BEALE&CO

CONSTRUCTION, ENGINEERING AND INFRASTRUCTURE

Document Retention under the GDPR and the Data Protection Act 2018

Author:
James Hutchinson

Date:
December 2018

The Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018. It implements the General Data Protection Regulation (GDPR) as well as, supplementing and bolstering it.

Under the fifth data protection principle of the GDPR, personal data cannot be kept for longer than you need it. However, there is no specific time limit. How long you retain data will depend on the purpose for holding the data.

Article 5(1)(e) of the GDPR states:

> "*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*".

This principle is similar to the position that was under the Data Protection Act 1998 – so what has changed?

Specific Exemptions

The GDPR and DPA 2018 specifically set out exemptions where data can be kept for longer than "necessary". These include keeping data for public interest archiving, scientific or historical research, or statistical purposes. If you are keeping data for any of these purposes, this must be your only purpose for holding data and you cannot later use the data for another purpose particularly, for making decisions that may affect an individual whose data you hold. Further, you cannot hold data "just in case" it might be useful in the future.

Also, under the legislation individuals rights must be protected if you decide to keep the data. If any of the exemptions apply, pseudonymisation may be appropriate in some cases to protect the data. Although, it should be noted that pseudonymisation is not a defence to Art 5 of the GDPR or under the DPA 2018 if data you hold does not fall under one of the specified exemptions. However, akin to the principle under the 1998 Act, if you anonymise the data, you can keep it for as long as you like.

New Policy Standards

You now need a policy setting standard document retention periods (where possible) in order to comply with the new GDPR documentation provisions. Such policies can help your organisation establish standard retention periods for different types of personal data. It is important to document and evidence these periods to comply with the GDPR provisions.

The Information Commissioner's Office (**ICO**) makes the following recommendations about setting retention periods:

- You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies.
- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.
- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there

is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise (consider the standard limitation periods e.g. contract, tort, personal injury).

- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If you keep personal data to comply with a requirement like this, you will not be considered to have kept the information for longer than necessary.

- You should consider any relevant industry standards or guidelines. For example, the ICO has agreed that credit reference agencies are permitted to keep consumer credit data for six years. Industry guidelines are a good starting point for standard retention periods and are likely to take a considered approach. However, they do not guarantee compliance. You must still be able to explain why those periods are justified, and keep them under review.

In Practice

Organisations must keep a system in place to enforce their document retention policies, and regularly review the retention of documents at appropriate periods, in order to allow for early deletion if it is no longer necessary to retain the data. There is no specific rule about how long a predetermined period to review should be. Factors that should be considered in determining this include the level of resources an organisation may have and the privacy risk to individuals. However, reviewing retention regularly before a lengthy predetermined period or where there is high risk of impact on individuals is good practice.
For large organisations it may be useful to have automated systems in place that can delete information after a predetermined period, or at least flag records that need to be reviewed.

As the GDPR does not specify how long personal data is to be kept, it is up to the data processor to be able to reasonably justify how long data is retained for based on the purpose for retention. It is also important to be able to justify why the data needs to be held in a particular form that may allow individuals to be identified. If it is not necessary to identify individuals, the data should be anonymised. However, once it has been anonymised, attempts should not be made to re-identify personal data. Section 167 of the DPA 2018 creates a new offence of re-identifying personal data that has been de-identified.

Right to be Forgotten

Individuals have an absolute right to erasure. Therefore, if an individual asks you to delete or review whether you still need their data, you must review whether there is a clear and justified need to keep it for your specific purpose. If you can justify holding the data, you must be prepared to respond to any subject access requests and compliance with any other rights the individual may have such as, security and confidentiality of data. Section 169 of the DPA 2018 creates an offence for altering, defacing, blocking, erasing, destroying or concealing information with the intention of preventing disclosure.

Data Sharing

In many industries, such as the construction industry, it is commonplace to share data relating to individuals when working on the same projects or where there may be a potential merger between two or more entities. In such a situation, it is important to update any contracts and incorporate appropriate provisions in an agreement that determine what happens if you no longer need to share data. The most appropriate way to deal with this is to have provisions that require you to either return the documents to the organisation that supplied them without keeping any copies, or deleting the data.

Article 28 of the GDPR requires certain provisions to be included in contracts that involve processing of personal data. Many construction contracts such as the NEC4 provide guidance on incorporating standard clauses in to the contract in order to comply with the GDPR regulations. However, it may not always be advisory to follow this, as “one size does not fit all”.

Further, if you have been provided with personal data of individuals by another stakeholder involved in a project, you must still ensure compliance with the GDPR principles.

Document Retention under the GDPR and the Data Protection Act 2018

Comment

As mentioned above, the GDPR provisions relating to document retention have similarities to the 1998 Act. However, it places a higher evidential burden to be able to justify retention. Therefore, it is important for organisations to be able to comply with this and assess the risk of retention.

A starting point is to check any industry guidelines for retention periods of holding documents. However, it should be noted that this does not guarantee compliance with the GDPR. A proportionate approach needs to be taken in every case where you balance your needs with the individual's right to privacy, and take a fair and justified approach.

For further information please contact:

James Hutchinson
Partner
+44 (0) 20 7469 0408
j.hutchinson@beale-law.com

If data is not being used, organisations should consider anonymising or deleting it in order to avoid falling foul of the GDPR provisions where non-compliance carries far higher fines than under the 1998 Act. Personal data held for too long is highly likely to be in breach of the regulations. The DPA 2018 also sets out criminal offences for some data protection breaches.

Once the UK leaves the EU, the position should remain similar. The European Union (Withdrawal) Act 2018 will incorporate the GDPR into UK law and the DPA 2018 will continue to supplement the GDPR provisions.

.