

# Data Protection and Privacy Policy

FE fundinfo's Data Protection and Privacy Policy

Sorin Pop

02/10/2019

**FE fundinfo**

2<sup>nd</sup> Floor Golden House  
30 Great Pultney Street  
London W1F 9NN  
United Kingdom

# Document Information

<b>Author</b>	<b>Sorin Pop</b>
<b>Version</b>	4.0
<b>Date</b>	02 October 2019
<b>Classification</b>	Company Confidential
<b>Status</b>	Published

## Document Update (recent)

<b>Author</b>	<b>Version</b>	<b>Change</b>	<b>Date</b>
<b>Sorin Pop</b>	2.1	Annual Review	8 Oct 2018
<b>Sorin Pop</b>	4.0	Updated for rebranding	2 Oct 2019

## Document Review (recent)

<b>Review panel</b>	<b>Version</b>	<b>Date</b>
<b>Richard Thorpe</b>	2.1	12 Oct 2018
<b>Paul Ronan</b>	4.0	10 Oct 2019

## Document Approval (recent)

<b>Approval panel</b>	<b>Version</b>	<b>Date</b>
<b>Richard Thorpe</b>	2.1	12 Oct 2018
<b>Paul Ronan</b>	4.0	10 Oct 2019



# Contents

<b>1. Introduction</b>	<b>3</b>
1.1. Reason for Policy	3
1.2. Objectives of Policy	3
1.3. Applicability	3
1.4. Policy Statement	3
1.5. Policy overview	3
<b>2. Definitions</b>	<b>5</b>
<b>3. Data Protection Policy</b>	<b>7</b>
3.1. FE fundinfo responsibilities	7
3.2. Responsibilities and consequences of non-compliance	8
3.3. Principles related to the processing of personal data	8
3.4. Respecting the rights of data subjects	9
3.5. Records keeping	11
3.6. Personal data breaches	11
3.7. Data protection impact assessment	12
3.8. Transferring personal data outside FE fundinfo	13
3.9. Overseas transfers	13
3.10. Data protection training	14
3.11. Legal basis for processing of personal data	14
3.12. Processing special categories of personal data	15
3.13. Data protection officer	16
3.14. Relationship with the Information Security Policy	16
<b>4. Privacy in Electronic communication</b>	<b>17</b>
<b>5. Policy assurance</b>	<b>17</b>
<b>6. Policy review</b>	<b>18</b>
<b>7. Annex 1 – Referenced documents</b>	<b>18</b>
<b>8. Annex 2 – Current holders of named roles</b>	<b>19</b>



# 1. Introduction

## 1.1. Reason for Policy

To define FE fundinfo's approach to the processing of personal data and the standards it will adopt to ensure compliance with the relevant legislation and the privacy rights and expectations of the data subjects whose personal data it processes.

## 1.2. Objectives of Policy

To set out minimum standards and best practice requirements adopted by FE fundinfo to ensure that it meets the requirements of the relevant legislation and the privacy expectations of the persons whose personal data it processes, and the steps it will take to ensure that it meets those standards.

## 1.3. Applicability

This policy applies to all permanent, temporary employees, and contractors who have access to, or reason to otherwise process personal data on behalf of FE fundinfo.

It applies across all FE fundinfo locations and to the personal data of any individual regardless of where in the world they are located.

This policy also applies to all processing undertaken by any wholly owned subsidiary company of FE fundinfo.

## 1.4. Policy Statement

In undertaking its business purpose, FE fundinfo needs to process personal data which relates to staff, suppliers and customers. This policy sets out the standards which must be adhered to when personal data is being processed by, or on behalf of, FE fundinfo.

In summary FE fundinfo's overall approach is that it respects the rights of individuals and is committed to not invading or endangering their privacy unnecessarily; it considers the legislative requirements to be the minimum that must be achieved and will, wherever possible, adopt and implement standards which go beyond basic compliance with the law.

