**GDPR Workshop**

**Subject Rights**

The GDPR provides the following rights for individuals:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object
* Rights in relation to automated decision making and profiling.

Information about all rights are included below, but I suspect that for the vast majority of us, the rights to be informed, access, rectification and erasure will be the most common.

**Right to be Informed**

You need to let people know the following, probably by giving a summary and referencing your privacy policy. You should include the following:

* Identity and contact details of the controller
* Purpose of the processing and the lawful basis for the processing
* The legitimate interests of the controller or third party, where applicable
* Who else might receive the personal data, and what they will do with it
* Retention period or criteria used to determine the retention period
* The existence of each of data subject’s rights
* The right to withdraw consent at any time, where relevant
* The right to lodge a complaint with a supervisory authority
* The source the personal data originates from and whether it came from publicly accessible sources
* Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
* The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Not all will apply to all communications.

**The right of access**

Under the GDPR, individuals will have the right to obtain confirmation that you are holding and processing their data, and to be given access to that data.

You must provide a copy of the information free of charge, in the format it was requested (electronic or paper), usually within one month. You must verify their identity first. You can only charge a reasonable fee for repetitive or unfounded requests.

You can refuse to respond to a request, but must explain why to the individual, informing them of their right to complain.

**The right to rectification**

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

This includes others who have received information from you - unless this proves impossible or involves disproportionate effort.

You can refuse to respond to a request, but must explain why to the individual, informing them of their right to complain.

**The right to erasure**

Also known as “the right to be forgotten” enabling an individual to request deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure applies when:

* Personal data is no longer necessary in relation to the purpose for which it was originally collected
* Consent is withdrawn
* When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
* The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
* The personal data has to be erased in order to comply with a legal obligation.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

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

This includes others who have received information from you - unless this proves impossible or involves disproportionate effort.

**The right to restrict processing**

Individuals have a right to block processing of personal data, whilst you can still store the personal data.

You can retain just enough information about the individual to ensure that the restriction is respected in future.

The right applies when:

* Where the individual contests the accuracy of the data, you should then restrict the processing until you have verified the accuracy of the personal data.
* An individual has objected to the processing and while you are considering whether your organisation’s legitimate grounds override those of the individual.

This includes others who have received information from you - unless this proves impossible or involves disproportionate effort.

You must inform individuals if you decide to lift a restriction on processing.

**The right to data portability**

This allows individuals to obtain and reuse their personal data for their own purposes, ie moving, copying or transferring personal data easily from one IT environment to another in a safe and secure way.

It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to data portability only applies:

* To personal data an individual has provided to a controller
* Where the processing is based on the individual’s consent or for the performance of a contract
* When processing is carried out by automated means

You must provide the personal data in a structured, commonly used and machine-readable form (eg CSV files).

The information must be provided free of charge, and you may be required to transmit the data directly to another organisation if this is technically feasible.

You must respond without undue delay, and within one month, etc.

**The right to object**

Individuals have the right to object to processing based on other lawful interests, marketing and research.

You can continue processing if you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, if the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object along with their other rights.

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

Rights in relation to automated decision making and profiling.

**Rights in relation to automated decision making and profiling**

This section is complicated and relates to automatic processing of data (no human decision making). Refer to the ICO for more detail.

**Suggested Activities**

* Discuss how you would deal with a subject access request, leading to a request for erasure.
	+ Can you identify all the date you hold?
	+ Would you have to comply with the erasure request?