Department for Digital, Culture Media & Sport

Data Protection Bill

Factsheet – The Information Commissioner and Enforcement

(Clauses 112 - 168)

What are we going to do?.

- Retain the Information Commissioner as the UK's independent data protection regulator.
- Place a duty on data controllers to notify the Commissioner as well as individuals concerned of data breaches that risk affecting individuals' rights.
- Increase maximum penalties for regulatory breaches from £500K to £18m.
- Create new offences to deal with emerging threats.

Minister for Digital, Matt Hancock said:

"The Information Commissioner plays a critical role in our data protection system in enforcing data protection laws and informing the public.

"Our Data Protection Bill will ensure the Commissioner is given the right powers to ensure consumers are appropriately safeguarded. We continue to work with her office and consumer groups to educate people about how to protect themselves."

How are we going to do it?

- The Data Protection Act 1998 provides a statutory basis for the Information Commissioner and the source of her powers in respect of data protection regulation. The Bill makes provision to allow the Commissioner and her office to continue to operate under our new data protection laws.
- The Commissioner's functions and duties, including powers to make codes of practice and guidance are all preserved by the Bill to allow the Commissioner to support business to achieve compliance.

- The Bill requires data controllers for both general data and law enforcement purposes to notify the Commissioner within 72 hours of a data breach taking place, if the breach risks the rights and freedoms of an individual. In cases where there is a high risk, businesses must notify the individuals affected.

- The Bill provides for maximum fines up to £18m, consistent with the GDPR, and also requires the Commissioner to issue guidance about enforcement.

- The Bill modernises many of the offences currently contained within the Data Protection Act, as well as creating two new offences - the 're-identification of de-identified personal data' and the 'alteration etc of personal data to prevent disclosure' - to allow the Commissioner to deal with a wider range of offending behaviour.

Background

The Information Commissioner is an independent official whose role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner investigates complaints as well as conducting proactive investigations. As well as an enforcer, the Commissioner acts to inform and educate data controllers, and the wider public, to improve standards.

In 2010, the Commissioner was given the power to enforce monetary penalties, and their powers of enforcement have increased since.

The Bill modernises the offences contained within current legislation, as well as creating two new offences of the 're-identification of de-identified personal data' and the 'alteration etc of personal data to prevent disclosure'. The Bill and these offences give the ICO more holistic regulatory powers.

The Bill includes a number of provisions for the Commissioner, including:

- Giving the Commissioner and her staff powers to inspect personal data where international obligations make inspection necessary.
- Putting an obligation on the Commissioner to produce annual performance reports for the consideration of Parliament.
- Allowing the Commissioner to recoup fees from controllers, as set by the Secretary of State.

- Allowing the Commissioner to issue ‘information’, ‘assessment’, and ‘enforcement’ notices where necessary to ensure data controllers are processing personal data within the data protection framework.
- Provision of an appeals system to challenge the Commissioner’s decisions and monetary penalties imposed before an independent Tribunal.

Department for Digital, Culture Media & Sport

Key Questions and Answers

- **What impact will increased fines have on organisations?**
  The Bill provides the Information Commissioner with a wide range of corrective powers to build compliance. Fines would only ever be imposed as a last resort and will be applied in a fair and proportionate way.

- **Why does the bill contain so many criminal offences?**
  The very worst cases of data misuse can potentially cause serious distress to large numbers of people. The Data Protection Act 1998 contains several offences that we are transferring into the new Bill. But we are also creating new offences to tackle controllers who deliberately destroy personal data to frustrate subject access requests; and to deal with offenders who circumvent an organisation's encryption mechanisms to unlawfully obtain personal data.

- **How will those working to test security systems be protected from prosecution for the new re-identification offence?**
  If research and testing is carried out on behalf of the controller who de-identified the information, then no offence will be committed. The new offence also provides for defences if re-identification was necessary for the law enforcement purposes, to comply with a legal obligation or was otherwise justified in the public interest.

Department for Digital, Culture, Media & Sport
14 September 2017