Policy and procedure

Data controller ("the Organisation"):	KKB Group

Data protection policy and procedure

In order to carry out its business, the organisation needs to gather and use information about identifiable individuals. These include employees, customers, suppliers, business contacts and other people the organisation has a need to contact. We are, therefore, committed to treating this information with the utmost care and confidentiality.

This policy outlines how data will be collected, handled, stored and disposed of to meet the requirements of the General Data Protection Regulations 2018 (GDPR). It ensures that the Organisation: -

- Follows recognised best practice in complying with the legislation
- Protects the rights of the identifiable individuals whose data is held
- Is transparent about how data is collected, stored and processed
- Protects itself from the risks associated with a data breach

The General Data Protection Regulations 2018 (GDPR) replace the Data Protection Act 1998. The legislation outlines how the Organisation must collect, handle, store and dispose of personal information. Whether held electronically or as a hard copy, under the legislation, the personal data shall be treated under the six data protection principles. In brief they say that the data shall be processed as follows: -

- Lawfulness, fairness and transparency: Collected lawfully, fairly and in a transparent manner
- Purpose limitation: Collected only for a specified, explicit and legitimate purpose; it shall not be processed further in a manner incompatible with the original purpose
- Data minimisation: Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accuracy: Accurate and, where necessary, kept up to date. The Organisation shall take every reasonable step to ensure that any inaccurate personal data is rectified or erased without undue delay
- Storage limitation: Kept in a form which permits identification of the subject of the data for no longer than is necessary for the purpose for which the data was collected
- Integrity and confidentiality: Processed in a manner that ensures appropriate security of the data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

The Organisation is responsible for, and must be able to demonstrate compliance with, the data protection principles above. Within the legislation, this is the principle of accountability. As stated, the above is a brief summary of the data protection principles. Full details of the individual principles and the specific requirements of the legislation are held within the data protection procedure, which follows.

Each functional head is responsible for ensuring that their departmental procedures comply with the requirements of the data protection principles. As stated above, the full requirements of each data protection principle are outlined within the data protection procedure, which shall be used to determine procedural compliance. If a specific departmental procedure is not compliant, it shall be amended accordingly. The functional heads are also responsible for ensuring that their management team and respective reports are aware of the impact that the legislation has on their specific roles. To ensure compliance with the legislation, employees must adhere to this policy and its associated procedures when processing personal data on the Organisation's behalf in the proper performance of the duties and responsibilities of their role.

The Organisation takes compliance of this policy and associated procedures very seriously. Any breach of the policy and procedures will be regarded as misconduct and will be dealt with under the Organisation's disciplinary procedure. A significant or deliberate breach of the policy and procedures constitutes a gross misconduct offence and could lead to summary dismissal.

The Organisation's "data compliance manager" has responsibility for data protection compliance within the business. Employees should contact them if they have any questions about the operation of the policy and associated procedures or need further information about data protection legislation.

If any employee wishes to make an internal complaint that the Organisation is failing to comply with the legislation, they can raise this as a formal grievance within the Organisation's grievance procedure.

Procedure

The General Data Protection Regulations 2018 (GDPR) has six data protection principles that the Organisation and all employees must comply with at all times in their personal data processing activities.

Policy and procedure

Data protection principles

1. Lawfulness, fairness and transparency

The data protection legislation provides that personal data processing is only lawful in certain circumstances. These include where:

- consent has been given to the processing of personal data for one or more specific purposes
- the processing is necessary for the performance of a contract, e.g. an employment contract, or in order to take steps to entering into a contract
- the processing is necessary for compliance with our legal obligations
- the processing is necessary to protect the "data subject's" vital interests (or someone else's vital interests)
- the processing is necessary to pursue the Organisation's legitimate interests (or those of a third party), where the "data subject's" interests or fundamental rights and freedoms do not override the Organisation's interests; the purposes for which the Organisation processes personal data for legitimate interests must also be set out in an appropriate privacy notice

The Organisation must only process personal data on the basis of one or more of these lawful bases for processing. Each processing activity must be reviewed before it starts and then regularly while it continues. The Organisation must satisfy itself that the activity is necessary, the most appropriate lawful basis (or bases) for that activity must be selected. When determining whether the Organisation's legitimate interests are the most appropriate basis for lawful processing, a legitimate interests assessment must be conducted, a record of which shall be kept.

