GDPR apply?

It applies to data 'controllers' and 'processors'.

A controller is: 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**'[1]

A processor is: 'a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**'[2].

In our regulated business as an asset manager, we are a data controller as we determine the purpose and means of processing the personal data that we hold. Generally, asset managers hold personal data in relation to investors in our funds and/or managed accounts, marketing contacts/business prospects and personnel. We may involve a processor to assist us but we ensure that such relationships are governed by GDPR-compliant contracts.

In our non-regulated business, we are a data controller as we determine the purpose and means of processing the personal data we hold. As an Angel network, we seek to connect Angel investors (seeking a potential return) with start-up businesses (requiring funding to grow their new venture). As such, we may collect and hold personal data as part of our rigorous due diligence on the start-up company (which relates to the individuals who own/control that business) and also the Angels wishing to invest. We may involve a processor to assist us but we ensure that such relationships are governed by GDPR-compliant contracts.

In order to process data, organisations are required to have a valid 'lawful basis'. There are 6 lawful bases, of which, organisations must have at least one:

[1] Art 4(7), GDPR
[2] Art 4(8), GDPR

1. **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract that we have with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary or us to comply with the law (not including contractual obligations as per 2 above).
4. **Vital interests:** the processing is necessary to protect a person's life.
5. **Public task**: the processing is necessary to perform a task in the public interest or for official functions and the task has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this cannot apply to an organisation which is a public authority processing the data to perform official tasks).

More detail is provided on the lawful bases for processing below, see heading 'Lawful Bases for processing'.

There are exemptions from GDPR where processing is performed by a natural person for a purely personal/household purpose and (in certain circumstances) where it is performed by a law enforcement agency or by EU institutions.

What is Personal Data?

Personal data is data related to a living individual who can be directly/indirectly identified from it or other information which is in the possession of/is likely to come into the possession of the data controller. It is defined broadly and includes information such as:

- Name
- Date of birth
- Address/location identifiers
- Online identifiers (such as IP address)
- Identification number(s) (such as client reference numbers, passport numbers, bank account details, etc)

Key-coded/'pseudonymised' data may also be personal data depending on how easy it is to attribute it to a specific person.

What is 'Special Category' Personal Data?

This refers to sensitive data which requires greater protection due to its private or potentially intrusive nature. In addition to requiring one of the 6 lawful bases for processing, organisations which process 'special category' data must also, in addition, meet one of the additional conditions for processing special category data under Art 9 of GDPR. Special category data includes information relating to an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health

- Sex life
- Sexual orientation

There are additional requirements in order to process 'special category' data (at Art 9(2)) which are, in summary:

a) The data subject has given explicit consent
b) Processing is necessary to carry out the specific rights of the controller or of the data subject in relation to employment and social security and social protection law
c) Processing is necessary to protect the vital interests of the data subject
d) Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body in relation to present/past members or certain connected persons of that body and are not disclosed outside that body.
e) Processing relates to personal data which is manifestly made public by the data subject
f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in a judicial capacity.
g) Processing is necessary for reasons of substantial public interest
h) Processing is necessary for the purposes of preventative or occupational medicine
i) Processing is necessary for reasons of public health e.g. protecting against serious cross border threats to health or ensuring safety of health care or medical products
j) Processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes.

What is Criminal Offence Data?

This refers to the processing of criminal conviction and offence data ("Criminal Offence Data"), which is similar to Special Category Data but requires greater protection due to its private or potentially intrusive nature.

For instance, details of criminal convictions uncovered about staff typically gathered during pre-employment screening will be Criminal Offence Data. In addition, details of criminal convictions uncovered in respect of existing directors of investee companies in private equity / venture capital type investments, typically gathered during legal due diligence, will also be Criminal Offence Data.

We are not permitted to keep a comprehensive register of criminal convictions, unless doing so under the control of an official authority.

There are additional requirements in order to process 'criminal offence' data (see sub-chapter titled '**Processing Criminal Offence Data'** below).

Do I need to pay a data protection fee to the ICO?

Organisations should check the ICO guide "The Data Protection Fee: A guide for controllers":

https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

As a general rule, if you are providing financial services and advice, research or consultancy services, you will be required to pay a data protection fee to the ICO. There are 3 tiers of fee which vary between £40 and £2,900. The tier which applies to the Organisation depends upon the following factors:

- Staff numbers

- Annual turnover
- Whether the organisation is a public authority
- Whether the organisation is a charity
- Whether the organisation is a small occupational pension scheme.

The fee tiers are as follows:

Tier	Fee	Criteria
1 – 'micro organisations'	£40	Maximum turnover £632k for the financial year; **OR** No more than 10 staff* members
2 – 'small & medium organisations'	£60	Maximum turnover of £36 million for the financial year; **OR** No more than 250 staff members
3 – 'large organisations'	£2,900	You do not meet the criteria for tiers 1 or 2.

* *This is broadly defined to include all employees, workers, office holders and Partners and is the average number who worked at the Organisation during the financial year (part-time staff are counted as one member of staff).*

If you were already registered under the Data Protection Act, you only need to pay the above fee when your existing registration expires. The ICO will issue Organisations with a reminder when the fee is about to fall due.

If you were not previously registered with the ICO, you must register either online (https://ico.org.uk/for-organisations/register/) or call 0303 123 113 for assistance.

Lawful bases for processing

The requirement to have a lawful basis is not new, instead, it replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 ("DPA"). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

The six lawful bases for processing are broadly similar to the old DPA conditions for processing, although there are some differences. We must review our existing processing, identify the most appropriate lawful basis, and ensure that it applies. It is most likely to be the same as our existing condition for processing.

Processing must be 'necessary'

Many of the lawful bases depend on the processing being "necessary". This does not mean that processing always has to be essential, however, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

Organisations cannot argue that processing is necessary because they have chosen to operate their business in a particular way. Instead, the question is whether the processing is necessary for the stated purpose.

Deciding upon which lawful basis to apply

We should consider which lawful basis best fits the circumstances in terms of our specific purposes and the context of the processing data. Where more than one basis applies, we will identify and document each at the outset.

