



# Data Protection Bill

## Introduction

Following the publication of its [Statement of Intent](#) on Data Protection in August 2017, the government has now laid the [Data Protection Bill](#) in the House of Lords.

As expected, the Bill's content reflects what the government set out in its previous Statement of Intent and confirms that the Bill will be used to bring the EU's General Data Protection Regulation (GDPR) into UK Statute, strengthen the rights of individuals with regard to their personal data and enhance the role of the data regulator, the Information Commissioners Office (ICO), in supervision and enforcement. This Bill will also replace the UK's existing 1998 Data Protection Act (Act).

### Three core objectives of the Bill

- Maintaining trust – ensuring the UK has robust storage and security of data.
- Future trade - ensuring the UK has the ability to participate in the international transfer and processing of data.
- Security - ensuring the UK has the ability to collect, share and process personal data that is crucial for law enforcement.

## Bill contents

While the government has committed to implement the tenets of GDPR in order to shore up the UK's ability to operate with cross-border data post-Brexit, the Bill also retains elements of the previous Act in order to provide organisations who process data with adequate exemptions. Where appropriate, provisions from the existing Act have been rolled over into the Bill to create these exemptions.

In this regard and with particular relevance to financial services, the Bill will allow for the processing of data, without individual consent, for financial services firms pricing risk, making decisions on an individual's creditworthiness or in their efforts to detect fraud and money-laundering. With regard to issues for insurers specifically, the Bill also provides exemptions for automated profiling.

## Key components of the Bill

- **Protecting individuals** - The Bill will seek to apply greater protection to individuals and strengthen personal rights over data.
  - **Consent** to use an individual's data must be 'explicit' and companies collecting data will no longer be able to automatically 'opt-in' customers to their data policy.
  - **Improved data access** will allow individuals to more easily understand what data companies hold on them.
  - **Enhanced data portability** will make it easier for customers to move data between services providers.
  - The **right to be forgotten** will empower individuals to ask for their personal data to be erased.
  - Individuals will also have a greater say in how their data is used in their automated **profiling** when using a service.
- **Protecting organisations** - The Bill puts in place strengthened data requirements on organisations, amending rules as necessary to make the UK's regime relevant for the modern digital economy and in line with adequate individual protections.
  - **Enhanced accountability** will make companies that collect and process data more accountable to regulators, in this case the ICO. As part of this, a business must notify the ICO of any data breach within 72 hours of it happening.
  - **Reducing the risk of a business's exposure to data breaches** by requiring high risk data processors to carry out regular impact assessments to prevent inappropriate usage of an individual's data.



# Data Protection Bill

- Putting in place **simpler rules** to bring forward a clearer regime which is more easily understood by data controllers and processors.
- **Strengthening the regulator** - The Bill will seek to ensure that criminal justice agencies have a data regime that allows them to continue to tackle the changing nature of crime but without compromising the rights and safeguards intended by the Bill itself.
  - **Enhanced investigative powers** for the ICO.
  - **Increased sanctions** which will increase the maximum fine the regulator can issue to £1.7 million or 4% of a company's global turnover.
  - **Enhanced criminal sanctions** which will see a new offence for intentionally or recklessly using data to identify an individual.
  - **Protection for whistle-blowers** will be ensured through relevant exemptions to the Bill.
  - The mandatory appointment of a **Data Protection Officer** in companies that handle and process data.

## Implementing the Bill and UK specific requirements

The new Bill is underpinned by three international regimes, which form the core of the law in this area:

- The General Data Protection Regulation
- The Data Protection Law Enforcement Directive
- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

## Relationship with Brexit Position Paper

The Bill is also in line with the narrative and ambition the government set out in its [Brexit Position Paper](#) on data sharing, in which it intends for the UK to maintain a post-Brexit relationship with the EU similar to the status-quo. This future relationship will be reliant on the UK's own data regime being deemed adequate with the EU's. The UK government expects to achieve such adequacy by implementing the tenets of GDPR through the UK's Data Protection Bill.

## Next steps

Having been introduced into the Lords at first reading on 14 September 2017, the Bill will now progress to second reading on 10 October 2017, where Peers will have the opportunity to debate the principles of the Bill and give an indication of amendments or revisions they wish to make. Following this, the Bill will then move to committee stage where it will receive thorough line-by-line scrutiny from Peers.

## Contact

For further information on this subject, please contact:



**Deborah Newberry**

Head of Public Affairs

t + 44 20 7667 9508

[deborah.newberry@kennedyslaw.com](mailto:deborah.newberry@kennedyslaw.com)

For further details and for full team profiles please see our website:

**[kennedyslaw.com](http://kennedyslaw.com)**