Where the Organisation relies on consent as the lawful basis for processing, this requires the "data subject" to have given a positive statement, active opt-in or clear affirmative action; pre-ticked boxes, inactivity or silence do not constitute consent. If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, where appropriate, separate consents must be obtained for different types of processing. People also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

The legislation also specifies that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

- the "data subject" has given their explicit consent to the processing of their personal data for one or more specified purposes
- the processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the Organisation or the "data subject" under employment law or social security law in the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the "data subject"
- the processing is necessary for the establishment, exercise or defence of legal claims

The Organisation may from time to time need to process special categories of personal data and criminal records personal data. The Organisation and its employees must only process special categories of personal data and criminal records personal data where there is also one or more of these special lawful bases for processing. Before processing any special categories of personal data and criminal records personal data, the "data compliance manager" must be notified so that they may assess whether the processing complies with one or more of these special conditions.

A clear record must be kept of all consents, including explicit consents, which covers what the "data subject" has consented to, what they were told at the time and how and when consent was given. This enables the Organisation to demonstrate compliance with the data protection requirements for consent.

Under the legislation, the transparency principle requires the Organisation to provide specific information to "data subjects" through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices may comprise general privacy statements applicable to a specific group of subjects e.g. employees, or they may be stand-alone privacy statements covering processing related to a specific purpose. Whenever

Policy and procedure

Lawfulness, fairness and transparency

the Organisation collects personal data directly from "data subjects", including for employment purposes, the Organisation must provide the "data subject" with all the information required to be included in a privacy notice.

This includes:

- the identity and contact details of the Organisation (as data controller) and any representative
- where applicable, the identity and contact details of the "data compliance manager"
- the purposes for which the personal data will be processed
- the lawful basis or bases for processing
- where the Organisation is relying on its legitimate interests (or those of a third party) as the lawful basis for processing, what those legitimate interests are
- the categories of personal data, unless they were obtained directly from the "data subject"
- the third-party sources that the personal data originate from, unless they were obtained directly from the "data subject"
- the recipients, or categories of recipients, with whom the personal data may be shared
- details of transfers to non-EEA countries and the suitable safeguards applied
- the retention period for the personal data or, if that is not possible, the criteria to be used to determine the retention period
- the existence of the "data subject's" rights, i.e. subject access, rectification, erasure, restriction of processing, objection and data portability
- the right to withdraw consent to processing at any time, where consent is being relied on as the lawful basis for processing
- the right to lodge a complaint with the Information Commissioner's Office
- whether the provision of personal data is part of a statutory or contractual requirement or obligation, or a requirement necessary to enter into a contract, and the possible consequences of failing to provide the personal data
- the existence of any automated decision-making, including profiling, and meaningful information about how decisions are made, the significance and consequences

The Organisation must issue a privacy notice, which can be by electronic means, when the "data subject's" personal data is first collected from them. If the personal data has been obtained from third parties, the Organisation must provide the privacy notice information within a reasonable period of having obtained the personal data, but at the latest within one month. However, if the personal data is to be used to communicate with the "data subject", the privacy notice information is to be provided, at the latest, when the first communication takes place, or if disclosure of the personal data to another recipient is envisaged, it is to be provided, at the latest, when the data is first disclosed. Employees must comply with these rules on privacy notices when processing personal data on the Organisation's behalf in the proper performance of your job duties and responsibilities.

The Organisation will issue privacy notices to its employees from time to time.

Privacy notices can also be obtained from the Organisation's "data compliance manager".

2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the "data subject" when they were first obtained, for example in an appropriate privacy notice, unless the "data subject" has been informed of the new purposes and the terms of this policy are otherwise complied with, e.g. there is a lawful basis for processing. This also includes special categories of personal data and criminal records personal data

3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Organisation will only collect personal data to the extent that are required for the specific purposes notified to the "data subject". Employees must only process personal data where their job duties and responsibilities require it.