The organisation must not adopt a one-size-fits-all approach. No one basis should be considered as being better, safer or more important than the others.

In deciding which basis best fits our circumstances, we should consider a variety of factors, including:

- What is our purpose – what are we trying to achieve?
- Can we reasonably achieve it in a different way?
- Do we have a choice over whether or not to process the data?

Contractual basis - Where there exists a contractual basis for processing personal data, for example under a client agreement for investment services or as an investor in a fund that we manage, then the appropriate lawful basis will be obvious – 'contract'.

If we are processing data for other than contractual purposes, then we are likely to have a choice between relying upon legitimate interests or consent. However, we should consider the wider context, including:

- Would individuals expect this processing to take place?
- What is our relationship with the individual?
- What is the impact of the processing on the individual?
- Is the individual concerned likely to object?
- Are we able to stop the processing at any time on request?

Legitimate interests - We may prefer to opt for legitimate interests as our lawful basis if we wish to keep control over the processing and take responsibility for demonstrating that it is in line with the individual's reasonable expectations and doesn't have an unwarranted impact on them.

Consent - On the other hand, if we prefer to give individuals full control over and responsibility for their data, including the ability to change their mind as to whether it can continue to be processed, we may want to consider relying on the individuals' consent.

When must we decide on our lawful basis

Organisations can choose a new lawful basis or decide that a different basis is more appropriate, however, it is important to get this right from the outset as it will be much harder to swap between lawful bases at will if you find that your original basis was invalid and we will be in breach of the GDPR if we did not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

What happens if we have a new purpose

If our purpose for processing data change over time, or we have a new purpose, we may not need a new lawful basis as long as our new purpose is compatible with the original purpose.

However, this does not apply to processing based on consent, as consent must always be specific and informed. In such circumstances, we would need to either get fresh consent which specifically covers the new purpose or find a different basis for the new purpose.

As a general rule, if the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with our original purpose for collecting the data.

Notwithstanding, even if the processing for a new purpose is lawful, we must also consider whether it is fair and transparent and give the individual information about the new purpose.

Documenting our lawful basis

We are required to be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify our decision. We therefore must keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies

The Group maintains the ICO's template spreadsheet as a record of which lawful basis it has applied for each client/investor/company/Angel/Marketing recipient and staff member. The Organisation's populated version is saved as a restricted access document and the link to the template is provided in Appendix VI (Recordkeeping policy).

Disclosing our lawful basis

We must inform people upfront about our lawful basis for processing their personal data. We include this within the Organisation's Privacy Notice sent to all individuals (see **appendices IV and V, Privacy Notices** for staff/contractors and Clients/website use, respectively).

As GDPR brings in new accountability and transparency requirements, we must therefore clearly document our lawful basis (see section titled '**Recordkeeping**').

Processing Special Category Personal Data

Where we seek to process special category data, we must identify and document both our 'lawful basis' for processing and a 'special category' condition for processing.

Our choice of lawful basis does not dictate which special category condition we must apply, and vice versa. For example, if we use consent as our lawful basis, we are not restricted to using explicit consent for special category processing.

Processing Criminal Offence Data

Where we seek to process Criminal Offence Data, which includes data about criminal convictions, criminal offences or related security measures, we must identify and document both our 'lawful basis' for processing and a 'separate condition' for processing this type of data.

Territorial Scope

GDPR applies to all EU countries and any individual or organisation trading with them. Therefore, GDPR will still apply to a company based outside the EU who is processing the data of an EU data subject.

'Accountability Principle'

Article 5(2) of GDPR requires organisation to be able to demonstrate that we comply with the principles of the Regulation and state explicitly that this is our responsibility.

The Data Protection principles of GDPR are that personal data must be:

1	processed ***lawfully, fairly and in a transparent manner*** in relation to the data subject ('lawfulness, fairness and transparency');
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, in

	accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3	***adequate, relevant and limited to what is necessary*** in relation to the purposes for which they are processed ('data minimisation');
4	***accurate and, where necessary, kept up to date***; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
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 are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6	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 ('integrity and confidentiality').

Our Organisation demonstrates that we meet the above principles as we have created policies and procedures which outline the measures taken to meet the requirements. Our policies are as follows:

- GDPR Policy (this Policy)
- Completed ICO GDPR Documentation Controller Template
- Subject Access Request Policy
- Consent Policy
- Data Breach Recording and Response Plan
- Recordkeeping policy (personal data)
- Privacy Notices (for Staff and clients/investors whose personal data we hold).

Our procedures are as follows:

- All staff must read this document and confirm, by email, to the Compliance Officer, that they have done so (to ensure they have a basic understand of GDPR).
- The Compliance Officer is the main point of contact for data protection at the Organisation.
- The Compliance Officer is responsible for updating/maintaining the data protection recordkeeping (maintains the ICO GDPR Documentation Controller Template). Refer to appendix VI (recordkeeping policy).
- All subject Access Requests must be forwarded to the Compliance Officer
- All data breaches must be notified to the Compliance Officer
- Privacy Notices are sent to all clients/investors (upon take-on) and staff (upon joining)
- Any transfers of data outside of the EU must be pre-notified to the Compliance Officer
- Annual regulatory/financial crime training includes an overview GDPR (personnel attending this training are the same as those working within the non-regulatory business therefore it will apply to all persons within RLC Ventures).
- The appendices to this document are our working policy documents and we monitor these as part of our compliance monitoring programme.

After due consideration, our Organisation has determined that it does not require a Data Protection Officer ("DPO"). This is on the basis that the GDPR only requires the following to appoint a DPO:

- Public authorities (except for courts acting in their judicial capacity);
- Organisations whose core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- Organisations whose core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

The organisation is a data controller and therefore, as a corporate entity, must comply with GDPR. The Governing Body of the Organisation has nominated the Compliance Officer as having responsibility for the general day-day oversight of the Organisation's GDPR compliance. Any concerns relating to the Organisation's adherence to GDPR must be escalated to the Governing Body (via the Compliance Officer) who have ultimate responsibility for the data protection systems and controls and the Organisation's compliance with GDPR.

