FCAAuthorisation.*Info*

GDPR Compliance Policy

Amendments to this Policy

From time to time this policy will be updated to reflect changes to FCA Authorisation Company business or changes to the regulations to which we are subject. The Appointed Person will ensure that all appropriate amendments are made to this manual. The dates of the amendments are recorded below. Please ensure that you have the most up-to-date version of this manual by confirming the correct version number with Appointed Person.

Version	Status	Date	Amendment Comments	By Whom
0.1	Draft	May 2018		Compliance Consultant
1.0	Published	May 2018	Up To Date	Compliance Consultant

Document Governance

Policy Owner	Lee Werrell
Approver	Lee Werrell
Date approved	May 2018
Date last reviewed	May 2018
Review frequency	Annual
Next review date	May 2019
Responsible for document management	Principle
Security classification	Restricted

GDPR Compliance Policy

Contents

FCA Authorisation Company GDPR Compliance Policy 4
Data Protection Control and Processing 4
Introduction 4
Definitions 4
Our Commitment 5
Lawful Bases For Processing 5
How We Implemented The GDPR 6
Lawfulness, fairness and transparency 8
Our Lawful Bases for Processing 9
Consent: Our business has reviewed how we ask for and record positive consent 9
Legal Obligation: When is the lawful basis for legal obligations likely to apply? 10
Vital Interests: What are 'vital interests'? 11
Public Task: 11
Legitimate Interests: 11
Special Category Data: What's different about special category data? 11
Criminal Offence Data: 12
Individual's Rights 13
Right to be informed including privacy notices: 13
Right of access: 14
Right to rectification and data quality: 14
Right to erasure including retention and disposal: 15
We will keep data as explained in "How We Implemented The GDPR" above 15
Right to restrict processing: 15
Right of data portability: 16
Right to object: 16
Rights related to automated decision making including profiling: 17
Accountability: 18
Data Protection Impact Assessments (DPIA): 19
Information Security & Technical and Organisational Measures 21
GDPR Roles and Employees 21
Data Protection Officers 21
Data security, international transfers and breaches 22

FCA Authorisation Company GDPR Compliance Policy

Data Protection Control and Processing

Introduction

The ***EU General Data Protection Regulation ("GDPR")*** came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information whether customer or employee.

Definitions

"FCAAuthorisation.info" is a trading style of IYC Cubed Limited Registered in England & Wales under Reg no 08878921.

"FCA Authorisation" is registered with the Information Commissioner as part of and under the registration of Z1449155 in the name of IYC Cubed Limited.

Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life; or sexual orientation where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

LINK: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Our Commitment

FCA Authorisation Company *('we' or 'us' or 'our')* are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

We are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and implementation objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

Lawful Bases For Processing

What are the lawful bases for processing?
There are six lawful bases for processing and are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) **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 if we were a public authority processing data to perform our official tasks.)*

Documenting Lawful Processes: How we document our lawful basis
The principle of accountability requires that we are able to demonstrate that we are complying with the GDPR and have appropriate policies and processes. This means that we need 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 keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies.

It is our responsibility to ensure that we can demonstrate which lawful basis applies to the particular processing purpose.

See the accountability section of this guide for more on this topic.

How We Implemented The GDPR

We already have a consistent level of data protection and security across our organisation, however it was our aim to be fully compliant with the GDPR by 25th May 2018.

Our preparation included: -

- ***Information Audit*** – we carried out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed. We logged this information appropriately and review it when there is any change in reasons for processing.
- ***Policies & Procedures –*** we have implemented this new data protection policy and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
    - ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
    - ***Data Retention:*** we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We maintain a client's details for two calendar years and delete the data within 30 days of this.

- ***Data Erasure:*** we have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- ***International Data Transfers & Third-Party Disclosures*** We store or transfer personal information outside the EU and have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures would therefore include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- ***Subject Access Request (SAR)*** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- ***Legal Basis for Processing*** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- ***Direct Marketing*** - we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and

method for opting out and providing unsubscribe features on all subsequent marketing materials.

- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data*** **-** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Lawfulness, fairness and transparency

Information we hold: Mapping Data Flows

We organised an information audit across our business to identify the data that we process and how it flows into, through and out of our business.

Having audited our information, we then identified any risks.