## 1.5. Policy overview

Section 3 of this document sets out in detail how FE fundinfo will comply with the relevant legislation and the standards it has set itself, in summary the key points are:

- FE fundinfo will produce policies, procedures, guidelines and work instructions which if followed correctly will facilitate the achievement of compliance with the



requirements of the relevant legislation by individuals processing personal data in the course of their FE fundinfo duties.

- Everyone who processes personal data on behalf of FE fundinfo is responsible for ensuring they comply with the requirements of this policy and the relevant legislation.
- All processing of personal data undertaken by FE fundinfo must be in compliance with the Principles set out in this Policy. Individuals processing personal data on behalf of FE fundinfo should ensure they adhere to the Principles in addition to any specific requirements of this policy, procedures or work instructions related to it. Breach of the Principles is a breach of the GDPR or the UK Data Protection Act 2018. In the event of any conflict between the Principles and this policy, procedures or work instructions the Principles have precedence.
- Everyone who processes personal data on behalf of FE fundinfo will respect the privacy rights of the data subject and ensure they do not undertake any processing which breaches the rights granted under the GDPR and/or the UK Data Protection Act 2018.
- Everyone who processes personal data on behalf of FE fundinfo shall ensure that sufficient records are kept of their processing to enable FE fundinfo to meet the requirements of the 'Accountability Principle'.
- Everyone who processes personal data on behalf of FE fundinfo shall ensure they take all appropriate and reasonable precautions to prevent a personal data breach occurring. In the event they become aware of such a breach they will report the matter immediately to the Data Protection Officer.
- Everyone who processes personal data on behalf of FE fundinfo shall ensure that they apply 'privacy by design and default' practices. All projects, processes or procedures which involve the processing of personal data shall first be subject to a screening process to determine whether a Data Protection Impact Assessment (DPIA) is required. If a DPIA is deemed necessary it will be undertaken, and any identified remedial actions implemented, before personal data is processed.
- Personal data shall only be transferred outside FE fundinfo where there is a legitimate business reason for doing so to a recipient who has been subject to due diligence checks and is bound by a contract which specifies the purposes for which the data is transferred and restricts the use of the data to those purposes. Further, before any data is transferred overseas the Data Protection Officer must be notified and their approval to the transfer obtained.
- Everyone who processes personal data on behalf of FE fundinfo, including accessing personal data, must complete the mandatory online data protection training session and demonstrate their understanding by successfully completing the accompanying test(s).
- All processing of personal data undertaken by FE fundinfo must be undertaken under one of the specified legal bases set out in this Policy. The particular legal



basis being used must be identified and recorded in the Data Inventory Register prior to any processing being undertaken.

- The processing of Special Category personal data will only be undertaken when at least one of the exemptions from the general prohibition as set out in this Policy has been identified and recorded in the Data Inventory Register.
- FE fundinfo will designate a Data Protection Officer in accordance with the requirements of Section 4 of the GDPR and/or similar clause in the UK Data Protection Act 2018.
- In the event of a conflict between the requirements of the Information Security Policy and this Data Protection Policy which relates to the processing of personal data, the provisions of this Policy shall have precedence.

## 2. Definitions

For ease of use this policy utilises the definitions set out in the General Data Protection Regulation and/or the UK Data Protection Act 2018. The most relevant/important of these definitions are:

**‘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 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;

**‘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;

**'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**'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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 'consent' of the data subject 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;

**'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 transmitted, stored or otherwise processed;

In addition, the following bespoke definitions are adopted for the purposes of this policy:

**'implementation date'** means the date on the which the UK Data Protection Act 2018 becomes law

**'relevant legislation'** means whichever of the following statutes are in force at the relevant time and relevant location:

- |                             |   |
|-----------------------------|---|
| UK Legislation:             | The Data Protection Act 2018, ( <b>DPA</b> )<br>The Privacy and Electronic Communications (EC Directive) Regulations 2003 ( <b>PECR</b> ) |
| Switzerland:                | The Swiss Federal Data Protection Act 1992 ( <b>DPA</b> )<br>Telecommunication Act 1997<br>Swiss Unfair Competition Act 2007              |
| Czech Republic legislation: | The General Data Protection Regulation 2016 ( <b>GDPR</b> )<br>Electronic Communication Act 127/2005                                      |