Transfer of Data (outside EU)

Chapter 5 of GDPR requires that certain conditions must be met before personal data can be transferred outside of the EU. These are outlined below. Note that the Firm may use a Server services which are based outside of the EU. However, this is not a 'transfer of data' but a 'transit' (as the data is not accessed/manipulated in the Server's jurisdiction) therefore the rules on transfer of data to do not apply in this instance[3].

'Adequacy'

The transfer of personal data may take place where the European Commission has decided that the third country/territory/specific sector within that third country has an 'adequate level of protection' in terms of holding and processing of data. Therefore, personal data may not be transferred to a country or territory outside the EU unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

At the time of writing, the European Commission recognizes the following third country jurisdictions as meeting the adequacy requirements:

- Andorra
- Argentina
- Canada (commercial organisations)
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- US (limited to the 'Privacy Shield Framework'[4])

[3] Principle 8, Data Protection Act.

[4] The Privacy Shield Framework took effect in Aug 2016 and protects the fundamental rights of anyone in the EU whose personal data is transferred to the US for commercial purposes. Please click this link for more information: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

At the time of writing, adequacy talks are ongoing with respect to:

- Japan
- South Korea

Please note that the above adequacy decisions do not cover data exchanges where required under Art 36 of the Police Directive.

Where an Organisation wishes to transfer data to a third country for which there is not an EC decision on data protection adequacy, it may only do so if it has made sure that certain 'appropriate safeguards' are in place and that enforceable data subject rights and effective legal remedies for data subjects are available[5]. The following section outlines what is meant by 'appropriate safeguards'.

'Appropriate Safeguards'

We may transfer personal data outside the EU (and to a country which has not received a positive 'adequacy decision' from the EC) where the counterparty receiving the personal data has provided adequate safeguards, individuals' rights are enforceable and effective legal remedies are available following transfer. Adequate safeguards include:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between Organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission[6];
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Where data is transferred intra-group, Organisations are most likely to ensure that appropriate safeguards are in place by ensuring that there are binding corporate rules in place governing the transfers. This might be documented in the Organisation's procedures manuals, compliance manual or IT security policy.

We may transfer data to another company within our Group and we understand that we have a corporate responsibility to ensure that individuals rights under GDPR are enforceable and legal remedies must be available to them post-transfer. Any transfers which sit outside of the

[5] Art 46(1), GDPR

[6] European Commission model contract clauses for data transfers between EU and non-EU countries may be found at this link: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

documented corporate rules relating to transfers outside of the EU should be approved by the Compliance Officer prior to transfer.

Where data is transferred to an external entity (where that entity is not within a jurisdiction with an 'adequacy decision'), Organisations are most likely to ensure that appropriate safeguards are in place by ensuring that there is a standard clause in place. Where the Organisation relies on third party service providers such as Administrators, Custodians, Law Organisations it must ensure that the Third Parties outside of the EU have in place sufficient levels of protection that are equivalent to those required by the Act.

Where adequate safeguards cannot be met, the Organisation should terminate its contract or ensure that no personal data is being transferred.

Where the Organisation contracts with a non-EU third party, it expects that the European Commission approved standard contractual clauses (or equivalent) which regulate the transfers of certain Personal Data between itself and other non-EU service providers are in place. All third-party transfers should be approved by the Compliance Officer prior to transfer outside the EU.

'Derogations' (from the transfer of data requirements)

Although not encouraged, there are a number of limited circumstances where Personal Data can be transferred outside of the EU:

1. Consent. Where the Organisation can transfer personal data overseas if it has the individual's consent, which should be given clearly and freely and may later be withdrawn by the individual
2. Contract performance. Where it is necessary to perform a contract of services.
3. Substantial Public interest. This is a high threshold to meet and it is most likely to be relevant in areas such as preventing and detecting crime; national security; and collecting tax.
4. Vital Interest. The Organisation can transfer personal data overseas where it is necessary to protect the vital interests of the individual. This relates to matters of life and death.
5. Public Registers. The Organisation can transfer overseas part of the personal data on a public register, as long as the person transferred complies with any restrictions on access to or use of the information in the register.
6. Legal Claims. Where necessary for the execution of legal proceedings
7. Where it is being sent to a country recognized by the Commission as offering adequate protection (this would include to US organisations which are EU-US Privacy Shield Certified.)

Please revert to the Compliance Officer if in any doubt.

One-off/Infrequent transfers/small number of data subjects

Even where 'adequacy', 'appropriate safeguards', 'derogations' do not apply, personal data may still be transferred outside of the EU. However, it is subject to certain conditions which include the requirement to inform the relevant supervisory authority of the transfer and provide additional information to individuals (under Art 13 and 14 of GDPR) and inform them what 'compelling legitimate interests' are being pursued. Transfers of data on this basis are only permitted where it:

- is not being made by a public authority where executing its public powers;
- is not repetitive (similar transfers are not made on a frequent/periodic basis);
- involves data related to only a limited number of individuals;

- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

Data Subject Rights

GDPR protects the following 8 rights of individuals:

The right to be informed

GDPR requires that Organisations are specific about how they use the personal data that they hold on individuals and they must actively inform those individuals about what information they hold, the basis for processing their data, the types of data held and shared with others (if applicable) and their individual rights.

Organisations must provide individuals with a 'Privacy Notice' which contains the above information (so called 'privacy information') in a clearly worded and transparent way. This must be provided to individuals 'within a reasonable period' of obtaining the personal data and no later than 1 month. The Privacy Notice must be accessible to individuals and individuals must be made aware of it. For instance, if an Organisation publishes it's Privacy Notice on it's website, it should ensure that Clients are aware of it.

The Organisation has separate Privacy Notices (for Staff/contractors and for Clients/website) which may be found at Appendices IV and V to this document.

The right of access

GDPR allows individual data subjects to access their personal data (and supplementary information) so that they aware of and can verify the lawfulness of the processing.