We have document our findings in the Information Asset Register. This register will be reviewed any time a new process or purpose of the data is used.

As we have less than 250 employees then we must keep records of any processing activities that:

- are not occasional;
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

Lawful bases for processing personal data: Our business has identified the lawful bases for processing and appropriately documented them. Our decision on the lawful bases for processing will have an effect on individual's rights. For example, if we rely on someone's consent to process their data, they will have a stronger right to have their data deleted. It is important that we inform individuals how we intend to process their personal data and what our lawful bases are for doing so, for example in our privacy notice(s).

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

Our Lawful Bases for Processing

Consent: Our business has reviewed how we ask for and record positive consent
Consent is not always required, and we should always assess whether another lawful bases is more appropriate.

Consent means offering people genuine choice and control over how we use their data. We can build trust and enhance our business by using consent properly.

The GDPR builds on the original DPA standard of consent in several areas and contains much more detail. For example we must now;

- Keep our consent requests separate from other terms and conditions.
- Require a positive opt-in. Use unticked opt-in boxes or similar active opt-in methods.
- Avoid making consent a precondition of service.
- Be specific and granular. Allow individuals to consent separately to different types of processing wherever appropriate.

- Name our business and any specific third party organisations who will rely on this consent.
- Keep records of what an individual has consented to, including what we have told them, and when and how they consented.
- Tell individuals they can withdraw consent at any time and how to do this.

Consent: Our business systems record and manage ongoing consent

We continue to review consent as part of our ongoing relationship with individuals.

We keep our client's consent under review and refresh it if anything changes. We have a system or process to capture these reviews and record any changes.

Children: Marketing to Children

We do not offer any services or market to children. All users of this site should be 18 years or older.

Contract: When is the lawful basis for contracts likely to apply?

We have a lawful basis for processing if:

- we have a contract with the individual and we need to process their personal data to comply with our obligations under the contract.
- we haven't yet got a contract with the individual, but they have asked us to do something as a first step (eg provide a quote) and we need to process their personal data to do what they ask.

Legal Obligation: When is the lawful basis for legal obligations likely to apply?
In short, when we are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that our overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

We should be able to easily identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, we can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Vital Interests: What are 'vital interests'?
It's clear from Recital 46 of the GDPR that vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death. It is likely to be particularly relevant for emergency medical care, when anyone needs to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

This basis does not apply to our company.

Public Task:
This can apply if we are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

This basis does not apply to our company.

Legitimate Interests:
Article 6(1)(f) gives us a lawful basis for processing where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

- Purpose test: are we pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be our own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

We will complete a legitimate interest assessment if we have to rely on this bases.

This basis is not likely to apply to our company.

Special Category Data: What's different about special category data?
We must still have a lawful basis for our processing under Article 6, in exactly the same way as for any other personal data. The difference is that we will also need to satisfy a specific condition under Article 9. See the definition above

This is because special category data is more sensitive, and so needs more protection.

Criminal Offence Data:
This means we must either be processing the data in an official capacity or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill.

Even if we have a condition for processing offence data, we can only keep a comprehensive register of criminal convictions if we are doing so in an official capacity.

This basis is not likely to apply to our company.

Individual's Rights

Data Subject Rights

In addition to the policy and procedures mentioned above that ensure individuals can enforce their data protection rights, we operate a system of data retention that easily accommodates any request the data subject may make.

- If a verbal request is received, we will confirm the request by email or text message to their recorded contact address or number.
- If a written request is made, we will confirm receipt of the request by return.

We provide easy to access information via our website, of an individual's right to access any personal information that we process about them.

The individual may request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store their personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Right to be informed including privacy notices:

When we provide privacy notices to individuals.

Individuals need to know that their data is collected, why it is processed and who it is shared with.

We publish this information in our privacy notice on our website and within any forms or letters we send to individuals.

The information will be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The information we supply is determined by whether or not we obtained the personal data directly from the individual or from a third party. The only exception is that third-party provision does not require "details of whether individuals are under a statutory or contractual obligation to provide the personal data".

Communicate the processing of children's personal data

Our business does not offer online services directly to children.

Right of access:

We have a process to adequately recognise and respond to individuals' requests to access their personal data

Individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that we provide in a privacy notice.

