Council of the European Union

Brussels, 27 June 2019
(OR. en)

10647/19

LIMITE

DAPIX 220
CRIMORG 92
ENFOPOL 324

NOTE

From:	UK delegation
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	6661/1/09 REV 1 ADD 2 REV 1
Subject:	Evaluation procedure for implementing the data exchange provisions pursuant to Council Decisions 2008/615/JHA and 2008/616/JHA (Prüm Decisions) - reply to questionnaire on data protection with particular regard to dactyloscopic data

1. Legislation[1]

(a) Please confirm that, pursuant to Article 25 of Council Decision 2008/615/JHA, the national law provides a level of protection of personal data at least equal to the resulting from the Council of Europe Convention of 28 January 1981 and its Additional Protocol of 8 November 2001 and that the data protection regime applicable to Prüm data exchanges takes account of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe.

[1] The reply to the questionnaire on data protection has to be amended due to progress made at national level regarding the implementation of the "Prüm Decisions". The current reply updates and supplements the previous information in particular with regard to the provisions concerning the exchange of fingerprints.

The UK Data Protection Act 2018 (the Act) conforms with the level of data protection required and sets out the principles which mirror those contained in the current Regulation (EU) 2016/679 and EU Directive (Directive 2016/680). We enclose a copy of the Act for your reference.

In accordance with Article 10.c of the Rules of Procedure for the meetings of the Ministers Deputies, the Representative of the United Kingdom reserved the right of her Government to comply or not with Principles 2.2 and 2.4 of the Recommendation**.**

Paragraph 2.2 provides a general regulatory principle that, where data concerning an individual have been collected and are stored without his knowledge he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced. This procedure will be unnecessary if the police have decided to delete the data collected unbeknown to the individual.

The Committee of Ministers of the Council of Europe accepted that Principle 2.2 may prove difficult to implement where street videos and similar mass surveillance methods are an issue and information has been collected on a great number of persons. It is for this reason that the principle recommends informing those subjected to a secret surveillance that data are still held on them only "where practicable". The police themselves will be expected to take the decision.

Principle 2.4 treats the issue of sensitive data and reflects the concern expressed in Article 6 of the Data Protection Convention that the collection and storage of particular categories of data should be restricted. It may be the case that the collection of certain sensitive data will be necessary for the purposes set out in Principle 2.1. However, in no circumstances should such data be collected simply in order to allow the police to compile a file on certain minority groups whose behavior or conduct is within the law. The collection of such data should only be authorised if "absolutely necessary for the purposes of a particular inquiry". The expression "a particular inquiry" should be seen as a general limitation; such an inquiry should be based on strong grounds for believing that serious criminal offences have been or may be committed. The collection of sensitive data in such circumstances should, moreover, be "absolutely necessary" for the needs of such inquiries.

The reference to sexual behaviour does not apply where an offence has been committed.

(b) Please provide details that the national legislative process is completed and provide a copy of the relevant national legislation.

The provisions in the Act that refer to the principles for processing data for law enforcement purposes are as follows:

- Section 35: Processing of personal data must be lawful and fair
- Section 36: Data is collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
- Section 37: Data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed
- Section 38: Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Section 39: Data must be kept for no longer than is necessary for the purpose for which it is processed
- Section 40: Data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (section 40)

(c) Please confirm that all the provisions of chapter 6 of Council Decision 2008/615/JHA are or have been incorporated into the national regulations and are applicable / are implemented.

The Act sets out the principles which mirror those contained in the current Regulation (EU) 2016/679 and EU Directive (Directive 2016/680) and include reference to the principles in the regulations set out above. Part 3 of the Act, outlines the data protection requirements for law enforcement processing;

- Schedule 7 sets out Competent Authorities, and;
- Schedule 8 sets out Conditions for sensitive processing under Part 3

2. Data protection authorities

(a) Pursuant to Article 19 of Council Decision 2008/616/JHA, please provide details on the independent data protection authorities or judicial authorities which will be responsible for legal checks on the supply or receipt of personal data, as referred to in Article 30(5) of Council Decision 2008/615/JHA.