Where an individual makes a 'subject access request' to access personal data, the Organisation must provide that information promptly, in a commonly used electronic format and at the latest within one month receipt (unless the requests are complex or numerous in which case it must be provided within a further two months). Organisations may refuse a request where it is manifestly unfounded or excessive (or they may charge a reasonable fee based upon the cost of processing the request).

The right to rectification

Individuals have a right to request the rectification of inaccurate or incomplete personal data and the Organisation has one month to respond. This refers to the accuracy principle whereby data 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'[7].

The right to erasure

Individuals can exercise their right to have their personal data erased in certain circumstances, for example, where it is no longer necessary for the original purpose it was collected, or the individual objects to their data being held for direct marketing purposes. However, the right to erasure is not absolute. An individual may not have their personal data erased where, for instance, it is necessary to comply with a legal obligation or for the establishment, exercise or defence of legal actions, or, where it is in the public interest. Where a valid request under the right to erasure is

[7] GDPR, Art 5(1)(d)

The right to restrict processing

Similar to the right to erasure, the right to restrict processing is not an absolute right. Individuals can request that the processing of their personal data is restricted in certain circumstances, for instance, when the individual believes there are inaccuracies in the data the Organisation holds and wishes to restrict processing whilst it is verified, or, where the Organisation no longer needs to process the personal data but the individual wishes the Organisation to retain it to establish, exercise or defend a legal claim. Processing is 'restricted' where the Organisation stores the personal data but may not use it. The Organisation must take measures to ensure that the data is flagged as restricted or inaccessible to persons who may inadvertently process it. An Organisation may only process stored restricted data where the individual consents or where there are applicable legal or public interest reasons for doing so.

The right to data portability

Individuals may obtain and transfer their personal data from one IT platform/service to another, without undue obstruction, where the data is being processed by automated means e.g. price comparison websites.

The right to object

Where the Organisation processes personal data on the basis of 'legitimate interest' (or public interest/official authority), direct marketing (including profiling) and for scientific research/statistics purposes, the individual has a right to object. The Organisation must ensure that it's privacy notice explicitly notifies individuals of this right, and in any event, 'at the point of first communication'. If the Organisation receives an objection in relation to its direct marketing activities, it must cease processing data for this purpose immediately (and where such marketing takes place online the Organisation must offer an opt-out). The Organisation may only continue to process data following an objection if it can demonstrate compelling legitimate grounds which override the interests, rights and freedoms of the individual, or, the processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

There are separate and detailed requirements relating to where Organisations process data in line with automated individual decision making and profiling. Organisations conducting such activities should refer to the detailed guidance has been issued by the Article 29 Working Party (WP29) and the ICO:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

IT security

Please note that the following is HIGH LEVEL GUIDANCE ONLY (as this document does not purport to be specialist IT advice). It is for the Organisation to consider its IT arrangements/controls in line with GDPR.

One of the principles under GDPR - the 'security principle' - requires that data must be processed securely and in line with 'appropriate technical and organisational measures'. This is not a new

requirement as the Data Protection Act already required Organisations to have data security measures in place. The key requirement is that Organisations must be able to prevent the personal data that they hold from being accidentally or deliberately compromised. This applies in relation to (a) cybersecurity (the protection of networks and information systems) and (b) physical and organisational measures, and is outlined in more detail below.

GDPR requires Organisations to put in place IT security measures that are proportionate. Art 32(1) of GDPR states:

"*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate technical and organisational measures to ensure a level of security appropriate to the risk***".

Where an Organisation is processing data, they should consider the following factors, as proportionate:

Obscuring	Consider whether pseudonymisation and encryption is appropriate (updated ICO guidance on encryption not available yet)
'CIA triad'	Ability to ensure the ongoing '**c**onfidentiality, **i**ntegrity, **a**vailability' of information security. The Organisation's IT security measures should guarantee all 3 are met.
Resilience	Are the processing systems and services able to continue operating under adverse conditions e.g. a physical/technical incident and can they be restored to a working state.
Security Event	Consider how the Organisation would restore the availability and access to personal data in a 'timely manner' if there was a physical/technical incident e.g. ensure there is a back-up process.
Testing	GDPR requires Organisations to test the effectiveness of IT security measures. Frequency and detail of these depends upon the nature and scale of processing.
Code of certification	If your security measures include a product/service which adheres to a GDPR code of Conduct (once these have been approved) or Certification (once these have been issued), this can demonstrate your compliance with the Security requirements.

Cybersecurity – Factors to consider.

The ICO's guidance on security suggests that Organisations look at the following factors when reviewing IT systems (and whether specialist external advice is required, depending on the sophistication of your systems, usage requirements and technical expertise of staff):

System security	Check the security of your network and information systems, including those which process personal data
Data security	Check the security of the data held in the Organisation's systems e.g. ensuring appropriate access rights/authorisations and that data is held securely.
Online security	Check the security of your website and any other online service or application you use
Device security	Consider implementing policies on 'Bring-your-own-device' (BYOD) if applicable.

	Note that this link relates to pre-GDPR guidance on BYOD is currently under review by the ICO (so please check the website for updates). https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

You may wish to consider the requirements of 'Cyber Essentials' (the Government scheme which outlines basic IT security controls which are simple enough to be self-implemented by companies themselves). Cyber Essentials provides guidance on five technical controls which, if implemented, will indicate that you are operating under an appropriate (minimum) level of security. They are, in summary:

1. **Use a firewall to secure your internet connection:** A firewall creates a 'buffer zone' between your IT network and external networks whereby incoming traffic can be filtered to determine whether it poses a threat to your network or not.
2. **Choose the most secure settings for your devices and software**: Check the settings on new software and devices to ensure that any default settings (which may present more opportunities for cyber attackers to gain unauthorised access to your data) are changed. Change all default passwords and implement extra security such as two-factor authentication (2FA) where appropriate.
3. **Control who has access to your data and services**: implement access controls for software, settings, online services and device connectivity functions to ensure permissions are appropriate to the functions staff or users are performing.
4. **Protection from viruses and malware**: implement anti-malware systems, consider 'whitelisting' (creating a list of applications allowed on a device whereby unlisted applications are then blocked) and 'sandboxing' (sandboxed applications run in an isolated environment with very restricted access to the rest of your device/network).
5. **Keep your devices and software up to date**: Ensure staff click on any updates to software/applications issued by the manufacturers/developers as these fix security vulnerabilities in addition to adding new features.