Policy and procedure

Data minimisation

They must not process personal data for any reason which is unrelated to their job duties and responsibilities. In addition, employees must ensure that any personal data they collect is adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

When personal data is no longer needed for specified purposes, employees must ensure that it is destroyed, erased or anonymised in accordance with the Organisation's rules on data retention and destruction set out below.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that any personal data that is inaccurate is erased or rectified without delay.

It is important that the personal data the Organisation holds about individual employees as a "data subject" is accurate and up to date. Employees are required to keep the Organisation informed if their personal data changes, e.g. they change their home address, so that the records can be updated. The Organisation cannot be held responsible for any errors in individual employee's personal data in this regard unless they have notified the Organisation of the relevant change. The Organisation will promptly update employee's personal data if they advise the Organisation that they have changed or that they are inaccurate.

Employees must also ensure that the personal data the Organisation holds about other "data subjects" is accurate and up to date where this is part of their job duties or responsibilities. This includes special categories of personal data and criminal records personal data. Employees must check the accuracy of any personal data at the point of their collection and at regular intervals thereafter. Employees must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

5. Storage limitation

Personal data must not be kept in a form which permits identification of "data subjects" for longer than is necessary for the purposes for which the personal data is processed.

The Organisation will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special categories of personal data and criminal records personal data. You must comply with the Organisation's rules on data retention and destruction set out below.

The Organisation will generally hold personal data, including special categories of personal data and criminal records personal data, for the duration of an employee's employment or engagement. The exceptions are:

- criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a criminal record check, unless, in exceptional circumstances, the information has been assessed by the Organisation as relevant to the ongoing working relationship
- it will only be recorded whether a criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the Organisation as relevant to the ongoing working relationship
- if it has been assessed as relevant to the ongoing working relationship, a criminal record check will nevertheless be deleted after six months or once the conviction is "spent" if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession)
- disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment).

Once an employee has left employment or their engagement has been terminated, the Organisation will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of their employment or engagement.

Policy and procedure

Storage limitation

However, this is subject to the following: -

- any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and
- the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. The Organisation will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to six years after the termination of their employment or engagement.

Overall, this means that the Organisation will "thin" the file of personal data that it holds on employees one year after the termination of their employment or engagement, so that the Organisation will only continue to retain for a longer period that which is strictly necessary.

The Organisation will generally hold personal data, including special categories of personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of our business relationship with them.

Once our business relationship with a client, customer or supplier has been terminated, the Organisation will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of the business relationship, but this is subject to:

- any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and
- the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a County Court or High Court

Overall, this means that the Organisation will "thin" the file of personal data that it holds on clients, customers and suppliers for one year after the termination of the business relationship, so that the Organisation will only continue to retain for a longer period that data which is strictly necessary.

All personal data, including special categories of personal data and criminal records personal data, must be reviewed before destruction or erasure to determine whether there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above. If you are responsible for maintaining personal data and are not clear what retention period should apply to a particular record, please contact the "data compliance manager" for guidance.

Personal data which are no longer to be retained will be permanently erased from our IT systems or securely and effectively destroyed, e.g. by cross-shredding of hard copy documents, burning them or placing them in confidential waste bins or by physical destruction of storage media, and the Organisation will also require third parties to destroy or erase such personal data where applicable. Employees must take all reasonable steps to destroy or erase personal data that the Organisation no longer requires.

In some circumstances the Organisation may anonymise personal data so that a "data subject's" identification is no longer permitted. In this case, the Organisation may retain such personal data for a longer period.

6. Integrity and confidentiality

Personal data must be 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.

The Organisation takes the security of personal data seriously and has implemented and maintained security safeguards which are appropriate to the size and scope of the business, the amount of data held and identified risks.

Where appropriate, the Organisation will use encryption and pseudonymisation of personal data. Steps have also been taken to ensure ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner.

Policy and procedure

Integrity and confidentiality

In turn, employees are responsible for protecting the personal data that the Organisation holds, and they must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage. Employees must be particularly careful in protecting special categories of personal data and criminal records personal data. They must follow all procedures, and comply with all technologies and safeguards, that the Organisation puts in place to maintain the security of personal data from the point of collection to the point of destruction.

