Department for Digital, Culture Media & Sport

Data Protection Bill

Factsheet – Overview

What are we going to do?

- Make our data protection laws fit for the digital age in which an ever increasing amount of data is being processed.
- Empower people to take control of their data.
- Support UK businesses and organisations through the change.
- Ensure that the UK is prepared for the future after we have left the EU.

Culture Secretary, Karen Bradley said:

"The Data Protection Bill will give people more control over their data, support businesses in their use of data, and prepare Britain for Brexit.

“In the digital world strong cyber security and data protection go hand in hand. This Bill is a key component of our work to secure personal information online.”

How are we going to do it?

- Replace the Data Protection Act 1998 with a new law that provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice.
- Set new standards for protecting general data, in accordance with the GDPR, give people more control over use of their data, and provide new rights to move or delete personal data.
- Preserve existing tailored exemptions that have worked well in the Data Protection Act, carrying them over to the new law to ensure that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services.
- Provide a bespoke framework tailored to the needs of our criminal justice agencies and national security organisations, including the intelligence agencies, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of the global threats the UK faces.

Department for Digital, Culture Media & Sport

Background

The Data Protection Bill was announced in the Queen's Speech on 21 June 2017. It will implement the government's manifesto commitments to update data protection laws.

The Data Protection Act 1998 has served us well and placed the UK at the front of global data protection standards. With this Bill we are modernising the data protection laws in the UK to make them fit for purpose for our increasingly digital economy and society.

As part of this the Bill we will apply the EU's GDPR standards, preparing Britain for Brexit. By having strong data protection laws and appropriate safeguards, businesses will be able to operate across international borders. This ultimately underpins global trade and having unhindered data flows is essential to the UK in forging its own path as an ambitious trading partner. We will ensure that modern, innovative uses of data can continue while at the same time strengthening the control and protection individuals have over their data.

The main elements of the Bill are:-

General data processing

- Implement the GDPR standards across all general data processing.
- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained.
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Set the age from which parental consent is not needed to process data online at age 13.

Law enforcement processing

- Provide a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes.
- Allow the unhindered flow of data internationally whilst providing safeguards to protect personal data.

National Security processing

- Ensure that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and enforcement

- Enact additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.
- Empower the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

Factsheets covering these measures will be published alongside the Bill https://www.gov.uk/government/collections/data-protection-bill-2017

Key Questions and Answers

- **How does the Bill differ from GDPR?**
  The Bill is a complete data protection system, so as well as governing general data covered by GDPR, it covers all other general data, law enforcement data and national security data. Furthermore, the Bill exercises a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection.

- **What is the impact on business?**
  Organisations which already operate at the standard set by the Data Protection Act 1998 should be well placed to reach the new standards.

  The Bill will mean that UK organisations are best placed to continue to exchange information with the EU and international community, which is fundamental to many businesses.

  The Information Commissioner is already working to help businesses to comply with the new law from May 2018 and will be taking a fair and reasonable approach to enforcement after that date.

- **Does the Bill require organisations to improve cyber security?**
  Effective data protection relies on organisations adequately protecting their IT systems from malicious interference. In implementing the GDPR standards, the Bill will require organisations that handle personal data to evaluate the risks of processing such data and implement appropriate measures to mitigate those risks. For many organisations such measures will likely need to include effective cyber security controls.