Organisations should, as a matter of good practice, review the above guidelines on the Cyber Essentials website and complete the checklists on the 'advice' page (you are advised to keep a record of your completed checklist):

https://www.cyberessentials.ncsc.gov.uk/advice/

Physical Security – Factors to consider

The ICO's guidance on security suggests that Organisations look at the following factors when reviewing the Organisation's physical security:

Access (pre-entry)	Review the quality of doors and locks and the protection of the premises by alarms, security lighting or CCTV.
Access (post-entry)	How is physical access controlled e.g. visitor passes, on-duty receptionist/onsite security officer, temporary fob access to restricted areas
Disposal of data	Check how hard copies of personal data destroyed e.g. office shredder, secure disposal outsourced to third party (what due diligence performed at outset)? Electronic waste e.g. decommissioning of computers/devices.
Storage	How is IT equipment stored, in particular mobile devices – how secure is this? Are cabinets containing hard copies of personal data lockable/fob-entry room?

What must I consider if I am using a Data Processor?

If one or more organisations process personal data on the Organisation's behalf, these are data processors under GDPR. Organisations must be aware that, as data controller, they remain responsible for ensuring compliance with GDPR. However, the data processor must also comply with the security provisions under GDPR.

Data controllers using a data processor must ensure that they obtain the following assurances from a Data processor which is processing data on their behalf:

- Obtain sufficient guarantees from the data processor about its security measures;
- Ensure that the contract stipulates that the processor takes all measures appropriate to the nature, scope, context and purposes of processing under Art 32 of GDPR ('security of processing') i.e.
    - Pseudonymisation and encryption of personal data
    - Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident
    - Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures ensuring the security of the processing.
- Ensure that the contract includes a requirement that the processor makes available all information necessary to demonstrate compliance i.e. to enable the Organisation/authorised third party to audit and inspect the processor

Staff Training

Recital 83 and art 32(4) of GDPR require that any person acting under the Organisation's authority, with access to personal data, only processes that data where they have been explicitly instructed to do so. The ICO additionally interprets this provision as requiring Organisations to train staff so that they understand the Organisation's security policy and procedures relating to personal data.

The ICO recommends that Organisation's conduct both initial and refresher training, by a suitably knowledgeable person, including the following topics:

- The Organisation's responsibilities as a data controller
- Staff responsibilities for protecting personal data – outlining that they may commit a criminal offence if they deliberately access or disclose personal data without authority.
- Proper procedures to identify callers
- The Dangers of people attempting to get hold of personal data by deception (incl. how to identify 'phishing' attacks or encouraging staff to alter information when they are not permitted to do so).
- Restrictions on the personal use of systems by staff e.g. to avoid computer viruses/spam).

The Organisation includes a high-level summary of GDPR as part of it's annual regulatory and financial crime training provided to all staff at the Organisation and notifies staff where the Organisation's GDPR policies are located.

Recordkeeping

The Compliance Officer is responsible for the Organisation's data retention procedures, including determining the Organisation's data retention, archiving, and destruction schedule of all (physically stored data and electronic storage device) data – this may vary from different investment service or investment product. In doing so, the Compliance Officer shall have regard to the legal, compliance, business needs and privacy obligations.

The Organisation must document the following, and in doing so may seek to rely on the Information Commissioner's Office (ICO) pro forma templates:

- An information audit (or data-mapping exercise) of what personal data we hold and where it is stored; and
- Why personal data is used, who it is shared with and how long it is kept.

The (ICO) pro forma templates can be found here, and includes a template for both Controllers and Data Processors:

> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Data Retention periods

In establishing the Organisation's data retention periods, the Compliance Officer must:

- Consider applicable legal, compliance and data protection requirements;
- Consult with senior management and different business units (if applicable) on the collection, storage and archiving of data;
- Identify both internal and external entities that collect, store or archive Organisation data; and
- Consider specific retention requirements for sensitive data and procedures for handling stored information during litigation periods.

During the data retention period, the Compliance Officer is responsible to ensure that archived data is retrievable. This specifically includes ensuring that as/when new software or hardware is implemented that the IT team ensures that the new system(s) can read legacy data, and that encrypted data is easily retrievable.

When establishing retention periods, the Compliance Officer may seek to rely on the Information Commissioner's Office (ICO) guidance:

> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/

Appendix I: Subject Access Request Policy

Overview

The purpose of this policy is to provide the Organisation with the procedure should it receive a Subject Access Request ("SAR") from a data subject.

What is a SAR?