Where the Organisation uses third-party service providers to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those third parties to safeguard the security of personal data. Employees can only share personal data with third-party service providers if you have been authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services
- sharing the personal data complies with the privacy notice that has been provided to the "data subject" (and, if required, the "data subject's" consent has been obtained)
- the third party has agreed to comply with our data security procedures and has put adequate measures in place in ensure the security of processing
- the third party only acts on our documented written instructions
- a written contract is in place between the Organisation and the third party that contains specific approved terms
- the third party will assist the Organisation in allowing "data subjects" to exercise their rights in relation to data protection and in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments
- the third party will delete or return all personal data to the Organisation at the end of the contract
- the third party will submit to audits

Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, approval of its terms must be sort from the "data compliance manager".

Personal data may only be shared with other employees if they have a business need to know in order to properly perform their job duties and responsibilities.

Hard copy personnel files, which hold personal data gathered during the working relationship, are confidential and must be stored in locked filing cabinets. Only authorised employees, who have a business need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised employees. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised employees have access to the data.

The Organisation has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

The legislation require the Organisation to notify any personal data breach to the Information Commissioner's Office within 72 hours after becoming aware of the breach and, where there is a high risk to the rights and freedoms of the "data subjects", to the "data subjects" themselves. Formally, a personal data breach, is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises the confidentiality, integrity or availability of personal data or the safeguards that the Organisation, or our third-party service providers, have put in place to protect them. The Organisation has procedures in place to deal with any suspected personal data breach and you are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact the "data compliance manager", retain any evidence you have in relation to the breach and follow the Organisation's data breach policy and response plan.

Policy and procedure

Accountability

The Organisation is responsible for, and must be able to demonstrate compliance with, the six data protection principles above. This means that appropriate and effective technical and organisational measures must be implemented to ensure compliance. Employees are required to fully assist and co-operate with the Organisation in this regard. In particular, the Organisation has:

- appointed a "data compliance manager" to be responsible for data protection compliance and privacy matters within the business
- kept written records of personal data processing activities implemented a privacy by design approach when processing personal data and will conduct and complete data protection impact assessments (DPIAs) where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system, in particular using a new technology, is likely to result in a high risk to the rights and freedoms of "data subjects" integrated data protection requirements into our internal documents, including this data protection policy and procedure, other related policies and privacy notices
- introduced a regular training programme for all employees on the data protection legislation and on their data protection duties and responsibilities and the Organisation also maintains a training record to monitor its delivery and completion – employees must undergo all mandatory data protection training
- introduced regular reviews of our privacy measures and our policies, procedures and contracts and regular testing of our systems and processes to monitor and assess our ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

The Organisation also keeps records of its personal data processing activities and its employees are required to assist it in ensuring these records are full, accurate and kept up to date. The Organisation is required to implement privacy by design measures when processing personal data. To this end, as the processes and systems, tend to be are under the control of individual employee's, each employee shall carry out a review to determine what privacy by design measures can be implemented within their area of control.

Where a type of data processing, e.g. the launch of a new product or the adoption of a new program, process or IT system which is under your control, is likely to result in a high risk to the rights and freedoms of "data subjects", employees must assist us in conducting and completing a Data Processing Impact Assessment (DPIA). This includes (but is not limited to):

- systematic and extensive automated processing and automated decision-making activities, including profiling, and on which decisions are based that have legal effects, or similar significant effects, on "data subjects"
- large-scale processing of special categories of personal data or criminal records personal data
- large-scale systematic monitoring of publicly accessible areas, e.g. using CCTV

Before any form of new technology, program, process or system is introduced, employees must contact the "data compliance manager" in order that a DPIA can be carried out.

A DPIA will comprise a review of the new technology, program, process or system. It must contain the following:

- a description of the processing operations and the purposes,
- an assessment of the necessity and proportionality of the processing in relation to those purposes,
- an assessment of the risks to individuals and the measures in place to address or mitigate those risks and demonstrate compliance

Automated processing is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, and automated decision-making occurs when an electronic system uses an individual's personal data to make a decision without human intervention.

