October 2017

Data Protection Policy

1. Objectives

1.1. To ensure that we use personal information (for example of staff, vendors, website visitors and third parties like directors, investors, finance professionals, complainants and witnesses) in accordance with the law.

1.2. To set out the standards that should be adhered to when handling personal information.

2. Scope

2.1. This policy applies to all Executive Staff and Non-Executive Members (individually and together, **you**).

3. Background

3.1. What is UK data protection law?

3.1.1. UK data protection law gives individuals certain rights and protections in connection with the way their personal information (any information that relates to them, such as a name, contact details, allegations of criminal activity, etc.) is used.

3.2. How does UK data protection law affect the FRC?

3.2.1. The use of personal information is critical to us in order to:

(1) perform our regulatory functions and activities; and

(2) carry out internal management and administration.

3.2.2. From start to finish, these activities involve the use of personal information which will be covered by UK data protection law. In many scenarios, we are determining the purposes and means by which that personal information is processed. This means that we are considered as a "controller" of personal information and we are subject to explicit requirements under UK data protection law.

3.2.3. We perform regulatory functions which involve the processing of personal information that is important and, in certain cases, sensitive to individuals. This may include details of alleged or actual criminal offences and medical information as part of an ongoing audit or investigation. Therefore, in order to ensure public confidence in us and our capacity to perform our functions, it is critical that we safeguard personal information and uses it in accordance with UK data protection law.

3.3. What are we doing about it?

3.3.1. We treat compliance with out data protection obligations seriously. This is why we maintain this Policy to ensure that the personal information we collect and use is handled in accordance with UK data protection law.

3.4. What are the consequences if we get it wrong?

3.4.1. Getting it wrong is serious for our ability to function as a trusted regulator. It could also lead to complaints from individuals, compensation claims, fines from regulators and reputational damage. Furthermore, if you deliberately fail to observe this Policy, we will consider disciplinary action against you.

4. The Rules

4.1. Ensuring transparency

We must be open, honest and fair when using personal information.

Understanding the Rule

i) Being open, honest and fair in the way we use and share personal information is an important step to demonstrate good data protection practices. Individuals should be properly notified about how we use and share their personal information.

Practical Steps

ii) Fair processing information notices must be provided to individuals, if possible at the time of collection of that information or as soon as practicable after that.

iii) You should also be provided with a fair processing information notice where we collect and use personal information about you. All our employment and contractor contracts should include suitable wording notifying that individual of how we will use their information.

4.2. Using personal information for a specified and lawful purpose only

We must only use personal information specified and lawful purposes.

Understanding the Rule

i) We must only collect the personal information for the purposes which are identified to an individual at the time of collection (or, where this is not possible, which are subsequently notified to them within a reasonable time) and which are permitted by law.

ii) This rule means that we must identify and publicise the purposes for which personal information will be processed in external-facing documents and in employment and vendor contracts.

iii) If required by law, we must seek individuals' consent for the collection, use or disclosure of their personal information – this may be the case, for example, when collecting and using individuals' sensitive personal information. See rules 3.9 and 3.10 for further information.

Practical Steps

iv) When collecting personal information from individuals, we must ensure that the privacy notice made available to those individuals contains all of the purposes for which the personal information may be used.

v) In addition, when collecting information, we must never collect personal information in a way that is unlawful or where we have no legitimate basis for using that personal information.

vi) When collecting sensitive personal information, we must ensure that we have obtained an individual's explicit consent or can rely upon another lawful processing ground.

4.3. Ensuring data quality

We must keep personal information accurate, complete and up to date.

Understanding the Rule

i) Processing inaccurate information can be harmful to individuals and to us. We must actively encourage individuals to inform us when their personal information changes.

Practical Steps

ii) In the employment context, staff must (and must, by systematic reminders, be actively encouraged to) update their details.

iii) All third parties and vendors must be actively encouraged to update their contact details by inviting them, when communication occurs, to notify us of any changes in their personal information.