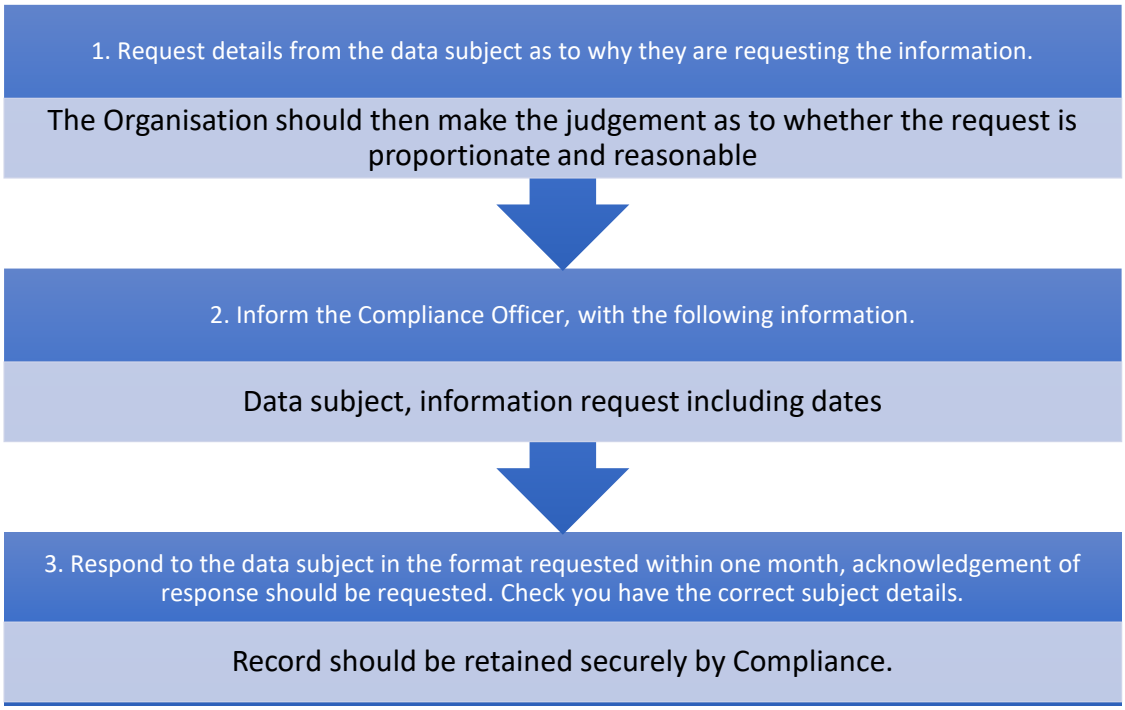
A SAR is a request for personal information that the Organisation may hold about a data subject. If a subject wishes to exercise their subject access right, the request must be made in writing. The purpose of a SAR is to make subject aware of and allow them to verify the lawfulness of processing of their personal data.

Under the GDPR a data subjects have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

1. The reasons for processing data
2. A description of the personal data being held
3. Details on any other entity who has or will have access to their information
4. Any details of the origin of their data if it was not collected from them.

Procedure

The Organisation has one month to respond to a SAR, any SAR's should be reported directly to the Compliance Officer and the following procedure initiated:



Appendix II: Consent Policy (N/a)

The Organisation does not currently rely upon consent as the lawful basis for processing.

If a member of staff believes/wishes to apply consent as a lawful basis for processing, please refer to the Compliance Officer in the first instance.

Appendix III: Data Breach Recording Policy

Overview

In accordance with Article 34 and 35 of the General Data Protection Regulation the Organisation is required to have in place a Personal Data Breach Policy. This policy in concerned with how breaches in person data is reported.

What is a Data Breach?

A data breach can be defined as the following "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

There are three different types of beaches listed:

1. Breach in Confidentiality – an unauthorised or accidental disclosure of, or access to, personal data.
2. Breach in Integrity – an unauthorised or accidental alteration of personal data.
3. Breach in Availability – unauthorised or accidental loss of access to, or destruction of, personal data e.g. deletion of data accidentally or by an unauthorised person, a lost decryption key in the case of encrypted data, or unavailability due to a power failure or service attack.

What should the Organisation do in the event of uncovering a breach?

Firstly the Organisation should assess whether the breach is notifiable to the ICO. Not all breaches are reportable, if the information is encrypted, the information is already in the public domain etc

Under Article 33 of the GDPR the Organisation should asses the risks posed to the data subject including loss of control over or confidentiality of personal data, identity theft, damage to reputation, discrimination, fraud and financial loss.

Next the Organisation must assess the likelihood and impact of the breach taking into account the following factors:

- ***Type of breach.*** Confidentiality, availability, integrity.
- ***Nature, sensitivity and volume of personal data.***
- ***Severity of consequences for individuals.***
- ***Number and characteristics of affected individuals.***
- ***Ease of identification of individuals***

Notification Requirements

A Organisation has 72 hours to notify the DPA once it has become aware of a data protection breach. In the event that any member of staff is aware of a data breach the Compliance Officer should be informed immediately.

In the event that a breach affects individuals in more than one member state, the Organisation will need to notify its lead supervisory authority. Once its been assessed that the breach requires reporting, the notification should include the following information:

1. The nature of the personal data breach (including categories of data and approximate number of data subjects impacted),
2. The name and contact details of the Organisation's data protection officer,
3. An analysis of the likely consequences of the breach, and
4. What measures taken or proposed to be taken to mitigate the negative impact of the breach and how this will be prevented going forward.

The data subject must be notified without “undue delay”. The notification must contain information including in plain English the nature of the breach, the contact details of the Organisation and the consequences of the breach to the subject.

Record Keeping

The GDPR requires controllers to keep records of any personal data breaches, even if the breaches were not notifiable. These records must contain details of the breach, its effects and consequences, and any remedial action taken. The Organisation should also suggests documenting any justifications for not reporting the breach.

Penalties for Failure to Comply

The fine for a failure to report a breach can be up to the higher of 2% turnover or €10 million. The Organisation should note however that a failure to notify may show systematic security failures which could constitute a separate breach of the GDPR and attract a separate fine up to the same level.

Appendix IV: Privacy Notice (Staff & Contractors)

Introduction

RLC Ventures (the "Organisation") is committed to protecting and respecting your privacy. This Policy explains how your personal information is processed by the Organisation, including any affiliates listed in the Data Controllers and Contact section below (hereinafter also collectively referred to as "us", or "we").

This Policy covers personal information relating to you that we may collect in relation to your employment. This policy describes how you can access and make certain choices about how we use your personal information.

Your personal information that we may collect

We may collect and process data the below listed information with respect to your employment.

We may collect this information from a number of sources, including directly from you, via our affiliates, delegates, partners, service providers, professional advisors, or third-party entities with whom we undertake due diligence checks upon you. In doing so, we will ensure that the information we collect is proportionate to our stated purposes.

Where relevant, we may collect and process personal information related to persons related to you. In such circumstances, it is your responsibility to ensure you have permission from that third-party for us to collect their information and you remain responsible for ensuring that the third-party understands how their information is being used.