The Information Commissioner is the independent authority for data protection within the UK. She is appointed by Her Majesty the Queen by Letters Patent.

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

(b) Where more than one national supervisory authority is in place and competent, how will they cooperate (cf. Art. 30 of Council Decision 2008/615/JHA)?

Not applicable, the Information Commissioner has responsibility for the UK.

(c) Which concrete powers are available to the supervisory authority in case there is misuse in the processing of data (cf. Art. 30 of Council Decision 2008/615/JHA)?

Section 40 of the Act, as applied by regulation 51(1)(a) of the 2014 Regulations, provides the Information Commissioner with powers of enforcement. Regulation 51 also confers powers under sections 55A to 55E to impose monetary penalties and prosecution under s60.

These powers are designed to promote compliance with the Act and the Act and the Privacy and Electronic Communications Regulations (PECR) apply to the whole of the UK. The main powers available to the ICO are outlined in Part 6 & 7 of the Act, with further details included in the Schedules 12-16. A summary of the main Commissioner powers are as follows:

- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue monetary penalty notices up to a maximum of 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year (whichever is higher);
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.

(d) Have working contacts with the national data protection authorities in this area been established (cf. Art. 30 of Council Decision 2008/615/JHA)?

The Act requires every organisation that processes personal information to register with the ICO, unless they are exempt. Failure to do so is a criminal offence. The ICO publishes the name and address of these Controllers, as well as a description of the kind of processing they undertake. In relation to Prüm, the Home Office, Metropolitan Police Service (MPS) and National Crime Agency (NCA) are registered with the ICO with the following registration numbers;

Home Office: Z7271689.

National Crime Agency: ZA019117

Metropolitan Police: Z4888193

Additionally, the MPS, NCA and Home Office work collaboratively on the Prüm project in compliance with their respective obligations under the Act.

3. Procedural measures

(a) How is the purpose limitation (cf. Art. 26 of Council Decision 2008/615/JHA) practically ensured?

Section 36 of the Act specifies purpose limitation of law enforcement processing. This states the principle that data is only processed and used for the purpose for which it was obtained, as described in (c) below. Further procedures exist to ensure compliance with these principles. The Information Commissioner also has powers to enforce this provision (financial penalties and prosecution).

(b) Which concrete authorities are enabled to process the data supplied (cf. Art. 27 of Council Decision 2008/615/JHA)?

The MPS, the NCA and Home Office. The MPS and NCA are Home Office delivery partners and are enabled to process the data supplied relevant to their area.

(c) How do you practically guarantee that personal data can only be processed by competent authorities (cf. Art. 27 of Council Decision 2008/615/JHA)?

Controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Controllers may only disclose personal data in accordance with their registration with the ICO and the Data Protection Principles set out in Part 3, Chapter 2 of the Act**.**

The requirement to process personal data fairly and lawfully is set out in the first data protection principle and is one of six such principles at the heart of data protection. The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed.

(d) Under what concrete procedures can authorities supply the processed data to other entities (cf. Art. 27 of Council Decision 2008/615/JHA)?

The Secretary of State for the Home Department issued a statutory Code of Practice on the Management of Policing Information ('MoPI'). Police forces use MoPI as a guide for handling data more generally. For more specific uses of data they will adhere to the relevant Data Protection Impact Assessment (DPIA).

Section 63 of the Police and Criminal Evidence Act 1984 (PACE) allows fingerprints (and DNA) legitimately retained in the England and Wales to be used to prevent and detect crime outside England and Wales. PACE codes of practices D and G are used as official operational guidance in England and Wales. Similar rules apply in Scotland and Northern Ireland.

The specific practical steps, beyond law, that a police officer takes to ensure that he or she does not use the data acquired for another investigation that is beyond the original purpose for which the information was gathered, is an operational matter for individual police forces, in line with the aforementioned codes of practice and operational guidance.