India legislation	Indian IT Act 2000
Hong Kong legislation:	Personal Data (Privacy) Ordinance (PDPO)
Singapore legislation	Personal Data Protection Act 2012 (PDPA)
Australia legislation	Federal Privacy Act 1988 (amended by Privacy Amendment (Enhancing Privacy Protection) Act 2012) Privacy Amendment (Notifiable Data Breaches) Act 2017
EU Legislation (covering Germany, France, Spain, Italy):	The General Data Protection Regulation 2016 ( <b>GDPR</b> )  The Regulation on Privacy and Electronic Communications ( <b>EPR</b> )

## 3. Data Protection Policy

### 3.1. FE fundinfo responsibilities

***FE fundinfo will produce policies, procedures, guidelines and work instructions which if followed correctly will facilitate the achievement of compliance with the requirements of the relevant legislation by individuals processing personal data in the course of their FE fundinfo duties.***

This policy, and the procedures referred to in Section 3.4, 3.6 and 3.7 of it, are owned by the Data Protection Officer and it is her/his responsibility to ensure they are kept up to date and communicated appropriately throughout the business.

Additional policies relevant to this policy referenced in the 'Annex 1 – Referenced Documents' section are owned by the departments/teams indicated. The Data Protection Officer should be consulted on the contents of those policies to ensure they meet the requirements of the legislation and align with this policy.

Specific data handling procedures, guidelines or work instructions may also be produced by other departments, teams or line managers but if they involve the handling of personal data, they must be approved by the Data Protection Officer.





## 3.2. Responsibilities and consequences of non-compliance

***Everyone who processes personal data on behalf of FE fundinfo is responsible for ensuring they comply with the requirements of this policy and the relevant legislation.***

In addition, line managers are required to ensure that the processing undertaken by individuals reporting to them complies with the requirements of this policy and the relevant legislation.

In the event any individual considers that the processing they are undertaking does not comply with this policy, or the relevant legislation, they should cease the processing and raise the issue with their line manager and the Data Protection Officer.

If any individual considers that the provisions of this policy, or any of the procedures or work instructions related to it, breach the requirements of the relevant legislation they should report this immediately to the Data Protection Officer.

Failure to comply with the requirements of this policy or the relevant legislation constitutes a serious breach of the applicable Code of Conduct and may result in action, which could include dismissal, being taken under the Disciplinary Procedure Policy as appropriate.

## 3.3. Principles related to the processing of personal data

***All processing of personal data undertaken by FE must be in compliance with the Principles set out below. Individuals processing personal data on behalf of FE should ensure they adhere to the Principles in addition to any specific requirements of this policy, procedures or work instructions related to it. Breach of the Principles is a breach of the GDPR and/or DPA 2018. In the event of any conflict between the Principles and this policy, procedures or work instructions the Principles have precedence and the conflict should be reported to the Data Protection Officer.***

The UK Data Protection Act 2018 principles relating to the processing of personal are identical with the General Data Protection Regulation (GDPR) principles.

The six GDPR principles are a restatement of six of the eight principles under the DPA and will apply from the date this policy is adopted, they require that personal data shall be:



- processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**‘purpose limitation’**);
- 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**‘accuracy’**);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**‘storage limitation’**);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**‘integrity and confidentiality’**).

The two data protection principles which are set out in the DPA but have not been reproduced in the GDPR relate to the rights of data subjects and international transfers. These are now set out as specific Articles within the regulation and addressed in Section 3.4 and 3.8 of this policy.