4.4. Ensuring data relevancy

We collect only relevant personal information.

Understanding the Rule

i) We must only collect personal information for purposes that have been specified to the individual, and take care to ensure that the personal information we collect is not excessive.

ii) We must not collect personal information which is irrelevant to the purposes for which it is sought.

Practical Steps

iii) When collecting personal information from individuals, we must ensure that we do not collect data which is outside of the scope of that set out in the privacy notice provided to those individuals.

iv) We must guard against collecting excessive amounts of personal information from individuals. For example, you are unlikely to have to collect details about an auditor's race / ethnicity if you are investigating him for regulatory compliance.

4.5. Retaining data

We must not use personal information for longer than is necessary.

Understanding the Rule

i) Any personal information relating to individuals should only be kept where there is a regulatory or legal need to do so.

Practical Steps

ii) Statutes or regulations may require that certain personal information be retained for a specified length of time, and it may also be prudent to keep certain personal information for a precise period so that we are able to defend properly any legal claims or manage an on-going audit or investigation.

iii) Documents (including paper and electronic versions and e-mail) containing personal information must not be kept indefinitely and should always be deleted and destroyed once they have become obsolete or when that personal information is no longer required. Personal information should not be retained simply on the basis that it might come in useful one day without any clear view of when or why. For further information, please see the **Records Management Policy** and any **Record Retention Schedule** implemented by your operating unit.

4.6. Honouring individuals' rights

We must respect individuals' rights.

Understanding the Rule

i) We will reply to queries and complaints in reasonable time and to the extent reasonably possible concerning our processing of personal information. We are firmly aware of the right of individuals to access personal information held about them.

ii) Individuals including staff members, vendors and third parties are entitled (by making a request to the FRC) to be supplied with a copy of any personal information held about them (including both electronic and paper records), subject to applicable exemptions. For further information, please see the **FRC Individual Rights Policy**.

iii) Other data protection rights include:

(1) Individuals may object to our use of their personal information.

(2) Individuals may ask us to change the information that we hold on them because they consider our information to be inaccurate or out-of-date.

(3) Individuals may ask us to confirm that no decision taken by us is based solely on the processing of their personal information by automatic means for the purpose of evaluating matters relating to them, for example, their creditworthiness or professional competency.

Practical Steps

iv) Where we receive a request from an individual exercising the right to access their information, we must follow the steps set out in our **Individual Rights Policy**. Our procedure provides a timeline of events to ensure that valid requests are processed in line with applicable law.

v) Where we receive a request from an individual exercising any other data protection right we must notify the FOIA Team immediately by forwarding their request to FOIA@frc.org.uk.

4.7. Taking appropriate security measures

We must protect personal information securely.

Understanding the Rule

i) Personal information must be kept secure. Technical and organisational security measures are necessary to prevent the unauthorised or unlawful processing or disclosure of personal information and the accidental loss, destruction of, or damage to, personal information.

Practical Steps

ii) We must monitor the level of security applied to a set of information, taking into account current standards and practices.

iii) In particular, we must observe the security of information requirements set out in applicable FRC Information Policies .

4.8. Ensuring adequate protection for overseas transfers

We must ensure protection for international transfers of personal information.

Understanding the Rule

i) International transfers of personal information outside of the European Economic Area ("**EEA**") are not allowed without appropriate steps being taken to ensure the adequate protection of the transferred data. Such steps include the FRC entering into standard contractual terms with the proposed recipient of the transferred data.

Practical Steps

ii) We must not transfer any personal information outside the EEA without appropriate steps being taken. Please contact the Governance and Legal Team if you are transferring personal information to any other service providers or third parties based outside the EU, Iceland, Liechtenstein or Norway or if this may arise in the future.

4.9. Safeguarding the use of sensitive personal information

We must take particular care when using sensitive personal information.

Understanding the Rule

i) Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. This information is subject to more stringent protection than other personal information, so our standards of care must be higher when dealing with this type of information.