4. Technical and organisational measures

(a) Are procedures of notification of incorrect data as well as technical and organisational measure for (automatic) detection in place (cf. Art. 28 of Council Decision 2008/615/JHA)?

The fourth principle of the Act imposes an obligation to ensure that data is accurate, and where necessary, kept up to date. This means the controller shall:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

The Controller is obliged to provide all the recipients with information about the blocking, correction, supplementing or deleting of personal data without undue delay. Where data is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. UK competent authorities are each independently liable for any damages caused to a person, as the result of them entering factually inaccurate data or storing data unlawfully.

The NCA is the National Contact Point for Prüm for Step 2. The Case and Information Management System (CIMS) operated by NCA is compatible with the EU regulations on data protection. CIMS automatically records activity related to a file, including to whom the data has been sent. On this basis, should there be any contention regarding the accuracy of the data, this is automatically noted from the Police National Computer (PNC) until its resolution. The log is reviewed and actioned accordingly.

The Protection of Freedoms Act 2012 (PoFA) introduced a regime to govern the retention and use by the police of DNA samples, profiles and fingerprints (through amendments to PACE). This provides for the indefinite retention of fingerprint records and DNA profiles from persons convicted of a recordable offence (a criminal offence for which the police are required to keep a record on their systems). PoFA strikes a balance between protecting the freedoms of those who are not convicted of an offence, whilst ensuring that the police continue to have the capability to protect the public and bring criminals to justice.

PoFA was brought in as a response to the 2008 judgment of the European Court of Human Rights in the case of *S and Marper v UK*. In this case, the court ruled that the blanket retention of DNA profiles taken from innocent people posed a disproportionate interference with the right to private life, in violation of Article 8 of the European Convention on Human Rights.

The retention periods of fingerprints and DNA profiles in relation to the provisions set out in PoFA apply to retention on the both PNC and the UK's Law Enforcement Automated Fingerprint Identification System (AFIS) -IDENT1, and results in automatic deletion from the police database within 24 hours once the record expires.

The post of the Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner') was also established by PoFA in order to:

- keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints;
- decide applications by the police to retain DNA profiles and fingerprints (under section 63G of PACE);
- review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints;
- provide reports to the Home Secretary about the carrying out of his functions.

(b) What measures are in place to ensure data's "flagging" (cf. Art. 24 and 28(2) of Council Decision 2008/615/JHA)?

The Act gives rights to individuals in respect of the personal data that organisations hold about them. Under section 45 (Part 3):

- A data subject is entitled to obtain from the controller —

  (a) confirmation as to whether or not personal data concerning him or her is being processed, and

  (b) where that is the case, access to the personal data and the information set out in subsection (2).

- Details of the information are set out in section 45(2), with further details of the data subject's rights outlined in sections 46-54

Compliance with this is provided for by the functionality of the PNC, which is the master system of record for personal data held by law enforcement.

In broad terms, the Controller for biometric information collected by law enforcement is the chief officer of the police force that enrolled that information, insofar as they determine the manner and use of that data. A data subject would therefore notify the relevant Controller that they contested the content of the biometric information, and appropriately-authorised staff, acting on behalf of the Controller, would raise the relevant flag on PNC, this would then co-ordinate the relevant actions on the core biometric data stores.

(c) What measures are in place to ensure data's "blocking" and "deleting" (cf. Art. 28 of Council Decision 2008/615/JHA)?

For biometric data captured and retained by UK law enforcement, data retention within the biometric data stores is managed by PNC, using a series of rules including:

- the legislative regime where the biometrics were enrolled,
- the age of the data subject at the point of arrest,
- the outcome of the judicial process,
- the seriousness of the offence,
- other specialist, authorised retention reasons

These rules are defined by legislation, including PACE and PoFA and utilise the presumption of deletion by default. If the rules do not generate a reason to retain the biometric information, then PNC instructs deletion from the police's biometric data stores. Deletion may also be requested manually, for which a full audit trail is kept.