### **3.4. Respecting the rights of data subjects**

***Everyone who processes personal data on behalf of FE fundinfo will respect the privacy rights of the data subject and ensure they do not undertake any processing which breaches the rights granted under the GDPR and/or DPA set out below.***

The GDPR and/or DPA, grant certain rights to data subjects and FE fundinfo will issue procedures and work instructions to ensure that those rights are respected and are easily exercisable by the data subjects whose personal data it is processing. The rights granted to data subjects are:



- Right of access: The data subject has the right to confirmation of the processing undertaken and to a copy of the personal data being processed. This copy must be provided free of charge and within one calendar month. FE fundinfo has detailed 'Subject Access Request Procedures' which set out how this right will be provided for.
- Right to rectification: inaccurate data must be corrected without delay and incomplete data completed upon request. Any requests to exercise this right should be forwarded to the Data Protection Officer without delay.
- Right to erasure: also known as the 'right to be forgotten' this provides that under certain circumstances the data subject can oblige the data controller to erase personal data relating to them without undue delay. Any requests to exercise this right should be forwarded to the Data Protection Officer without delay.
- Right to restrict processing: under certain circumstances the data subject can object to processing other than storage of their personal data. Any requests to exercise this right should be forwarded to the Data Protection Officer without delay.
- Right to data portability: this entitles the data subject to a copy of their personal data in a structured and commonly-used machine readable format and allows them to require it to be transmitted to another data controller. FE fundinfo must be prepared to honour any such requests which should be forwarded to the Data Protection Officer without delay
- Right to object to processing: a data subject may object to processing including the profiling of the data subject, which is undertaken under the public interests or legitimate interests' bases and can also object to the processing of their data for direct marketing purposes. Any requests to exercise this right should be forwarded without delay to the Data Protection Officer for actioning.
- Right not to be subject to automated individual decision-making: data subjects can object to 'automated processing' (which includes profiling) if that processing results in decisions which have a legal effect concerning him or her (or similarly significantly affects them) being made solely on the basis of that processing. At the current time no such processing is undertaken by FE fundinfo, if any is anticipated or planned advice should be sought from the Data Protection Officer.

In addition to the above explicit rights the provisions of Articles 13 and 14 of the GDPR, and/or similar clauses in DPA, specify that certain information must be given to a data subject who is the subject of data processing at specific times, this is sometimes referred to as the 'Right to be informed' but is in fact an obligation on the data controller. The obligation is met by advising the data subject how their data will be used, for how long, the legal basis for the processing and how it will be kept secure. This information should be given when the data is collected and whenever it is to be used for a purpose which is



different to the one for which it was originally collected. Most commonly this will be done by reference to FE fundinfo's Privacy Policy and to specific Privacy Statements provided by the Data Protection Officer as part of the design of data collection forms. To ensure that sufficient notice is drawn to the Privacy Policy and the requirements of these articles are met advice should be sought from the Data Protection Officer before any data collection is undertaken or any personal data is used for new or novel purposes.

### **3.5. Records keeping**

***Everyone who processes personal data on behalf of FE fundinfo shall ensure that sufficient records are kept of their processing to enable FE fundinfo to meet the requirements of the Accountability Principle as set out below. Specific work instructions may be issued to provide guidance on the records which should be kept.***

In addition to the Data Protection principles set out in 3.3 above, Article 5 of the GDPR, and/or similar clauses in DPA, states that the controller shall be responsible for, and be able to demonstrate compliance with, the data protection Principles; this is commonly known as the Accountability Principle.

Compliance with the Accountability Principle requires significant record keeping of all data processing undertaken by FE fundinfo, in particular the following records shall be maintained

- A Data Inventory Register detailing the personal data assets processed, the nature of the processing, the systems used, the legal basis, the time for which the data will be retained and how it will be disposed of.
- Data Protection Impact Assessments undertaken.
- Privacy Policies and Privacy Statements and the dates and circumstances when they were used.
- Copies of the wording used to obtain consent and records of how and when consent was given by individuals to the processing of their personal data.
- A Data Breach Register
- Records of data protection training and tests relating to it.
- Copies of this policy and the procedures referred to in it and by which compliance with it is ensured, the dates those policies/procedures applied and the reasons why they were withdrawn or amended.

