FREEDOM
prime uk

Freedom Prime UK Ltd
Data Protection Policy

DOCUMENT AUTHOR:	Alexander Feoktistov
DOCUMENT OWNER:	Alexander Feoktistov
STATUS:	Approved
APPROVED BY:	Governing body of Freedom Prime UK Ltd
DATE CREATED:	17/12/2021
LAST UPDATED:	17/12/2021
NEXT REVIEW:	16/12/2022
VERSION:	DP01

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Freedom Prime UK Ltd.
Company number 13495620

30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767

www.freedomprime.co.uk
info@freedomprime.co.uk

Contents

Freedom Prime UK Ltd.
Company number 13495620

30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767

www.freedomprime.co.uk
info@freedomprime.co.uk

Freedom Prime UK Ltd.
Company number 13495620

30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767

www.freedomprime.co.uk
info@freedomprime.co.uk

1 Introduction

This policy explains how Freedom Prime (UK) Ltd ('Freedom Prime', 'us', 'we', 'our', 'the firm') complies with the General Data Protection Regulations and the Data Protection Act 2018 when processing personal data.

This policy applies to all personal data we process (wholly or partly) regardless of whether data is stored electronically, on paper, or on any other media. It applies to:

- Freedom Prime.
- All staff of Freedom Prime.
- All contractors working on behalf of Freedom Prime.

Protecting the integrity and confidentiality of personal data is a critical responsibility which we take seriously at all times. We are exposed to potential fines of up to €20 million or 4% of total worldwide annual turnover (whichever is higher) depending on the nature of the breach if we fail to comply with the GDPR.

You must read, understand and comply with this policy when processing personal data on our behalf and complete any training necessary to meet the requirements. This policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this policy is mandatory and any breach may result in disciplinary action.

If you have any questions about this policy, please contact the Data Protection Officer/Compliance Team.

1.1 The Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) came into effect on the same day as the GDPR. It was bought in for a number of reasons:

a) To repeal and replace the previous Data Protection Act 1998.
b) To incorporate the GDPR into UK law.
c) To ensure that post Brexit the UK can freely exchange personal data with the EU.
d) To exercise the derogations which allow member states discretion in some areas.
e) To extend GDPR standards to other types of processing not covered by EU law.
f) To implement the Data Protection Law Enforcement Directive.
g) To provide a specific data protection regime for the intelligence services.
h) To clarify the role of the Information Commissioner's Office ("ICO"); and
i) To increase the maximum fines in line with the GDPR and introduce two new criminal offences.

The DPA 2018 is structured into seven parts with eighteen schedules – it must be read alongside the GDPR to understand the complete legal framework.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

2 What is personal data?

Personal data is 'any information relating to an identified or identifiable natural person' (the data subject).

This creates a wide scope beyond the obvious information which identifies a person such as their name, address, and date of birth. It includes information from which a person can be directly or indirectly identified. For example, it can include identification numbers, location data, online identifiers such as cookies and one or more factors which are specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person. Note that additional requirements apply to the processing of sensitive personal data referred to as 'special categories of personal data'. See Section 5.3 for further information. Please see Annex One for the full definitions.

2.1 What does processing of personal data mean?

The GDPR applies to the processing of personal data. Processing covers anything which we do to, or with, personal data such as when we collect, record, organise, store, disclose, and delete it. It covers processing which is undertaken wholly or partly by automated means and where the data forms part of a filing system. We have not identified any personal data which we hold which does not fall within the scope of processing under the GDPR.

2.2 What personal data do we process?

Using our data inventory, we have identified that we process personal data relating to the following:

- Clients.
- Users.
- Members, including participants.
- Employees.
- Contractors.
- Third parties.
- Investors including prospective investors.
- Ultimate beneficial owners or trust beneficiaries; and
- Professional contacts.

If you wish to process data from any other sources, you should speak to the Data Protection Officer in the first instance.

We process this personal data for a wide variety of reasons, for example we process information from our clients in relation to the transmission of orders; from clients to verify identification and comply with our legal obligations such as those relating to anti-money laundering; or to process payroll information for our staff. Full details are included in our data inventory.