Where you are involved in any data processing activity that involves automated decision-making or profiling, you must comply with the Organisation's guidelines.

Direct Marketing

The Organisation is subject to certain rules when marketing our clients and customers. If you are involved in direct marketing to customers, you must comply with the Organisation's guidelines on this. In particular, a "data subject's" prior consent is required for electronic direct marketing. There is a limited exception for existing clients and customers which allows the Organisation to send marketing texts and e-mails if we have obtained their contact details in the course of a sale to that person, we are marketing similar products or services to them and we gave that person an opportunity to "opt in" to our marketing when first collecting their details and the option to "opt out" in every subsequent message.

If a "data subject" objects to direct marketing, it is essential that this is actioned in a timely manner and their details should be suppressed as soon as possible. You can retain just enough information to ensure that marketing preferences are respected in the future.

Transferring personal data outside of the European Economic Area (EEA)

The data protection legislation restricts transfers of personal data to countries outside the EEA in order to ensure that the level of data protection afforded to "data subjects" is maintained.

The Organisation may transfer personal data to countries outside the EEA, provided one of the following applies:

- there is an adequacy decision by the European Commission in respect of the particular country, i.e. that country is deemed to provide an adequate level of protection for personal data
- appropriate safeguards are in place, such as binding corporate rules or standard data protection clauses approved by the European Commission
- the "data subject" has provided their explicit consent to the proposed transfer after being informed of any potential risk.

"Data subject" and rights to access personal data

Under the data protection legislation, "data subjects" have the right, on request, to obtain a copy of the personal data that the Organisation holds about them by making a written Data Subject Access Request (DSAR). This allows the "data subject" to check what personal data the Organisation is lawfully processing.

The "data subject" has the right to obtain:

- confirmation as to whether or not their personal data are being processed
- access to copies of their specified personal data
- other additional information

The other additional information (which should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language) comprises:

- the purposes of the processing and the categories of personal data concerned
- the recipients, or categories of recipients, to whom the personal data have been or will be disclosed, in particular recipients in non-EEA countries
- where the personal data are transferred to a non-EEA country, what appropriate safeguards are in place relating to the transfer
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the "data subject's" rights to request rectification or erasure of their personal data or restriction of processing of their personal data or to object to such processing
- their right to lodge a complaint with the Information Commissioner's Office if they think the Organisation has failed to comply with their data protection rights
- where the personal data are not collected from them, any available information as to their source
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the envisaged consequences of such processing for them

Policy and procedure

"Data subject" and rights to access personal data

When a "data subject" makes a DSAR, the Organisation will log the date on which the request was received and confirm their identity. Where there are reasonable doubts concerning the "data subject's" identity, before complying with their DSAR, the Organisation will request them to provide such additional information necessary to confirm their identity. The Organisation will then search databases, systems and other places where the personal data which are the subject of the DSAR may be held. Where we process a large quantity of personal data about a "data subject", we may ask them to first specify the information that their DSAR relates to.

If the "data subject" makes their DSAR electronically, the Organisation must provide a copy of the personal data in a commonly used electronic format, unless they specifically request otherwise. If the "data subject" wants additional copies of the personal data, the Organisation will charge a reasonable fee, which is based on our administrative costs of providing the additional copies.

The Organisation will normally respond to a DSAR and provide copies of the personal data within one month of the date of receipt of the request. However, this time limit for responding may be extended by a further two months if the request is complex or there are a number of requests made by the "data subject". If the Organisation intends to extend the time limit, the "data subject" will be contacted within one month of the DSAR's receipt to inform them of the extension and to explain why it is necessary.

Before providing the personal data to the "data subject" making the DSAR, the Organisation will review the personal data requested to see if it contains the personal data of other "data subjects". If they do, we may redact the personal data of those other "data subjects" prior to providing the "data subject" with their personal data, unless those other "data subjects" have consented to the disclosure of their personal data. We will also check whether there are any statutory exemptions from disclosure that apply to the personal data that are the subject of the DSAR. If a statutory exemption applies to any of the personal data, those personal data may not be disclosed.