### **3.6. Personal data breaches**

***Everyone who processes personal data on behalf of FE fundinfo shall ensure they take all appropriate and reasonable precautions to prevent a personal data breach***



***occurring. In the event they become aware of such a breach they will report the matter immediately to the Data Protection Officer.***

Personal data breaches, except those which are unlikely to result in a risk to the rights and freedoms of the data subjects, must be notified to the local (country specific) Supervisory Authority without undue delay and within 72 hours of the controller becoming aware of the breach. The decision as to whether or not the breach represents a risk to the rights and freedoms of the data subject requires an in-depth knowledge of the issues involved and how personal data could be misused to create such a risk. The individual who discovers the data breach is unlikely to possess sufficient knowledge of these issues to make this judgement and therefore all personal data breaches should be reported without delay to the Data Protection Officer (using the procedures set out in the FE fundinfo's Personal Data Breach Incident Response Process) who will assess the risks to the data subject(s) and if appropriate report the breach to the local Supervisory Authority.

The FE fundinfo's Personal Data Breach Incident Response Process also require 'near-misses' (i.e. events that could have led to a data breach if it were not for specific intervening action being taken to prevent the breach and/or circumstances which have the potential to lead to a data breach) to be reported so that action can be taken to assess and mitigate the risk of a similar event causing a breach in the future

### **3.7. Data protection impact assessment**

***Everyone who processes personal data on behalf of FE fundinfo shall ensure that they apply 'privacy by design and default' practices by, for example, collecting only the personal data required for a specified purpose and ensuring that the data is only accessible to those who need it to carry out their FE fundinfo tasks. All projects, processes or procedures which involve the processing of personal data shall first be subject to a screening process to determine whether a Data Protection Impact Assessment (DPIA) is required. If a DPIA is deemed necessary it will be undertaken, and any identified remedial actions implemented, before personal data is processed.***

The GDPR, and/or DPA, introduces the concept of 'privacy by design and default'. In essence this requires the controller to ensure that all its processing operations are designed to minimise the risk to the privacy of the data subjects. This involves measures such as encryption, data minimisation, pseudonymisation, and role-based access protocols. FE will ensure that privacy by design and default is enshrined in policies, procedures and work instructions which relate to the processing of personal data.

Processing which uses new technologies, or which because of its nature, scope, context or purposes is likely to result in a high risk to the rights and freedoms of the data subjects



is, under the GDPR and/or DPA, subject to the requirement to carry out an assessment of the impact of the processing operations on the protection of personal data – a Data Protection Impact Assessment. FE fundinfo has Data Protection Impact Assessment Procedures in place which must be adhered to whenever a new data processing operation which involves the collection of personal data, or the use of personal data already collected in a way which is different to that for which it was originally collected, is planned.

### **3.8. Transferring personal data outside FE fundinfo**

***Personal data shall only be transferred outside FE fundinfo where there is a legitimate business reason for doing so to a recipient who has been subject to due diligence checks and is bound by a contract which, by incorporation of mandatory standard clauses, specifies the purposes for which the data is transferred and restricts the use of the data to those purposes.***

FE fundinfo may engage with third parties to carry out work for it which will require personal data to be transferred to that third party (e.g. sending a list of customers email addresses to a specialised emailer company to fulfil a marketing campaign). These third parties are known as 'Data Processors'. FE fundinfo will only use Data Processors that are able to satisfy it, and provide guarantees, that they have appropriate organisational and technical measures in place to ensure the data is processed in compliance with the GDPR and DPA, and who have signed a binding contract which specifies the purpose for which the personal data is transferred, restricts the processing to that purpose, specifies the duration of the contract and sets out how the data will be dealt with at the end of the contract. The FE fundinfo's Legal and Compliance team have drafted standard contract clauses to ensure the requirements of the GDPR and DPA, are met when contracting with a third party to carry out data processing on behalf of FE fundinfo and these clauses must be incorporated into every contract appointing a data processor. Responsibility for incorporating these clauses and carrying out initial and ongoing due diligence checks rests with the managers owning each FE fundinfo product/service.