2.3 Processors and controllers

The GDPR applies to those who act as a controller and/or a processor. A controller is someone who determines the purpose and means of processing personal data. A processor is someone who is

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

responsible for processing the personal data on behalf of a controller. Different requirements will apply depending on whether we are the controller or the processor.

Freedom Prime acts as controller and processor and has put in place appropriate procedures which comply with GDPR obligations accordingly.

Freedom Prime UK Ltd.
Company number 13495620

30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767

www.freedomprime.co.uk
info@freedomprime.co.uk

3 Territorial scope

The GDPR applies to the processing of personal data by a controller or processor in the European Union (EU) and the United Kingdom (UK), regardless of whether or not the processing takes place in the EU or UK.

4 Principles

4.1 Principles relating to the processing of personal data

The GDPR sets out a number of principles which firms must comply with when they process personal data. These principles are central to our data protection obligations and sit at the heart of our policies and procedures - we are accountable and must be able to demonstrate our compliance with these.

The six principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner (lawful processing).
- collected for specified, explicit and legitimate purposes (purpose limitation).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Accurate, and where necessary, kept up to date (data accuracy).
- Kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation); and
- Processed in a manner that ensures appropriate security of personal data (security).

4.2 Fair and lawful processing

We must process personal data in a lawful, fair, and transparent way. The GDPR sets out specific legal grounds which we can use to process personal data. If we cannot meet one or more of those legal reasons, we cannot process the personal data. Further information on the lawful basis for processing is set out in Section 5.

We must also ensure that personal data is processed fairly, for example we only use it for a specified purpose, and that we are transparent in what we are doing. This means that we must provide the individual with information about how we process their personal data in a concise and intelligible manner using clear and plain language. There are specific requirements about the information which must be disclosed, and we set out this information in our privacy notice.

4.3 Purpose limitation

In line with GDPR, we will only process personal data, where we have a clear and legitimate purpose for doing so. The personal data that we collect must be relevant and limited to our data processing activities. If we wish to process personal data for another purpose later on, we need to consider whether we can use an existing lawful basis or consent unless the new purpose is compatible with the original purpose. It is also important that we are transparent and can explain to individuals the reason(s) why we are processing their data. This is set out in our privacy notice.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

4.4 Data minimization

We cannot collect excessive personal data – it must be adequate, relevant, and limited to what is necessary for the purpose required. This means we cannot collect data now for some general and unspecified future use.

4.5 Data accuracy

We must ensure that the personal data we process is accurate and kept up to date. We have established a process to ensure that data is regularly reviewed and updated to reflect any changes to a data subject's circumstances, where necessary. Staff must inform us of any changes to their personal data at the earliest opportunity.

Where we identify personal data, which is inaccurate we must take steps to erase or update that information as soon as possible.

4.6 Storage limitation

We will regularly review our data inventory to ensure we only keep personal data in a form which permits the identification of the individual, for as long as the information is necessary for our data processing activities. We may in limited circumstances keep personal data for longer periods, where we intend to process information for archiving purposes or to meet our regulatory and legal obligations. Further details of our record keeping requirements are set out in our Recordkeeping Policy.

4.7 Data security and integrity

We must process personal data in a way which keeps it secure, ensuring that any information that we collect from individuals is not lost, destroyed, or damaged. We must protect the data we process from unauthorized or unlawful processing by another party (for example, hacking or illegal distribution).

Freedom Prime UK Ltd.
Company number 13495620

30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767

www.freedomprime.co.uk
info@freedomprime.co.uk

5 Lawful processing

A fundamental principle of the GDPR states that we can only process personal data where we have a lawful basis to do so. If there are no lawful bases available, our processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.

There are six lawful bases available:

- The individual has given their consent (consent).
- The processing is necessary for the performance of a contract with the individual (contract).
- Processing is necessary to comply with a legal obligation to which we are subject (legal obligation).
- Processing is necessary to protect the vital interests of the individual or another natural person (vital interests).
- Processing is necessary for performance of a task carried out in the public interest or by a public authority (public task); and
- The processing is necessary for our legitimate interests or those of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (legitimate interests).

5.1 Consent

This lawful basis can be used for processing providing we have a valid consent which covers the processing of personal data for each specified purpose.

Consent must be:

- Freely given.
- Be specific, informed and unambiguous; and
- Be made by statement or a clear affirmative action which signifies agreement.

