Clarkslegal

Privacy matters: How the 8 data subject rights protect personal data

Data Protection

Privacy matters: How the 8 data subject rights protect personal data

In today's digital era, protecting personal data has become a top priority. With cyber threats on the rise and frequent data breaches making headlines, it is essential to understand how compliance with data subject rights protects personal data.

In this publication, we will delve into the significance of the 8 data subject rights in safeguarding personal information. From the right to be informed about how personal data is being used to the right to rectify inaccuracies, these rights empower individuals to have control over their personal data.

The UK General Data Protection Regulation (UK GDPR) has set the framework for these rights, ensuring that individuals have a say in how their data is collected, stored, and processed.

Join us as we explore the 8 data subject rights under the UK GDPR and discover how they play a vital role in preserving your organisation’s privacy standards in an increasingly interconnected world.

01. RIGHT TO BE INFORMED (ARTICLES 13 & 14)

It is a transparency requirement that individuals are to be informed about their personal data being collected and used by an organisation. This is known as providing the individuals with 'privacy information', commonly provided in a privacy notice, where it includes the organisation informing the individuals about its purposes for processing their personal data, its retention policy i.e. how long it will be retaining that personal data, and who this personal data will be shared with.

The Information Commissioner's Office (ICO) states that individuals must be provided with this information at the time their personal data is collected from them. If the personal data is collected from a different source, then such privacy information must be provided to the individuals the personal data relates to, within a reasonable time of obtaining the data and, in any case, no later than one month. The ICO also establishes that if the personal data is to be disclosed to a third party, then privacy information must be provided to the individuals, at the latest, when the data is disclosed to that third party.

It is important to note that such privacy information must be provided in a concise and intelligible manner; clear and plain language should be used so as to enable the reader to understand the information.

02. THE RIGHT OF ACCESS (ARTICLE 15)

Individuals' right to access and receive their personal data can be accomplished by submitting what is commonly known as a data subject access request ('DSAR') to an organisation. Once the organisation receives a DSAR, it must perform a reasonable search of its documents and provide the individual submitting the DSAR with copies of their personal data found by the search.

Such requests can be made verbally or in writing, and must be responded to without delay. For more information on the legal and practical considerations for those facing or making DSARs, watch our on-demand webinar on 'Overview of Data Subject Access Requests' here.

03. THE RIGHT TO RECTIFICATION (ARTICLE 16)

According to the Data Protection Act 2018, personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

Individuals have a right to ask that their personal data held by an organisation be rectified if it is inaccurate, or added to if it is incomplete. Organisations can implement this by placing the rectification on record to supplement the current record. Even if an organisation is satisfied that the personal data it holds on the individual making the request is in fact accurate, there is an obligation to take reasonable steps to reconsider this view, in light of the request.

Organisations may face difficulties where the personal data they are being asked to rectify, consists of opinion data which an individual alleges is inaccurate. Opinions are of course, subjective, and so the safest course of action would be to make it clear that this is opinion data.

There are exemptions which allow organisations to refuse to comply with a request for rectification, and these are that the request is manifestly unfounded, or the request is excessive.

04. THE RIGHT TO ERASURE (ARTICLE 17)

This is also known as the right to be forgotten. Many people are understandably cautious about their personal data being stored in an organisation's files and prefer that, whatever personal data is held on them, is not continuously stored.

Organisations already have an obligation to only collect personal data for specified purposes and must dispose of that data once those purposes are no longer fulfilled. Individuals therefore have a right to have their personal data erased once it is no longer necessary for that data to be retained by an organisation.

When an organisation relies on an individual's consent for holding their personal data, if that individual withdraws their consent, the organisation must erase this personal data.

This right is emphasised when the individual in question is a child, as there is an enhanced protection of children's personal data under the UK GDPR.

There are exceptions to the right to erasure, such as that the personal data is being processed to comply with a legal obligation or for public interest purposes.

05. THE RIGHT TO RESTRICT PROCESSING (ARTICLE 18)

Individuals have a right to restrict the processing of their personal data in some circumstances, such as where the data has been unlawfully processed and the individual does not want the personal data to be erased in accordance with the right under Article 17 above.

Individuals usually make such requests when they are disputing the accuracy of the personal data and the organisation needs time to investigate this.

There are different methods that could be used to restrict processing personal data, to comply with such a request:

- The organisation can temporarily remove published personal data from its website
- The organisation can make the personal data unavailable to certain individuals or groups

In such instances, the personal data can still be stored by the organisation, but all processing of it shall cease, for the time being.

06. THE RIGHT TO DATA PORTABILITY (ARTICLE 20)

This includes the right to receive a copy of one's personal data from the data controller in a commonly used format, to store it for personal use on a personal device, or to have the personal data transferred from one data controller to another. This is different to the right to access one's data under Article 15.

07. THE RIGHT TO OBJECT TO PROCESSING (ARTICLE 21)

Individuals can object to the processing of their personal data at any time, depending on the organisation's purposes for processing and its lawful basis for doing so.

Here are some of the circumstances in which individuals can object to processing:

- When the personal data is processed for direct marketing. There is an absolute right to object to this and no exemptions are available to an organisation to refuse
- Where the personal data is being processed for the organisation's legitimate interests, or for a public task. An organisation may refuse to comply if it has compelling legitimate grounds which override the individual's interests, which is why the individual must state their reasons for making such a request.

08. RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING (ARTICLE 22)

Automated decision making refers to decisions made automatically, without human involvement, for example in online aptitude tests. Although automated decision making can be a quick way to reach decisions and a very useful method of finding out traits of individuals, there are risks that this could impact people's legal rights.

The UK GDPR therefore places limitations on the use of automated decision making with legal or other significant effects, by allowing organisations to carry this out only if it is necessary for entering into a contract with the individual, or performing that contract; if it is authorised by law; or if the individual explicitly consented to it.

There is a more stringent limit for special category data, as this can only be processed under Article 22 if the individual explicitly consented or it is necessary for the public interest.

LEGAL SUPPORT

If your organisation is facing one of the requests described in this guide and requires advice on the nature of these requests, you can get in touch with our Data Protection team here.

Ashan Arif
PARTNER

View profile

ashan.arif@clarkslegal.com

0118 958 5321

Clarkslegal

For more information on how we can help your business: clarkslegal.com
email: contact@clarkslegal.com · Reading: 0118 958 5321 · London: 020 7539 8000