Data Protection and Cybercrime

Graham Sutton

Former Policy Advisor
Department of Constitutional Affairs, UK

What is data protection?

- A set of legislative rules which regulate the way in which information about individuals is handled.
- It can be considered as a sub-set of privacy: “personal information privacy”

International data protection instruments

- European Convention on Human Rights
- Council of Europe Data Protection Convention and Additional Protocol
  - Sectoral recommendations, including one on data protection and the police
- EU Data Protection Directive
- OECD Guidelines

Cybercrime Convention

- Preamble draws attention to
  - The right to the protection of personal data in the 1981 Council of Europe Data Protection Convention
  - Council of Europe Recommendations on data protection in the police sector; and data protection in the telecommunications sector.
- Article 15: "Each Party shall [in applying Section 1]...provide for the adequate protection of human rights and liberties, including rights ... under the [European Convention on Human Rights]..."
- No special data protection rules, so the general rules apply.

European Convention on Human Rights

- Article 8.1: “ Everyone has the right to respect for his private and family life, his home and his correspondence.”
- Article 8.2: Provides exemptions for “national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.
- Exemptions must be: “in accordance with the law” and “necessary in a democratic society”.

Data Protection: Purpose

- Data Protection Convention: Article 1

  “ The purpose of this convention is to secure ... for every individual... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.”

Data Protection: Balance

- Police Data Protection Recommendation: Preamble

  “Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other.”

Data Protection: Scope

- Scope is very broad:
  - Applies to all activities, including law enforcement.
  - Applies to anything done with personal data: from collection to destruction, including disclosing and merely holding data (“processing”)
  - “Personal data” covers all information about identifiable individuals. Some information (for example about race, religion, political opinions) is called “sensitive data”. Special rules apply.
  - Personal data can be in the form of text, images or sound

The Main Rules
The Data Protection Principles

- Personal data must be:
  - processed fairly and lawfully
  - collected for a specified, legitimate purpose and not further processed “incompatibly”
  - adequate, relevant and not excessive
  - accurate and, where necessary, kept up to date
  - not kept for longer than required for the original purpose

First Principle: Lawfulness

- Processing (which includes collection) must have a proper legal base
- Some countries' laws (including those of all EU countries) have special criteria for processing personal data. One of these must be met, in addition to having a legal base in general law

First Principle: Fairness

- Fairness means, among other things, making sure that individuals know what is happening to their data
- If possible they should be informed at the time when their data are collected
- If data must be collected for police purposes without individuals' knowledge, they should be informed as soon as this would not prejudice the police activity

Second Principle: Purpose and compatibility

- Personal data collected for police purposes should be processed only for those purposes.
- They may be disclosed to other bodies only consistent with the principle of “compatibility”
- The Recommendation on Data Protection and the Police sets out strict conditions for disclosures. The conditions vary according to the type of recipient (other police bodies; other public bodies; private bodies)

Third Principle: Proportionality

- Personal data collected for police purposes should be limited to what is necessary for “the prevention of a real danger or the suppression of a specific criminal offence” (Recommendation on Data Protection and the Police)
- Data that prove not to be necessary for the purpose for which they were collected should be deleted as soon as that becomes apparent
- Different considerations might apply according to the category of persons whose data are collected
  - suspects
  - victims
  - witnesses

Fourth Principle: Accuracy

- In principle, only accurate data should be collected
- Particular care should be taken with “soft” data such as intelligence data
- If data turn out not to be accurate, they should be corrected
- If it is necessary to retain inaccurate data (for example, for evidential purposes) the inaccuracy should be made clear

Fifth Principle: Time Limits

- Personal data should be deleted when they are no longer needed for the purpose for which they were collected – including the possible need for review of the case
- The need to retain data, especially “soft” data, should be regularly reviewed
- Subject to appropriate safeguards, personal data may be retained longer for historical, scientific or statistical research purposes

Individuals' rights

- Individuals have the right to
  - find out whether their personal data are being processed
  - get access to the data
  - have inaccurate data corrected and unlawfully processed data blocked or erased

Derogations

- Derogations from the data protection principles and the right of access are permitted in the interests of
  - protecting State security, public safety, the monetary interests of the State, the suppression of criminal offences;
  - protecting the individual concerned or the rights and freedoms of others
- Derogations must be “provided for by law” and “necessary in a democratic society”

Security

- Appropriate security measures should be taken against accidental or unauthorised destruction, loss, unauthorised access, alteration or disclosure, and any other form of unlawful processing
- Measures should include
  - physical security
  - technological means
  - organisational means
    - training
    - need to know

International transfers (1)

- Given nature of cybercrime, essential that law enforcement agencies should be able to co-operate across international borders, including sharing personal data where necessary
- Basic rule: personal data may not be transferred to a country which does not provide an “adequate” level of protection
- For Council of Europe purposes, all countries that have ratified the Data Protection Convention are “adequate”
- Otherwise, “adequacy” is assessed on a case by case basis, having regard to all the circumstances

International transfers (2)

- Exceptions from the “adequacy” requirement where there are legitimate prevailing interests, especially important public interests; or where there are adequate safeguards
- Domestic data protection law, including restrictions on disclosures, must also be met
- There should be strict conditions on the use for which the personal data transferred may be used, including restrictions on further disclosures

Supervision

- Processing of personal data is subject to oversight by an independent data protection supervisory authority
- The authority has the power to
  - investigate and intervene in processing
  - bring violations to court
  - deal with individuals' complaints

Thank you