Where we use consent as a lawful basis for processing, we will ensure that:

- The individual is required to positively opt-in. We will not use any pre-ticked boxes or other methods of consent.
- There is a transparent explanation of what the individual is consenting to.
- The explanation is written in clear, plain language which is easy to understand.
- We will ask for a consent for each distinct processing operation.
- The consent will be separate from our other terms and conditions.
- There is an easy process for the withdrawal of consent.
- We name any third parties who will rely on the consent.
- We keep the consent under review and update it if anything changes; and
- Ensure that consent is not a pre-condition to providing our products and services.

5.2 Contract

This lawful basis can be used for processing if:

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

- We have a contract with the individual and we need to process their personal data to comply with our obligations under the contract; or
- Where we do not yet have a contract with the individual, but they have asked us to perform an action (for example, provide a quote) and we need to process their personal information to do this.

This lawful basis can only be used if it is necessary for the processing. It does not apply if there are other reasonable and less intrusive ways in which we can proceed. We will not require additional consent to process personal data using this lawful basis unless we are processing a special category of data or the contract is with anyone under, or reasonably considered to be under, the age of 18. If we can reasonably provide our products or services without processing their personal data, this basis will not be available.

5.3 Legal obligation

This lawful basis can be used for processing if we need to comply with a common law or statutory obligation (it does not apply to contractual obligations). For example, where we need to process personal data to comply with our legal obligation to disclose employee salary details to the relevant governmental tax office, or where we are obliged to submit notifications such as a Suspicious Activity Report to the National Crime Agency or other relevant body. If we can reasonably comply without processing the personal data, then this basis will not be available.

5.4 Vital interests

This lawful basis for processing can be used where we need to process personal data to protect someone's life. It is very limited in scope and generally applies only to matters of life and death. It is unlikely that we will need to ever use this lawful base.

5.5 Public task

This lawful basis can be used where the processing is necessary in order to perform a task in the public interest or for other official functions and the task has a clear basis in law. It is unlikely that we will need to ever use this lawful base.

5.6 Legitimate interests

This lawful basis can be used for processing where it is necessary for our legitimate interests or those of a third party except where these interests are overridden by the interests, fundamental rights, or freedoms of the individual.

There are potentially a wide range of legitimate interests including the use of client or employee data, marketing, fraud prevention, intra-group transfers or IT security. As with other legal bases, the processing must be necessary, and we cannot rely on this legal base if there are other reasonable and less obtrusive ways of achieving the same result.

Most importantly, we must balance the rights of the individual against our legitimate interests and must ensure we consider and protect the rights and interest of data subjects. When considering using this legal base we will apply the following tests:

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

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

5.7 Considerations relating to lawful processing

We must decide which lawful basis we will use before we start to process personal data, based on the available information. It is important to choose this carefully because it is difficult to swap to a different basis at a later stage because this is inherently unfair to the individual. We will therefore carefully assess upfront which basis is appropriate and document this.

If we find that our purposes change over time, or we have a new purpose we may not need a new lawful basis as long as the new purpose is compatible with the original, unless we are relying on consent in which case a new consent will be required or a different basis for processing. Any such changes must be approved by Data Protection Officer.

We must also ensure that we keep a record of which basis we rely on for each processing purpose, and document why we believe it applies. This information is set out in our data inventory.

5.8 Principles relating to the processing of special category data

Special category data is personal data which is more sensitive and therefore needs more protection. Special category data includes information about an individual's:

- Race.
- Ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometric data were used for identification purposes.
- Health.
- Sex life; or
- Sexual orientation.

Please see Annex One for a full list of definitions.

As part of our data inventory, we have confirmed that we do process special categories of personal data. We are only able to process this personal data if we have a legal basis to do so, and we are able to meet one or more of the following conditions:

- The individual has given us their explicit consent to processing for one or more specific purposes.
- The processing is necessary in order that we can comply with our rights and obligations, or those of the individual, in relation to employment law, social protection law or social security law.
- The processing is necessary to protect the vital interests of the individual.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

- The information has manifestly been made public by the individual.
- The processing is necessary in relation to legal proceedings, for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights.

