Home Office

Department for Digital, Culture Media & Sport

Data Protection Bill

Factsheet – National security data processing

(Clauses 80 - 111)

What are we going to do?

- Update the laws governing the processing of personal data by the intelligence services and others for the purposes of safeguarding national security.

- Ensure that the laws in this area are in-line with international standards, while ensuring that the intelligence community and others can continue to keep the UK safe at a time of a heightened and unprecedented terrorist threat.

Security Minister, Ben Wallace said:

"We must ensure that that our intelligence services are able to continue to keep this country safe from a range of threats, while still being subject to internationally recognised data protection standards.

"This Bill will help to build on previous legislation to make sure the laws in this area remain up-to-date and the UK's high standards of data protection are upheld."

How are we going to do it?

- Domestic processing of personal data by the intelligence services is currently governed by the Data Protection Act 1998. The Bill creates a new framework for data processing, providing for a separate regime to regulate the processing of personal data by the intelligence services. This regime will be based on the international standards, which are going to be provided for in an updated Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" ("modernised Convention 108"), which is currently in the final stages of negotiation.

Background

National security is outside the scope of EU law. Consequently, the processing of personal data for national security purposes is not within scope of the GDPR or the Law Enforcement Directive ("LED"). As a result, the provisions of the GDPR and LED were not designed to be applicable to processing by the intelligence services.

The Bill therefore provides a specific data protection regime for the processing of personal data by the intelligence services based on the standards provided for in the modernised Convention 108, which unlike EU law, was also designed to apply to national security and national security agencies.

The intelligence services already comply with robust data handling obligations. These are supported by rigorous physical, technical and procedural controls which include vetting of personnel, handling restrictions based on classification of data and firewalling of internal IT and access restrictions. These controls already provide for strong protection.

The regulatory structure applying to the intelligence services is also found in other legislation which already imposes restrictions on their activities, including relating to their acquisition, use and retention of personal data.

Key national security data processing provisions for the intelligence services

- Part 4 of the Bill provides a specific specific regime for the intelligence services, which will ensure that the processing of personal data by these agencies is subject to appropriate and proportionate controls, which recognises the critical role of the intelligence services in tackling the current and future threats to national security.

- It sets out the six data protection principles which apply to personal data processed under this Part of the Bill:

  ➔ processing must be lawful, fair and transparent;
  ➔ the purposes of processing must be specified, explicit and legitimate;
  ➔ personal data must be adequate, relevant and not excessive;
  ➔ personal data must be accurate and kept up to date;
  ➔ personal data must be kept no longer than is necessary;
  ➔ personal data must be processed in a secure manner.

- It sets out the the rights of individuals over their data, these include:

  - ➔ rights to certain general information, including about the processing undertaken by a controller and about data subjects' rights under this Chapter;
  - ➔ rights of access by the data subject;
  - ➔ rights in relation to automated decision-making, including the right not to be subject to such decision-making;
  - ➔ the right to object to processing where the processing would constitute an unwarranted interference with the interests or rights of the data subject;
  - ➔ the right to rectification of inaccurate data and of erasure of data where the processing of the data would infringe the data protection principles.

Other processing of data where there is a national security interest

Section 28 of the DPA currently provides for an exemption from the provisions of that Act (including the data protection principles and the rights of data subjects) if the exemption from the provision is necessary for the purpose of safeguarding national security, for example, to avoid tipping off a terrorist suspect. The exemption may only be applied to the extent it is necessary to do so to safeguard national security, and no further.

The Bill seeks to replicate the approach taken in the DPA, in terms of continuing the current well established system in order to protect national security. As a result, the Bill:

- Ensures that the intelligence services can, as now, be exempted from the provisions of the regulatory scheme where it is necessary to safeguard national security.

- Provide for analogous, but tailored, national security exemptions for other data controllers and processors (that is, persons responsible for complying with data protection law) operating under the applied GDPR or law enforcement schemes where, and only to the extent that, this is necessary to safeguard national security.

- Makes clear to data controllers and processors that national security issues do not fall within the GDPR (as nationals security is outside the scope of EU law), allowing for such processing to be done under the applied GDPR regime, which contains an exemption from standards where necessary to safeguard national security.

- Preserves the ability to apply to a Cabinet Minister (or Attorney General or the Advocate General for Scotland) to issue a certificate certifying that a national security exemption is a necessary and proportionate measure to safeguard national security. Such a certificate will continue to be conclusive evidence of that fact in any legal proceedings.

This approach ensures consistency with the existing DPA, ensuring the intelligence services are held to a high standard of protection of personal data are comparable to those in other parts of the Bill where possible, but not at the cost of national security.

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

Home Office
14 September 2017