We provide a copy of the information free of charge. However, we may charge a 'reasonable fee' when a request:

- is manifestly unfounded or excessive, particularly if it is repetitive, unless the client refuses to respond; or
- is for further copies of the same information (that's previously been provided). This does not mean that we can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

Responding to a Subject Access Request:

Information must be provided without delay and at least within one calendar month of receipt. We can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation).

A calendar month ends on the corresponding date of the next month (eg 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (eg 31 January to 28 February).

We must verify the identity of the person making the request, using "reasonable means".

If the request is made electronically, we should provide the information in a commonly used electronic format.

Right to rectification and data quality:

How we ensure personal data held by us remains accurate and up to date

Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

We will always respond to a request without delay and at least within one month of receipt.

We can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). If we have disclosed the personal data to a data processor (third party) we must inform them of the rectification where possible.

We will regularly review the information we process or store to identify when we need to do things like correct inaccurate records. We will maintain a Records Management Policy, with rules for creating and keeping records (including email addresses) if our records grow or are above 500 names.

Right to erasure including retention and disposal:

We securely dispose of personal data that is no longer required or where an individual has asked us to erase it?

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary in relation to the purpose for which it was originally collected/processed;
- the individual withdraws consent;
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- it was unlawfully processed (ie otherwise in breach of the GDPR);
- it has to be erased in order to comply with a legal obligation; or
- it is processed in relation to the offer of information society services to a child.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

We will keep data as explained in "How We Implemented The GDPR" above

Right to restrict processing:

We maintain adequate procedures to respond to an individual's request to restrict the processing of their personal data, subject to the legal basis for processing as discussed above.

Right of data portability:

We maintain adequate and proportional processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to effective usability, if applicable.

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

They can receive personal data or move, copy or transfer that data from one business to another in a safe and secure way, without hindrance.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- where the processing is carried out by automated means. Information must be provided without delay and at least within one month of receipt. We can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation).

We must provide the personal data in a structured, commonly used and machine-readable format. Examples of appropriate formats include CSV and XML files.

We must provide the information free of charge.

If the individual requests it, we may be required to transmit the data directly to another business where this is technically feasible.

Right to object:

We have adequate procedures to handle an individual's objection to the processing of their personal data.

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation".

However, for processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority or for purposes of scientific/historical research and statistics we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

- the processing is for the establishment, exercise or defence of legal claims.

Individuals also have the right to object to any processing undertaken for the purposes of direct marketing (including profiling). We will stop processing for direct marketing as soon as we receive an objection. There are no exemptions or grounds to refuse.

We will inform individuals of their right to object "at the point of first communication" and clearly lay this out in our privacy notice.

Rights related to automated decision making including profiling:

We have identified whether any of our processing operations constitute automated decision making and have procedures in place to deal with the requirements.

This category does not impact on our business.

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or similarly significant effect on the individual.

The right does not apply if the decision:

- is necessary for entering into or performance of a contract between us and the individual;
- is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- is based on the individual's explicit consent, and our business has put in place suitable measures to safeguard the individual's rights, freedoms and legitimate interests.

If suitable measures to safeguard the rights of data subjects are required, these must include at least:

- obtain human intervention;
- express their point of view;
- obtain and explanation of the decision and challenge it.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;

- location; or
- movements.

If the decision involves the processing of special categories of personal data then the exceptions available to justify the processing are more limited.

Processing can only take place if:

- we have the explicit consent of the individual and suitable measures to safeguard their rights, freedoms and legitimate interests are in place; or
- the processing is necessary for reasons of substantial public interest, proportionate to the aim pursued.

We will exercise particular caution if using automated decision making in relation to a child.

Accountability:

Our business has this data protection policy to permit all staff access to understanding how data is processed within the business.

The GDPR requires us to show how we comply with the principles.

Accountability:

Our business monitors our compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

Documenting policies alone is often not enough to provide assurances that staff are adhering to the processes they cover. We will ensure that we have a process to monitor compliance to data protection and security policies.

Measures that are detailed within the policies should be regularly tested to provide assurances as to their continued effectiveness.

Accountability:

Where relevant our business provides data protection awareness training for all staff.

We brief all staff handling personal data on their data protection responsibilities when they join our company.

Data processor contracts:

Whenever we use a processor we will have a written contract in place.

The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract.