5.9 Principles relating to the processing of criminal offences

Under GDPR, the rules around 'special category data' do not apply to criminal offence data, instead separate safeguards have been put in place. Criminal offence data refers to personal data relating to criminal convictions and offences or related security measures. This includes information about criminal allegations, proceedings, and convictions as well as security measures. Criminal offence data can only be processed where we have a lawful basis to do so, and we are processing the data in an official capacity or we have a specific legal authorisation to do so.

Note that we have an obligation under the Financial Services and Markets Act 2000 in the UK and The Financial Services Act 2000 to ensure all employees are fit and proper.

As part of our data inventory, we have confirmed that we do process criminal offence personal data. We are only able to process this personal data if we have a legal basis to do so, and we are processing the data in an official capacity or we have specific legal authorisation to do so.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

6 Rights of data subjects

The GDPR provides specific rights for individuals in terms of how we process their personal data:

a) The right to be informed.
b) The right of access.
c) The right to rectification.
d) The right to erasure.
e) The right to restriction.
f) The right to data portability.
g) The right to object; and
h) Rights in relation to automated decision making and profiling.

6.1 Charging and timing

We must provide information in relation to points b) to h) as soon as possible and within one month at the latest. We can extend that period by a further two months if the request is complex or there are multiple requests, but we must keep the data subject informed of any delays. Where we have reasonable doubts concerning the identity of the individual making the request, we can ask for additional information to confirm their identity. For any requests made electronically, we will provide the information to the data subject in a commonly used electronic format.

All the information provided under points a) to h) must be provided free of charge. Where requests from the data subject are manifestly unfounded, excessive or repetitive we can charge a reasonable fee to cover our administrative costs or refuse to act on the request. Any requests to levy a charge must be approved by the compliance team.

6.2 Right to be informed

The GDPR specifies the information that we must provide to data subjects. We set this out in our privacy notice. This information must be communicated in an easily accessible way and written in clear and plain language. It must also be provided free of charge.

The type of information we must provide, is determined by whether or not we obtained the personal data directly from the individual or a third party. Please see the table below which sets out the differences.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

Information*	Personal data obtained from data subject	Personal data obtained from a third party
Our identity and contact details as the Data Controller (or, where applicable, our representative) and, if applicable, the identity and contact details of the Data Protection Officer	✓	✓
The purpose of the processing and the lawful basis for the processing	✓	✓
Details of our legitimate interests as the Data Controller or third party (if applicable)	✓	✓
Details of the categories of personal data		✓
Any recipients or categories of recipient of the personal data	✓	✓
Details of third-party country transfers and safeguards	✓	✓
Data storage periods or the criteria used to determine this	✓	✓
The existence of each of the data subject's rights	✓	✓
The data subject's right to withdraw consent at any time	✓	✓
The data subject's right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement and possible consequences of failing to provide the personal data	✓	
The existence of an automated decision making including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Individual	✓	✓

* Not all type of information listed (for completeness) in the table may be relevant to Freedom Prime.

If we obtain personal data directly from the individual, we must provide this information at the same time. If the personal data is not obtained directly, we must provide this information within a reasonable period (one month) unless the data is used to communicate with the individual, in which case we must make this disclosure at the latest, when the first communication takes place. If we

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

envisage disclosing personal data to another recipient, we must provide this information before disclosure is made.

Our standard practice is to always provide this information; however, we are not required to do so if the following apply:

- In circumstances where we have not obtained the information directly from the data subject where:
  - The data subject already has the information.
  - Providing the information proves impossible or would involve a disproportionate effort.
  - Obtaining or disclosure is expressly laid down by law to which we are subject, and which provides appropriate measures to protect the data subject's legitimate interests; or
  - The personal data must remain confidential subject to an obligation of professional secrecy (including statutory) regulated by law, including a statutory obligation of secrecy.

If we intend to process the personal data further for a different purpose to the one the personal data was collected for, we will provide the individual with information (prior to processing) on that other purpose and with any relevant further information referred to above.

6.3 Right of access

Data subjects have the right to:

- Confirm their personal data is being processed.
- Access their personal data; and
- Obtain other supplementary information.

