Department for Digital, Culture Media & Sport

Data Protection Act 2018

Factsheet – Overview

What does the Act do?

- Makes our data protection laws fit for the digital age when an ever increasing amount of data is being processed.
- Empowers people to take control of their data.
- Supports UK businesses and organisations through this change.
- Ensures that the UK is prepared for the future after we have left the EU.

DCMS Secretary of State, Matt Hancock said:

"The Data Protection Act gives people more control over their data, supports businesses in their use of data, and prepares Britain for Brexit.

“In the digital world strong cyber security and data protection go hand in hand. The 2018 Act is a key component of our work to secure personal information online.”

How does the Act do it?

- Provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice.
- Sets new standards for protecting general data, in accordance with the GDPR, giving people more control over use of their data, and providing them with new rights to move or delete personal data.
- Preserves existing tailored exemptions that have worked well in the Data Protection Act 1998, ensuring that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services.
- Provides a bespoke framework tailored to the needs of our criminal justice agencies and the intelligence services, 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 Act 2018 achieved Royal Assent on 23 May 2018. It implements the government's manifesto commitment to update the UK's data protection laws.

The Data Protection Act 1998 served us well and placed the UK at the front of global data protection standards. The 2018 Act modernises data protection laws in the UK to make them fit-for-purpose for our increasingly digital economy and society.

As part of this the 2018 Act applies 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 have ensured 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 2018 Act are:

General data processing

- Implements GDPR standards across all general data processing.
- Provides clarity on the definitions used in the GDPR in the UK context.
- Ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained.
- Provides 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.
- Sets the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

Law enforcement processing

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

Intelligence services processing

- Ensures 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

- Enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allows 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.
- Empowers 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.

Additional factsheets covering these measures are available from https://www.gov.uk/government/collections/data-protection-act-2018

Department for Digital, Culture Media & Sport

Key Questions and Answers

- **How does the Act differ from the GDPR?**
  The Act is a complete data protection system, so as well as governing general data covered by the GDPR, it covers all other general data, law enforcement data and national security data. Furthermore, the Act 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 Act means 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 has been working to help businesses to comply with the new Act from 25th May 2018 and is taking a fair and reasonable approach to enforcement after that date.

- **Does the Act 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 Act requires 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 include effective cyber security controls.

Department for Digital, Culture, Media & Sport
23 May 2018