In the future, standard contractual clauses may be provided by the European Commission or the ICO and may form part of certification schemes. However, at the moment no standard clauses have been drafted.

We are liable for our processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor that adheres to an approved code of conduct or certification scheme may help us to satisfy this requirement.

Processors must only act on our documented instructions. They will however have some direct responsibilities under the GDPR and may be subject to sanctions if they don't comply.

Information risks:

We actively manage information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

We set out how we (and any of our data processors) manage information risk. We employ strategies to help manage the risk, such as:

- assessing what can go wrong (how, how often, how much damage)
- keeping staff up to date and agile with new technology
- taking special care over sensitive information and transfer arrangements
- ensuring staff are able to identify risks and escalate them

Data Protection by Design:

We have implemented appropriate technical and organisational measures to integrate data protection into our processing activities.

Under the GDPR, we have a general obligation to implement appropriate technical and organisational measures to show that we have considered and integrated data protection into our processing activities. Under the GDPR, this is referred to as data protection by design and by default.

Data Protection Impact Assessments (DPIA):

We understand when we must conduct a DPIA we have appropriate processes in place to action this.

We currently do not hold any sensitive data that would require a DPIA.

DPIAs help us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to our reputation which might otherwise occur.

We must carry out a DPIA when:

- using new technologies; and
- when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes but is not limited to:

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences; and
- large scale systematic monitoring of public areas.

The DPIA should contain the following information:

- a description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by our business;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an assessment of the risks to individuals; and
- controls that we put in place to address any risks we've identified (including security)

Data Protection Impact Assessments (DPIA):

We have a DPIA framework which links to our existing risk management and project management processes.

A DPIA can address multiple processing operations that are similar in terms of the risks, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing.

We will start to assess the situations where it will be necessary to conduct one, including:

- Who will do it?
- Who else needs to be involved?
- Will the process be run centrally or locally?

If the processing is wholly or partly performed by a data processor, then that processor must assist us in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

Information Security & Technical and Organisational Measures

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process.

GDPR Roles and Employees

Due to the size of our company, we do not have an appointed Data Protection Officer, and the principle will be the point of contact for all enquiries.

We understand that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our implementation plans. We have implemented an employee training program specific to the which will be provided to all employees and forms part of our induction and annual training program.

If there are any questions about our implementation for the GDPR, please contact Lee Werrell at fcaa@improveyourcondition.com.

Data Protection Officers

We have nominated an Appointed Person (AP)

It is important to make sure that someone in our business, or an external data protection advisor, takes responsibility for data protection compliance.

We may need to appoint a DPO if we:

- are a public authority (expect for courts acting in the judicial capacity);
- carry out large scale systematic monitoring of individuals (eg online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The AP should work independently, report to the highest management level and have adequate resources to enable our organisation meets its GDPR obligations.

The AP's minimum tasks are to:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Management Responsibility:

Our decision makers and key people are keen to demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

We will make sure that decision makers and key people in our business are aware of the requirements under the GDPR.

Decision makers and key people should lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within our business, for data protection.

They should take the lead when assessing any impacts to our business and encourage a privacy by design approach.

They should help to drive awareness amongst all staff regarding the importance of exercising good data protection practices.

Data security, international transfers and breaches

Security policy:

Our business uses this information security policy supported by appropriate security measures.

We must process personal data in a manner that ensures appropriate security.

Before we can decide what level of security is right for us, we will need to assess the risks to the personal data we hold and choose security measures that are appropriate to our needs.

Keeping our IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise.

If we are processing personal data within our IT system(s) we recognise the risks involved and take appropriate technical measures to secure the data.

The measures we have put in place fit our business's needs.

We have a separate ***Information Security policy*** which details our approach to information security, the technical and organisational measures that we will implement and the roles and responsibilities staff have in relation to keeping information secure.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Breach notification:

We have effective processes to identify, report, manage and resolve any personal data breaches.

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We understand that we only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals and in that event, we must notify those concerned directly and without undue delay.

In all cases we will maintain records of personal data breaches, whether or not they were notifiable to the ICO.

A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows us to provide additional information in phases.

We make sure that our staff understand what constitutes a personal data breach, and that this is more than a loss of personal data. We have an internal breach reporting procedure in place. This will facilitate decision-making about whether we need to notify the relevant supervisory authority or the public.