In addition to a copy of their personal data an individual may also request the following additional information:

- Confirmation as to whether or not their personal data is being processed.
- The purpose of the processing.
- The categories of personal data being processed.
- Recipients (current and future) of the personal data, in particular those in third countries or international organisations.
- The envisaged storage period or the criteria used to determine that period.
- Their right to request rectification, erasure, restriction or objection of processing.
- Their right to lodge a complaint with a supervisory authority (the Information Commissioner).
- The source of the personal data, where this is not the individual themselves.
- The use of automated decision making, including profiling and in those cases meaningful information on the logic involved and any consequences of processing; and
- Where appropriate, the safeguards for personal data transferred to a third country or international organisation.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

6.4 Right to rectification

A data subject has the right to request that we correct any inaccurate or incomplete personal data that we process. If we do not take any action in relation to such a request, we must explain why and advise the individual that they can make a complaint to the ICO.

6.5 Right to erasure and the right to be forgotten

A data subject has the right to request that we erase any personal data concerning them where:

- It is no longer needed for the reason it was originally collected.
- They withdraw their consent to the processing.
- They object to the processing and there's no overriding legitimate interest for continuing the processing.
- It has been unlawfully processed.
- It must be erased for compliance with a legal obligation; or
- It was collected in relation to the offer of information society services to a child.

If we have received a request for erasure and we have made that personal data public, because for example we have published the information on the internet or shared it with third parties, we must tell those other parties about the request for erasure unless we can demonstrate this would involve a disproportionate effort.

We may reject requests for erasure if the processing is necessary for:

- Exercising the right of freedom of expression and information.
- Complying with a legal obligation for the performance of a public interest task or exercise of official authority.
- Public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- Exercising or defending a legal claim.

6.6 Right to restriction

A data subject has the right to request that we stop or supress the processing of their personal data where:

- The accuracy of it is being disputed and we are verifying this.
- Where the individual objects to processing on the basis that it is necessary for the performance of a public interest task or for our legitimate interests, and this is pending verification of whether we have legitimate grounds to override this.
- The processing is unlawful and the individual requests restriction instead of erasure; or
- We no longer need the personal data, but it is required by the data subject to establish, exercise or defend a legal claim.

When we receive such a request, we can continue to store the personal data but must not process it further. If the restricted personal data has previously been disclosed to a third party, we must also

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

inform them about the restriction. We must tell individuals when we decide to lift a restriction on processing.

6.7 Right to data portability

A data subject has the right to obtain and reuse the personal data that they have provided to us for different purposes. This means they must be able to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way. If we receive such a request, we must provide the personal data in a structured, commonly used and machine-readable format. For example, by using midata or CSV files.

This right only applies if:

- The processing was based on consent or for the performance of a contract; or
- The processing is carried out by automated means.

The individual can either ask us to provide this to them directly or to transfer it to a third-party organisation on their behalf where this is technically feasible. If we do not take any action in relation to such a request, we must explain why and advise the individual that they can make a complaint to the ICO if in the UK.

6.8 Right to object

A data subject has the right to object to processing:

- Based on legitimate interests or the performance of a task in the public interest (including profiling) where the objection relates to their own particular situation.
- for direct marketing (including profiling); and
- for the purposes of scientific/historical research and statistics (unless the processing is necessary for the performance of a task carried out for reasons of public interest).

We must ensure that we explicitly inform the individual of this right at the first point of communication. This must be separate from any other information. We provide this information in our privacy notice. Where any of our processing activities fall into the above categories online, we must also provide a way for the individual to object online.

Following a request objecting to processing we must stop processing that personal data unless we can demonstrate:

- Compelling legitimate grounds for processing which override the interest, rights and freedoms of the individual; or
- Processing is required to establish, exercise or defend legal rights.

There are no exemptions or grounds to refuse any objection to processing for direct marketing purposes. Any such requests must be dealt with immediately.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

6.9 Rights for automated decision making and profiling

A data subject has the right not to be subject to a decision based solely on automated processing (including profiling), which produces legal effects on him or her. An effect is a decision which would have a serious negative impact on an individual or something which adversely affects their legal rights.

- Automated individual decision making – making a decision solely by automated means without any human involvement; and
- Profiling – automated processing of personal data to evaluate certain things about an individual.

We may only carry out solely automated decision making if the decision is:

- Necessary for entering into, or the performance of, a contract between us and the individual.
- Is authorised by law; or
- Is based on the individual's explicit consent.