### **3.9. Overseas transfers**

***Before any data is transferred overseas the Data Protection Officer must be notified and their approval to the transfer obtained.***

If personal data is to be transferred overseas specific measures must be in place to ensure that the rights and freedoms of the data subjects are protected.

The GDPR and DPA have three mechanisms by which overseas transfers can be safely made, an adequacy decision, appropriate safeguards or binding corporate rules. Which of these measures is appropriate depends on the nature and circumstances of the transfer and advice should be sought from, and permission granted by, the Data Protection Officer before any such transfer is undertaken.



### 3.10. Data protection training

***Everyone who processes personal data on behalf of FE fundinfo, including accessing personal data, must complete the mandatory online data protection training session and demonstrate their understanding by successfully completing the accompanying test(s).***

In order to ensure compliance with this policy and with the regulatory requirements relating to the processing of personal data, all individuals employed by FE fundinfo are required to complete a mandatory online data protection training session. They are also required to demonstrate their understanding of the contents of the training module and of this policy by successfully completing an online test. The training session and accompanying test should ideally be completed as soon as the individual has access to FE fundinfo systems but in any event within two months of the commencement of their employment.

Further refresher training should be undertaken at intervals dependant on the individual's role but at least once every three years.

Additional online training modules may be made available to educate individuals about specific topics covered by this policy, line managers should review these modules and the roles of individuals in their team to determine if any should be a mandatory requirement of an individual's Personal Development Plan.

Contractors who have access to FE fundinfo systems and who are engaged in the processing of personal data should also be required to undertake the online data protection training session, and complete the test, as soon as they are granted access to the system. The training/testing should be refreshed at least once every three years; individuals whose role involves regular contact with personal data will be expected to complete refresher training once a year.

### 3.11. Legal basis for processing of personal data

***All processing of personal data undertaken by FE fundinfo must be undertaken under one of the specified legal bases as set out below. The particular legal basis being used must be identified and recorded in the Data Inventory Register prior to any processing being undertaken.***

Under the GDPR, and/or DPA, there are six 'legal bases' for the processing of personal data. The processing of personal data is only lawful (as required by the first Principle) if one of these legal bases apply, they are:





- the data subject has given consent to the processing of his or her personal data for one or more specific purposes (**'consent'**);
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (**'contract'**);
- processing is necessary for compliance with a legal obligation to which the controller is subject (**'legal obligation'**);
- processing is necessary in order to protect the vital interests of the data subject or of another natural person (**'vital interests'**);
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (**'public interest'**);
- 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 (**'legitimate interests'**).

### 3.12. Processing special categories of personal data

*The processing of Special Category personal data will only be undertaken when at least one of the exemptions as set out below from the general prohibition has been identified and recorded in the Data Inventory Register.*

Special category data is the description applied in the GDPR, and/or DPA, to certain types of personal data considered particularly sensitive, they are also commonly known as 'sensitive personal data'. The types of data considered to be 'special category' are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data (when used to uniquely identify an individual)
- Data concerning health
- Data concerning an individual's sex life or sexual orientation.

As a general rule, the processing of special category personal data is prohibited unless one of the following conditions apply (these can be considered additional legal bases for the processing of special category data).





- The data subject has given their explicit consent for one or more specified purposes
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interest of the data subject or another person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of the legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim. The data should relate to members, former members or others with regular contact with the body and data should not be disclosed outside the body without specific consent.
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

### **3.13. Data protection officer**

***FE fundinfo will designate a global Data Protection Officer in accordance with the requirements of Section 4 of the GDPR and similar section in DPA. A local Data Protection Officer shall be designated in the countries where the local data protection law requires it.***

The GDPR/DPA requires that certain businesses designate a Data Protection Officer (DPO) to carry out specified tasks related to ensuring compliance with the legislation. FE fundinfo has determined that it is one of the businesses required to designate a DPO on the basis that it is engaged in regular and systematic monitoring of data subjects on a large-scale. FE fundinfo businesses operating in Switzerland must designate a local Data Protection Officer.