Individual staff or contractors employed by the Organisation

We may collect and process your: personal details, including your name, address, email and telephone numbers, date of birth, nationality; previous employment details, including your previous employers' name, your position or title and other reference related materials obtained you're your previous employer; details in order for the Organisation to meets its obligations under Financial Conduct Authority rules (or in line with applicable legal or statutory requirements in relation to our non-regulated business), including information required to undertake required criminal/credit background checks, information on your fitness and propriety, and any information relating to you that we are required to maintain in respect of any regulatory investigation; detail of your banking records, in order to allow us to pay you in respect of your employment contract / contract for services.

Our legal bases and purpose for holding your personal information

Unless specifically stated otherwise in a Privacy Notice provided to you, we use your personal information in the following ways and based upon the following lawful bases:

Individuals connected with our investment services

1. In order to achieve our legitimate interests. In doing so, we ensure that: your rights and interests are considered and protected and it has a minimal privacy impact upon you; we are able to demonstrate that we use your data in a proportionate manner and you would not likely be surprised or likely to object to our usage; we can lawfully disclose personal data to a third-parties where we can demonstrate that this disclosure is justified. This includes information obtained pre-employment, for example as part of the interview and employment process;

2. In order to fulfil our contractual obligations to you in order to facilitate the provision of your employment / contract for services with us;
3. To comply with our legal or regulatory obligations. For instance, under the UK Financial Conduct Authority SUP rules (Approved Persons);
4. Based upon reasons of substantial public interest; and
5. Where your personal information is public information by your own actions.

When we may disclose your personal information

We may disclose your personal information with the following category of recipients, and based upon the legal bases and purposes set-out above:

1. Our affiliates, including where relevant third-party investment funds that we either manage or advise.
2. Our partners and service providers, including service providers appointed by the third-party investment funds that we either manage or advise and our appointed representatives;
3. Any law enforcement, court, regulator or other government authority in order for us to comply with a legal obligation laid down by UK or EU law. This includes the provision of information relating to any affiliate of the Organisation.
4. A prospective buyer of our business, including where we intend to sell part of our business or merge with another third-party.

How and where we store your personal information

We store your physically held personal information in our UK offices. Whereas we store your electronically held personal information on backed-up servers provided by our service providers which might not be located in the EU.

We take all reasonable steps to protect your personal information; however, where you choose to transmit your personal data to us via the internet, we do not guarantee the security of the personal information transmitted and therefore any transmission is at your own risk.

We may transfer your personal information to our affiliates, partners or service providers that are based outside of the European Economic Area. In such circumstances, we will ensure that your personal information is adequately protected to European Commission approved standards.

Your rights as a Data subject

In certain circumstances, in relation to your data, you have the right to:

1. The right to be informed
2. The right of access,
3. The right to rectification,
4. The right to erasure,
5. The right to restrict processing,
6. The right to data portability,
7. The right to object, and
8. Rights in relation to automated decision making and profiling.

Further details of your rights can be found at the ICO website, however, please note that your rights are subject to our overarching legal responsibilities:

> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

If you wish to exercise any of these rights, please contact the relevant data controller (listed below).

How long we retain your personal information

We reserve the right to retain your personal information for as long as we reasonably believe it to be necessary in order to facilitate our legitimate interests, in order for us to comply with our legal or regulatory obligations, where based upon reasons of substantial public interest, or where your personal information remains public information by your own actions. For further information, please contact the relevant data controller (listed below).

Our responsibilities when we make changes to our Privacy Policy

We may make changes to our Privacy Policy at any time and may do so without expressly notifying you of these changes. However, should the legal bases or purpose for processing your personal information changes then we shall expressly notify you.

Our Data Controllers and how to contact us

Questions or individual data requests relating to this Policy should be addressed to the relevant data controller. For the purpose of the data protection legislation, the relevant data controllers are:

Data Controller	Responsible for
RLC Ventures Ltd 91-93 Buckingham Palace Rd Victoria, London SW1W 0RP GDPR contact person: Reece Chowdhry	All investment and business administration activities.

Appendix V: Privacy Notice (Clients & Website Use)

Introduction

RLC Ventures (the "Organisation") is committed to protecting and respecting your privacy. This Policy explains how your personal information is processed by the Organisation, including any affiliates listed in the Data Controllers and Contact section below (hereinafter also collectively referred to as "us", or "we").

This Policy covers personal information relating to you that we may collect through any medium, including specifically in relation to the investment services we provide to you, via our partners and service providers, or through our website. This policy describes how you can access and make certain choices about how we use your personal information.

Your personal information that we may collect

We may collect and process data the below listed information with respect to persons connected with the Angel networking and investment services that we provide. As well as collecting personal data from our clients, we may also process personal data about relevant persons connected with the investment services, for example investors in our funds, co-investors, directors of investee startup companies, etc.

We may collect this information from a number of sources, including directly from you, via our affiliates, delegates, partners, service providers, professional advisors, or third-party entities with whom we undertake due diligence checks upon you. In doing so, we will ensure that the information we collect is proportionate to our stated purposes.

Where relevant, we may collect and process personal information related to persons related to you. In such circumstances, it is your responsibility to ensure you have permission from that third-party for us to collect their information and you remain responsible for ensuring that the third-party understands how their information is being used.

Individuals connected with our investment services

We may collect and process your: personal details, including your name, address, email and telephone/fax numbers, date of birth, nationality; employment details, including your employers name, your position or title and your corporate contact details; information on your financial circumstances, including your profession, income, assets and liabilities, as well as sensitive and/or criminal data as part of our standard due diligence process.

Individuals connected with our partners and service providers

We may collect and process your: contact information, including your name, address, position, email and telephone/fax numbers; financial details, including relevant details for invoicing and billing; and KYC documentation, if and where required under relevant Anti-Money Laundering or Counter Terrorism Financing ("AML/CTF") legislation.

