GDPR Guidance and Interpretation
from Customer Commons and Kantara CISWG

Assumption – We are building a website/wiki that can stand on its own within CustomerCommons.org (and a Kantara site should Kantara agree) as guidance to individuals, and also act as a reference that others can build on. Our objective is to maximize the positive impact of GDPR for individuals.

References
http://www.eugdpr.org/ (the official site)
http://www.gdprwiki.com/

INTRO
The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

Enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key things you as an individual need to know about the GDPR are below.

Scope
Definitions

An Individuals Rights/ Your Rights Under GDPR

1) The right to be informed

What this means (guidance for organizations):
The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasizes the need for transparency over how you use personal data.

What this means (guidance for individuals):
You have the ability to ask the data controller, who is obligated to provide 'fair processing information' to them, typically through a simple to understand privacy notice. Being clear over how your personal data is used.

Examples: (individuals)
A person goes to a website and doesn't completely understand the privacy notice, they contact the person responsible for understanding what will happen to their data. This person then explains in simpler terms what will happen to the data, why it is being collected. etc...

2) The right to access

What this means (guidance for organizations)
Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

What this means (guidance for individuals):
Individuals have the right to obtain: what personal data is being used, who is allowed access to such data and other related information in the privacy notice.

These are similar to existing subject access rights under the DPA Data Protection Act.

Examples: (individuals)
A person has shared data and has forgotten why.

3) The right to rectification

What this means (guidance for organizations):
Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
What this means (guidance for individuals):
If personal data is not correct or complete, individuals have the ability to have it corrected.

Examples: (individuals)
You go to a website whose main purpose is collecting public data about you and notice some of the information is not correct, by contacting the company and alerting them they must correct the data in a timely fashion.

4) The right of Erasure

What this means (guidance for organizations):
The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

What this means (guidance for individuals):
Individuals are empowered to request personal data to be deleted and removed, it is also known as 'the right to be forgotten'. Principally underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing, when not bound by a legal restriction.

Examples: (individuals)
You’ve been sharing data with a known entity deciding you wish to no longer be associated with this entity in any way whatsoever. You contact them and request they remove all and any personal data regarding your relationship with them. They, in turn, delete this information as long as they are not legally bound by some other jurisdiction and or law.

5) The right to restrict processing

What this means (guidance for organizations):
Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

What this means (guidance for individuals):
Individuals can stop the processing of personal data. The restriction of processing under the GDPR is similar.

Either the data controller or processor are permitted to store the personal data, but no longer use it. They may retain just enough information about the individual to ensure no further use is respected in future.

6) The right to portability

What this means (guidance for organizations):
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

What this means (guidance for individuals):
Individuals are permitted to download a copy of their personal data and easily use it in another way, without hindrance to usability.

7) The right to object

What this means (guidance for organizations):
Individuals have the right to object to:
- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

What this means (指导 for individuals):
Individuals can stop the use of their personal data via a request.

8) Rights related to automated decision making and profiling

What this means (guidance for organizations):
The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.
Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

**What this means (guidance for individuals):**

Individuals are protected by safeguards against the risk of potentially damaging outcomes were taken without any human intervention in the process. The processing of personal information through automated decision should cause no harm.

**Examples**

Other Relevant Aspects of GDPR

Breach Notification

Forward Looking Scenarios