In certain circumstances, the rules-based deletion of biometric information (such as the DNA profile of a missing person) may prejudice the interests of the data subject, however it may not be appropriate for that biometric information to be made available for automated comparison against a biometric probe. In these situations, biometric records may be "suspended" from matching. In the case of fingerprints, this is mediated by PNC.

(d) Which technical and organisational measures to ensure personal data protection and security have been put in place (cf. Art. 29 of Council Decision 2008/615/JHA)

All personal information held by the Home Office, NCA and the Metropolitan Police is located in physically secured data centres. Access control is layered to ensure that only those who are appropriately trained, security cleared, and require legitimate access to the data, are permitted. Training and security clearance are reviewed on a regular basis.

Those who have access are further restricted by read/amend/delete permissions according to their role requirement, all of which are fully logged and audited. Records that are altered or amended are done so following appropriate authorisation and full audit trail, following full verification procedures. Levels of access are reviewed on a regular basis, and access is removed when no longer required.

Systems access is logged individually through unique-issue usernames and a password-system. Transaction enquiry audits are regularly conducted to ensure access to personal data is legitimate, accountable, and in relation to the duties required of them by their respective organisations. The Act sets out what may or may not be done with personal data. Penalties for misuse or unlawful access of data are severe: misuse will likely lead to dismissal and potential prosecution for breaching the Act.

(e) Which logging measures for non-automated supply and non-automated receipt of personal data have been put in place (cf. Art. 30 (1) and (2b) of Council Decision 2008/615/JHA)?

All UK Government systems which receive, create, store or disseminate information containing personal data or policing data are considered classified, are secured, and are required to undergo formal accreditation prior to use and at regular intervals thereafter in accordance with the UK Government Security Policy Framework.

The NCA's International Crime Bureau (UKICB) receives a notification every time UK data is shared with other EU Member States in response to a Prüm Fingerprint search. The notification specifies the identifier of the records that have been matched and serve to assist with any Step 2 follow up.

CIMS is a dedicated case management and workflow facility accessed via terminals connected to the NCA corporate system, located within the UKICB at the NCA's North-West Hub. Staff authenticate the system before gaining access to the CIMS functionality. All access, failed access to and operations on the information using the application is logged. These logs are stored on a separate audit sub-system (the logs and audit system will not contain any operational data, with the exception of a unique reference which allows tracking of audit events to cases) and auditing is performed by a dedicated Audit Team.

When a case is received by the UKICB, CIMS creates a workflow to determine if the case should remain open or be closed. If it is determined that the case should be closed the CIMS user should decide whether to place the case on an 'automatic deletion' or 'manually review' schedule in accordance with guidance in connection with sexual offences.

After the initial three-year retention period the case will either be automatically deleted or an UKICB officer will be required to review the case to establish if it needs to be retained for a further period of time. If a case requires a manual review there will be the option to delete the case or retain it for a further period of time, determined in line with UK national law and guidance. The case will be logically deleted at this stage: it will be hidden from case officers and will appear to be deleted but will remain within CIMS for audit purposes. After Logical Deletion, cases will be available for a further period of two years for audit purposes only. After this two-year period expires, the system automatically runs a scheduled 'purge' job to remove the data entirely , thereafter there is no way to retrieve this data or perform a 'logical restore'.

For non-UK enquiries, if no action has been taken by the UK, then the UKICB will delete all the data, including any supplementary information when requested to do so. However, if 'action' has been taken, then the case will automatically be retained for an initial period of three years, with a decision made on whether to place the case on an automatic deletion, or manual review schedule. Again, after the initial three-year retention period, the case will either be automatically deleted or a UKICB officer will be required to review the case to establish if the case needs to be retained for a further period of time, following the process outlined above.

(f) Are specially authorised officers designated to carry out automated searches or comparisons? (cf. Art. 30 (2a) of Council Decision 2008/615/JHA)?

Yes, security vetted staff that have been deemed competent. See also response to (d) and (e) above.

(g) Which recording measures for supply and receipt of personal data have been put in place (cf. Art. 30 (2b) of Council Decision 2008/615/JHA)?

