



Data Protection Act 2018

Factsheet – Intelligence services processing

(Sections 82 – 113)

What does the Act do?

- Updates the laws governing the processing of personal data by the intelligence services.
- Ensures 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 Act helps 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 does the Act do it?

Prior to the passage of the Data Protection Act 2018, domestic processing of personal data by the intelligence services was governed by the Data Protection Act 1998. The 2018 Act 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 is based on the international standards, which will be provided for in an amended Council of Europe “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (the “modernised Convention 108”; the Council of Europe adopted an amending Protocol on the 18 May 2018).

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 General Data Protection Regulation (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 2018 Act 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 processing 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 data processing provisions for the intelligence services

- Part 4 of the 2018 Act provides a specific regime for the intelligence services, which ensures 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 2018 Act:
 - 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 rights of individuals over their data, including:
 - rights to certain general information, including about the processing undertaken by a controller and about data subjects' rights under this Part;
 - 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.

National security exemption

Section 28 of the 1998 Act provided 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 was necessary for the purpose of safeguarding national security, for example, to avoid tipping off a terrorist suspect. The exemption could only be applied to the extent it was necessary to do so to safeguard national security, and no further.

The 2018 Act replicates the approach taken in the 1998 Act, in terms of continuing the well-established approach to protecting national security. As a result:

- Section 110 provides that the intelligence services can be exempted from the specified provisions of the regulatory scheme where it is necessary to safeguard national security (the 2018 Act also provides for other exemptions for the intelligence services in Schedule 11).
- Section 111 provides that a certificate, signed by a Cabinet Minister (or the Attorney General or the Advocate General for Scotland) is conclusive evidence that an exemption relied upon by the intelligence services from any or all of the specified data protection requirements is required for the purpose of safeguarding national security.



This approach is consistent with the approach taken previously in the 1998 Act and ensures that the intelligence services are held to a high standard of protection of personal data comparable to those in other parts of the 2018 Act where possible, but not at the cost of national security.

The 2018 Act also goes further than the 1998 Act, requiring greater transparency over national security certificates. Where a Minister issues a national security certificate under the 2018 Act, he or she is required to send a copy to the Information Commissioner, who must publish a record of the certificate (section 130). Whilst the expectation is that most certificates will be published in full, the Commissioner must not publish the text, or part of the text, of the certificate where the Minister determines that to do so would be against the interests of national security, contrary to the public interest or might jeopardise the safety of a person.