Department for Digital, Culture Media & Sport

Data Protection Act 2018

Factsheet – The Information Commissioner and Enforcement

(Sections 114 – 181)

What does the Act do?

- Retains the Information Commissioner as the UK's independent data protection regulator.
- Places a duty on data controllers to notify the Commissioner as well as individuals concerned of data breaches that risk affecting individuals' rights.
- Increases maximum penalties for regulatory breaches from £500k to £17m.
- Creates new offences to deal with emerging threats.

DCMS Secretary of State, 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 Act ensures the Commissioner has the powers she needs to ensure consumers are appropriately safeguarded. We will continue to work with her office and consumer groups to educate people about how to protect themselves."

How does the Act do it?

- The Data Protection Act 1998 provided a statutory basis for the Information Commissioner and the source of her powers in respect of data protection regulation. The 2018 Act 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 issue guidance are all preserved by the 2018 Act to allow the Commissioner to support business to achieve compliance.
- The 2018 Act 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 Act provides for maximum fines of up to £17m, or 4% of global tunrover consistent with the GDPR, and also requires the Commissioner to issue guidance about enforcement.

- The Act 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 the Commissioner's powers of enforcement have increased since.

The 2018 Act 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.

- Providing an appeals system to challenge the Commissioner's decisions, and monetary penalties imposed, before an independent Tribunal, or, in certain circumstances, a court.

Key Questions and Answers

❖ What impact will increased fines have on organisations?

The Act 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 Act contain so many criminal offences?

The very worst cases of data misuse can cause serious distress to large numbers of people. The Data Protection Act 1998 contains several offences that we have transferred into the new Act. But we have also created 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 pseudonymisation mechanisms.

❖ How are those working to test security systems 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 law enforcement purposes, to comply with a legal obligation, undertaken with a view to testing the effectiveness of the de-identification, or was otherwise justified in the public interest.

Department for Digital, Culture Media & Sport

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