If we are processing a special category of data, we can only carry out this processing if we have explicit consent or it is necessary for reasons of substantial public interest.

When we process personal data in this way for contractual purposes or with the individual's consent, we must implement the following safeguards to protect their rights, freedoms and legitimate interests:

- Provide meaningful information about the logic involved in the decision-making process as well as the significance and envisaged consequences for the individual.
- Use appropriate mathematical or statistical procedures.
- Ensure the individual can:
    - obtain human intervention.
    - express their point of view; and
    - obtain an explanation of the decision and challenge it.
- Put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors; and
- Secure personal data in a way that is proportionate to the risks and prevents discriminatory effects.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

7 Accountability

As part of our responsibilities as a data controller under GDPR we are required to implement appropriate measures, both technical and organisational, to show that we are complying with the data protection regulations.

It is important that we can demonstrate that we understand and can apply the principles of GDPR to our day-to-day processing activities. This will include:

- Establishing a data protection compliance programme and governance arrangements
- Implementing privacy controls and maintaining them on an ongoing basis.
- Complying with our processing obligations including:
    - determining and documenting a lawful basis for processing.
    - maintaining a record of our processing activities.
    - providing data subjects with a compliant privacy notice.
    - satisfying specific requirements when relying on consent.
    - processing special categories of data in line with the requirements.
    - honouring the rights of individuals; and
    - complying with cross border data transfer restrictions and maintaining compliant transfer mechanisms.
- Making explicit arrangements with any joint data controllers and data processors.
- Embedding privacy measures into our day-to-day policies and processes.
- Using technological measures to require or ensure compliance.
- Maintaining appropriate records of our privacy arrangements and compliance.
- Providing our staff with training on data protection and privacy matters; and
- Regularly testing our privacy measures.

7.1 Privacy by design and default

We must show that we are embedding data protection into all our processing activities by design and default. This means that we must implement appropriate technological and organisational measures, such as pseudonymisation, in a way which is effective and ensures compliance. To achieve this, we have implemented measures which meet the principles of data protection by design and default including:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Creating and improving security features on an ongoing basis.

Our commitment to data privacy by default and design is embedded in our everyday activities and any new project through the adoption of appropriate policies and procedures. Examples include:

- Building new IT systems for storing or accessing personal data.
- Developing new policies or governance arrangements that have privacy implications for our data subjects.
- Creating a new data sharing initiative; and
- Using data for new purposes.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

7.2 Data protection impact assessment

A data protection impact assessment (DPIA) is a tool which we can use to identify the risks and the possible impact of our processing activities. An effective DPIA includes:

- A description of the processing operations and the purposes, including our legitimate interests.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to the data subjects; and
- The measures in place to address the risks, including security risks, and to demonstrate that we comply.

We must undertake a DPIA when we:

- Use new technologies; and
- 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 can include, but is not limited to:

- Systematic and extensive processing activities, including profiling and where decisions that have legal, or similar, effects on individuals.
- Large scale processing of special categories of data or personal data relating to criminal convictions and offences; and
- Large scale, systematic monitoring of public areas.

7.3 Training

We will ensure all staff are provided with adequate training to enable them to comply with the GDPR requirements.

7.4 Data processors

Freedom Prime is the data controller in relation to all of the firm's data processing activities. We do not act as a data processor, and we do not have any data processors carrying out processing activities on our behalf.

Using our data inventory, we have identified that we use data processors to undertake processing on our behalf. For example, sponsors or registrars. The GDPR sets out certain requirements when using a data processor (see below).

As a data processor we must only act on the documented instructions of a controller and also have certain direct responsibilities:

- Not to use a sub-processor without the prior written agreement of the data controller.
- To co-operate with any supervisory authorities such as the ICO.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

- To ensure processing is secure.
- To keep records of processing activities.
- To notify any data protection breaches to the data controller; and
- To employ a Data Protection Officer, where appropriate and obligated.
-

7.5 Appointment of a data processor

When we appoint a data processor, we must have a written contract in place. This also applies to any data processor who sub-contracts to another third-party processor. As a minimum the contract must include the following terms requiring the processor to:

- Only process data and act on our written instructions as the controller, including transfers of data to third countries or international organisations.
- Ensure that the people processing the data are subject to a duty of confidence when processing any information relating to a data subject.
- Comply with the security measures we require.
- Obtain our written authority to use a sub-contractor to process our personal data.
- Assist us in allowing data subjects to exercise their rights.
- Assist us in meeting our data security obligations including in relation to personal data breaches and DPIAs.
- Advise us if they are doing something which infringes the GDPR or any other relevant law.
- Delete or return all personal data at the end of the contract; and
- Allow us to undertake audits and inspections.