Practical Steps

ii) We must always assess whether sensitive personal information is essential for the proposed use.

iii) We must only collect sensitive personal information when it is absolutely necessary in the context of our regulatory functions. For example, we should not collect information about alleged or actual criminal offences where it is not required for the purposes of an audit, investigation or other regulatory activity.

4.10. When to obtain consent for sensitive personal information

We must only use sensitive personal information where we have obtained the individual's explicit consent, unless we have another lawful basis for doing so

Understanding the Rule

i) There are certain conditions in place which we must comply with when we collect and use sensitive personal information.

ii) One such condition is that people must expressly agree to the collection and use of such information. This permission to our use of sensitive personal information must be freely given, specific and informed.

iii) Sensitive personal information may be collected and used without the explicit consent of an individual where we have another lawful basis to collect and use this type of information.

Practical Steps

iv) Where applications or other forms are used to collect sensitive personal information, they must include suitable wording expressing the individual's consent.

v) Consent must be demonstrable. Therefore, when it is collected verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their responses are able to be verified.

vi) Where consent is not obtained, we must take steps to ensure that there is another lawful basis under UK data protection law for the collection and use of such information. These may include that the processing is necessary for the purpose of, or in connection with, any legal proceedings or that the processing is necessary for the exercise of our statutory or regulatory functions. However, **you should not assume** that either basis automatically applies to your intended collection, use or transfer of sensitive personal information. **You should refer any queries to the Governance and Legal Team**.

4.11. Legitimising marketing

We must always allow members to opt out of receiving marketing information such as our alerts

Understanding the Rule

i) Another important data protection right that individuals have is the right to object to the use of their personal information for marketing purposes and we must honour all such opt-out requests, where any marketing is carried out. This applies even where individuals have previously opted-in to receiving marketing communications from us.

Practical Steps

ii) We must ensure that the fair processing information notice made available when personal information is collected includes the relevant mechanisms for collecting individuals' consent to receiving marketing communications, and that it tells individuals how they may change their marketing preferences. Please contact the Governance and Legal Team for further information.

4.12. Honouring opt-outs

We must always suppress from marketing initiatives the personal information of individuals who have opted out of receiving marketing information

Understanding the Rule

i) It is essential that individuals' choices are accurately identified prior to sending any marketing communications. A failure to comply with an individual's opt-out choice (e.g. by sending an e-mail alert to an individual who has previously indicated to us that he or she does not wish to receive mailings) may lead to complaints from the individual and possible scrutiny or enforcement action being taken by regulators.

Practical Steps

ii) We must take all necessary steps to prevent the sending of marketing materials to individuals who have opted out. In certain instances, it may also be necessary to obtain opt-in consent from individuals before sending them marketing communications – this may be the case, for example, when sending e-mail or text marketing messages. Please contact the Governance and Legal Team for further information.

4.13. Using subcontractors

We must ensure that our service providers adopt appropriate and equivalent security measures to ours.

Understanding the Rule

i) The law requires that, where one of our suppliers or service providers has access to personal information of past, present and prospective staff, vendors, and external stakeholders like directors, investors and finance professionals, we must impose strict contractual obligations dealing with the security of that information.

Practical Steps

ii) We must always enter into a written contract with any service provider that processes personal information on our behalf. **All contracts with suppliers and service providers should include contractual provisions approved by Governance and Legal Team**.

5. Responsibilities and Data Privacy Organisation

5.1. The Governance and Legal Team and, where applicable, local area data privacy representatives, the IT Team and the HR Team are primarily responsible for adopting, implementing and maintaining this Policy.

6. Who to Contact

6.1. If you have a question about this Policy, please contact: the FRC General Counsel or a member of the Governance and Legal Team.

7. Compliance

7.1. This policy may be officially monitored for compliance by the *[Executive Director of Strategy & Resources or their nominee]* from time to time and may include random and scheduled inspections.

October 2017