Individuals connected with our website

We may collect and process your: personal details, including your name, address, email and telephone/fax numbers, as well as your login identification and password details; and technical information, including your IP address, browser information, and details relating to your visit behavior on our website. Further details are provided under our '**Cookie Policy**' heading below.

Our legal bases and purpose for holding your personal information

Unless specifically stated otherwise in a Privacy Notice provided to you, we use your personal information in the following ways and based upon the following lawful bases:

Individuals connected with our investment services

1. In order to achieve our legitimate interests. In doing so, we ensure that:
    a. your rights and interests are considered and protected and there is a minimal privacy impact upon you;
    b. we are able to demonstrate that we use your data in a proportionate manner and you would not likely be surprised or likely to object to our usage;
    c. we can lawfully disclose personal data to a third-parties where we can demonstrate that this disclosure is justified;

2. To comply with our legal or regulatory obligations. For instance, under the UK Financial Conduct Authority Conduct of Business rules and/or relevant AML/CTF legislation;
3. Based upon reasons of substantial public interest; and
4. Where your personal information is public information by your own actions.

Individuals connected with our partners and service providers

1. In order to fulfil our contractual obligations to you in order to facilitate the provision of goods or services. This includes where you have asked us to do something before entering into a contract, for example to provide a quote;
2. To comply with our legal or regulatory obligations. For instance, under relevant AML/CTF legislation;
3. Based upon reasons of substantial public interest; and
4. Where your personal information is public information by your own actions.

Individuals connected with our website

1. In order to achieve our legitimate interests. This may include electronic communications between us; the provision of investment information to you; details in order for us to manage and improve our website; for us obtaining and recording details relating to your visit behaviour on our website;
2. To comply with our legal or regulatory obligations. For instance, under relevant AML/CTF legislation;
3. Based upon reasons of substantial public interest; and
4. Where your personal information is public information by your own actions.

When we may disclose your personal information

We may disclose your personal information with the following category of recipients, and based upon the legal bases and purposes set-out above:

5. Our affiliates, including where relevant third-party investment funds that we either manage or advise.
6. Our partners and service providers, including service providers appointed by the third-party investment funds that we either manage or advise and including our appointed representatives where appropriate;
7. Any law enforcement, court, regulator or other government authority in order for us to comply with a legal obligation laid down by UK or EU law. This includes the provision of information relating to any affiliate of the Organisation.
8. A prospective buyer of our business, including where we intend to sell part of our business or merge with another third-party.

How and where we store your personal information

We store your *physically held* personal information in our UK offices. Whereas we store your *electronically held* personal information on third party backed up servers that might not be located in EU. We understand that we have to ensure that service providers do comply with GDPR requirements.

We take all reasonable steps to protect your personal information; however, where you choose to transmit your personal data to us via the internet, we do not guarantee the security of the personal information transmitted and therefore any transmission is at your own risk.

We may transfer your personal information to our affiliates, partners or service providers that are based outside of the European Economic Area. In such circumstances, we will ensure that your personal information is adequately protected to European Commission approved standards.

Your rights as a Data subject

In certain circumstances, in relation to your data, you have the right to:

5. The right to be informed
6. The right of access,
7. The right to rectification,
8. The right to erasure,
9. The right to restrict processing,
10. The right to data portability,
11. The right to object, and
12. Rights in relation to automated decision making and profiling.

Further details of your rights can be found at the ICO website, however, please note that your rights are subject to our overarching legal responsibilities:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

If you wish to exercise any of these rights, please contact the relevant data controller (listed below).

How long we retain your personal information

We reserve the right to retain your personal information for as long as we reasonably believe it to be necessary in order to facilitate our legitimate interests, in order for us to comply with our legal or regulatory obligations, where based upon reasons of substantial public interest, or where your personal information remains public information by your own actions. For further information, please contact the relevant data controller (listed below).

Our responsibilities when we make changes to our Privacy Policy

We may make changes to our Privacy Policy at any time and may do so without expressly notifying you of these changes. However, should the legal bases or purpose for processing your personal information changes then we shall expressly notify you.

Our Data Controllers and how to contact us

Questions or individual data requests relating to this Policy should be addressed to the relevant data controller. For the purpose of the data protection legislation, the relevant data controllers are:

Data Controller	Responsible for
RLC Ventures Ltd 91-93 Buckingham Palace Rd Victoria, London SW1W 0RP GDPR contact person: Reece Chowdhry	All investment and business administration activities.
SFC Capital Partners Ltd Co registration no: 09226119 1-6 SPEEDY PLACE CROMER STREET LONDON ENGLAND WC1H 8BU GDPR contact person: Marguerite Crossfield	Investment and business administration activities related to our regulated activities. Principal firm to Appointed Representatives.
Bennet Brooks Co registration no: 02648803 St. George's Court Winnington Avenue Northwich CW8 4EE ichiban@bennettbrooks.co.uk 0845 330 3200	Provision of delegated investment services by the Organisation.

Our Cookie Policy

A cookie is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. We only use cookies that are required for the essential operation of our website. These cookies are typically deleted from your device once the browsing session is terminated.

You can choose to block cookies that we may deliver to your device through settings on your web-browser; however, in doing so you may not be able to access or utilise all aspects of our website.

Appendix VI: Recordkeeping Policy

Overview

As a data controller, we are required to document the information required under Art30(1) of GDPR, namely:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Recordkeeping procedure (Compliance Officer and Staff)

The Organisation ensures that it keeps a record of the above information, for the RLC Ventures, by completing the ICO's '***Documentation Template for Controllers***' (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/).

It is the Compliance Officer's responsibility to ensure that this spreadsheet is maintained, kept up to date and saved in a suitably secure location with restricted access.

It is company policy that staff observe the following (in order that our records remain up to date):

- Notify the Compliance Officer of any changes to their own personal data or are put on notice of any changes to that of the Organisation's clients/business contacts.
- Notify the Compliance Officer of any potential/actual breaches of data protection
- Notify the Compliance Officer of any data subject access requests
- Check with the Compliance Officer before sharing or transferring personal data to a third party or location outside the Organisation's secure IT environment.