Whilst the Organisation will normally provide a copy of the personal data in response to a DSAR free of charge, the Organisation reserves the right to charge a reasonable fee, based on our administrative costs of providing the personal data, when a DSAR is manifestly unfounded or excessive, particularly if it repeats a DSAR to which we have already responded. Alternatively, where a DSAR is manifestly unfounded or excessive, we reserve the right to refuse to respond altogether. Where we refuse to act on a request in this way, we will set out our written reasons why to the "data subject" within one month of receipt of their DSAR. We will also inform them of their right to complain to the Information Commissioner's Office or to seek a judicial remedy in the courts.

If an employee wishes to exercise their "data subject" access rights, they should complete the "data subject" access request form, or put the request in an e-mail, and send it to the "data compliance manager".

If an employee receives a DSAR from another "data subject", they must immediately forward it to the "data compliance manager" who will deal with responding to it.

Other "data subject" rights in relation to their personal data

"Data subjects" have a number of other rights in relation to their personal data. When we process "data subjects" personal data, we will respect those rights. It is the Organisation's policy to ensure that requests by "data subjects" to exercise their rights in respect of their personal data are handled in accordance with the data protection legislation.

Subject to certain conditions, and in certain circumstances, "data subjects" have the right to:

- be informed – this is normally satisfied by issuing them with an appropriate privacy notice
- request rectification of their personal data - this enables them to have any inaccurate or incomplete personal data we hold about them corrected or completed, including by their providing a supplementary statement
- request the erasure of their personal data - this enables them to ask us to delete or remove their personal data where there's no compelling reason for their continued processing, e.g. it's no longer necessary in relation to the purpose for which they were originally collected or if there are no overriding legitimate grounds for the processing
- restrict the processing of their personal data - this enables them to ask us to suspend the processing of their personal data, e.g. if they contest the accuracy and so want us to verify the accuracy or the processing is unlawful but they do not

Policy and procedure

Other "data subject" rights in relation to their personal data

want the personal data to be erased

- object to the processing of their personal data - this enables them to ask us to stop processing their personal data where we are relying on the legitimate interests of the business as our lawful basis for processing and there is something relating to their particular situation which makes them decide to object to processing on this ground
- data portability - this gives them the right to request the transfer of their personal data to another party so that they can reuse them across different services for their own purposes
- not be subject to automated decision-making, including profiling - this gives them the right not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them
- prevent direct marketing - this enables them to prevent our use of their personal data for direct marketing purposes
- be notified of a data breach which is likely to result in a high risk to their rights and freedoms

If, as a "data subject", you wish to exercise any of these rights, please contact the "data compliance manager".

If a "data subject" invokes any of these rights, you must take steps to verify their identity, log the date on which the request was received and seek advice from the "data compliance manager" if you need assistance in dealing with the matter. The following response procedures apply as applicable:

- response to requests to rectify personal data - unless there is an applicable exemption, we will rectify the personal data without undue delay and we will also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed, e.g. our third-party service providers, unless this is impossible or involves disproportionate effort
- response to requests for the erasure of personal data - we will erase the personal data without undue delay provided one of the grounds set out in the data protection legislation applies and there is no applicable exemption (and, where the personal data are to be erased, a similar timetable and procedure to that applying to responding to DSARs will be followed). We will also communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. Where we have made the personal data public, we will take reasonable steps to inform those who are processing the personal data that the "data subject" has requested the erasure by them of any links to, or copies or replications of, those personal data
- response to requests to restrict the processing of personal data - where processing has been restricted in accordance with the grounds set out in the data protection legislation, we will only process the personal data (excluding storing them) with the "data subject's" consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. Prior to lifting the restriction, we will inform the "data subject" that it is to be lifted. We will also communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort
- response to objections to the processing of personal data - where such an objection is made in accordance with the data protection legislation and there is no applicable exemption, we will no longer process the "data subject's" personal data unless we can show compelling legitimate grounds for the processing which overrides the "data subject's" interests, rights and freedoms or we are processing the personal data for the establishment, exercise or defence of legal claims. If a "data subject" objects to the processing of their personal data for direct marketing purposes, we will stop processing the personal data for such purposes
- response to requests for data portability - unless there is an applicable exemption, we will provide the personal data without undue delay if the lawful basis for the processing of the personal data is consent or pursuant to a contract and our processing of those data is carried out by automated means (and a similar timetable and procedure to that applying to responding to DSARs will be followed)

In the limited circumstances where the "data subject" has provided their consent to the processing of their personal data for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on consent before its withdrawal.