All records which are exchanged across the Prüm Fingerprint interface will be audited in a dedicated audit database, in accordance with the Prüm specification. After 2 years, records are house-kept, in accordance with the Prüm specification.

(h) Which measures are in place to protect recorded data against abuse and to delete them after the conservation period of two years (cf. Art. 30 (4) of Council Decision 2008/615/JHA)?

Measures in place to protect recorded data against abuse as per answers above. Prüm services come under Police Regulations for access control as other secure law enforcement systems, misuse will likely lead to dismissal and potential prosecution for breaching the Act.

5. Data subjects' rights

(a) Have procedures been put in place to ensure data subjects' rights, in particular as to his/her access? How are data subjects informed about these rights? (cf. Art. 31 of Council Decision 2008/615/JHA)?

These rights and duties are set out in sections Section 45 of the Act and are referred to as ‘the right of data subject access’. Information on how individuals can access their personal information held by organisations is found on the ICO website (https://ico.org.uk/for-the-public/personal-information/), including an exemplar letter to send. It is good practice for organisations to have guidance and a standardised form on their website. The guidance:

- makes it clear where the request should be sent to;
- highlights the fee and explains the options for payment;

- specifies the information that the requester will need to provide to confirm their identity;
- gives details of a point of contact for any questions.

While using a form is not mandatory, when it is used it helps to identify subject access requests. The form includes a 'for office use only' section providing instructions to the receiver on what to do with the form, and space to record certain information to assist in processing the request (such as the date the form was received, whether identification has been checked, and whether a fee has been paid).

The Home Office and the Prüm delivery partners all comply with the ICO's guidance. In addition, the Home Office and NCA publish Personal Information Charters. The Personal Information Charter (also referred to as a privacy notice) contains the standards expected when the organisations ask for, or hold, personal information. It also covers what they require of individuals to help keep their information up-to-date, how subjects can request a copy of the personal information held about them, and how to report a concern.

(b) Describe the process of invocation data subjects' rights to access. (cf. Art. 31 of Council Decision 2008/615/JHA)

Under the Act data subjects, in certain circumstances, have the right to:

- request access to personal information to receive, through a Subject Access Request (SAR), a copy of the personal information held about them and check that it is being lawfully processed and that it is accurate.
- request rectification of the personal information, to have any incomplete or inaccurate information corrected.
- request erasure of personal information, to ask for personal information to be deleted or removed where there is no lawful reason to continue processing it.
- request the restriction of processing of personal information, to ask for the suspension of the processing of personal information.

Data subjects can make a SAR in writing to their local force, with most forces offering an online form. Organisations should ensure they take reasonable and proportionate steps to respond effectively to requests and must be able to satisfy the requirement to confirm the identity of the person making the request, to ensure their request is valid. The organisation has to reply within a month, starting from the day they receive both the fee and the information they need to identify the subject and the information.

Under the Equality Act 2010 (which replaced previous legislation, such as the Race Relations Act 1976 and the Disability Discrimination Act 1995) an organisation has a duty to make sure that its services are accessible to all service users. Responses can be requested in a particular format to make this accessible, such as Braille, large print, email or audio format.

Complaints should initially be directed at the organisation responsible. If a member of the public has engaged with the organisation but is still dissatisfied, they may report their concern to the ICO. Anyone who believes they are directly affected by the processing of personal data may ask the ICO to assess whether it is likely or unlikely that such processing complies with the Act. This is referred to as a compliance assessment.

The ICO may serve an enforcement notice if an organisation has failed to comply with the subject access provisions. An enforcement notice may require an organisation to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence.

(c) Describe the reason for limiting the data subjects' right to access. (cf. Art. 31 of Council Decision 2008/615/JHA)?

With regards to limiting data subject right to access, section 45 in Part 3 of the Act outlines as follows:

(4) The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to —

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay —

(a) that the rights of the data subject have been restricted;

(b) of the reasons for the restriction;

(c) of the data subject's right to make a request to the Commissioner under section 51;

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

(7) The controller must —

(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.