Ministry of JUSTICE

Circular 2011/01

Title:	**Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008/977/JHA.**
From:	Information Policy Division, Ministry of Justice
Distribution date:	25 January 2011
Implementation date:	Immediate
Contact:	See end
Broad subject:	Compliance with data protection requirements
Sub category:	Data Protection Framework Decision
Sent to:	the Director of Public Prosecutions, the National Police Improvement Agency, the Ministry of Defence, the Ministry of Defence Service Police, the Crown Office and Procurator Fiscal Service (Scotland), the Association of Chief Police Officers in Scotland, the Scottish Police Services Authority, the Home Office, the Driver Vehicle Licensing Agency, the Department of Work and Pensions, the Information Commissioner's Office, the Department of Health Counter Fraud and Security Management Service, the Northern Ireland Department for Justice, the Serious Organised Crime Agency, the Serious Fraud Office, the UK Border Agency, the Judicial Office for England and Wales, the Association of Chief Police Officers, the Foreign and Commonwealth Office, the Identity and Passport Service, Her Majesty's Revenue and Customs, the Department for Communities and Local Government, the Financial Services Authority, the Department for Transport, the Welsh Assembly Government, the Northern Ireland Department for Justice.

The purpose of this circular is to set out the requirements that UK Competent Authorities must meet in order to comply with the EU Data Protection Framework Decision 2008/977/JHA. In most cases they will be able to meet those requirements by maintaining their current levels of good practice.

Introduction

Member States were required to implement the 'Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008/977/JHA' (the Data Protection Framework Decision (DPFD)) by 27 November 2010.

The DPFD sets out the minimum data protection safeguards in the area of police and judicial cooperation. In the UK, the Data Protection Act 1998 (DPA) already provides a minimum data protection standard for all personal data processing. As such, the vast majority of the provisions of the DPFD are already provided for in UK law. Furthermore, where any gaps exist, consultation has confirmed that other legislation and best practice ensure operational compliance.

This circular sets out the requirements that UK Competent Authorities must meet, in addition to their obligations under the DPA, in order to comply with the DPFD.

What is the scope of the DPFD

The DPFD only applies to Competent Authorities. Competent Authorities are defined in Article 2(h) as:

> *Agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other Competent Authorities of the Member States that are authorised by national law to process personal data within the scope of the DPFD.*

The scope of the DPFD does not extend to all personal data. Rather, the scope is limited to personal data that fits the following criteria:

a. Only personal data that is being processed for the purpose of law enforcement and judicial co-operation;
b. Only personal data that has been received from another European Economic Area (EEA) Member State (i.e. not data sourced from within the UK or from a third country such as the US) or a body set up by the EU (such as Eurojust or Europol); and
c. Only data that is not related to National Security.

It is important to note that only data within this scope is covered by the DPFD and this circular.

1. Establishment of time-limits for erasure and review

The DPFD requires Competent Authorities to do two things in this regard:

a. put in place appropriate time-limits for the erasure of personal data within the scope of the DPFD. In cases where this is not appropriate, Competent Authorities do not have to provide an exact date to erase this data but should have a date set in advance, for the consideration of this data for deletion; and
b. have procedures in place to ensure that these time-limits are observed.

The DPA already regulates the retention of personal data through a combination of the third and fifth data protection principles in the DPA, and consultation has confirmed that the necessary procedures, such as record retention schedules, are generally already in place. As the DPFD only requires that time-limits are in place and does not stipulate their duration, it is very likely that existing systems will be sufficient to meet this requirement.

Competent Authorities must ensure that they have time limits for erasure and review procedures in place.

2. Verification of quality of data that are transmitted or made available

The DPFD requires Competent Authorities to do three things in this regard:

a. When transmitting data - That UK Competent Authorities ensure that they notify the receiving Competent Authority, as soon as possible in the event that incorrect personal data within the scope of the DPFD is transmitted, including if it is unlawfully transmitted;
b. When receiving data that has not been specifically requested - That UK Competent Authorities verify that personal data is required for the purpose for which it was transferred; and
c. In the event that such personal data is received but not required for the purpose that it was transmitted, that it is rectified, erased or blocked.

A combination of the fourth and seventh data protection principles regulate the incorrect and unlawful transmission of personal data in the UK. In addition, when circumstances require personal data to be erased, blocked or rectified, this is provided for by section 14 of the DPA.

Consultation has confirmed that UK Competent Authorities will generally perform the above notification and verification tasks already through a combination of compliance with the data protection principles, existing administrative measures and as a result of steps to maintain good data sharing relationships with other Competent Authorities. **Competent Authorities must ensure that they have these procedures in place.**

3. Logging and documentation.

The DPFD requires Competent Authorities to do one thing in this regard:

a. Ensure that all transmissions of personal data within the scope of the DPFD are logged or documented. These logs or documents must be sufficient to allow verification of the lawfulness of the '*data processing, self monitoring and ensuring proper data integrity and security'.*

Consultation has confirmed that UK Competent Authorities generally already do this in practice to ensure that transfers have been made in a lawful and accurate manner. This requirement is met already through a combination of general compliance with the data protection principles, existing administrative measures and the result of operational necessity. Most computer systems used by UK Competent Authorities will already provide an audit trail of transfers, and the DPFD does not specify any particular form these logs or documents should take. **Competent Authorities must ensure that they an appropriate system in place.**

4. Prior consultation

The DPFD requires Competent Authorities (who intend to process personal data within the scope of the DPFD as part of a new filing system) to consult the Information Commissioner's Office when:

1. the processing will involve sensitive personal data (under the DPA); or
2. the type of processing holds specific risks for the fundamental rights and freedoms of the data subject, particularly risks to privacy. This is particularly likely to be the case if the type of processing involves:
    a. using new technologies; or
    b. using new mechanisms or procedures.