7.6 Data inventory

We are not required to keep a record of our processing activities because:

- We employ fewer than 250 individuals: and
- Our processing activities are
    - only undertaken on an occasional basis.
    - do not result in a risk to the rights and freedoms of individuals; and
    - do not involved processing special categories of data or criminal conviction and offence data.

7.7 Security of processing

We have an obligation to process the personal data of individuals securely. This includes protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage. We have put the following technical and organisational measures in place to do this:

- Pseudonymisation and encryption of personal data.
- Regular reviews to ensure the ongoing confidentiality, integrity and availability of our processing systems and services.
- A system which allows restoration and access to personal data in the event of a physical or technical incident; and

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

- A process for regularly testing, assessing and evaluating the effectiveness of our security measures.

You must not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data.

7.8 Data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches which are both accidental and deliberate. Examples include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Whenever a security incident takes place, we will quickly establish whether a personal data breach has occurred and if so, promptly take steps to address it. In all cases where you know or suspect there has been a data breach you must not attempt to investigate the matter yourself. You must immediately contact: Head of compliance.

Once we have identified that a breach has occurred, we will:

- Determine the severity of the breach and the risk posed to data subjects.
- Take immediate steps to prevent further breaches occurring.
- Establish whether we have any notification obligations (see below); and
- Identify the underlying reason for the breach and take appropriate preventative steps.

7.9 Breach notification requirements

Once a breach has been identified we must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If there is a high risk, we must report it to the ICO. This assessment will be undertaken by Head of compliance within the compliance team. who will assess each incident on a case-by-case basis? Breaches can be reported on the ICO website.

In the event of a high-risk personal data breach, we will notify the ICO, without undue delay, and where possible, no later than 72 hours after having become aware of it. Where we are unable to notify the ICO within 72 hours, we must explain the reasons for the delay. Failure to notify can lead to a significant fine.

When providing the notification, we must provide the following information:

- A description of the nature of the data breach, including where possible:
    - the categories and approximate number of data subjects concerned; and

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

    - the categories of the personal data records concerned.
- The name and contact details of the DPO.
- The likely consequences of the personal data breach; and
- The measures that we have taken to address the data breach, and where possible, what actions we have taken to mitigate any possible adverse effects.

Where the breach is high risk in nature, we will also inform individuals of the breach, as soon as possible and without undue delay. The DPO will determine when this threshold is reached. We are not obliged to provide this information where:

- We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person not authorised to access it.
- We have taken appropriate steps to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.
- It would involve a disproportionate effort. In these instances, we would instead issue a public communication or similar measure where the data subjects are informed

When we tell individuals about a breach, we must describe the nature of the breach in clear and plain language and provide:

- The name and contact details of the DPO where information can be obtained.
- A description of the likely consequences of the breach; and
- A description of the measures taken, or proposed to be taken, to deal with the breach, including any measures taken to mitigate any possible adverse effects.

7.10 Data Protection Officer

We have appointed a Data Protection Officer (DPO) who will act as the focus point for our data protection activities and who will take responsibility for ensuring we meet our privacy obligations.

Our DPO is COO. They can be contacted in the following ways:

Mr Alexander Feoktistov

The DPO will report directly to The Board. We will ensure they are able to operate independently and are provided with adequate resources to fulfil their role. The responsibilities of the DPO will include:

- Informing and advising of our obligations under GDPR.
- Providing appropriate information and training to staff.
- Monitoring compliance with GDPR and other data protection laws.
- Managing internal data protection activities.
- Advising on data protection impact assessments.
- Conducting compliance monitoring and risk assessments.
- Providing advice.
- Acting as the contact point and manager for any data protection breaches.
- Co-operating with the supervisory authority.
- Acting as the contact point for the supervisory authority on issues relating to processing; and

Acting as the contact point for data subjects.