The DPO has a direct reporting line to FE fundinfo's CTO but day to day line management of the DPO may be allocated to another person.

This decision will be reviewed annually to take into account new guidance which may be issued by the Supervisory Authorities across all countries FE fundinfo operates from.

### **3.14. Relationship with the Information Security Policy**

***In the event of a conflict between the requirements of the***



***Information Security Policy and this Data Protection and Privacy Policy which relates to the processing of personal data, the provisions of this Policy shall have precedence.***

The Information Security Policy sets out FE fundinfo's approach to managing all the data that it uses, including personal data. Compliance with the Information Security Policy is a prerequisite of compliance with the Data Protection Policy.

## 4. Privacy in Electronic communication

Along with the privacy requirement of personal data deriving from applicable data protection law and regulations, FE fundinfo must comply with the applicable privacy and electronic communication regulations. These are applicable for FE fundinfo products/services dealing with both business and consumer customers.

The main aspects that must be taken into account are:

- Unsolicited marketing
- Cookies
- Data security (confidentiality and data protection)

Any FE fundinfo websites which permits user interaction must provide a Privacy Policy.

## 5. Policy assurance

The Compliance Duty Holder needs to be assured that this policy is working i.e.

- It is doing what it is supposed to do on the ground
- It is effective at delivering the organisational objectives

This will be achieved this by having:

- A Data Protection Officer to oversee the policy.
- An Information Security Management Framework in place to oversee the management and compliance of FE fundinfo with the Policy.
- Regular audits carried out and reports issued by the Information Security department to assess compliance with policy.



## 6. Policy review

Reviews of this policy will take place at least once a year. However additional reviews may be triggered by any of the following items assessed by the Information Security department and the Data Protection Officer:

- Escalation of related strategic risks
- Significant ethical changes
- Regulatory changes, in particular the coming into force of the GDPR/The E-Privacy Regulation or the UK DPA 2018
- Guidance issued by the ICO which significantly impacts this Policy
- External or internal incidents (e.g. data breach, negative publicity)
- New technology
- Financial changes
- Changes to governance.

## 7. Annex 1 – Referenced documents

### **Related FE fundinfo Policies, Procedures & Guidance:**

- Information Security Policy
- Records Control Policy
- Subject Access Request Procedures
- FE fundinfo's Data Protection Breach Incident Response Process
- FE fundinfo's Incident Responding Procedures
- FE fundinfo's Security Incident Response Procedures
- Data Protection Impact Assessment Procedures
- Due Diligence and Networking Research data collection and retention procedures

### **Related FE Forms & Instructions:**

- Data Inventory Register
- Data Breach Register



- FE fundinfo's Suppliers Register

## 8. Annex 2 – Current holders of named roles

Role name	Role Holder	Contact details
Data Protection Officer (global excluding Switzerland)	Sorin Pop	<a href="mailto:Sorin.Pop@financialexpress.net">Sorin.Pop@financialexpress.net</a> +44-1483-783940
Switzerland Data Protection Officer	Daniel Walter	<a href="mailto:Daniel.Walter@fundinfo.com">Daniel.Walter@fundinfo.com</a>
Compliance Duty Holder	Dominic Timberlake	<a href="mailto:Dominic.Timberlake@financialexpress.net">Dominic.Timberlake@financialexpress.net</a>
CTO	Paul Ronan	<a href="mailto:Paul.Ronan@financialexpress.net">Paul.Ronan@financialexpress.net</a>
IT Manager	Sundar Kumaravel	<a href="mailto:Sundar.K@financialexpress.net">Sundar.K@financialexpress.net</a>
Information Security Manager	Sorin Pop	<a href="mailto:Sorin.Pop@financialexpress.net">Sorin.Pop@financialexpress.net</a>