Policy and procedure

Other "data subject" rights in relation to their personal data

If, as a "data subject", an employee wishes to withdraw their consent to the processing of their personal data for a specific purpose, they should contact the "data compliance manager". Once the notification that consent has been withdrawn has been received, the Organisation will no longer process their personal data for the purpose they originally agreed to, unless the Organisation has another lawful basis for processing.

If a "data subject" invokes their right to withdraw their consent, seek advice from the "data compliance manager" if assistance is required in dealing with the matter.

"Data subjects" also have the right to make a complaint to the Information Commissioner's Office at any time.

Employee obligations in dealing with personal data

Employees must comply with the policy, associated procedures and the data protection principles at all times in their personal data processing activities where they are acting on behalf of the Organisation in the proper performance of their job duties and responsibilities. The Organisation relies on its employees to help it meet its data protection obligations to "data subjects".

Under the data protection legislation, employees should also be aware that they are personally accountable for their actions and can be held criminally liable. It is a criminal offence for employees to knowingly or recklessly obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of the Organisation. This includes, for example, taking clients' or customers' contact details or other personal data without the Organisation's consent on the termination of employment, accessing another employee's personal data without authority or otherwise misusing or stealing personal data held by the Organisation. It is also a criminal offence to knowingly or recklessly re-identify personal data that has been anonymised without the consent of the Organisation, where the Organisation has de-identified the personal data, and it is a criminal offence to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a "data subject" following a "data subject" access request. Where unlawful activity is suspected, the Organisation will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the data protection legislation and this may result in criminal proceedings being instigated against a specific employee. The Organisation may also need to report the alleged breach to a regulatory body. This conduct would also amount to a gross misconduct offence under the Organisation's disciplinary procedure and could lead to summary dismissal.

Employees must also comply with the following guidelines at all times:

- only access personal data that they have authority to access and only for authorised purposes, e.g. if they need them for the work they do for the Organisation, and then only use the data for the specified lawful purpose for which they were obtained
- only allow other employees to access personal data if they have the appropriate authorisation and never share personal data informally
- do not disclose personal data to anyone except the "data subject". In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Organisation's website or posted on the Internet in any form unless the "data subject" has given their explicit consent to this
- be aware that those seeking personal data sometimes use deception to gain access to them, employees should always verify the identity of the "data subject" and the legitimacy of the request
- where the Organisation provides code words or passwords to be used before releasing personal data, employees must strictly follow the Organisation's requirements in this regard
- only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail
- if an employee receives a request for personal data about another employee or "data subject", they should forward this to the "data compliance manager"
- ensure any personal data held is kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with the Organisation's rules on computer access and secure file storage

Policy and procedure

Employee obligations in dealing with personal data

- do not access another employee's personal data, e.g. their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence
- do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without the Organisation's consent as this will be treated as gross misconduct and it is a criminal offence
- do not write down (in electronic or hard copy form) opinions or facts concerning a "data subject" which it would be inappropriate to share with that "data subject"
- do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable the task to be properly carried out within their duties and responsibilities, the employee shall have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by line management
- ensure that, when working on personal data as part of job duties and responsibilities when away from the workplace and with the authorisation of line management, employees shall continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- do not store personal data on local computer drives, their own personal computer or on other personal devices
- do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by cross-shredding hard copies
- ensure that they attend all mandatory data protection training
- refer any questions about data protection legislation or compliance with this policy to the "data compliance manager"
- compliance with the data protection legislation and the terms of this policy is each employee's personal responsibility.