Freedom Prime UK Ltd. 30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE www.freedomprime.co.uk
Company number 13495620 tel: +44 20 37467767 info@freedomprime.co.uk

8 Transfer of data to third countries

We have identified that we may transfer personal data outside of both the EEA and the UK to other third countries and international organisations. A full list of recipients is detailed in our data inventory.

We will ensure that any transfer of personal data to a third country or international organisation (including any onward transfer to another third country or international organisation) is undertaken in accordance with one of the following GDPR requirements:

- It is transferred on the basis of an EU Commission adequacy condition; or
- The transfer is subject to appropriate safeguards (see below); or
- GDPR provides an exemption or derogation (see below).

Any proposal to transfer personal data outside of the UK must be referred to the Data Protection Officer

8.1 Transfers on the basis of an adequacy decision

Transfers of personal data to the following countries can be made without further authorisation because they are subject to an EC adequacy decision:

- Andorra.
- Argentina.
- Canada (commercial organisations).
- Faroe Islands.
- Guernsey.
- Israel.
- Isle of Man.
- Jersey.
- New Zealand.
- Switzerland.
- Uruguay; and
- US (limited to the privacy shield framework).

8.2 Appropriate safeguards

In the absence of an adequacy decision, we may still transfer personal data where we have put appropriate safeguards in place and on the condition that enforceable data subject rights and effective legal remedies are available. Appropriate safeguards can be provided in the following ways:

- A legally binding and enforceable agreement between public authorities or bodies.
- Binding corporate rules (see below).
- Contractual clauses:
    - standard contractual clauses adopted by the Commission or adopted by a national authority and approved by the Commission.
    - contractual clauses agreed authorised by the ICO; or
    - provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

- An approved code of conduct; or
- An approved certification mechanism as provided for in the GDPR.

8.3 Binding corporate rules

Binding corporate rules are agreements which govern transfers of personal data made between organisations within a corporate group or a group of enterprises engaged in joint economic activity. They must contain certain information which is specified in the GDPR and are subject to a formal approval mechanism involving the ICO.

8.4 Contractual clauses

Current Commission decisions on contractual clauses will remain in force until they are amended, repealed or replaced however are subject to legal challenge.

8.5 Codes of conduct and certification mechanisms

Currently no codes of conduct have been adopted.

8.6 Derogations

In the absence of an adequacy decision or appropriate safeguards, we may also transfer personal data outside of the UK when the transfer is:

- Is made with the individual's informed consent, after having been informed of the possible risks of such transfers.
- Necessary for the performance of a contract between us and the individual or for pre-contractual steps taken at the individual's request.
- Necessary for the performance of a contract made in the interests of the individual between us and another natural or legal person.
- Necessary for important reasons of public interest.
- Necessary for the establishment, exercise or defence of a legal claim.
- Necessary to protect the vital interests of the individual or other persons, where the individual is physically or legally incapable of giving consent; or
- Made from a register which under EU law is intended to provide information to the public (and which is open to consultation by either the public in general or any person able to show a legitimate interest in inspecting the register).

8.7 One-off and infrequent transfers

In very limited circumstances we may transfer personal data outside of the UK even when none of the above apply. Such transfers are only permitted where the transfer:

- Is not being made by a public authority.
- Is not repetitive.
- Involved data related only to a small number of individuals.
- Is necessary for the purpose of our compelling legitimate interests (provided those interests are not overridden by the interests of the individual); and
- Is made subject to suitable safeguards put in place by us to protect the personal data.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

Annex One: Definitions

Binding corporate rules

'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Biometric data

Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Consent

Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller

Means 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; where the purposes and means of such processing are determined by EU law, the controller or the specific criteria for its nomination may be provided for by EU law.

Cross border processing

Means either:

a) 'processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Genetic data

Means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Identifiable living individual (DPA 2018)

Means a living individual who can be identified, directly or indirectly, in particular by reference to:

(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Personal data

Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk

to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing
Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor
Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling
Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation
Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Representative
Means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Freedom Prime UK Ltd.
Company number 13495620
30 Churchill Place, Canary Wharf, London, United Kingdom, E14 5RE
tel: +44 20 37467767
www.freedomprime.co.uk
info@freedomprime.co.uk