The Government Data Handling Review of June 2008 mandated the use of Privacy Impact Assessments (PIA) across central Government when any new policy or initiative is likely to involve the use of personal data and / or sensitive personal data,

and Competent Authorities already regularly consult the Information Commissioner where a PIA highlights such a risk. **Competent Authorities must continue to ensure that this is the case.**

5. Processing of personal data received from or made available by another Member State

The DPFD puts restrictions on when personal data can be processed for a further purpose (other than the one for which it was collected). It requires Competent Authorities only to do so under the following conditions:

a. When it will be processed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which it was transmitted or made available;
b. When it will be processed for other judicial and administrative proceedings (which include activities by regulatory and supervisory bodies) directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
c. When it will be processed for the prevention of an immediate and serious threat to public security; or
d. **any other purpose only with the prior consent** of the transmitting Member State or with the consent of the data subject, given in accordance with national law.

In practice, UK Competent Authorities will generally already need to meet the requirements through general compliance with the data protection principles; particularly the first, second and third data protection principles. In addition, consultation has confirmed that consent is required as part of existing agreements that facilitate the exchange of data, often on a bilateral basis, and in existing administrative measures.

Competent Authorities must ensure that all personal data within the scope of the DPFD is only further processed with prior consent unless the further processing is for a purpose consistent with (a), (b) and (c) above.

6. Transfer to Equivalent Authorities in third States or to international bodies

The DPFD restricts when Competent Authorities may transfer personal data they have been given by another Member State to a third State or international body outside of the EEA. It requires Competent Authorities only to transfer personal data

within the scope of the DPFD to third States or international bodies with the prior consent of the Member State from which the data was obtained and when:

1. it is transferred to bodies that have obligations for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (such as banks, communication service providers and regulatory bodies) where these transfers are part of the legitimate activities of Competent Authorities; and
2. when an adequate level of data protection can be ensured (as per the same system used in the DPA); and
3. when the transfer is necessary for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

This is a strict limitation and is not a requirement of the DPA. However, it is important to note that the DPFD specifically allows Member States to decide how to obtain the consent of the Member State from which the data was obtained. Consultation has confirmed that UK Competent Authorities are largely compliant through the terms of data sharing agreements that have been agreed to facilitate the transfer of personal data relating to police and judicial cooperation. If consent has been obtained in advance for broad categories of data it is likely to be acceptable for the purposes of the DPFD.

Competent Authorities must ensure that data sharing agreements include consent clauses for transferring personal data within the scope of the DPFD in a manner consistent with the above, or that consent is obtained before that data is transferred.

7. Transmission to private parties in Member States

The DPFD puts restrictions on when personal data may be transferred to private parties. Such transfers are prohibited unless the consent of the Competent Authority from which the data was obtained has been received, and no legitimate specific interests of the data subject prevent transmission. Furthermore, the transfer must be essential for either:

a. the performance of a task lawfully assigned to it;
b. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
c. the prevention of an immediate and serious threat to public security; or
d. the prevention of serious harm to the rights of individuals.

In these circumstances, the UK Competent Authority transmitting the received data to a private party must inform the private party of the exclusive purposes for which the data may be used.

UK Competent Authorities will normally meet most of the requirements of the above through a combination of compliance with the data protection principles and existing administrative measures. The DPA does not require consent to be sought before a transmission to a private party is made, however, as with transfers to third countries, consultation has confirmed that UK Competent Authorities are largely compliant with this requirement through the terms of data sharing agreements agreed to facilitate the transfer of personal data relating to police and judicial cooperation. Therefore, if UK Competent Authorities have already obtained consent (from the transferring Competent Authority) for broad categories of personal data, which provides for onward transfers to private parties, it is likely to be acceptable for the purposes of the DPFD.

UK Competent Authorities must ensure their existing practices only allow personal data within the scope of the DPFD to be transferred to private parties in a manner consistent with the above.

8. Information on request of the Competent Authority

Article 15 of the DPFD requires Competent Authorities who receive personal data within the scope of the DPFD to provide information on request to the Competent Authority that provided the data about their processing of that personal data. Consultation has confirmed that since Competent Authorities would normally share data as part of an existing agreement, they would usually provide such information upon request in exchange for the data and in order to maintain that agreement.

Competent Authorities must ensure that they provide such information upon request.

Further work and further information

Information about further work on this area and more technical guidance on compliance with this circular can be obtained from the Ministry of Justice at the following address:

Mark.Buttigieg@justice.gsi.gov.uk